Multipartite entanglement and secret key distribution in quantum networks

Masahiro Takeoka,¹ Eneet Kaur,²,¹ Wojciech Roga,¹ and Mark M. Wilde²,³

¹National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan
²Hearne Institute for Theoretical Physics and Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA
³Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

(Dated: December 24, 2019)

Distribution and distillation of entanglement over quantum networks is a basic task for Quantum Internet applications. A fundamental question is then to determine the ultimate performance of entanglement distribution over a given network. Although this question has been extensively explored for bipartite entanglement-distribution scenarios, less is known about multipartite entanglement distribution.

Here we establish the fundamental limit of distributing multipartite entanglement, in the form of GHZ states, over a quantum network. In particular, we determine the multipartite entanglement distribution capacity of a quantum network, in which the nodes are connected through lossy bosonic quantum channels. This setting corresponds to a practical quantum network consisting of optical links. The result is also applicable to the distribution of multipartite secret key, known as common key, for both a fully quantum network and trusted-node based quantum key distribution network.

Our results set a general benchmark for designing a network topology and network quantum repeaters (or key relay in trusted nodes) to realize efficient GHZ state/common key distribution in both fully quantum and trusted-node-based networks. We show an example of how to overcome this limit by introducing a network quantum repeater.

Our result follows from an upper bound on distillable GHZ entanglement introduced here, called the “recursive-cut-and-merge” bound, which constitutes major progress on a longstanding fundamental problem in multipartite entanglement theory. This bound allows for determining the distillable GHZ entanglement for a class of states consisting of products of bipartite pure states.

I. INTRODUCTION

The “Quantum Internet” is a recent conceptualization of a quantum network, along with applications based on entanglement and secret key distribution over the network [1, 2]. While research efforts have been devoted to bipartite entanglement and secret key distribution over quantum networks so far, the full potential of the Quantum Internet emerges when it is extended to multipartite entanglement and secret key distribution, especially, GHZ states [3] and common secret keys. GHZ state and common secret key distribution in quantum networks has a variety of applications, including multi-party quantum key distribution (QKD) [4], quantum secret sharing [5], and quantum network clocks [6], as well as fundamental research of quantum mechanics [7, 8]. In addition, GHZ state distribution is closely related to the generation of an important class of multipartite entanglement, known as graph states [9–14]. However, since quantum channels in real networks inevitably include loss and noise, the maximum distribution rate of GHZ states for each quantum channel is limited. Therefore, efficient schemes for distributing GHZ states and common keys over the quantum network have been explored [9–17]. Then a fundamental question arises: what is the ultimate limit of multipartite entanglement and secret key distribution over a given quantum network?

A similar question has been extensively explored recently for distribution of bipartite entanglement and secret key over a point-to-point quantum channel [18–21], a point-to-multipoint (broadcast) channel [22] and quantum networks [23, 24]. The maximum achievable rate (i.e. ultimate limit of the rate) of entanglement per quantum channel use assisted by unlimited amount of local operations and classical communication (LOCC), is defined as the entanglement capacity. The maximum achievable rate (i.e. ultimate limit of the rate) of secret key distributions per quantum channel use assisted by unlimited amount of local operations and classical communication (LOCC), is defined as the secret key distribution capacity. The above works established the capacity for bipartite entanglement/secret key distribution in a certain class of channels/networks, including a pure-loss bosonic channel/network, providing a fundamental potential and limit of real world quantum networks.

Despite recent efforts [25–28], however, less is known for the multipartite entanglement/secret key distribution capacity. This is mainly due to the little knowledge on the upper bound of the GHZ version of distillable entanglement/secret key, although it is one of the fundamental problem in quantum information theory for long time [7, 29]. For example, the distillable GHZ entanglement is not known even for a very simple tripartite state, \( |\psi\rangle_{ABC} = |\Phi\rangle_{AB}|\Phi\rangle_{AC}|\Phi\rangle_{BC} \), where \( |\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \) is the Bell state.

In this paper, we introduce an upper bound on the distillable GHZ entanglement/common secret key and then use it to establish the fundamental limit of multipartite entanglement/secret key distribution rate in quantum network. A quantum network considered here is illustrated in Fig. 1. The nodes (users) are linked by point-
FIG. 1. Quantum network consisting of nodes (parties) and point-to-point quantum channels. All or part of the nodes wish to share entanglement or common key by using quantum channels and LOCC among the nodes.

We first introduce an upper bound on the distillable GHZ entanglement/common key for multipartite states, which we refer to as the recursive cut-and-merge (RCM) bound. This bound itself gives substantial progress on the longstanding problem of multipartite entanglement theory and allows for determining the distillable GHZ entanglement for a certain class of multipartite states, including the product of bipartite states mentioned above.

Second, we consider the multipartite entanglement/secret key distribution over all nodes in a given quantum network. By using the RCM bound, we establish a fundamental upper bound on the GHZ entanglement/common key distribution capacity for an arbitrary network topology in which the nodes of the network are linked by teleportation-simulable channels, which includes various important channels such as bosonic Gaussian channels. Especially, we establish the capacity for a network consisting of lossy bosonic channels, which gives a benchmark for a practical optical quantum network.

Third, we consider how the ‘network quantum repeater’ can overcome the capacity of the repeaterless network. We show an example of such a repeater and also derive a fundamental upper bound on the capacity in the scenario with the repeaters.

These results provide fundamental benchmarks for the performance of the Quantum Internet. In addition, we show that all of the above results are applicable to multipartite key distribution via a trusted node based network, which is already deployed in field globally [30–33]. In what follows, we focus on GHZ entanglement distribution to simplify the presentation. Its extension to the common key distribution scenario discussed previously is given in Sec. IV.

