PHYSICAL REVIEW A **96**, 032332 (2017)

Aggregating quantum repeaters for the quantum internet

Koji Azuma[1,2,*] and Go Kato[3,2,†]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[2]*NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3]*NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

(Received 18 April 2016; revised manuscript received 17 August 2017; published 22 September 2017)

The quantum internet holds promise for accomplishing quantum teleportation and unconditionally secure communication freely between arbitrary clients all over the globe, as well as the simulation of quantum many-body systems. For such a quantum internet protocol, a general fundamental upper bound on the obtainable entanglement or secret key has been derived [K. Azuma, A. Mizutani, and H.-K. Lo, Nat. Commun. **7**, 13523 (2016)]. Here we consider its converse problem. In particular, we present a universal protocol constructible from any given quantum network, which is based on running quantum repeater schemes in parallel over the network. For arbitrary lossy optical channel networks, our protocol has no scaling gap with the upper bound, even based on existing quantum repeater schemes. In an asymptotic limit, our protocol works as an optimal entanglement or secret-key distribution over any quantum network composed of practical channels such as erasure channels, dephasing channels, bosonic quantum amplifier channels, and lossy optical channels.

DOI: 10.1103/PhysRevA.96.032332

I. INTRODUCTION

In the internet, if a client communicates with a far distant client, the data travel across multiple networks. At present, the nodes and the communication channels in the networks are composed of physical devices governed by the laws of classical information theory, and the data flow obeys the celebrated max-flow min-cut theorem [1,2] in graph theory. However, in the future, such classical nodes and channels should be replaced with quantum ones, whose network follows the rules of quantum information theory, rather than the classical one. This network, called *quantum internet*, could accomplish tasks that are intractable in the realm of classical information processing, and it "provides opportunities and challenges across a range of intellectual and technical frontiers, including quantum computation, communication and metrology [3]."

So far, the main interest in the quantum internet has been the realization of quantum repeaters, especially specialized to linear networks [4–20]. On the other hand, it must be one of the most fundamental trials to grasp the full potential of a general quantum internet. Along this line, recently, Azuma, Mizutani, and Lo derived [21] a general fundamental upper bound—called the AML bound—on the performance for its use for supplying two clients with entanglement or a secret key, by generalizing the Takeoka-Guha-Wilde bound [22,23]. Interestingly, this AML bound can be estimated and applied to *any* private-key or entanglement distillation scheme that works over *any network topology* composed of arbitrary quantum channels with arbitrary local operations and unlimited classical communication (LOCC). For the case of *linear* networks composed of lossy optical channels, it has been shown [21] that existing intercity quantum key distribution protocols [24–26] and quantum repeater schemes [9,11,16,18,19] have no scaling gap with the AML bound. In addition, in the case of a multipath network composed of a wide range of teleportation stretchable quantum channels [27–29] (including lossy optical channels), Pirandola has provided [30] a protocol that determines a single path to supply two clients with a secret bit or an entangled pair by minimizing the number of uses of the paths between them. However, it remained as a highly nontrivial open problem to find a *universal* protocol (beyond quantum repeaters) which works over *any network topology* (rather than only linear or multipath networks) composed of *arbitrary* quantum channels and with no scaling gap with the AML bound. This is because, in general, there is a huge conceptual gap in complexity of the problem between linear networks and arbitrary networks.

In this paper, however, we present such a universal quantum internet protocol working over any network topology, inspired by the form of the AML bound analogous to the max-flow min-cut theorem. In particular, we provide a protocol constructible from any given quantum network, which runs quantum repeater schemes in parallel over the network to provide entanglement to two clients. The performance of this protocol is derived from Menger's theorem [31] in graph theory. By this, it is shown that our protocol based on *existing* quantum repeater schemes has no scaling gap with the AML bound for arbitrary lossy optical channel networks. This is notable in the sense that the existing repeater schemes—proposed as feasible in the near future—have already had the potential to be comparable with the best quantum internet protocols for two clients—which have, though, not yet been discovered in a practical form. Moreover, in an asymptotic limit, our protocol is shown to be optimal for any quantum network composed of practical channels such as erasure channels, dephasing channels, bosonic quantum amplifier channels, and lossy optical channels, irrespective of its purpose, i.e., entanglement distribution or secret-key distribution. This means that our protocol achieves a quantum or private capacity of such practical networks. In general, the optimality of our protocol is associated with outstanding problems in quantum information theory such as additivity questions for quantum channels and questions on the existence of a gap between the quantum capacity and the private capacity.

