nature COMMUNICATIONS

ARTICLE

Received 17 Feb 2016 | Accepted 12 Oct 2016 | Published 25 Nov 2016

DOI: 10.1038/ncomms13523 OPEN

Fundamental rate-loss trade-off for the quantum internet

Koji Azuma[1], Akihiro Mizutani[2] & Hoi-Kwong Lo[3,4,5]

The quantum internet holds promise for achieving quantum communication—such as quantum teleportation and quantum key distribution (QKD)—freely between any clients all over the globe, as well as for the simulation of the evolution of quantum many-body systems. The most primitive function of the quantum internet is to provide quantum entanglement or a secret key to two points efficiently, by using intermediate nodes connected by optical channels with each other. Here we derive a fundamental rate-loss trade-off for a quantum internet protocol, by generalizing the Takeoka–Guha–Wilde bound to be applicable to any network topology. This trade-off has essentially no scaling gap with the quantum communication efficiencies of protocols known to be indispensable to long-distance quantum communication, such as intercity QKD and quantum repeaters. Our result—putting a practical but general limitation on the quantum internet—enables us to grasp the potential of the future quantum internet.

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan. [2] Department of Materials Engineering Science, Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan. [3] Center for Quantum Information and Quantum Control (CQIQC), University of Toronto, Toronto, Ontario M5S 3G4, Canada. [4] Department of Physics, University of Toronto, 60 St. George St., Toronto, Ontario M5S 1A7, Canada. [5] The Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto, 10 King's College Road, Toronto, Ontario M5S 3G4, Canada. Correspondence and requests for materials should be addressed to K.A. (email: azuma.koji@lab.ntt.co.jp).

In the conventional Internet, if a client, Alice, wants to communicate with another client, Bob, an Internet protocol determines the path that the data follow to travel across multiple networks from Alice to Bob. Analogously, in the future, according to a request for performing quantum communication between Alice and Bob, a quantum internet[1] protocol will supply the resources—such as a secret key (secret bits) for the purpose of the unconditionally secure communication[2,3] and quantum entanglement (ebits) for the purpose of the quantum teleportation[4]—to Alice and Bob by utilizing proper intermediate nodes connected by optical channels—for instance, optical fibres—with each other[1] (Fig. 1a). To such an optical network, photon loss in the optical channels is the dominant impediment in general[5]. Nonetheless, as long as Alice and Bob are not too far away from each other, say over a couple of hundred kilometres, the intermediate nodes would not be necessary, because the current point-to-point quantum communication has already been very efficient as well as ready for practical use[6]. Besides, in terms of the communication efficiency for the distance, known optical schemes[2,7–13] for the point-to-point links are shown to have no scaling gap with an upper bound on the quantum capacity and the private capacity of the lossy optical channel, called Takeoka–Guha–Wilde (TGW) bound[14,15].

In general, the TGW bound can be estimated and applied to any secret key or entanglement distillation scheme by two parties who are allowed to use their given arbitrary quantum channel(s) as well as arbitrary local operations and arbitrary classical communication (LOCC). In fact, by using this feature, the TGW bound is used to upper bound the quantum capacity and the private capacity of the lossy optical channel. This is notable because it is intractable to estimate the quantum capacity and the private capacity in general, owing to possibly non-additive nature[16] of quantum channels. On the other hand, Pirandola, Laurenza, Ottaviani and Banchi (PLOB) have succeeded[17] in determining the quantum capacity and the private capacity of the lossy optical channel, via finding out the teleportation stretchability of the lossy optical channel and deriving an upper bound—called PLOB bound—applied to any teleportation stretchable quantum channel. In terms of the communication efficiency described by obtained ebits or secret bits per used optical mode, the PLOB bound is, at most, twice as tight as the TGW bound for lossy optical channels. But it is still an open question which of these bounds is tighter for general quantum channels. The TGW bound applies to arbitrary quantum channels, while the PLOB bound applies only to teleportation stretchable quantum channels (although including many practical bosonic channels[17]).

Despite the differences in advantage and disadvantage between the TGW bound and the PLOB bound, perhaps most importantly in practice, both of them show that there remains not much room to improve known optical quantum communication schemes[2,7–13] for point-to-point links further. Unfortunately, the point-to-point communication is not efficient enough to achieve the quantum internet. For example, the point-to-point quantum communication over 1,000 km needs[18] to take almost one century to provide just one secret bit or one ebit for Alice and Bob under the use of a typical standard telecom optical fibre with loss of about $0.2\,\mathrm{dB\,km^{-1}}$. Therefore, for the request from far distant Alice and Bob, the quantum internet necessitates long-distance quantum communication schemes utilizing intermediate nodes, such as intercity quantum key distribution (QKD) protocols[19–21] and quantum repeaters[18,22–36]. In particular, these schemes would be in greater demand for the quantum internet than the point-to-point quantum communication, analogously to the current Internet, where a client communicates with a far distant client via repeater nodes routinely and even unconsciously. Therefore, it is important to go beyond upper bounds (such as the TGW bound and the PLOB bound) for point-to-point links and work out fundamental and general upper bounds for a quantum internet. *A priori* working out bounds on secure key rates and entanglement generation rates for a general quantum internet topology is highly non-trivial because there are many intermediate nodes, various elements such as quantum memories and optical devices and many different protocols such as entanglement generation, entanglement swapping, entanglement distillation and quantum error correction. For this reason, up till now, a good fundamental and general upper bound on secure key rates and entanglement generation rates for the quantum internet has been missing.

The main point of this paper is to present a fundamental and practical limitation on the quantum internet. In particular, we derive rate-loss trade-offs for any two-party quantum communication over the quantum internet—composed of the use of optical fibres connecting nodes as well as arbitrary LOCC, by tailoring the TGW bound to being applicable to any network topology. The key insight is reduction. Given any quantum network (which might be a subnetwork of a quantum internet), Alice's node A and Bob's node B, we can consider any bipartition of the nodes in the quantum network, V_A including node A and V_B containing node B (cf. Fig. 1a). By regarding all nodes in V_A as local at A and all nodes in V_B as local at B—which could never increase the difficulty of quantum communication between A and B, one could reduce any network flow as a flow over a point-to-point link between A and B only. Therefore, an upper bound on the key rate or the entanglement generation rate for the point-to-point links automatically carries over to an upper bound to the quantum network. As this upper bound for point-to-point links, we simply use the TGW bound with respecting its generality, in contrast to Pirandola's contemporary work[37], which instead uses the PLOB bound to obtain a good bound for multipath networks composed of lossy optical channels. Our reduction idea is a simple observation. Nonetheless, rather remarkably, we will show here that the obtained bounds are excellent in the sense that they have no scaling gap with achievable quantum communication efficiencies of known protocols for intercity QKD and quantum repeaters, in terms of rate-loss trade-offs. Moreover, thanks to inheriting the generality of the TGW bound, in contrast to Pirandola's bounds[37] applied only to teleportation stretchable quantum channel networks, our bounds can be estimated and applied to any situation that can be regarded as the quantum internet as Kimble has considered[1], including the simulation of the quantum many-body systems as well as purely quantum communication tasks. As a non-trivial example to imply this, we present upper bounds on the performance of any Duan–Lukin–Cirac–Zoller (DLCZ)-type quantum repeater protocol[18,23,24,30] by considering not only loss of optical channels but also time-dependent decay of matter quantum memories. These bounds conclude that the coherence time of the matter quantum memories should be, at least, larger than 100 μs for enjoying the blessing of the DLCZ-type quantum repeaters even if they are equipped with any single-shot quantum error correction, as well as any entanglement distillation. The key to obtain these results is the fact that our bounds essentially depend only on the number of the channel uses to establish a quantum communication resource for Alice and Bob and the squashed entanglement[14,15] of the used quantum channels—which is a single-letter formula that can be evaluated as a function of a single-channel use.