II. GHZ ENTANGLEMENT DISTILLATION FROM SHARED BIPARTITE STATES

Before going to quantum networks, we start with a simpler problem where the distant $M$ users initially share $n$ copies of $M$-partite quantum states and intend to distill $k$ copies of GHZ states, defined as $|\Phi_{\text{GHZ}}^{(M)}\rangle := (|0\cdots0\rangle + |1\cdots1\rangle)/\sqrt{2}$, via LOCC (Fig. 2(a) and (b)). The distillable GHZ entanglement $E_{\text{GHZ}}^D$ is defined as the maximum achievable rate $r = k/n$ of GHZ-state generation in the limit as $n \to \infty$ (see Appendix A for a rigorous definition). As mentioned above, $E_{\text{GHZ}}^D$ is not known even for a simple triangle share of Bell states, $|\Phi_{\text{ABC}}\rangle = |\Phi_{\text{AB}}\rangle|\Phi_{\text{AC}}\rangle|\Phi_{\text{BC}}\rangle$ (Fig. 2(b)). Intuitively, since the generation of one GHZ state requires two Bell states at least, it seems that $E_{\text{GHZ}}^D$ is at most 1.5. However, the currently known upper bounds for $E_{\text{GHZ}}^D$ [7, 34, 35] are not better than the entropy of entanglement of a bipartitioned system, which evaluates to two in this case. Thus, there remains a significant gap.

To close the gap, we develop a new upper bound, dubbed the ‘recursive cut-and-merge (RCM) bound’ and denoted by $E_{\text{rcm}}$:

**Theorem 1** The distillable GHZ entanglement of an $M$-partite state $\rho$ is bounded from above as

$$E_{\text{GHZ}}^D(\rho) \leq E_{\text{rcm}}(\rho).$$

Note that the bound in Theorem 1 is a weak converse bound, meaning that it holds in the asymptotic limit of many copies of the state $\rho$ and in the limit as the distillation error tends to zero. See Appendix B for the formal definition of $E_{\text{rcm}}(\rho)$ and the proof of Theorem 1.

The RCM bound is applicable to arbitrary multipartite states but particularly useful for a product of bipartite states. Consider the $M$-partite product of bipartite
states, \( \rho_{A_1 \cdots A_M} = \rho_{A_1 A_2}^{A_1 A_2} \otimes \rho_{A_2 A_3}^{A_2 A_3} \otimes \cdots \otimes \rho_{A_{M-1} A_M}^{A_{M-1} A_M} \). Then we can bound its distillable GHZ entanglement as follows:

**Theorem 2** The distillable GHZ entanglement of a product of bipartite states \( \rho_{A_1 \cdots A_M} \) is bounded as follows:

\[
\min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_i I_C(A_j; A_k)_{\rho_i} \leq E_D^{\text{GHZ}}(\rho) \leq \min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_i E_R(A_j; A_k)_{\rho_i},
\]

where \( \mathcal{P} \) denotes the partitioning of an \( M \)-partite system and the sum is taken over all states \( \rho_i \) across the groups of the partition \( \mathcal{P} \). Also, \( E_R(A_j; A_k)_{\rho_i} \) is the relative entropy of entanglement (REE) of the bipartite state \( \rho_{A_j A_k}, I_C(A_j; A_k)_{\rho_i} = \max\{I_C(A_j; A_k)_{\rho_i}, I_C(A_k; A_j)_{\rho_i}\}, \) and \( I_C(A; B)_{\rho} \) is the coherent information of \( \rho_{AB} \).

**Proof.** The second inequality (upper bound) is directly implied by the RCM bound from Theorem 1.

The first inequality (lower bound) is derived as follows. First, \( n \) copies of each bipartite state \( \rho_{A_j A_k}^{A_j A_k} \) are used to generate Bell states between \( A_j \) and \( A_k \). This is possible at least with rate equal to \( I_C(A_j; A_k) \) [36]. Then we use a protocol that consists of generating a GHZ state from pairs of Bell states via local CNOT gates, partial measurements, and the conditional bit flip. To generate a GHZ state over all parties, one has to choose a set of Bell states connecting all parties. Furthermore, these connections should be carefully chosen such that one can maximize the amount of GHZ states to be generated. This optimization problem is known in graph theory as the Steiner tree packing problem. Applying the celebrated graph theorem by Tutte [37] and Nash-Williams [38], we obtain (2) as the maximum achievable rate of GHZ state generation. See Appendix C for details. Note that the Steiner tree packing approach is applied to the similar problems in [26–28].

A simple consequence of Theorem 2 is that if \( I(A_j; A_k)_{\rho_i} = E_R(A_j; A_k)_{\rho_i} \) for all \( i \), we can determine a precise expression for the distillable GHZ entanglement of a state \( \rho_{A_1 \cdots A_k} \). In particular, when the states \( \rho_{A_j A_k} \) are all pure, we find that

\[
E_D^{\text{GHZ}}(\rho) = \min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_i H(A_j)_{\rho_i},
\]

where \( H(A_j)_{\rho_i} \) is the partial von Neumann entropy of the pure state \( \rho_{A_j A_k} \).

Now we can answer the question that arose in the introduction of our paper. Namely, consider a product of Bell states:

\[
|\phi\rangle_{ABC} = |\Phi\rangle_{AB}^{m_1} |\Phi\rangle_{AC}^{m_2} |\Phi\rangle_{BC}^{m_3}
\]

Applying the observation in (3), we find that

\[
E_D^{\text{GHZ}}(\phi) = \min \left\{ m_1 + m_2, m_1 + m_3, m_2 + m_3, \frac{1}{2}(m_1 + m_2 + m_3) \right\},
\]

as discussed in detail in Appendix D. Substituting \( m_1 = m_2 = m_3 = 1 \), we obtain \( E_D^{\text{GHZ}}(\phi) = 1.5 \) as expected.

### III. GHZ Entanglement Distribution Capacity for Quantum Networks

We now apply the above result to a quantum communication scenario, i.e., GHZ state distribution in the quantum network illustrated in Fig. 1. In the network, each node is allowed to send arbitrary quantum states through the channels and also can use unlimited LOCC among all nodes to distill GHZ states (see Appendix A).