[*] azuma.koji@lab.ntt.co.jp
[†] kato.go@lab.ntt.co.jp

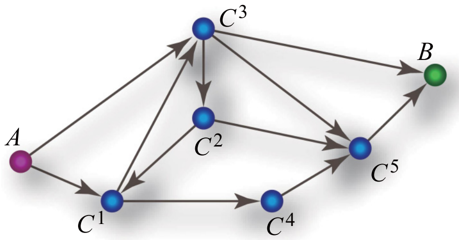

FIG. 1. Quantum network. The network is associated with a directed graph $G = (V,E)$ with set V of vertices and set E of edges, where V is composed of Alice's node A, Bob's node B, and intermediate nodes $C^1, C^2, \ldots,$ and C^n ($n = 5$ here) and a directed edge $e = X \to Y$ in E for $X,Y \in V$ specifies a quantum channel $\mathcal{N}^e$ to send a subsystem in node X to node Y. The goal here is to give Alice and Bob pbits or ebits by using quantum channels $\{\mathcal{N}^e\}_{e\in E}$ and LOCC.

II. QUANTUM INTERNET PROTOCOL FOR TWO CLIENTS

Let us begin by reviewing quantum internet protocols for two clients [21]. The quantum internet protocol will serve a subnetwork to two clients, called Alice and Bob, to provide resources for quantum communication, private bits (pbits) or Bell pairs (ebits). The subnetwork is associated with a directed graph $G = (V,E)$ with set V of vertices and set E of edges (see Fig. 1 as an example), where V is composed of Alice's node A, Bob's node B, and intermediate nodes $C^1, C^2, \ldots,$ and C^n and an edge $e = X \to Y$ in E for $X,Y \in V$ specifies a quantum channel $\mathcal{N}^e (= \mathcal{N}^{X\to Y})$ to send a subsystem in node X to node Y. In general, the protocol begins by sharing a separable state and then by using a quantum channel $\mathcal{N}^{e_1}$ with $e_1 \in E$. This is followed by LOCC among all the nodes, giving 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 ith round ($i = 2,3,\ldots$), depending on the previous outcome $\boldsymbol{k}_{i-1} = k_{i-1}\cdots k_2k_1$ (with $\boldsymbol{k}_0 := 1$), the protocol may use [32] 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 $\hat{\rho}_{\boldsymbol{k}_i}^{ABC^1C^2,\ldots,C^n}$ corresponding to an outcome k_i with probability $p_{k_i|\boldsymbol{k}_{i-1}}$. In a final round, say an lth round, the protocol provides a quantum state $\hat{\rho}_{\boldsymbol{k}_l}^{AB} := \mathrm{Tr}_{C^1C^2,\ldots,C^n}(\hat{\rho}_{\boldsymbol{k}_l}^{ABC^1C^2,\ldots,C^n})$ close to a target state $\hat{\tau}_{d_{\boldsymbol{k}_l}}^{AB}$ in the sense $\|\hat{\rho}_{\boldsymbol{k}_l}^{AB} - \hat{\tau}_{d_{\boldsymbol{k}_l}}^{AB}\|_1 \leqslant \epsilon$ with $\epsilon > 0$, from which $\log_2 d_{\boldsymbol{k}_l}$ ebits for quantum teleportation or $\log_2 d_{\boldsymbol{k}_l}$ pbits for the one-time pad are distilled. Therefore, the protocol provides $\log_2 d_{\boldsymbol{k}_l}$ ebits or pbits with probability $p_{\boldsymbol{k}_l}$, where $p_{\boldsymbol{k}_i} := p_{k_i|\boldsymbol{k}_{i-1}} \cdots p_{k_3|\boldsymbol{k}_2} p_{k_2|\boldsymbol{k}_1} p_{k_1}$.

In general, the protocol is characterized by the average numbers $\{\bar{l}^e\}_{e\in E}$ of times quantum channels $\{\mathcal{N}^e\}_{e\in E}$ are used. $\bar{l}^e$ with respect to the channel $\mathcal{N}^e$ is described by $\bar{l}^e = \sum_{i=0}^{l-1} \langle \delta_{e,e_{\boldsymbol{k}_i}} \rangle_{\boldsymbol{k}_i}$ with the Kronecker delta $\delta_{i,j}$, where $\langle f_{\boldsymbol{k}_i} \rangle_{\boldsymbol{k}_i}$ is the average of function $f_{\boldsymbol{k}_i}$ over possible outcomes $\boldsymbol{k}_i$ of the protocol, i.e., $\langle f_{\boldsymbol{k}_i} \rangle_{\boldsymbol{k}_i} = \sum_{\boldsymbol{k}_i} p_{\boldsymbol{k}_i} f_{\boldsymbol{k}_i}$ for the probability $p_{\boldsymbol{k}_i}$. Then, the average $\bar{l}$ of the total number of channel uses is represented by $\bar{l} := \sum_{e\in E} \bar{l}^e$. Note that $\bar{l}$ could be an average value rather than a constant in general, because there are protocols that determine their final round, depending on the outcome $\boldsymbol{k}_i$ (see [32]). Generally, the average obtained ebits or pbits $\langle \log_2 d_{\boldsymbol{k}_l} \rangle_{\boldsymbol{k}_l}$ may increase with $\bar{l}^e$. Hence, it would be better to define a set $\{m^e\}_{e\in E}$ of parameters m^e associated with an upper bound on average uses of channel $\mathcal{N}^e$, because we can then focus on the set $\mathcal{P}_{\mathrm{Q}}(\epsilon,\{m^e\}_{e\in E})$ $[\mathcal{P}_{\mathrm{P}}(\epsilon,\{m^e\}_{e\in E})]$ of protocols which present $\log_2 d_{\boldsymbol{k}_l}$ ebits (pbits) with an error $\leqslant \epsilon$ (in terms of the trace distance) by using quantum channel $\mathcal{N}^e$ $\bar{l}^e$ times on average for each $e \in E$, satisfying $\bar{l}^e \leqslant m^e$ for any $e \in E$.