Results

Quantum internet protocol for two clients. To obtain our bound, we need to define a general paradigm of two-party communication over the quantum internet (Fig. 1a). In the quantum internet, there are a variety of quantum channels connecting nodes, for example, depending on the lengths of optical

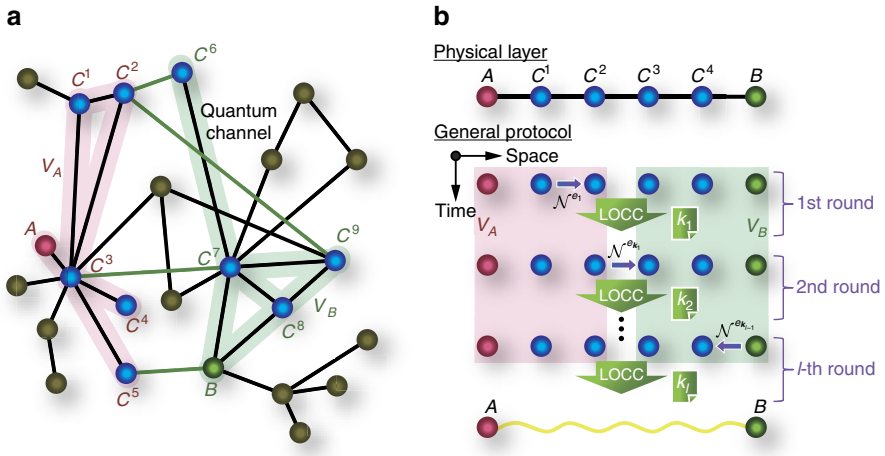

Figure 1 | Quantum internet and the most general protocol. (**a**) A general quantum internet where Alice (A) and Bob (B) request its internet protocol to supply them with resources for quantum communication, such as a secret-key and quantum entanglement. Accordingly, the protocol chooses a quantum network G (which might be a quantum subnetwork) associated with a directed graph $G=(V, E)$. The set V of vertices is composed of the nodes as $V=\{A, B, C^1, C^2, \ldots, C^n\}$ ($n=9$ here) and the set E of edges specifies quantum channels $\{\mathcal{N}^e\}_{e\in E}$ in such a way that $\mathcal{N}^{v_1\to v_2}$ represents a quantum channel to send a quantum system from node $v_1\in V$ to node $v_2\in V$. The protocol can combine the channels $\{\mathcal{N}^e\}_{e\in E}$ with LOCC arbitrarily. Then, we regard any protocol as the point-to-point communication between a single parity having nodes $V_A\subset V$ with A and another party having $V_B(=V\backslash V_A)$ with B. As a result, we obtain equation (1) showing that average obtainable ebits or secret bits are approximately upper bounded by the average of the squashed entanglement of used quantum channels between V_A and V_B. In **b**, we describe the most general protocol, by exemplifying a linear network with $n=4$. The protocol starts by preparing a separable state and then by using a quantum channel $\mathcal{N}^{e_1}$. In the i-th round ($i=1, 2, \ldots, l$), according to the previous outcomes $\boldsymbol{k}_{i-1}=k_{i-1}\ldots k_2k_1$ ($\boldsymbol{k}_0:=1$), the protocol may use a quantum channel $\mathcal{N}^{e_{\boldsymbol{k}_{i-1}}}$ with $e_{\boldsymbol{k}_{i-1}}\in E$, followed by LOCC providing a quantum state $\hat{\rho}_{\boldsymbol{k}_i}^{ABC^1C^2\ldots C^n}$ with a new outcome k_i. After an l-th round, Alice and Bob obtain a quantum state $\hat{\rho}_{\boldsymbol{k}_l}^{ABC^1C^2\ldots C^n}$, from which they can distil $\log_2 d_{\boldsymbol{k}_l}$ ebits or secret bits approximately.

channels. This necessitates to generalize the paradigm[14,15] of Takeoka *et al.* for the point-to-point communication, where it has been enough to treat only one optical channel between Alice and Bob. For instance, we need to allow the choice of which channel to use in the next round to depend on the outcomes of LOCC operations in previous rounds, in contrast to the paradigm of Takeoka *et al.*[14,15].

To make this more precise, let us define the most general protocol. We assume that any classical communication over the network is freely usable. Suppose that Alice (A) and Bob (B) call a quantum internet protocol to share a resource for quantum communication, a secret key or quantum entanglement, over the quantum network. Accordingly, the quantum internet protocol determines a subnetwork to supply the resource to Alice and Bob. The subnetwork is characterized by a directed graph $G=(V, E)$ with a set V of vertices and a set E of edges, where the vertices of G represent Alice's node, Bob's node and intermediate nodes $\{C^j\}_{j=1,2,\ldots,n}$ in the subnetwork, that is, $V=\{A, B, C^1, C^2, \ldots, C^n\}$, and an edge $e=v_1\to v_2\in E$ of G for $v_1, v_2\in V$ specifies a quantum channel $\mathcal{N}^{v_1\to v_2}$ to send a quantum system from node v_1 to node v_2 in the subnetwork. Then, the most general protocol proceeds in an adaptive manner as follows (cf. Fig. 1b, which exemplifies a linear network with $n=4$). The protocol starts by preparing the whole system in a separable state $\hat{\rho}_1^{ABC^1C^2\ldots C^n}$ and then by using a quantum channel $\mathcal{N}^{e_1}$ with $e_1\in E$. This is followed by arbitrary LOCC among all the nodes, which gives an outcome k_1 and a quantum state $\hat{\rho}_{k_1}^{ABC^1C^2\ldots C^n}$ with probability p_{k_1}. In the second round, depending on the outcome k_1, a node may use a quantum channel $\mathcal{N}^{e_{k_1}}$ with $e_{k_1}\in E$, followed by LOCC among all the nodes. This LOCC gives an outcome k_2 and a quantum state $\hat{\rho}_{k_2k_1}^{ABC^1C^2\ldots C^n}$ with probability $p_{k_2|k_1}$. Similarly, in the i-th round, according to the previous outcomes $\boldsymbol{k}_{i-1}:=k_{i-1}\ldots k_2k_1$ (with $\boldsymbol{k}_0:=1$), the protocol may use a quantum channel $\mathcal{N}^{e_{\boldsymbol{k}_{i-1}}}$ with $e_{\boldsymbol{k}_{i-1}}\in E$, followed by LOCC providing a quantum state $\hat{\rho}_{\boldsymbol{k}_i}^{ABC^1C^2\ldots C^n}$ with a new outcome k_i with probability $p_{k_i|\boldsymbol{k}_{i-1}}$. After a number of rounds, say after an l-th round, the protocol must present $\hat{\rho}_{\boldsymbol{k}_l}^{AB}=\mathrm{Tr}_{C^1C^2\ldots C^n}(\hat{\rho}_{\boldsymbol{k}_l}^{ABC^1C^2\ldots C^n})$ close to a target state $\hat{\tau}_{d_{\boldsymbol{k}_l}}^{AB}$ in the sense of $\|\hat{\rho}_{\boldsymbol{k}_l}^{AB}-\hat{\tau}_{d_{\boldsymbol{k}_l}}^{AB}\|_1\le\epsilon$ for $\epsilon>0$, from which Alice and Bob can distil $\log_2 d_{\boldsymbol{k}_l}$ secret bits or $\log_2 d_{\boldsymbol{k}_l}$ ebits. After all, the protocol results in presenting $\log_2 d_{\boldsymbol{k}_l}$ secret bits or ebits with probability $p_{\boldsymbol{k}_l}$ by using quantum channels $\{\mathcal{N}^e\}_{e\in E}$, where $p_{\boldsymbol{k}_l}:=p_{k_l|\boldsymbol{k}_{l-1}}\cdots p_{k_3|\boldsymbol{k}_2}p_{k_2|\boldsymbol{k}_1}p_{k_1}$.