Here we consider a quantum network \( \mathcal{N} \) that is teleportation simulable, i.e., consists of teleportation-simulable channels [39–41]. This class of channels includes practically important channels, such as Gaussian, Pauli, and dephasing channels. In these channels, for any input state, an action of the channel is simulable by a teleportation protocol by sharing resource states between the sender and the receiver where the resource state is independent of the actual input state and is often a maximally entangled state. Up to LOCC the shared resource state in the teleportation protocol is equivalent to the state shared after a transmission through the simulated channel. Therefore, \( n \) sequential transmissions with arbitrary LOCC between each transmission is up to LOCC equivalent to \( n \) copies of the shared resource states in the teleportation protocol.

Applying this into the GHZ entanglement distribution in the teleportation simulable quantum network, we find that its GHZ entanglement distribution capacity, \( Q^{\text{GHZ}}_{++}(\mathcal{N}) \), is equivalent to

\[
E_D^{\text{GHZ}}(\sigma_1^{A_1 A_2} \otimes \sigma_2^{A_2 A_3} \otimes \cdots \otimes \sigma_{M-1}^{A_{M-1} A_M}),
\]

where \( \sigma_i^{A_i A_k} \) is the resource state shared by nodes \( A_j \) and \( A_k \) (if no channel between \( A_j \) and \( A_k \), it is some product state). Thus plugging this teleportation simulation argument into Theorem 2, we have the following fundamental bound for \( Q^{\text{GHZ}}_{++}(\mathcal{N}) \).

**Theorem 3** The GHZ entanglement distillation capacity of a teleportation-simulable quantum network \( \mathcal{N} \) is bounded as

\[
\min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_i I_C(A_j; A_k)_{\sigma_i} \leq Q^{\text{GHZ}}_{++}(\mathcal{N}) \leq \min_{\mathcal{P}} \frac{1}{|\mathcal{P}| - 1} \sum_i E_R(A_j; A_k)_{\sigma_i},
\]
where \( \sigma_i \) is the resource state shared between nodes \( A_j \) and \( A_k \).

An important consequence of Theorem 3 is again that one can establish a precise formula for the GHZ entanglement distillation capacity of a given quantum network when all of its point-to-point links are teleportation-simulable and also \( I(C(A_j; A_k); \rho) = E_P(A_j; A_k) \), holds for all \( i \) (i.e., their LOCC-assisted quantum capacities are known). Several point-to-point quantum channels are known to satisfy these conditions. From a practical point of view, the most important channel of such is the pure-loss bosonic channel, which has a direct correspondence to optical quantum networks. For the pure-loss bosonic channel \( \mathcal{L}(\eta) \) with transmittance \( \eta \), its LOCC-assisted quantum capacity is known to be \( Q_{\leftrightarrow}(\mathcal{L}(\eta)) = -\log_2(1 - \eta) \) [20, 21]. Combining this with our Theorem 3, we obtain the following quantum network capacity:

**Theorem 4** The GHZ entanglement distribution capacity of the quantum network \( \mathcal{L} \) consisting of point-to-point pure-loss bosonic channels is given by

\[
Q_{\leftrightarrow}^{\text{GHZ}}(\mathcal{L}) = \min_{\rho} \frac{1}{|P| - 1} \sum_{jk} -\log_2(1 - \eta_{jk}),
\]

where \( \eta_{jk} \) is the transmittance of the pure-loss bosonic channel connecting node \( j \) and \( k \), and the sum goes over pairs across the partitions.

The above result gives the fundamental limit of the GHZ state distribution rate over optical quantum networks.

The upper bound in (7) can be extended to more general case. Suppose in the teleportation simulable quantum network \( \mathcal{N} \) with \( N \) nodes, \( \{A_1, \cdots, A_M\} \), GHZ states are distributed over only part of the nodes \( \{A_1, \cdots, A_N\} \) where \( N < M \). Let \( \bar{P} \) be the partitioning of these \( N \) nodes where the other \( M - N \) nodes are included in some of these partitions. Then we have the following upper bound:

**Theorem 5** The GHZ entanglement distillation capacity \( Q_{\leftrightarrow}^{\text{GHZ}}(\mathcal{N}; A_1, \cdots, A_N) \) is bounded by

\[
Q_{\leftrightarrow}^{\text{GHZ}}(\mathcal{N}; A_1, \cdots, A_N) \leq \min_{\rho} \frac{1}{|\bar{P}| - 1} \sum_i E_R(A_j; A_k)_{\sigma_i},
\]

where \( \bar{P} \) is the partitioning of \( N \)-partite system and the sum is taken over all states \( \rho_i \) across the groups of partition.

See Appendix E for the proof.

**IV. COMMON KEY DISTRIBUTION**

All of the above theorems hold not only for GHZ state distillation but also for common secret key distillation for multiple parties by replacing \( E_P^{\text{GHZ}} \) and \( Q^{\text{GHZ}} \) with \( K_0^R \) and \( P_0^K \), where \( K_0^R \) is the distillable common key and \( P_0^K \) is the common private capacity. Moreover, these theorems can also be applied to the trusted node based quantum key distribution (QKD) network. Thus our results provide a fundamental limit of common key distribution in the currently working QKD networks [30–33]. See Appendix F for the proofs.

**V. NETWORK QUANTUM REPEATER**

We now show how quantum repeater technology can overcome the fundamental limit (Theorem 4) of a repeaterless network consisting of pure-loss bosonic channels. Analogous to the bipartite entanglement distribution scenario, quantum repeaters can overcome the repeaterless capacity for GHZ-state distribution in a quantum network. We call such a device a network quantum repeater, and by an example, we show that richer designs for repeaters are possible in this setting than in the point-to-point setting.