III. AGGREGATED QUANTUM REPEATER PROTOCOL

We introduce our protocol belonging to the set $\mathcal{P}_{\mathrm{Q}}(\epsilon,\{m^e\}_{e\in E})$, which is referred to as an *aggregated quantum repeater protocol*. This protocol is based on running quantum repeater protocols in parallel over the quantum network by using quantum channels $\{(\mathcal{N}^e)^{\otimes \lfloor m^e \rfloor}\}_{e\in E}$, where $\lfloor z \rfloor$ represents the largest integer $\leqslant z$. The quantum repeater protocols used here are allowed to be existing quantum repeater schemes [4–20]. In fact, our protocol is defined as long as we have entanglement generation schemes over channels $\mathcal{N}^e$ and a means for entanglement swapping, including probabilistic ones. Of course, these devices can be more demanding for achieving better performance, but we will show that our protocol even based on existing quantum repeater schemes has pretty good performance for practical quantum networks.

Suppose that we have entanglement generation schemes, perhaps equipped with quantum error correction or entanglement purification, over quantum channels $\{\mathcal{N}^e\}_{e\in E}$, each of which provides a state $\hat{\rho}^e$ close to $\lfloor m^e \rfloor R_\delta^e$ copies of a Bell pair $|\Phi^+\rangle_e$, i.e., $\|\hat{\rho}^e - |\Phi^+\rangle\langle\Phi^+|_e^{\otimes \lfloor m^e \rfloor R_\delta^e}\|_1 \leqslant \delta$ with $\delta > 0$, by using quantum channel $(\mathcal{N}^e)^{\otimes \lfloor m^e \rfloor}$ and LOCC. By running these protocols all over the edges $e \in E$, we obtain a state $\bigotimes_{e\in E} \hat{\rho}^e$ with

$$\left\| \bigotimes_{e\in E} \hat{\rho}^e - \bigotimes_{e\in E} |\Phi^+\rangle\langle\Phi^+|_e^{\otimes \lfloor m^e \rfloor R_\delta^e} \right\|_1 \leqslant |E|\delta, \tag{1}$$

where $|E|$ is the cardinality of set E. Let us regard each of the Bell pairs $\bigotimes_{e\in E} |\Phi^+\rangle\langle\Phi^+|_e^{\otimes \lfloor m^e \rfloor R_\delta^e}$, a Bell pair $|\Phi^+\rangle_e$ for instance, as an undirected edge e' with the same two ends of e, and let E' be the set composed of all such edges e'. Then, the Bell-pair network, i.e., $\bigotimes_{e\in E} |\Phi^+\rangle\langle\Phi^+|_e^{\otimes \lfloor m^e \rfloor R_\delta^e}$, can be associated with an undirected graph defined by $G' := (V,E')$ (see Fig. 2 as an example). Here we invoke Menger's theorem in graph theory.

Menger's theorem (*edge version*) [31,33]—In any graph G' with two distinguished vertices A and B, the maximum number of pairwise edge-disjoint AB paths is equal to the minimum number of edges in an AB cut.

Let us divide the set V of nodes into two disjoint sets, V_A including A and V_B including B, satisfying $V_B = V \setminus V_A$. If $e \in E_{V_A \leftrightarrow V_B}$ denotes an edge whose two ends belong to V_A and V_B, respectively, then the minimum number M_δ of edges in an AB cut in the graph G' is described by

$$M_\delta := \min_{V_A} \sum_{e \in E_{V_A \leftrightarrow V_B}} \lfloor m^e \rfloor R_\delta^e. \tag{2}$$

Then, Menger's theorem states that there are M_δ pairwise edge-disjoint AB paths in graph G' (see Fig. 2 for example and see