Fundamental limitation on the quantum internet protocol. For the general adaptive quantum internet protocol, our main result is described as follows. Let us divide set V into two disjoint sets, V_A including A and V_B including B, satisfying $V_A=V\backslash V_B$ (and $V_B=V\backslash V_A$) (see Fig. 1 for the examples). For given $\boldsymbol{k}_i$, if the protocol uses a quantum channel $\mathcal{N}^{e_{\boldsymbol{k}_i}}$ between a node in V_A and a node in V_B, we write $\boldsymbol{k}_i\in K_{V_A\leftrightarrow V_B}$. For example, $\boldsymbol{k}_1\in K_{V_A\leftrightarrow V_B}$ in Fig. 1b. Then, for any choice of V_A (or V_B), the most general protocol has a limitation described by

$$\sum_{\boldsymbol{k}_l} p_{\boldsymbol{k}_l}\log_2 d_{\boldsymbol{k}_l}\le\sum_{i=0}^{l-1}\sum_{\boldsymbol{k}_i\in K_{V_A\leftrightarrow V_B}} p_{\boldsymbol{k}_i}E_{\mathrm{sq}}(\mathcal{N}^{e_{\boldsymbol{k}_i}})+g(\epsilon), \qquad (1)$$

where g is a continuous function[14,38] with the property of $\lim_{\epsilon\to 0}g(\epsilon)=0$ and $E_{\mathrm{sq}}(\mathcal{N})$ is the squashed entanglement[14,15] of channel $\mathcal{N}$. This bound is reduced to $\sum_{\boldsymbol{k}_l}p_{\boldsymbol{k}_l}\log_2 d_{\boldsymbol{k}_l}\le\sum_{i=0}^{l-1}\sum_{\boldsymbol{k}_i\in K_{V_A\leftrightarrow V_B}}p_{\boldsymbol{k}_i}E_{\mathrm{sq}}(\mathcal{N}^{e_{\boldsymbol{k}_i}})$ for $\epsilon\to 0$. The bound (1) is obtained by regarding the general protocol as bipartite communication between V_A and V_B and by applying the TGW

bound to the bipartite one (see Supplementary Note 1 for the proof). Since the bound holds for any choice of V_A, the bound shows that the average of the obtained secret bits or ebits is most tightly bounded by the choice of V_A minimizing the right-hand side of equation (1). Again, note that our bound (1) is applicable to any quantum network composed of arbitrary quantum channels, in contrast to Pirandola's one[37] with the assumption of the teleportation stretchability for quantum channels.

Application to general linear networks. As an instructive application of the bound (1), we first derive an upper bound for a general linear network as in Fig. 1b, which includes intercity QKD protocols and quantum repeater protocols as special cases. Here the goal of Alice and Bob is to share secret bits or ebits by using a quantum internet protocol with help of intermediate nodes $\{C^j\}_{j=1,2,\ldots,n}$. Suppose that the nodes A, C^1, C^2, …, C^n and B line in order (Fig. 1b), and nearest-neighbouring nodes are connected by quantum channels $\{\mathcal{N}^e\}_{e\in E}$, respectively. For clarity, if an edge e associated with a quantum channel $\mathcal{N}^e$ is $v_1\to v_2$ or $v_2\to v_1$ for v_1, $v_2\in V$, we refer to the edge as $v_1\leftrightarrow v_2$. Nodes A and B are dubbed C^0 and C^{n+1}, respectively (that is, $A=:C^0$ and $B=:C^{n+1}$). Then, as shown in Methods, from equation (1), we obtain a bound for the protocol

$$\frac{\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{\bar{m}_l}\leq \frac{1}{\sum_{j=0}^{n}\left[E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)\right]^{-1}}+\frac{g(\epsilon)}{\bar{m}_l}, \qquad (2)$$

where $\langle f_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}$ represents the average of function $f_{\boldsymbol{k}_l}$ over $\boldsymbol{k}_l$ and $\bar{m}_l$ is the average total number of channel uses. The first term of the right-hand side in this inequality is proportional to the harmonic mean of the squashed entanglement of channels $\{\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\}_{j=0,1,\ldots,n}$. Also, note that the left-hand side quantity—which is the average obtained secret bits or ebits per average total channel use—is different from Pirandola's measure[37] for the performance (see Methods).

Optimal scaling for intercity QKD and quantum repeaters. To show how good the bound (2) is, let us start by comparing it with the performance of intercity QKD protocols and quantum repeater protocols. For simplicity, suppose that all the nodes $\{C^j\}_{j=0,1,\ldots,n+1}$ are located at regular intervals between Alice and Bob separated over distance L and they are connected with optical fibres with transmittance $\eta_{L_0}:=e^{-L_0/l_{\rm att}}$ for attenuation length $l_{\rm att}$ and $L_0:=L/(n+1)$ with each other. Then, all the channels $\{\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\}_{j=0,1,\ldots,n}$ must be the same lossy optical channel $\mathcal{O}_{\eta_{L_0}}$ with transmittance η_{L_0}, for which Takeoka *et al.*[14,15] have already derived an upper bound on the squashed entanglement of the channel. This implies $E_{\rm sq}(\mathcal{N}^{C^j\leftrightarrow C^{j+1}})=E_{\rm sq}(\mathcal{O}_{\eta_{L_0}})\leq 2\log_2\left[\left(1+\eta_{L_0}\right)/\left(1-\eta_{L_0}\right)\right]$ for any $j=0,1,\ldots,n$, where the factor 2 in the front comes from the fact that a single use of an optical channel for transmission of an optical pulse corresponds to the sending of two optical modes associated with its polarization degrees of freedom. Then, the bound (2) is reduced to

$$\frac{\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{\bar{m}_l}\leq \frac{2}{n+1}\log_2\left(\frac{1+\eta_{L_0}}{1-\eta_{L_0}}\right)+\frac{g(\epsilon)}{\bar{m}_l}. \qquad (3)$$

In particular, this bound shows that the average secret bits or ebits per average total channel use, $\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}/\bar{m}_l$, are upper bounded by $2(n+1)^{-1}\log_2\left[\left(1+\eta_{L_0}\right)/\left(1-\eta_{L_0}\right)\right]$ for $\epsilon\to 0$, which is approximated to be $4[(n+1)\ln 2]^{-1}\eta_{L_0}$ for $L_0\gg 1$. The bound (3) is strong enough to show that the existing intercity QKD protocols and quantum repeater protocols are pretty good in the sense that they have the same scaling with this simple bound.