To do so, consider the simple example in Fig. 3(a), which is a rectangular quantum network \( \mathcal{N}_{\text{rec}} \) with four nodes \( A_1 \) to \( A_4 \) connected by six pure-loss channels (e.g., optical fibers). The variables \( l_0 \) and \( 2l_0 \) represent the distances of the channels, and the parameters \( \eta_i \) are the transmittance parameters with \( \eta_1 = \eta_0^2 \) and \( \eta_2 = \eta_0^{\sqrt{5}/2} \). We can derive its GHZ entanglement distribution capacity from Theorem 4. As a result, in the region of small \( \eta_0 \), the leading term of the capacity is \(-2\log_2(1 - \eta_0^2)\), which has the scaling \( O(\eta_0^2) \) (the detailed analysis of this section is in Appendix G).

Consider the same quantum network with a quantum repeater node \( R \) at the center (Fig. 3(b)), which we denote as \( \mathcal{N}_{\text{rec}}^{\text{R}} \). The diagonal channels are now cut by the repeater node, and each node connected to \( R \) has a loss of \( \bar{\eta}_2 = \eta_0^{\sqrt{5}/2} \).

Since \( R \) is connected by more than two channels, there is a variety of repeating strategies. Here we consider two different repeating protocols. In the first protocol

![Diagram of quantum network with four nodes and a repeater node](image)
(protocol 1), $R$ simply acts as two point-to-point quantum repeaters: one connects channels $A_1R$ and $A_3R$ and the other connects $A_2R$ and $A_4R$. Suppose $R$ works as an ideal repeater. Then the whole network is equivalent to a repeaterless network with the same topology as Fig. 3(a) where the loss of channels $A_1A_3$ and $A_2A_4$ are replaced by $\tilde{\eta_2}$. The optimal GHZ state generation rate of this network can be calculated from Theorem 4. For small $\eta_0$, the leading term of this rate is $-2\log_2(1-\eta_0^{5/2})$ which scales as $O(\eta_0^{1/4})$, thus showing an exponential rate improvement over the repeaterless case.

What about the optimality of the above repeater protocol? The upper bound of the GHZ distribution capacity with repeaters developed in Theorem 5 is a useful benchmark to see it. Figure 4(a) plots the GHZ distribution capacity without repeaters (Theorem 4 with Fig. 3(a)), the achievable rate with the repeater and protocol 1 (Fig. 3(b)), and the upper bound of the GHZ distribution capacity with the repeater (Theorem 5 with Fig. 3(b)). It shows how the network repeater boosts the scaling of the GHZ distribution rate and also protocol 1 is almost optimal (it exactly coincides with the upper bound for more than 25.6 dB losses) though there remains a small gap.

The gap can be further tightened by another protocol. In our second protocol (protocol 2), we separate the whole network into two parts: one is a rectangular network consisting of four links, $A_1A_2$, $A_2A_3$, $A_3A_4$, and the other is a star network where each $A_i$ is connected to $R$ via $A_iR$. For the former network, the optimal GHZ distribution rate is calculated from Theorem 4. For the latter network, the rate $-\log_2(1-\tilde{\eta_2})$ is achievable by the following strategy. First, each $A_i$ and $R$ generate Bell states with rate $-\log_2(1-\tilde{\eta_2})$ and then generate GHZ states by concatenating them at $R$. The GHZ-state generation rate is given by the sum of these two subprotocols. This is compared with protocol 1 and the upper bound in Fig. 4(a). Protocol 2 shows better performance than protocol 1 in the low loss region and saturates the upper bound for less than 2.1 dB losses. This shows the non-uniqueness of the optimality for network repeaters. It remains open how to fill the gap in the intermediate loss region. It is also an interesting future work to evaluate the optimality of GHZ generation protocols developed so far [9–17]. See Appendix G for detailed calculations.

VI. CONCLUSION

In this paper, we establish the fundamental limit of GHZ entanglement/common key distribution performance in a quantum network with and without network quantum repeaters. In particular, we determine the exact GHZ entanglement/common key distribution capacity of a quantum network connected by lossy bosonic channels, corresponding to a practical quantum network with optical links. To derive these results, we introduce an upper bound on the distillable GHZ entanglement/common key, referred as the RCM bound. The RCM bound itself demarcates significant progress on the longstanding problem of determining the distillable GHZ entanglement. The result is also applicable to establish the fundamental limit of distributing common keys over the trusted node based QKD networks, that are already deployed in field. Thus our results provide the fundamental benchmark for designing and implementing future Quantum Internet as well as the current trusted node based QKD networks.

FIG. 4. (a) GHZ distribution rates of the quantum network in Fig. 3 with no network repeater (blue), with repeater protocol 1 (green) and the upper bound of the GHZ distribution capacity with the network repeater (red) (the latter two are almost degenerated). (b) The same figure in the low loss regime with repeater protocol 2 (brown).

ACKNOWLEDGMENTS

We are grateful to Haoyu Qi and Masato Koashi for inspiring discussion. This work was supported by JST CREST Grant No. JPMJCR1772 and MEXT/JSPS KAKENHI Grant No. JP18H01157.
Appendix A: LOCC-assisted GHZ entanglement distillation protocol

A rigorous definition of GHZ entanglement distillation is as follows: $M$ parties, $A_1, \cdots, A_M$ share an $M$-partite state $\rho_{A_1 \cdots A_M}^{\otimes n}$, where $n$ is a positive integer. Then an $(n, R, \epsilon)$ GHZ entanglement distillation protocol $E_n$ for $\rho_{A_1 \cdots A_M}$ is defined as an LOCC, which generates a state $\omega_{A_1 \cdots A_M}$ such that
\[
\frac{1}{2} \| \omega - \Phi^{(M)}_n \|_1 \leq \epsilon, \tag{A1}
\]
where
\[
\Phi^{(M)}_n = \sum_{i=0}^{d_n-1} \frac{1}{\sqrt{d_n}} |i \cdots i \rangle_{A_1 \cdots A_M}, \tag{A2}
\]
and $d_n = \log_2 d_n$. The key rate $R = l_n/n$ is achievable if there exists an $(n, R - \delta, \epsilon)$ protocol for all $\epsilon \in (0,1], \delta > 0$, and sufficiently large $n$. The distillable GHZ entanglement $E_D^{GHZ}(\rho)$ is defined to be the supremum of all achievable rates:
\[
E_D^{GHZ}(\rho) = \sup \{ R | R \text{ is achievable} \}. \tag{A3}
\]
Note that a general formula for $E_D^{GHZ}(\rho)$ is not known, even if $\rho$ is a pure state.