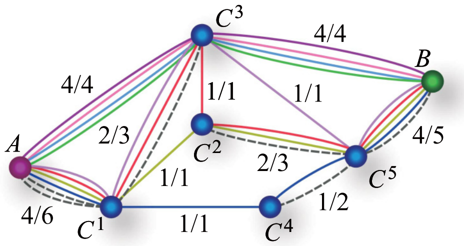

FIG. 2. Bell-pair network $\bigotimes_{e\in E}|\Phi^+\rangle\langle\Phi^+|_e^{\otimes\lfloor m^e\rfloor R_\delta^e}$ associated with $G'=(V,E')$. This is an example of the Bell-pair network for Fig. 1. Each undirected edge $e'\in E'$ represents a Bell pair $|\Phi^+\rangle_e$. The denominator and the numerator of a fraction describe $\lfloor m^e\rfloor R_\delta^e$ and how many Bell pairs are used and consumed in the aggregated quantum repeater protocol, respectively. Dashed edges are unused Bell pairs. Here the choice of $V_A=\{A,C^1,C^3\}$ in Eq. (2) gives $M_\delta=8$.

Ref. [33] for methods to find the paths). Since each P_i of these AB paths $\{P_i\}_{i=1,2,\ldots,M_\delta}$ corresponds to a linear chain of Bell pairs in the Bell-pair network $\bigotimes_{e\in E}|\Phi^+\rangle\langle\Phi^+|_e^{\otimes\lfloor m^e\rfloor R_\delta^e}$, the linear chain can be transformed into a Bell pair $|\Phi^+\rangle_{AB}$ by performing entanglement swapping $\mathcal{S}_{P_i}$ (including a Pauli correction) over the intermediate nodes on P_i. Then, from Eq. (1), we have

$$\begin{aligned}|E|\delta &\geqslant \left\|\bigotimes_{e\in E}\hat{\rho}^e-\bigotimes_{e\in E}|\Phi^+\rangle\langle\Phi^+|_e^{\otimes\lfloor m^e\rfloor R_\delta^e}\right\|_1\\ &\geqslant \left\|\mathrm{Tr}_{C^1C^2,\ldots,C^n}\circ\mathcal{S}\left(\bigotimes_{e\in E}\hat{\rho}^e-\bigotimes_{e\in E}|\Phi^+\rangle\langle\Phi^+|_e^{\otimes\lfloor m^e\rfloor R_\delta^e}\right)\right\|_1\\ &=\left\|\hat{\rho}^{AB}-|\Phi^+\rangle\langle\Phi^+|_{AB}^{\otimes M_\delta}\right\|_1,\end{aligned}\tag{3}$$

where $\mathcal{S}:=\mathcal{S}_{P_{M_\delta}}\circ\cdots\circ\mathcal{S}_{P_2}\circ\mathcal{S}_{P_1}$ and $\hat{\rho}^{AB}:=\mathrm{Tr}_{C^1C^2,\ldots,C^n}\circ\mathcal{S}(\bigotimes_{e\in E}\hat{\rho}^e)$. Therefore, the protocol, just like aggregating quantum repeater protocols, provides M_δ ebits with error $|E|\delta$ by using quantum channels $\{(\mathcal{N}^e)^{\otimes\lfloor m^e\rfloor}\}_{e\in E}$.

IV. THE OPTIMAL PROTOCOL AND A GENERAL UPPER BOUND

Clearly the aggregated quantum repeater protocol belongs to the set $\mathcal{P}_{\rm Q}(|E|\delta,\{m^e\}_{e\in E})\subset\mathcal{P}_{\rm P}(|E|\delta,\{m^e\}_{e\in E})$. Therefore, for any $Z\in\{{\rm Q},{\rm P}\}$, we have $M_\delta\leqslant\sup_{\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})}\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}$, i.e.,

$$\min_{V_A}\sum_{e\in E_{V_A\leftrightarrow V_B}}\lfloor m^e\rfloor R_\delta^e\leqslant\sup_{\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})}\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}\tag{4}$$

from Eq. (2). The right-hand side of this inequality represents the theoretical optimal performance for the set $\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})$ of protocols. Normally, it is highly nontrivial to obtain an explicit expression for this optimal performance, because the optimization should be taken over arbitrary protocols in the set $\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})$ which could include even ones based on multiparty entanglement purification, quantum network coding, and so on.