Let us first compare the bound (3) with the intercity QKD protocols[19–21]. This class of QKD protocols leads to a square root improvement in the secret key rate over conventional QKD schemes (without quantum repeaters) bounded by the TGW bound. Nonetheless, it is implementable[21] without the need of matter quantum memories or quantum error correction, which is in a striking contrast to quantum repeaters[18,22–36]. In particular, those intercity QKD protocols are modifications of the measurement-device-independent QKD[39] (mdiQKD), and all of them use a single (untrusted) intermediate node C in the middle of communicators Alice and Bob. Node C shares optical channels with Alice and Bob, whose transmittance is described by $\eta_{L/2}$. By using these channels, Alice and Bob send single photons to the node C. Then, using matter quantum memories[19,20] or using optical devices alone[21], the middle node C performs the Bell measurement only on pairs of photons that have successfully survived the loss during the transmission from Alice and Bob. Since the success of the Bell measurement provides secret bits, the average secret bits of these protocols per total channel use are in the order of the survival probability of photons, that is, $\eta_{L/2}$. However, this is exactly the same scaling of the bound (3), because the bound (3) is proportional to $\eta_{L_0}=\eta_{L/2}$ for $n=1$, $\epsilon\to 0$ and $L_0\gg 1$. In fact, this is easily confirmed by seeing Fig. 2a. Therefore, it is concluded that the intercity QKD protocols[19–21] have no scaling gap with the upper bound (3).

Next, let us compare the bound (3) with the performance of achievable quantum repeater protocols. Actually, there are many quantum repeater schemes[18,22–36], depending on the assumed devices of the repeater nodes $\{C^1, C^2, \ldots, C^n\}$. For instance, a protocol assumes repeater nodes equipped with atomic-ensemble quantum memories as well as optical devices[18,23]. To obtain better scaling, instead of the atomic-ensemble quantum memories, another protocols[22,27–29,32,34] use matter qubits satisfying[35,36] all the criteria given by DiVincenzo[40]. Moreover, there is even an all-photonic scheme[35] that does not use matter quantum memories at all and works by using only optical devices. However, since our aim here is to show the existence of a quantum repeater protocol that has the same scaling with the bound (3) in principle, let us introduce an idealized qubit-based protocol that uses a noiseless quantum computer with the function of the perfect coupling with single photons at each repeater node. This protocol is conceptually simple. But it gives a good lower bound of the secure key rate or the entanglement generation rate in the sense that it has the same scaling behaviour as the bound (3).

In the idealized qubit-based protocol, (i) node C^j ($j=0, 1, \ldots, n$) begins by producing a single photon, which is in maximally entangled state $|\Phi^+\rangle=(|0\rangle|H\rangle+|1\rangle|V\rangle)/\sqrt{2}$ with a qubit of a local quantum computer, where $\{|H\rangle, |V\rangle\}$ is an orthonormal basis for the polarization degrees of freedom of the single photon and $\{|0\rangle, |1\rangle\}$ is a computational basis of the qubit. (ii) Then, the node C^j sends its right-hand-side adjacent node C^{j+1} the single photon through the optical fibre with transmittance η_{L_0}. (iii) On receiving the photon from the node C^j, the node C^{j+1} performs a quantum non-demolition measurement to confirm the successful arrival of the single photon, and announces the measurement outcome to node C^j via a heralding signal. If this quantum non-demolition measurement proves the successful arrival of the single photon, the node C^{j+1} transfers the quantum state of the received photon into a qubit of the local quantum computer faithfully, establishing a maximally entangled state between quantum computers in the node C^j and in the node C^{j+1}. (iv) If the node C^j is informed of the loss of the sent photon in the transmission by the heralding signal from the right-hand-side adjacent node C^{j+1}, the nodes C^j and

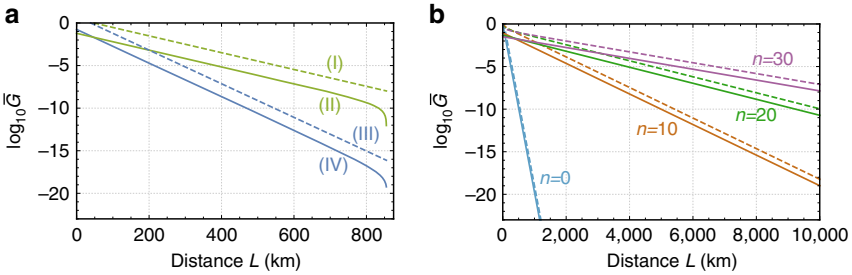

Figure 2 | Performance and upper bounds of protocols based on linear lossy optical channel networks. The performance is measured in terms of secret bits or ebits per average total channel use, $\bar{G}:=\langle \log_2 d_{\boldsymbol{k}_l} \rangle_{\boldsymbol{k}_l}/\bar{m}_l$, for the distance L between Alice and Bob. As in Fig. 1b, the protocols use intermediate nodes $\{C^1, C^2, \ldots, C^n\}$ connected by optical fibres with transmittance $\eta_l:=e^{-l/l_{\rm att}}$ for attenuation length $l_{\rm att}=22$ km with each other and located at regular intervals, say $L_0=L/(n+1)$. The solid curves represent achievable performance, while the dashed curves are the upper bounds in equation (3) for the linear network, for various n. In **a**, we provide the performance of mdiQKD protocols[21,39] using only a single intermediate node ($n=1$) equipped with feasible optical devices. In particular, lines (II) and (IV) represent the all-photonic intercity QKD protocol[21] and the original mdiQKD protocol[39], respectively. These lines just refer to the performance given in Fig. 3 of ref. 21 (see ref. 21 for the detail of the assumed optical devices). The key rate scales linearly with η_L for the mdiQKD[39], but it scales linearly with $\eta_{L/2}$ for the all-photonic intercity QKD[21]. We also show our bound (3) for $n=1$ as line (I) and the TGW bound[14] (corresponding to our bound with $n=0$) as line (III). Comparing lines (I) and (II), we can see that the all-photonic intercity QKD protocol has the same scaling with our bound (3) for $n=1$. In **b**, for various n, we provide the performance of the idealized qubit-based quantum repeater protocol, $(n+1)^{-1}\eta_{L_0}=(n+1)^{-1}\eta_{L/(n+1)}$, as solid lines and our bound (3) as dashed curves. We can see that there is essentially no scaling gap between our bound (3) and the idealized qubit-based protocol.