Appendix B: Recursive cut-and-merge (RCM) bound

In this appendix, we introduce the RCM bound and establish some of its properties. We start with a few definitions.

Definition 6 (Cut-and-merge) Let $\rho_{ABC}$ be a tripartite state. Let $B'$ and $C'$ be local systems belonging to $B$ and $C$, respectively. Then we define $\tilde{\rho}_{BB'CC'}$ to be the “cut-and-merge” of $\rho_{ABC}$ on $BC$, such that there exists a unitary $U_{B'C'}$ acting on system $B'C'$, with
\[
\tilde{\rho}_{BB'CC'} = U_{B'C'} \rho_{B'C'} \otimes \rho_{C'B'C'} U_{B'C'}^{\dagger}. \tag{B1}
\]
We restrict the local systems to have the following dimension constraints: $|B'| = |C'| = |A|$. Observe that the following equality holds
\[
\text{Tr}_{B'C'}[\tilde{\rho}_{BB'CC'}] = \text{Tr}_A[\rho_{ABC}]. \tag{B2}
\]
Definition 7 Let $\rho_{A_1 \cdots A_M}$ be a multipartite state shared between parties $A_1, \cdots, A_M$. Let $\mathcal{P}$ be a non-trivial partition of $\{A_1, \ldots, A_M\}$ and denote each cell in the partition as $G_i$ ($i = 1, \cdots, |\mathcal{P}|$). For each non-trivial $\mathcal{P}$, we define the following function:
\[
E_{\rho}^{\text{cm}}(\mathcal{P}) = \min \left\{ \frac{1}{|\mathcal{P}|-1} \left[ E_R(G_1;G_2 \cdots G_{|\mathcal{P}|})_{\rho} + \tilde{E}_R(G_2;G_3 \cdots G_{|\mathcal{P}|})_{\rho} + \cdots + \tilde{E}_R(G_{|\mathcal{P}|-1};G_{|\mathcal{P}|})_{\rho} \right] \right\}, \tag{B3}
\]
where the minimization is taken over all permutations of $\{G_1 \cdots G_{|\mathcal{P}|}\}$, $E_R(A;B)_\rho$ is the relative entropy of entanglement (REE) for bipartite state $\rho_{AB}$, and $\tilde{E}_R$ is defined for tripartite system $\rho_{ABC}$ as
\[
\tilde{E}_R(B;C)_\rho = \min_{\tilde{\rho}} E_R(BB';CC')_{\tilde{\rho}}, \tag{B4}
\]
where $\tilde{\rho}_{BB'CC'}$ is a cut-and-merge of $\rho_{ABC}$ on $BC$. The minimization is taken over all possible cut-and-merge of $\rho_{ABC}$.

Definition 8 (RCM bound) The recursive cut-and-merge (RCM) bound $E_{\text{rcm}}(\rho)$ of the state $\rho_{A_1 A_2 \cdots A_M}$ is given as
\[
E_{\text{rcm}}(\rho) = \min_{\mathcal{P}} E_{\rho}^{\text{rcm}}(\mathcal{P}), \tag{B5}
\]
where the minimization is over all non-trivial partitions $\mathcal{P}$.

For convenience, we give Theorem 1 of the main text again.

Theorem 1 The distillable GHZ entanglement of $\rho_{A_1 \cdots A_M}$ is bounded by
\[
E_D^{GHZ}(\rho_{A_1 \cdots A_M}) \leq E_{\text{rcm}}(\rho), \tag{B6}
\]
Note that for a bipartite system, $E_{\text{rcm}}(\rho)$ reduces to the bipartite REE. It is also worth to note that REE used in the definition of $E_{\text{rcm}}(\rho)$ could be replaced by another upper bound of $E_D$, such as the squashed entanglement. Rigorous discussion on this direction is remained to be a future work.

To prove the theorem, it is enough to show that the following properties hold for $E_{\text{rcm}}(\rho)$ [42]:

1. Monotonicity under LOCC
2. Normalization
3. Subadditivity on product states
4. Continuity

Two remarks before going to the proof of each property. First, it is known that the above properties hold for REE [42, 43]. We will use this fact many times. Second, $E_{\text{rcm}}(\rho)$ is the minimum of
\[
\frac{1}{|\mathcal{P}|-1} \left[ E_R(G_1;G_2 \cdots G_{|\mathcal{P}|})_{\rho} + \tilde{E}_R(G_2;G_3 \cdots G_{|\mathcal{P}|})_{\rho} + \cdots + \tilde{E}_R(G_{|\mathcal{P}|-1};G_{|\mathcal{P}|})_{\rho} \right]. \tag{B3}
\]
Since its first term is an REE, the proof of the above conditions often start by proving them for $E_R(B;C)_\rho$ with arbitrary $\rho_{ABC}$. 
1. Monotonicity under LOCC

We prove monotonicity under LOCC of the RCM bound for tripartite states. To do so, it suffices to prove that the RCM bound is convex, invariant under local unitary and satisfying the FLAGS condition [44].

Consider a cut-and-merge \(\tilde{\rho}_{BB'CC'}\) of a tripartite state \(\rho_{ABC}\). We first prove that \(\tilde{E}_R(B;C)_\rho\) is convex, invariant under local unitary and FLAGS. These properties can be proven for multipartite states by following similar strategies.