On the other hand, there is now the AML bound that upper bounds the performance of any quantum internet protocol defined in Sec. II as

$$\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}\leqslant\min_{V_A}\sum_{i=0}^{l-1}\sum_{\boldsymbol{k}_i\in K_{V_A\leftrightarrow V_B}}p_{\boldsymbol{k}_i}E_{\rm sq}(\mathcal{N}^{e_{\boldsymbol{k}_i}})+g(\epsilon).\tag{5}$$

Here g is a continuous function with the property of $\lim_{\epsilon\to0}g(\epsilon)=0$ (see Ref. [21] for the explicit expression), $E_{\rm sq}(\mathcal{N}^{X\to Y})$ is the squashed entanglement of the channel $\mathcal{N}^{X\to Y}$ (see [34] for its definition), and $\boldsymbol{k}_i\in K_{V_A\leftrightarrow V_B}$ represents that the protocol uses a quantum channel $\mathcal{N}^{e_{\boldsymbol{k}_i}}$ between a node in V_A and a node in V_B according to the outcome $\boldsymbol{k}_i$. Note that the squashed entanglement of the channel in Eq. (5) is a single-letter formula, that is, it can be evaluated as a function of a single channel use. In fact, by using this feature, upper bounds on the squashed entanglement for various noisy quantum channels have been derived [22,23,36]. For any $Z\in\{{\rm Q},{\rm P}\}$, by applying the AML bound (5) to protocols in the set $\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})$ and rephrasing it in terms of $\{\bar{l}^e\}_{e\in E}$, we obtain

$$\begin{aligned}&\sup_{\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})}\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}\\ &\quad\leqslant\min_{V_A}\sum_{e\in E_{V_A\leftrightarrow V_B}}m^eE_{\rm sq}(\mathcal{N}^e)+g(|E|\delta)\end{aligned}\tag{6}$$

from $\bar{l}^e\leqslant m^e$. Hence, combined with Eq. (4), the optimal performance of the set $\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})$ of protocols is sandwiched between the performance of the aggregated quantum repeater protocol and the AML bound in a symmetric manner.

For any $Z\in\{{\rm Q},{\rm P}\}$, the efficiency η_Z of the aggregated quantum repeater protocol to the optimal protocol can be lower bounded as

$$\eta_Z:=\frac{M_\delta}{\sup_{\mathcal{P}_Z(|E|\delta,\{m^e\}_{e\in E})}\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}\tag{7}$$

$$\geqslant\frac{(\min_{e\in E}\lfloor m^e\rfloor/m^e)\left[\min_{e\in E}R_\delta^e/E_{\rm sq}(\mathcal{N}^e)\right]}{1+g(|E|\delta)/\left[\min_{V_A}\sum_{e\in E_{V_A\leftrightarrow V_B}}m^eE_{\rm sq}(\mathcal{N}^e)\right]}\tag{8}$$

from Eqs. (2) and (6). This implies that, as long as our aggregated quantum repeater protocol is based on entanglement generation schemes with $R_\delta^e=\Omega[E_{\rm sq}(\mathcal{N}^e)]$ for $\lfloor m^e\rfloor$ and with $\delta\simeq0$, the efficiency is $\eta_Z=\Omega(1)$. This means that our protocol can provide the same number of ebits or pbits as the optimal protocol, by running our protocol merely $\eta_Z^{-1}=O(1)$ times more than the optimal protocol, irrespectively of the network topology and the physical size of the network.

V. AGGREGATING EXISTING QUANTUM REPEATER SCHEMES

The most practically interesting networks are purely optical networks composed of optical channels $\{\mathcal{O}^e\}_{e\in E}$. The dominant impediment to this network is photon loss in the channel $\mathcal{O}^e$ [37], which increases exponentially with the channel length L^e. In fact, the transmittance T^e of the channel $\mathcal{O}^e$ can be described as $T^e:=e^{-L^e/L_{\rm att}}$ with attenuation length $L_{\rm att}$ ($L_{\rm att}\simeq22$ km for a standard telecom optical fiber). So far, against the photon loss, to perform quantum communication efficiently over *linear networks*, quantum repeater protocols have been proposed with existing physical devices [4–20].

However, with Eq. (8), we can show that our protocol based on existing quantum repeater schemes has no scaling gap with the optimal protocol, even for *arbitrary network topology*.

Suppose that our protocol uses the single-photon-based entanglement generation schemes in existing quantum repeater protocols [5,6,11,12] (including the Duan-Lukin-Cirac-Zoller-type (DLCZ-type) schemes [5,12]). Simple linear-optics-based implementations of these schemes cause noisy and probabilistic nature of quantum operations. But, as long as the coherence time of quantum memories is reasonably long, these schemes can provide $R_\delta^e = \Omega(T^e)$ with $\delta \simeq 0$ without invoking complicated entanglement purification and quantum error correction [5,12]. This is because the success probabilities of the devices are independent of T^e and the so-called "built-in entanglement purification" [5] equips the schemes with resilience to realistic noise [5,12]. On the other hand, the squashed entanglement of the channel $\mathcal{O}^e$ is $E_{\rm sq}(\mathcal{O}^e) \leqslant 2\log_2[(1+T^e)/(1-T^e)]$ [22], whose upper bound is approximated by $4T^e/\ln 2$ for $T^e \ll 1$. Therefore, from Eq. (8), the efficiency η_Z as well as $R_\delta^e/E_{\rm sq}(\mathcal{O}^e)$ is $\Omega(1)$ for small T^e. The assumptions of $T^e \ll 1$ are satisfied by increasing the physical size of the optical network, i.e., the channel lengths $\{L^e\}_{e\in E}$, for a fixed graph G. Hence, with respect to the physical size of the optical network, our protocol based on the single-photon-based entanglement generation schemes has no scaling gap with the optimal protocol.