C^{j+1} repeat steps (i)–(iii). (v) If every node shares a maximally entangled state with the adjacent nodes, all the repeater nodes $\{C^1, C^2, \ldots, C^n\}$ apply the Bell measurement to a pair of local qubits that have been entangled with qubits in the adjacent repeater nodes. This gives Alice and Bob a pair of qubits in a maximally entangled state.

Let us estimate the performance of this idealized qubit-based protocol. Since the entanglement generation process (i)–(iii) is repeated until a single photon sent in step (ii) survives over the fibre transmission with transmittance η_{L_0}, the average of the number m of channel uses to obtain the entanglement between adjacent nodes in step (iii) is $\sum_{m=1}^{\infty} m\left(1-\eta_{L_0}\right)^{m-1}\eta_{L_0}=\eta_{L_0}^{-1}$. Hence, the idealized qubit-based protocol presents Alice and Bob a pair of qubits in a maximally entangled state by using $\bar{m}_l=(n+1)\eta_{L_0}^{-1}$ times of optical channels in total on average. Therefore, the average secret bits or ebits of the idealized qubit-based protocol per average total channel use is $(n+1)^{-1}\eta_{L_0}$, which is exactly the same scaling of the bound (3). This fact is also easily confirmed by seeing Fig. 2b.

Since the existing quantum repeater protocols[18,22–36] are based on more practical devices than the idealized qubit-based protocol, they would be less efficient than the idealized qubit-based protocol, owing to more imperfections caused by the practical devices. However, there are schemes[27–29,32,34,35] whose performance is essentially determined by distance L_0 even under the use of such more practical devices similarly to the idealized qubit-based protocol as well as our bound (3). This implies that the quantum repeater protocols[27–29,32,34,35] have no scaling gap with our bound (3).

Upper bounds for DLCZ-type quantum repeaters. The bound (3) has been shown to be useful for understanding the ultimate performance of intercity QKD protocols and quantum repeater protocols. However, the original bound (2) for the general linear networks should have another fascinating applications beyond the purely lossy optical channel network. To show this, as an example, here we apply our bound to an exponential scaling problem[35,41] of the DLCZ-type quantum repeater protocols[18,23,24,30] with time-dependent decay of matter quantum memories. This problem was first pointed out by Razavi *et al.*[41] by considering the practice of the matter quantum memories (although the DLCZ scheme was initially introduced[23] as a protocol with polynomial scaling by assuming infinite coherence time of atomic-ensemble quantum memories). More precisely, Razavi *et al.* show that for the matter quantum memory with finite coherence time and no fault-tolerant protection the performance of the DLCZ-type protocols degrades exponentially with $\sqrt{L}$, regardless of the used distillation scheme. However, we can obtain a more general and stronger result by using our bound (2). That is, from the bound (2), we can derive ultimate upper bounds on more general DLCZ-type quantum repeater protocols where even any single-shot quantum error correction for the matter quantum memories is allowed to be used in contrast to the paradigm of Razavi *et al.* Nonetheless, our bounds show that the coherence time of the matter quantum memories should be, at least, larger than 100 μs—which are comparable even with the up-to-date experimental result[42] with retaining the coupling efficiency with photons—for enjoying the blessing of the DLCZ-type quantum repeaters.

Although the details can be found in Supplementary Note 2, here we present the main observation used to derive the upper bound for the DLCZ-type schemes. Conventionally, these schemes use the set of repeater nodes $\{C^j\}_{j=1,2,\ldots,2n+1}$—which is composed of source repeater nodes $\{C^{2j}\}_{j=1,2,\ldots,n}$ and receiver repeater nodes $\{C^{2j+1}\}_{j=0,1,\ldots,n}$—between Alice $A(=:C^0)$ and Bob $B(=:C^{2n+2})$, where $n=2^s-1$ for $s\in\{0, 1, 2, \ldots\}$. The source repeater nodes and the receiver repeater nodes are located alternately and at regular intervals, and the adjacent source nodes (adjacent receiver nodes) are separated over distance $L_0=L/(n+1)$. The unique feature of the DLCZ-type schemes is to use only probabilistic Bell measurements not only for the entanglement generation but also for the entanglement swapping, because the schemes adopt their implementation with linear optical elements and photon detectors by respecting the simplicity and practicality[18,23,24,30]. In particular, the schemes (Supplementary Fig. 1) begin with independent and parallel entanglement generation processes between adjacent source repeater nodes C^{2j} and C^{2j+2}. These are accomplished by performing the Bell measurements at receiver node C^{2j+1} on pairs of optical pulses—each of which has been entangled with a matter quantum memory—from the adjacent nodes C^{2j} and

C^{2j+2} over lossy optical channels $\mathcal{O}_\eta$ a transmittance η. Then, entangled pairs connecting source repeater nodes separated by 2^iL_0 are converted to ones separated by $2^{i+1}L_0$ recursively ($i=0, 1, \ldots, s-1$), until Alice and Bob share entangled pairs. This is done by sequential applications of the entanglement swapping to matter quantum memories in a knockout tournament manner over source repeater nodes $\{C^{2j}\}_{j=1,2,\ldots,n}$. Here to perform the entanglement swapping as a step, source repeater node C^{2j} necessitates to receive heralding signals from distant repeater nodes to know which pairs of its own matter quantum memories should be subjected to the Bell measurements for the swapping. Hence, during the time t_{2j} from the beginning of entanglement generation to the arrival of the heralding signals, this repeater node C^{2j} needs to store entanglement in matter quantum memories with time-dependent decay modelled by a noisy qubit channel $\mathcal{M}_{t_{2j}}$. If we also respect the independence of the entanglement generation processes, as well as availability of only single-shot quantum error correction for matter quantum memories, the repeater node C^{2j} can thus be considered to be composed of three nodes $C^{2j}_{\rm L}$, $C^{2j}_{\rm F}$ and $C^{2j}_{\rm R}$. Here $C^{2j}_{\rm L}$ and $C^{2j}_{\rm R}$ are connected to C^{2j-1} and C^{2j+1} by the lossy optical channel $\mathcal{O}_\eta$ for the entanglement generation processes, respectively, and they are also linked by the noisy qubit channels $\mathcal{M}_{t_{2j}}$ to $C^{2j}_{\rm F}$ to perform the Bell measurements. Therefore, we can regard the DLCZ-type schemes as protocols working over a linear network (Supplementary Fig. 2) in the spacetime that is composed of vertices $V=\{A, C^1, C^2_{\rm L}, C^2_{\rm F}, C^2_{\rm R}, C^3, \ldots, B\}$ connected by the lossy optical channels $\mathcal{O}_\eta$ and the noisy qubit channels $\mathcal{M}_{t_{2j}}$. Since the minimum required memory time t_{2j} is determined by the location of the repeater node C^{2j} and the signalling time of the heralding signals, we can derive an upper bound on this linear network from equation (2) by deeming it as living merely in the space, rather than in the spacetime (Supplementary Note 2). Note that this implies that the upper bound may overestimate the performance of the DLCZ-type schemes, because the linear network over the space does not have any restriction[43] coming from the arrow of time in contrast to that in the spacetime.