**Proposition 9 (Convexity)** For any tripartite state \(\rho_{ABC}\), \(\tilde{E}_R(B;C)_\rho\) is convex. That is, for \(\rho_{ABC} = \sum_x q_x \rho_{ABC}^x\),

\[
\tilde{E}_R(B;C)_\rho \leq \sum_x q_x \tilde{E}_R(B;C)_{\rho^x}. 
\]  

(B7)

**Proof.** Suppose \(\tilde{\rho}_{opt}\) is an optimal state to minimize \(\tilde{E}_R(B;C)_{\rho^x}\). Then,

\[
\sum_x q_x \tilde{E}_R(B;C)_{\rho^x} = \sum_x q_x \tilde{E}_R(BB';CC')_{\tilde{\rho}_{opt}} 
\geq \tilde{E}_R(BB';CC')_{\sum_x q_x \tilde{\rho}_{opt}} 
\geq \min_{\tilde{\rho}} \tilde{E}_R(BB';CC')_{\tilde{\rho}} 
= \tilde{E}_R(B;C)_{\rho},
\]  

(B8)

where the first inequality follows from the convexity of REE. The second inequality holds since the right hand side is a global minimization over any decomposition of \(\rho\) which includes \(\rho = \sum_x q_x \rho^x\) as a special case. The equalities follow from the definitions. ■

**Proposition 10 (Local Unitary Invariance)** For any tripartite state \(\rho_{ABC}\), and a tripartite state \(\sigma_{ABC} = (U_A \otimes U_B \otimes U_C)(\rho_{ABC})(U_A^\dagger \otimes U_B^\dagger \otimes U_C^\dagger)\), where \(U_A, U_B,\) and \(U_C\) are some unitary operators acting on \(A, B,\) and \(C,\) we have that \(\tilde{E}_R(B;C)_\rho = \tilde{E}_R(B;C)_{\sigma}\).

**Proof.** Consider

\[
\sigma^1_{ABC} = (U_A \otimes I_B \otimes I_C)(\rho_{ABC})(U_A \otimes I_B \otimes I_C). 
\]  

(B9)

A cut-and-merge of \(\tilde{\sigma}^1_{ABC}\) on \(BC\) is defined as:

\[
\tilde{\sigma}^1_{BB'CC'} = (V_{B'C'} U_{B'}) (\rho_{BB'BC'} \otimes |0\rangle\langle 0|_C) (V_{B'C'} U_{B'})^\dagger \]  

(B10)

\[
= W_{B'C'} \rho_{BB'BC'} \otimes |0\rangle\langle 0|_C W_{B'C'}^\dagger
\]  

(B11)

where \(V_{B'C'}\) is a unitary operator acting on \(B'C'\) and \(W_{B'C'} = V_{B'C'} U_{B'}\). This is also a cut-and-merge on \(ABC\). Therefore, for any cut-and-merge \(\tilde{\sigma}^1_{BC'BC'}\) of \(\sigma^1_{ABC}\) on \(BC\) there exists a cut-and-merge \(\tilde{\sigma}^1_{BB'CC'}\) of \(\rho_{ABC}\) on \(BC\) such that \(\tilde{E}_R(BB';CC')_{\tilde{\sigma}^1} = \tilde{E}_R(BB';CC')_{\rho}\) and vice versa. Therefore, \(\tilde{E}_R(B;C)_\rho = \tilde{E}_R(B;C)_{\sigma}\). Since, the relative entropy of entanglement is invariant under local unitaries, it follows that \(\tilde{E}_R(B;C)_\rho = \tilde{E}_R(B;C)_{\sigma}\). ■

**Proposition 11 (FLAGS)** Let \(\rho_{ABCX} = \sum_x q_x \rho_{ABC}^x \otimes |x\rangle\langle x|_X\), where \(X = B''\) or \(C''\), and \(|x\rangle\langle x|\) are local, orthogonal flags. Then, the FLAGS condition [44],

\[
\tilde{E}_R(B;C)_\rho = \sum_x q_x \tilde{E}_R(B;C)_{\rho^x}, 
\]  

(B12)

holds, where \(X\) is implicitly included in \(B\) or \(C\).

**Proof.** Suppose \(X = B''\) or \(C''\) and these are included with \(B\) or \(C\), respectively. Let \(\rho_{ABCX} = \sum_x q_x \rho_{ABC}^x \otimes |x\rangle\langle x|_X\). Its cut-and-merge on \(BC\) has the form of

\[
\tilde{\rho}_{BB'CC'X} = \sum_x q_x \tilde{\rho}_{BB'CC'X}^x \otimes |x\rangle\langle x|_X
\]  

(B13)

As a consequence, we have

\[
\tilde{E}_R(B;C)_\rho = \min_{\tilde{\rho}} \tilde{E}_R(BB'X;CC')_{\tilde{\rho}}
\]  

(B14)

The first equality follows from the definition. The second equality follows from the fact that each \(\tilde{\rho} \otimes |x\rangle\langle x|\) is orthogonal to each other (B13). The third equality follows from the fact that REE satisfies the FLAGS condition. The fourth equality follows from the definition. The case when \(X\) is included with \(C\) can be proven similarly. ■

**Theorem 12 (LOCC monotone)** The RCM bound is a multipartite entanglement monotone. That is, it does not increase under local operations and classical communications (LOCC).

\[E_{rcm}(\rho) \geq E_{rcm}(\Lambda(\rho)),\]  

(B15)

where \(\Lambda\) is a LOCC operation.

**Proof.** We prove the above theorem for tripartite state \(\rho_{ABC}\). Its extension to general multipartite states is straightforward. We first prove that for any partition \(P_i\) of the systems \(\{A,B,C\}\), the following holds:

\[E_{rcm}^{\Lambda}(P_i) \geq E_{rcm}^{\rho}(\Lambda(P_i)).\]  

(B16)

It suffices to prove the above for the partition \(\{A\}, \{B\}, \{C\}\). The proof for the other partitions follows. We thus want to prove the following:

\[E_R(A;BC)_\rho + \tilde{E}_R(B;C)_\rho \geq E_R(A;BC)_{\Lambda(\rho)} + \tilde{E}_R(B;C)_{\Lambda(\rho)}.\]  

(B17)

We already know that REE is an LOCC monotone. Therefore, it is left to be proven that \(\tilde{E}_R(B;C)_\rho \geq\]
Since the permutation symmetry of the GHZ state, it suffices to show that
\[ E^{rcm}(\mathcal{P}_i) \geq E^{rcm}(\Lambda(\mathcal{P}_i)) \geq \min_{\mathcal{P}_i} E^{rcm}(\Lambda(\mathcal{P}_i)). \] (B18)

This implies
\[ E^{rcm}(\rho) \geq E^{rcm}(\Lambda(\rho)), \] concluding the proof. ■

2. Normalization

**Proposition 13** For
\[ |\Phi^{(M)}_i\rangle_{A_1\ldots A_M} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |iii\rangle_{A_1\ldots A_M}, \]
the RCM bound is \( E^{rcm}(\Phi^{(M)}_i) = \log_2 d \).