So far we have assumed that the entanglement swapping along the AB paths $\{P_i\}_{i=1,2,\dots,M_\delta}$ works deterministically. However, in practice, there might be the case where we can perform the entanglement swapping just probabilistically at best. For instance, we may be able only to use simple linear-optics-based Bell measurement as in DLCZ-type schemes [5,12]. Even in this case, our protocol has no scaling gap with the optimal protocol as long as the coherence time of quantum memories is reasonably long. Here we just need to implement the entanglement swapping along every AB path in a "knockout tournament" manner [5,12]. In fact, again thanks to the built-in entanglement purification [5], the infidelity of the final AB pair obtained from an AB path P_i increases only linearly with the number of nodes on P_i, while the overhead for channel uses along the AB path P_i increases only logarithmically with that number [5,12] (see [38]). That is, these overheads depend only on the graph G of the considered optical network, rather than its physical size. Therefore, with respect to the physical size, our protocol even based on existing quantum repeater schemes has no scaling gap with the optimal protocol.

VI. ASYMPTOTIC LIMITS

So far the average numbers $\bar{l}^e$ of channel uses have limitation in the form $\bar{l}^e \leqslant m^e$. We move on taking the asymptotic limits of our protocol, the optimal protocol, and the AML bound. We first introduce frequency $f^e := m^e/m$ with $m := \sum_{e\in E} m^e$. For a fixed $f^e > 0$, $m^e \to \infty$ holds in the limit of $m \to \infty$, for which, by optimizing the entanglement generation protocols for our protocol, R_δ^e can reach the quantum capacity $Q^{\leftrightarrow}(\mathcal{N}^e)$ of channel $\mathcal{N}^e$ assisted by unlimited forward and backward classical communication in the limit of $\delta \to 0$, that is, $R_\delta^e \to Q^{\leftrightarrow}(\mathcal{N}^e)$. Combined with Eq. (4) and the asymptotic limit of the AML bound (6), this gives

$$\begin{aligned}
&\min_{V_A} \sum_{e\in E_{V_A\leftrightarrow V_B}} f^e Q^{\leftrightarrow}(\mathcal{N}^e) \\
&\leqslant \lim_{\delta\to 0}\lim_{m\to\infty} \sup_{\mathcal{P}_Z(|E|\delta,\{mf^e\}_{e\in E})} \frac{\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{m} \\
&\leqslant \min_{V_A} \sum_{e\in E_{V_A\leftrightarrow V_B}} f^e E_{\rm sq}(\mathcal{N}^e),
\end{aligned} \tag{9}$$

for any $Z \in \{{\rm Q},{\rm P}\}$. Hence, the quantum capacity and the private capacity per average total channel use are sandwiched by the minimum AB cuts over functions $Q^{\leftrightarrow}$ and $E_{\rm sq}$ of the quantum channels $\{\mathcal{N}^e\}_{e\in E}$ (see [40] for another asymptotic limit on the capacities per time).

The right-hand side of Eq. (9) is the AML bound applied to arbitrary protocols that may include even multiparty entanglement purification and quantum network coding. However, this bound can be estimated thanks to being written in terms of the single-letter quantity. On the other hand, the left-hand side of Eq. (9) is the *tight* bound for the aggregated quantum repeater protocol that does not use such multiparty protocols at all. But, this bound is described in terms of the quantum capacities that are intractable to be estimated in general. Of course, since there is a set of quantum channels [41] for which the gap between the quantum capacity and the squashed entanglement of the channel can be arbitrary large, the sandwich relation (9) could be weak to bound the optimal performance of a quantum network including such channels. However, it is still an open problem whether this type of gap exists even for practically important quantum channels. For instance, remember that the sandwich relation (9) is excellent for purely optical networks composed of lossy optical channels $\{\mathcal{O}^e\}_{e\in E}$ as implied by $Q^{\leftrightarrow}(\mathcal{O}^e)/E_{\rm sq}(\mathcal{O}^e) \geqslant 1/2$ for any lossy optical channel $\mathcal{O}^e$ (thanks to $Q^{\leftrightarrow}(\mathcal{O}^e) = 2\log_2[1/(1-T^e)]$ per pulse [27]) and by Eq. (8) [showing $\eta_Z = \Omega(1)$ here, again].