In Fig. 3, we show the upper bounds on the linear network associated with the DLCZ-type quantum repeaters for the applications to the secret-key and entanglement generation between Alice and Bob. The difference between Fig. 3a and Fig. 3b stems from the fact that Alice and Bob need matter quantum memories for the case of the entanglement generation, while they do not for the case of the secret-key generation (see ref. 35 for instance). For the calculation of Fig. 3, the noisy qubit channel $\mathcal{M}_{t_{2j}}$ for the matter quantum memory is assumed to be modelled by a phase-flip channel with coherence time $\tau_{\rm c}$. In addition, we suppose that the transmittance η of the lossy optical channel $\mathcal{O}_\eta$ is described by $\eta=\eta_{\rm c}\eta_{L_0/2}$ with the coupling efficiency $\eta_{\rm c}$ and the velocity of the heralding signals is equivalent to the speed v of light in optical fibres. Under these conditions, in Fig. 3, the number n associated with the number of repeater nodes is optimized to maximize the upper bounds. The existence of optimal n here—which is in contrast to the case for upper bounds for purely optical channel networks as in Fig. 2—stems from the existence of local errors/loss in the repeater nodes.

Despite these optimistic assumptions, Fig. 3 shows that even the upper bounds on the DLCZ-type quantum repeater schemes decay exponentially with the communication distance L for $\tau_{\rm c}\leq 100\,\mu$s, although the threshold is comparable to the achieved coherence time in the up-to-date experiment[42]. This result may be reasonable by considering[35] that the transmission time of the heralding signal over, for example, 100 km is already in the order of 100 μs. Although Fig. 3 indicates that the upper bounds drastically improve with the coherence time $\tau_{\rm c}$ ($\geq 100\,\mu$s), this does not necessarily mean that there is a DLCZ-type quantum repeater scheme with similar performance, owing to the overestimation of the upper bounds.

Of course, if we are allowed to repeat quantum error correction on the matter quantum memories while waiting for the heralding signals to arrive, then the coherence time of the matter quantum memories is not an issue. However, such a scheme to use such repeated quantum error correction cannot be called anymore the DLCZ-type quantum repeater protocols[18,23,24,30] respecting the practical simplicity.

Discussion

We have presented a fundamental upper bound (1) on the performance of any two-party quantum communication scheme over arbitrary quantum network topology. Besides, we have focused on its application to the general linear quantum network. As a result, we have seen that the bound (2) for the linear network is powerful enough to present rate-loss trade-offs (3) with the same scaling as existing intercity QKD protocols and quantum repeaters. However, the goodness of our bound (1) should not be restricted only to linear networks. In fact, very recently, Azuma and Kato[44] have proposed a scheme that runs quantum repeater protocols between Alice and Bob in parallel over any given network, and they have shown that it has no scaling gap with our upper bound (1) for the case of lossy optical channel networks, irrespectively of the network topology. Since each of the quantum repeater protocols in this scheme is merely performed over a linear network, this protocol implies that it is important to optimize quantum repeater protocols via comparing its performance with our bound (2) for the linear network. More importantly, that fact suggests that our bound (1) is strong enough to evaluate the goodness of any protocol working over a general optical quantum network beyond linear ones.

In addition, we have treated a quantum internet protocol as if it supplies only a pair of clients, called Alice A and Bob B, with secret bits or ebits. Here we highlight that in fact our bound applies to multiple-pair cases where multiple pairs of parties try to establish secret bits or ebits at the same time. Suppose that there are m pairs of clients labelled by an index j so that a node $A^j\in V$ would like to share secret bits or ebits with another node $B^j\in V$ for $j=1, 2, \ldots, m$ by using a quantum network associated with a graph $G=(V, E)$. Then, if a quantum internet protocol presents pair A^jB^j with $\log_2 d^{(j)}_{\boldsymbol{k}_l}$ secret bits or ebits within an error $\epsilon(>0)$ with probability $p_{\boldsymbol{k}_l}$ for all $j=1, 2, \ldots, m$, the protocol obeys the following bound, which can be obtained similarly to equation (1) (see the proof in Supplementary Note 3): for any $V'\subset V$, we have

$$\sum_{j\in J_{V'\leftrightarrow V\setminus V'}}\left\langle \log_2 d^{(j)}_{\boldsymbol{k}_l}\right\rangle_{\boldsymbol{k}_l}\leq \sum_{i=0}^{l-1}\sum_{\boldsymbol{k}_i\in K_{V'\leftrightarrow V\setminus V'}} p_{\boldsymbol{k}_i}E_{\rm sq}(\mathcal{N}^{e_{\boldsymbol{k}_i}})+g(\epsilon), \quad (4)$$

where we write $j\in J_{V'\leftrightarrow V\setminus V'}$ when $A^j\in V'$ and $B^j\in V\setminus V'$ or when $B^j\in V'$ and $A^j\in V\setminus V'$. Therefore, our bound is applied to any multi-pair bipartite quantum communication protocol.

Despite the generalized bound (4), we have still focused on bipartite quantum communication protocols over a given network. However, our bound (1) is applicable even to any multi-party protocol[16,45] based on sharing a multipartite resource[46]—such as a multipartite private key[47] or a multipartite entangled state like a Greenberger–Horne–Zeilinger state and a cluster state—among plural clients. This is because such a multipartite resource is, usually, freely transformed into a corresponding bipartite resource—secret bits or ebits—between any two of the clients by using an additional LOCC operation, to which our bound (1) is applied. Therefore, our bound should provide an upper bound even to such a multi-party quantum communication protocol.