**Proof.** We first prove the tripartite case. We have four partitions which are as follows: \{A: B, C\}, \{AB: C\}, \{A: BC\}, \{AC: B\}. We now show that for each of this partition \( E^{rcm}(\mathcal{P}_i) = \log_2 d \). For the two partite partitions, the RCM bound is equal to REE. Due to the symmetry of the GHZ states, we know that \( E_R(A; BC) = E_R(B; AC) = E_R(C; AB) \).

Now, let us consider the tripartite partition. Due to the permutation symmetry of the GHZ state, it suffices to consider the following:
\[ E^{rcm}(\{A: B, C\}) = \frac{1}{2} \left( E_R(AB; C) + E_R(B; AC) \right). \] (B20)

The cut-and-merge of \( |\Phi^{(3)}_d\rangle_{ABC} \) on BC is always described as
\[ |\tilde{\Phi}^{(3)}_d\rangle_{B'C'}^{BC} = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |e_i\rangle_{B'C'} |ii\rangle_{BC}, \] (B21)
where \( |e_i\rangle_{B'C'} = U_{B'C'} |0\rangle_{B'} |i\rangle_{C'} \) is a bipartite orthogonal basis on \( B'C' \). Since \( |\tilde{\Phi}^{(3)}_d\rangle \) is a pure state, \( E_R(B'B'; C'C') \) is given by the partial entropy, i.e. the von Neumann entropy of
\[ Tr_{B'B'} |\tilde{\Phi}^{(3)}_d\rangle \langle \tilde{\Phi}^{(3)}_d| = \frac{1}{d} \sum_{i=1}^{d} Tr_{B'} |e_i\rangle \langle e_i|_{B'C'} \otimes |i\rangle \langle i|_{C'}. \] (B22)

From this, we have
\[ E_R(BB'; CC')_{\tilde{\Phi}^{(3)}_d} = \log_2 d + \frac{1}{d} \sum_{i=1}^{d} H(C')_{\rho^i}, \] (B23)
where \( \rho^i_{C'} = Tr_{B'} |e_i\rangle \langle e_i|_{B'C'} \). This is minimized to be
\[ \min_{\rho} E_R(BB'; CC')_{\tilde{\Phi}^{(3)}_d} = \log_2 d, \] (B24)
by taking \( |e_i\rangle_{B'C'} = |i\rangle_{B'} |0\rangle_{C'} \). Therefore, we have
\[ E^{rcm}(\{A: BC\}) = \frac{1}{2} (E_R(A; BC)_{\tilde{\Phi}^{(3)}_d} + E_R(B; AC)_{\tilde{\Phi}^{(3)}_d}) = \frac{1}{2} (2\log_2 d + \log_2 d) = \log_2 d, \] (B25)
which proves the the normalization condition. We can check the normalization condition for more than tripartite states by the similar calculation. ■

3. Subadditivity on product states

**Proposition 14** Let \( \tau_{A_1\ldots A_M} = \rho_{A_1\ldots A_M} \otimes \sigma_{A_1\ldots A_M} \). Then,
\[ E^{rcm}(\tau) \leq E^{rcm}(\rho) + E^{rcm}(\sigma). \] (B26)

**Proof.** We prove the above for a tripartite state \( \rho_{ABC} \). We have four partitions. For the bipartite partitions, the subadditivity follows since REE does. We now prove the subadditivity for \( E^{rcm}(\{A: BC\}) \). The first term of \( E^{rcm}(\{A: BC\}) \) is subadditive on product states since REE is so. Thus, we focus on the other term. We show that for a product state \( \rho_{A_0B_0C_0} \otimes \sigma_{A_1B_1C_1} \), the following holds:
\[ \tilde{E}_R(B_0B_1C_0C_1)_{\rho \otimes \sigma} \leq \tilde{E}_R(B_0B_1C_0)_{\rho} + \tilde{E}_R(B_1C_1)_{\sigma}. \] (B27)

We have the following set of equations:
\[ \tilde{E}_R(B_0B_1C_0)_{\rho} + \tilde{E}_R(B_1C_1)_{\sigma} = \min_{\rho} E_R(B_0B_1C_0)_{\rho} + \min_{\sigma} E_R(B_1C_1)_{\sigma} \geq \min_{\rho} \min_{\sigma} E_R(B_0B_1C_0C_1)_{\rho \otimes \sigma} \geq \tilde{E}_R(B_0B_1C_0C_1)_{\rho \otimes \sigma}, \] (B28)
where the first equality is from the definition, the first inequality is due to the subadditivity of REE, and the second inequality is due to the fact that the global minimization always gives a smaller value than the local minimizations. The same calculation holds for the general \( M \)-partite case. ■

4. Asymptotic continuity

We consider the tripartite case. However, its generalization to the multi-partite case is straightforward. We prove the following theorem:
Theorem 15 Denote

\[ E_{\text{rem}}^\infty(\rho) = \lim_{n \to \infty} \frac{1}{n} E_{\text{rem}}(\rho^\otimes n). \]  

Then

\[ \frac{1}{2} \| \rho_{AB} - \sigma_{AB} \|_1 \leq \varepsilon, \]  

implies

\[ |E_{\text{rem}}^\infty(\rho_{AB}) - E_{\text{rem}}^\infty(\sigma_{AB})| \leq \varepsilon \log_2 d + f(\varepsilon), \]  

where \( d = |ABC| \), \( f(x) = (1 + x) h \left( \frac{1}{1+x} \right) \), and \( h(x) \) is the binary Shannon entropy. Note that \( f(x) \to 0 \) as \( \varepsilon \to 0 \).