VII. ON THE OPTIMALITY

Finally, we show that the aggregated quantum repeater protocol is indeed optimal for a wide range of practical quantum networks. To show this, let $Q^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in E_{V_A\leftrightarrow V_B}})$ $[P^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in E_{V_A\leftrightarrow V_B}})]$ with $f^{V_A\leftrightarrow V_B} := \sum_{e\in E_{V_A\leftrightarrow V_B}} f^e$ denote the quantum capacity (the private capacity) between V_A and V_B, defined under the asymptotic limit of $m \to \infty$ for the paradigm where a fictitious party holding all the nodes in V_A and another fictitious party holding all the nodes in V_B are allowed to use quantum channels $\mathcal{N}^e$ between them (i.e., $e \in E_{V_A\leftrightarrow V_B}$) $\bar{l}^e (\leqslant mf^e)$ times on average and LOCC in order to distill ebits (pbits). Since any quantum internet protocol can be regarded as a bipartite protocol between V_A and V_B [21], we have

$$\begin{aligned}
&\lim_{\delta\to 0}\lim_{m\to\infty} \sup_{\mathcal{P}_{\rm Q}(|E|\delta,\{mf^e\}_{e\in E})} \frac{\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{m} \\
&\leqslant \min_{V_A} f^{V_A\leftrightarrow V_B} Q^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in E_{V_A\leftrightarrow V_B}})
\end{aligned} \tag{10}$$

for entanglement distillation for Alice and Bob and

$$\lim_{\delta\to 0}\lim_{m\to\infty}\sup_{\mathcal{P}_{\mathrm{P}}(|E|\delta,\{mf^e\}_{e\in E})}\frac{\langle\log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{m} \leqslant \min_{V_A} f^{V_A\leftrightarrow V_B} P^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in E_{V_A\leftrightarrow V_B}}) \quad (11)$$

for secret-key distillation for them. Hence, if quantum channels $\{\mathcal{N}\}_{e\in E}$ in the network satisfy

$$Q^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in V_A\leftrightarrow V_B}) \leqslant \sum_{e\in V_A\leftrightarrow V_B}\frac{f^e Q^{\leftrightarrow}(\mathcal{N}^e)}{f^{V_A\leftrightarrow V_B}}, \quad (12)$$

the aggregated quantum repeater protocol is optimal for the entanglement distribution from Eqs. (9) and (10). Similarly, if quantum channels $\{\mathcal{N}\}_{e\in E}$ in the network satisfy

$$P^{\leftrightarrow}(\{f^e/f^{V_A\leftrightarrow V_B},\mathcal{N}^e\}_{e\in V_A\leftrightarrow V_B}) \leqslant \sum_{e\in V_A\leftrightarrow V_B}\frac{f^e P^{\leftrightarrow}(\mathcal{N}^e)}{f^{V_A\leftrightarrow V_B}}, \quad (13)$$

$$P^{\leftrightarrow}(\mathcal{N}^e) = Q^{\leftrightarrow}(\mathcal{N}^e), \quad (14)$$

the aggregated quantum repeater protocol is optimal even for the secret-key distillation. In general, conditions (12)–(14) might not be satisfied [42–46]. However, our protocol is shown to be optimal for a wide range of practical quantum networks, irrespective of entanglement distribution or secret-key distribution. In fact, as shown [27] by Pirandola *et al.* (see [47]), all the conditions (12)–(14) are satisfied by a wide range of practical quantum channels such as erasure channels, dephasing channels, bosonic quantum amplifier channels, and lossy optical channels. This means that the aggregated quantum repeater protocol is optimal for arbitrary quantum networks composed of these practical channels. More importantly, the fact derived here shows that the optimality of the aggregated quantum repeater protocol is now related to fundamental questions on whether given quantum channels satisfy relations (12)–(14) or not.

Note added. Recently, another manuscript [30] appeared, including a protocol that works optimally for any distillable teleportation stretchable channel network under the "flooding" condition.

ACKNOWLEDGMENTS

We thank S. Bäuml, H.-K. Lo, A. Mizutani, W. J. Munro, L. Rigovacca, K. Tamaki, and R. Van Meter for valuable comments. This work was in part funded by ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan).

[1] L. R. Ford Jr. and D. R. Fulkerson, Canad. J. Math. **8**, 399 (1956).

[2] P. Elias, A. Feinstein, and C. E. Shannon, IRE Trans. Inf. Theory **2**, 117 (1956).

[3] H. J. Kimble, Nature (London) **453**, 1023 (2008).

[4] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[5] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

[6] P. Kok, C. P. Williams, and J. P. Dowling, Phys. Rev. A **68**, 022301 (2003).

[7] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).

[8] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[9] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).

[10] K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303(R) (2009).

[11] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, Nat. Photon. **4**, 792 (2010).

[12] N. Sangouard, C. Simon, N. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[13] K. Azuma, H. Takeda, M. Koashi, and N. Imoto, Phys. Rev. A **85**, 062309 (2012).