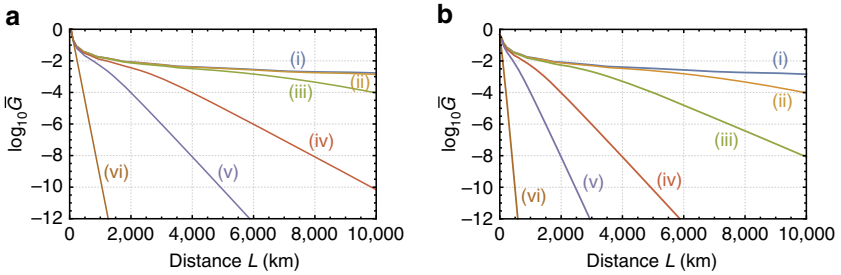

Figure 3 | Upper bounds for DLCZ-type quantum repeaters with time-dependent memory decay. The performance of the protocols[18,23,24,30] is measured in terms of the secret bits or ebits per average total channel use, $\bar{G}:=\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}/\bar{m}_l$, for the distance L between Alice and Bob. The protocols use repeater nodes $\{C^j\}_{j=1,2,\ldots,2n+1}$ located at regular intervals and connected by optical fibres with transmittance $\eta_l:=e^{-l/l_{\rm att}}$ ($l_{\rm att}=22$ km) with each other, as in Fig. 1b. We assume that the coupling efficiency to the fibres is $\eta_c=0.9$ and the speed of light in the fibres is $v=2.0\times10^8\,{\rm m\,s^{-1}}$. The source nodes $\{C^{2j}\}_{j=1,2,\ldots,n}$ are assumed to be equipped with matter quantum memories with dephasing, whose coherence time is (i) $\tau_c=1.0\times10^{-2}$ s, (ii) $\tau_c=5.0\times10^{-3}$ s, (iii) $\tau_c=2.5\times10^{-3}$ s, (iv) $\tau_c=1.0\times10^{-3}$ s, (v) $\tau_c=5.0\times10^{-4}$ s and (vi) $\tau_c=1.0\times10^{-4}$ s. The upper bounds for the protocols are obtained via being maximized over possible n. In **a** (In **b**), we show the upper bounds on the performance of the protocols for the application to QKD (for the application to entanglement distribution), where Alice and Bob do not need (Alice and Bob necessitate) to use matter quantum memories[35]. In **a** (In **b**), the upper bound (vi) is the same scaling of the intercity QKD protocols[19–21] with the performance in the order of $\eta_{L/2}$ (a point-to-point entanglement distribution protocol with the performance in the order of η_L), implying that $\tau_c\leq100\,\mu$s spoils the benefit to use the DLCZ-type quantum repeaters. Although these figures indicate that the upper bounds drastically improve with the coherence time τ_c ($>100\,\mu$s), this does not necessarily mean that there is a DLCZ-type scheme with similar performance, owing to the overestimation of the upper bounds.

We have also shown how to associate a class of practical quantum repeater protocols, called DLCZ-type quantum repeaters, with a linear quantum network composed of noisy qubit channels and lossy optical channels—corresponding to the models for matter quantum memories and optical fibres, respectively. Besides, by regarding the noisy qubit channels as the phase-flip channels for simplicity, from the upper bound (2) on the linear network, we have concluded that the coherence time of matter quantum memories should be, at least, longer than 100 μs to enjoy the blessing of the DLCZ-type quantum repeater schemes. However, this kind of correspondence between a practical quantum information processing (QIP) protocol and a quantum network is not unique, and it should have degrees of freedom a lot enough to derive good upper bounds on the performance of various kinds of QIP protocols. In particular, by finding out a proper correspondence between a given QIP protocol and a quantum network, our bounds (1) and (4) should present a fundamental upper bound, from which we can derive a non-trivial conclusion like the minimum coherence time required by the DLCZ-type quantum repeater schemes. For example, our bounds (1) and (4) would be useful for deriving the ultimate performance of the distributed quantum computation[30,48–51] and of more practical quantum repeaters with more complicated noise models. This versatility of our bounds would be in contrast to Pirandola's bound[37] restricted to teleportation stretchable quantum channel networks. This is because one would not be surprised if a practical QIP scheme involves quantum channels without teleportation stretchability.

While we have used mainly the TGW bound in our paper, it should be noted that our reduction idea is useful[44] for deriving a good bound for a general network topology from a bound for point-to-point quantum communication generally. We have just begun to grasp full implications of our bound (1): for instance, its tighter version for specific channels like Pirandola's one[37] or with deriving a better bound[52] for the squashed entanglement of the channel, its applications to the many-body quantum physics in any spacetime topology regarded as a quantum network[1] and to a more complicated quantum communication channel network—such as a multi-party protocol with broadcasting channels[53–55]—will be in a fair way to appear.

Methods

Upper bound (2) for the general linear network. Here we derive the bound (2) from the general bound (1). Since secret bits or ebits obtained through any quantum internet protocol must obey the bound (1), any scheme working over the general linear network should follow

$$\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}\leq \bar{m}_l^{C^j\leftrightarrow C^{j+1}}E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)+g(\epsilon) \tag{5}$$

for the choice of $V_A=\{C^0,\ldots,C^j\}$ with $j=0,1,\ldots,n$, where $\langle f_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}:=\sum_{\boldsymbol{k}_l}p_{\boldsymbol{k}_l}f_{\boldsymbol{k}_l}$ and $\sum_{i=0}^{l-1}\sum_{\boldsymbol{k}_l\in K_{V_A\leftrightarrow V_B}}p_{\boldsymbol{k}_l}$ for the choice of $V_A=\{C^0,\ldots,C^j\}$ is rephrased as the average number $\bar{m}_l^{C^j\leftrightarrow C^{j+1}}$ of times the quantum channel between nodes C^j and C^{j+1} is used. Since equation (5) holds for any $j=0,1,\ldots,n$, obtained secret bits or ebits are most tightly bounded as

$$\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}\leq \min_{j=0,1,\ldots,n}\bar{m}_l^{C^j\leftrightarrow C^{j+1}}E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)+g(\epsilon). \tag{6}$$

By assuming that we can freely choose $\left\{\bar{m}_l^{C^j\leftrightarrow C^{j+1}}\right\}_{j=0,1,\ldots,n}$ to maximize $\min_{j=0,1,\ldots,n}\bar{m}_l^{C^j\leftrightarrow C^{j+1}}E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)$ with the average total number $\bar{m}_l:=\sum_{j=0}^{n}\bar{m}_l^{C^j\leftrightarrow C^{j+1}}$ of channel uses fixed, we have

$$\min_{j=0,1,\ldots,n}\bar{m}_l^{C^j\leftrightarrow C^{j+1}}E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)\leq\frac{\bar{m}_l}{\sum_{j=0}^{n}\left[E_{\rm sq}\left(\mathcal{N}^{C^j\leftrightarrow C^{j+1}}\right)\right]^{-1}}, \tag{7}$$

where the equality holds when $\bar{m}_l^{C^0\leftrightarrow C^1}E_{\rm sq}\left(\mathcal{N}^{C^0\leftrightarrow C^1}\right)=\bar{m}_l^{C^1\leftrightarrow C^2}E_{\rm sq}\left(\mathcal{N}^{C^1\leftrightarrow C^2}\right)=\ldots=\bar{m}_l^{C^n\leftrightarrow C^{n+1}}E_{\rm sq}\left(\mathcal{N}^{C^n\leftrightarrow C^{n+1}}\right)$. This formulation highlights a difference in the performance measure from Pirandola's one[37] based on the restriction of $\bar{m}_l^{C^0\leftrightarrow C^1}=\bar{m}_l^{C^1\leftrightarrow C^2}=\ldots=\bar{m}_l^{C^n\leftrightarrow C^{n+1}}$. Combining equation (7) with equation (6), we obtain the bound (2).

Data availability. The data that support the findings of this study are available from the corresponding author on request.

References

1. Kimble, H. J. The quantum internet. *Nature* **453,** 1023–1030 (2008).
2. Bennett, C. H. & Brassard, G. in *Proc. IEEE Int. Conf. Comp. Sys. Signal Process.* 175–179 (Bangalore, India, 1984).
3. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
4. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1898 (1993).
5. Ladd, T. D. *et al.* Quantum computers. *Nature* **464,** 45–53 (2010).
6. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8,** 595–604 (2014).

7. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68,** 3121–3124 (1992).
8. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
9. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
10. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
11. Azuma, K. *et al.* Optimal entanglement generation for efficient hybrid quantum repeaters. *Phys. Rev. A* **80,** 060303 (R) (2009).
12. Azuma, K. & Kato, G. Optimal entanglement manipulation via coherent-state transmission. *Phys. Rev. A* **85,** 060303 (R) (2012).
13. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509,** 475–478 (2014).
14. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5,** 5235 (2014).
15. Takeoka, M., Guha, S. & Wilde, M. M. The squashed entanglement of a quantum channel. *IEEE Trans. Inf. Theory* **60,** 4987–4998 (2014).
16. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81,** 865 (2009).
17. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. Preprint at http://arxiv.org/abs/1510.08863 (2015).
18. Sangouard, N., Simon, C., de Riedmatten, N. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83,** 33–80 (2011).
19. Abruzzo, S., Kampermann, H. & Bruß, D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A* **89,** 012301 (2014).
20. Panayi, C., Razavi, M., Ma, X. & Lütkenhaus, N. Memory-assisted measurement-device-independent quantum key distribution. *New J. Phys.* **16,** 043005 (2014).
21. Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. *Nat. Commun.* **6,** 10171 (2015).
22. Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
23. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413–418 (2001).
24. Kok, P., Williams, C. P. & Dowling, J. P. Construction of a quantum repeater with linear optics. *Phys. Rev. A* **68,** 022301 (2003).
25. Childress, L., Taylor, J. M., Sørensen, A. S. & Lukin, M. D. Fault-tolerant quantum communication based on solid-state photon emitters. *Phys. Rev. Lett.* **96,** 070504 (2006).
26. van Loock, P. *et al.* Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.* **96,** 240501 (2006).
27. Jiang, L. *et al.* Quantum repeater with encoding. *Phys. Rev. A* **79,** 032325 (2009).
28. Fowler, A. G. *et al.* Surface code quantum communication. *Phys. Rev. Lett.* **104,** 180503 (2010).
29. Munro, W. J., Harrison, K. A., Stephens, A. M., Devitt, S. J. & Nemoto, K. From quantum multiplexing to high-performance quantum networking. *Nat. Photon.* **4,** 792–796 (2010).
30. Azuma, K., Takeda, H., Koashi, M. & Imoto, N. Quantum repeaters and computation by a single module: remote nondestructive parity measurement. *Phys. Rev. A* **85,** 062309 (2012).
31. Zwerger, M., Dür, W. & Briegel, H. J. Measurement-based quantum repeaters. *Phys. Rev. A* **85,** 062326 (2012).
32. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photon.* **6,** 777–781 (2012).
33. Li, Y., Barrett, S. D., Stace, T. M. & Benjamin, S. C. Long range failure-tolerant entanglement distribution. *New J. Phys.* **15,** 023012 (2013).
34. Mazurek, P. *et al.* Long-distance quantum communication over noisy networks without long-time quantum memory. *Phys. Rev. A* **90,** 062311 (2014).
35. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6,** 6787 (2015).
36. Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside quantum repeaters. *IEEE J. Sel. Top. Quant. Electron* **21,** 6400813 (2015).
37. Pirandola, S. Capacities of repeater-assisted quantum communications. Preprint at http://arxiv.org/abs/1601.00966 (2016).
38. Wilde, M. M. Squashed entanglement and approximate private states. *Quantum Inf. Process.* **15,** 4563–4580 (2016).
39. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
40. DiVincenzo, D. P. The physical implementation of quantum computation. *Fortschr. Phys.* **48,** 771–783 (2000).
41. Razavi, M., Piani, M. & Lütkenhaus, N. Quantum repeaters with imperfect memories: cost and scalability. *Phys. Rev. A* **80,** 032301 (2009).
42. Yang, S.-J., Wang, X.-J., Bao, X.-H. & Pan, J.-W. An efficient quantum light-matter interface with sub-second lifetime. *Nat. Photon.* **10,** 381–384 (2016).
43. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54,** 3824 (1996).
44. Azuma, K. & Kato, G. Aggregating quantum repeaters for the quantum internet. Preprint at http://arxiv.org/abs/1606.00135 (2016).
45. Kómár, P. *et al.* A quantum network of clocks. *Nat. Phys.* **10,** 582–587 (2014).
46. Wallnöfer, J., Zwerger, M., Muschik, C., Sangouard, N. & Dür, W. 2D quantum repeaters. Preprint at http://arxiv.org/abs/1604.05352 (2016).
47. Horodecki, P. & Augusiak, R. Quantum states representing perfectly secure bits are always distillable. *Phys. Rev. A* **74,** 010302 (R) (2006).
48. Cirac, J. I., Ekert, A. K., Huelga, S. F. & Macchiavello, C. Distributed quantum computation over noisy channels. *Phys. Rev. A* **59,** 4249 (1999).
49. Barrett, S. D. & Kok, P. Efficient high-fidelity quantum computation using matter qubits and linear optics. *Phys. Rev. A* **71,** 060310 (R) (2005).
50. Lim, Y. L., Beige, A. & Kwek, L. C. Repeat-until-success linear optics distributed quantum computing. *Phys. Rev. Lett.* **95,** 030505 (2005).
51. Spiller, T. P. *et al.* Quantum computation by communication. *New J. Phys.* **8,** 30 (2006).
52. Goodenough, K., Elkouss, D. & Wehner, S. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New J. Phys.* **18,** 063005 (2016).
53. Seshadreesan, K. P., Takeoka, M. & Wilde, M. M. Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. *IEEE Trans. Inf. Theory* **62,** 2849–2866 (2016).
54. Takeoka, M., Seshadreesan, K. P. & Wilde, M. M. in *Proc. 2016 IEEE Int. Symposium Inf. Theory* 2484–2488 (Barcelona, Spain, 2016).
55. Bäuml, S. & Azuma, K. Fundamental limitation on quantum broadcast networks. Preprint at http://arxiv.org/abs/1609.03994 (2016).

Acknowledgements

We thank S. Guha, S. Pirandola, M. Takeoka and M. M. Wilde for valuable discussions about their papers[14,15,17,37,38], and S. Azuma, S. Bäuml, G. Kato, R. Namiki and K. Tamaki for helpful discussions. K.A. thanks support from the Project UQCC by the National Institute of Information and Communications Technology and from the ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan). H.-K.L. acknowledges financial support from NSERC, CFI and ORF.

Author contributions

K.A. conceived the first version of the main concept with A.M. during their visit to H.-K.L.'s group at University of Toronto. Then, all the authors contributed to the refinement and generalization of the main concept and its presentation and writing of the present paper.

Additional information

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

Competing financial interests: The authors declare no competing financial interests.

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

How to cite this article: Azuma, K. *et al.* Fundamental rate-loss trade-off for the quantum internet. *Nat. Commun.* **7,** 13523 doi: 10.1038/ncomms13523 (2016).

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