[14] K. Azuma and G. Kato, Phys. Rev. A **85**, 060303(R) (2012).

[15] M. Zwerger, W. Dür, and H. J. Briegel, Phys. Rev. A **85**, 062326 (2012).

[16] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Nat. Photon. **6**, 777 (2012).

[17] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, New J. Phys. **15**, 023012 (2013).

[18] P. Mazurek, A. Grudka, M. Horodecki, P. Horodecki, J. Łodyga, Ł. Pankowski, and A. Przysiężna, Phys. Rev. A **90**, 062311 (2014).

[19] K. Azuma, K. Tamaki, and H.-K. Lo, Nat. Commun. **6**, 6787 (2015).

[20] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, IEEE J. Sel. Top. Quant. Electron **21**, 78 (2015).

[21] K. Azuma, A. Mizutani, and H.-K. Lo, Nat. Commun. **7**, 13523 (2016).

[22] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5**, 5235 (2014).

[23] M. Takeoka, S. Guha, and M. M. Wilde, IEEE Trans. Inf. Theory **60**, 4987 (2014).

[24] S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 012301 (2014).

[25] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New J. Phys. **16**, 043005 (2014).

[26] K. Azuma, K. Tamaki, and W. J. Munro, Nat. Commun. **6**, 10171 (2015).

[27] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

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

[29] J. Niset, J. Fiurášek, and N. J. Cerf, Phys. Rev. Lett. **102**, 120501 (2009).

[30] S. Pirandola, arXiv:1601.00966.

[31] K. Menger, Fund. Math. **10**, 96 (1927).

[32] We allow each round i to have an option not to use a quantum channel, depending on the previous outcome $\boldsymbol{k}_{i-1}$. This gives a freedom to finish the protocol in an adaptive manner [21]. Indeed, Duan-Lukin-Cirac-Zoller-type schemes adopt this strategy [5,6,12,13].

[33] J. A. Bondy and U. S. R. Murty, *Graph Theory*, Graduate Texts in Mathematics (Springer, London, 2008), Vol. 244.

[34] The squashed entanglement of the channel $\mathcal{N}^{X\to Y}$ is defined [22,23] by $E_{\rm sq}(\mathcal{N}^{X\to Y}) := \max_{|\phi\rangle_{xx'}} E_{\rm sq}^{x:y}[\mathcal{N}^{X\to Y}(|\phi\rangle\langle\phi|_{xx'})]$ for channel $\mathcal{N}^{X\to Y}$ to output a system y for a party Y for the input subsystem x' of a party X, where $E_{\rm sq}^{x:y}$ is the squashed entanglement [35] between system x of party X and system y of party Y.

[35] M. Christandl and A. Winter, J. Math. Phys. **45**, 829 (2004).

[36] K. Goodenough, D. Elkouss, and S. Wehner, New J. Phys. **18**, 063005 (2016).

[37] T. D. Ladd *et al.*, Nature (London) **464**, 45 (2010).

[38] Note that the essential of the original proposal of the DLCZ scheme [5] is to resolve the problem of the probabilistic nature of the two-qubit operations by adopting the knockout tournament manner. Now, this idea can be seen in many occasions such as [39] and [19].

[39] L.-M. Duan and R. Raussendorf, Phys. Rev. Lett. **95**, 080503 (2005).

[40] We can also consider another asymptotic limit on the capacities per time. Suppose that we use quantum channel $\mathcal{N}^e$ $\bar{l}^e(\leqslant m^e)$ times on average for time t. Let us introduce rate $r^e := m^e/t$. Then we have another asymptotic limit of Eqs. (4) and (6) as

$$\min_{V_A} \sum_{e\in E_{V_A\leftrightarrow V_B}} r^e Q^{\leftrightarrow}(\mathcal{N}^e) \leqslant \lim_{\delta\to 0}\lim_{t\to\infty} \sup_{\mathcal{P}(|E|\delta,\{tr^e\}_{e\in E})} \frac{\langle \log_2 d_{\boldsymbol{k}_l}\rangle_{\boldsymbol{k}_l}}{t} \leqslant \min_{V_A} \sum_{e\in E_{V_A\leftrightarrow V_B}} r^e E_{\rm sq}(\mathcal{N}^e). \quad (15)$$

[41] M. Christandl and A. Müller-Hermes, Commun. Math. Phys. **353**, 821 (2017).

[42] P. Horodecki, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **82**, 1056 (1999).

[43] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[44] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).

[45] G. Smith and J. Yard, Science **321**, 1812 (2008).

[46] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, Nat. Commun. **6**, 6908 (2015).

[47] Combine the results of $Q^{\leftrightarrow}(\mathcal{N}) = P^{\leftrightarrow}(\mathcal{N})$ for the specified channels $\mathcal{N}$ in Ref. [27] with the results in “Two-way quantum communication” in the Methods.