Proof. We first show the asymptotic continuity for the fixed partition and permutation. Let \( E_\rho(\mathcal{P}, X) \) be a function which has the same form as \( E_{\text{rem}}(\rho) \) but with fixed partition \( \mathcal{P} \) and fixed permutation \( X \) (i.e. no minimizations over \( \mathcal{P} \) and \( X \)).

Lemma 16

\[ \frac{1}{2} \| \rho_{AB} - \sigma_{AB} \|_1 \leq \varepsilon, \]  

implies that

\[ |E_\rho(\mathcal{P}, X) - E_\sigma(\mathcal{P}, X)| \leq \varepsilon \log_2 d + f(\varepsilon), \]  

for any \( \mathcal{P} \) and \( X \).

Proof. We give a proof separately for each partition. There are four possible partitions: \{A; BC\}, \{B; AC\}, \{C; AB\}, \{A; B; C\}. For bipartition \{A; BC\}, \( E_\rho(\{A; BC\}, ABC) = E_\rho(A; BC)_{\rho_\sigma} \). Now the right hand side is an REE which is known to be asymptotically continuous [45, 46]. By using the result in [46], we obtain

\[ |E_\rho^\infty(A; BC)_{\rho_\sigma} - E_\sigma^\infty(A; BC)_{\sigma_\sigma}| \leq \varepsilon \log_2 d_0 + f(\varepsilon), \]  

where \( d_0 = \min(|A|, |BC|) \). Similar results are obtained for the other bipartitions, too.

Consider the tripartition \( \mathcal{P}_3 = \{A; B; C\} \) with permutation \( X = ABC \):

\[ E_\rho(\mathcal{P}_3, ABC) = \frac{1}{2} (E_\rho^\infty(A; BC)_{\rho_\sigma} + E_\rho^\infty(B; C)_{\rho_\sigma}), \]  

and its asymptotic continuity. For the first term, (B33) can be applied. For the second term, observe that

\[ 2\varepsilon \geq \| \rho_{AB} - \sigma_{AB} \|_1 \]  

\[ = \| \rho_{BC} \otimes |0\rangle\langle 0|_{B'} - \sigma_{BC} \otimes |0\rangle\langle 0|_{B'} \|_1 \]  

\[ = \| U_{BC'}^\dagger (\rho_{BC} \otimes |0\rangle\langle 0|_{B'}) - U_{B'C'} (\sigma_{BC} \otimes |0\rangle\langle 0|_{B'}) \|_1 \]  

\[ = \| \tilde{\rho}_{BC} - \tilde{\sigma}_{BC} \|_1, \]  

where \( U_{BC'}^\dagger(\cdot) \) is a unitary operation acting on \( B'C' \). The third equality follows from the invariance of trace distance under unitary channels.

The above equation states that for each cut-and-merge \( \tilde{\rho}_{BB'CC'} \) of \( \rho_{ABC} \) on BC there exists a cut-and-merge \( \tilde{\sigma}_{BB'CC'} \) of \( \sigma_{ABC} \) on BC, such that (B35) holds.

Without loss of generality, we can assume that \( \tilde{E}_R^\infty(B; C)_{\rho} \leq \tilde{E}_R^\infty(B; C)_{\sigma} \). Then we have from (B35) that for the optimal cut-and-merge \( \tilde{\rho}_{BB'CC'}^\text{opt} \), there exists \( \tilde{\sigma}_{BB'CC'} \) such that \( \| \tilde{\rho}_{BB'CC'} - \tilde{\sigma}_{BB'CC'} \|_1 \leq \varepsilon \). Then applying the asymptotic continuity of REE [46], we obtain

\[ |\tilde{E}_R^\infty(B; C)_{\rho} - E_\rho^\infty(BB'; CC')_{\tilde{\sigma}}| \leq \varepsilon \log_2 d_1 + f(\varepsilon), \]  

where \( d_1 = \min(|BB'|, |CC'|) \leq \min(|BA|, |AC|) \).

Since \( \tilde{\sigma}_{BB'CC'} \) is not necessarily an optimal cut-and-merge to minimize \( E_\rho^\infty(BB'; CC')_{\tilde{\sigma}} \), we have

\[ \tilde{E}_R^\infty(B; C)_{\rho} \leq \tilde{E}_R^\infty(B; C)_{\sigma} \leq E_\rho^\infty(BB'; CC')_{\tilde{\sigma}}. \]  

Thus,

\[ |\tilde{E}_R^\infty(B; C)_{\rho} - \tilde{E}_R^\infty(B; C)_{\sigma}| \]  

\[ \leq |\tilde{E}_R^\infty(B; C)_{\rho} - E_\rho^\infty(BB'; CC')_{\tilde{\sigma}}| \]  

\[ \leq \varepsilon \log_2 d_1 + f(\varepsilon), \]  

and combining it with (B33), we obtain

\[ |E_\rho^\infty(\mathcal{P}_3, ABC) - E_\sigma^\infty(\mathcal{P}_3, ABC)| \leq \frac{1}{2} \left( |E_\rho^\infty(A; BC)_{\rho_\sigma} - E_\rho^\infty(A; BC)_{\sigma_\sigma}| + |\tilde{E}_R^\infty(B; C)_{\rho} - \tilde{E}_R^\infty(B; C)_{\sigma}| \right) \]  

\[ \leq \frac{1}{2} \{ \varepsilon (\log_2 d + \log_2 d_1) + 2f(\varepsilon) \}, \]  

As a consequence, we have

\[ |E_\rho^\infty(\mathcal{P}_3, ABC) - E_\sigma^\infty(\mathcal{P}_3, ABC)| \]  

\[ \leq \frac{1}{2} \{ \varepsilon (\log_2 d_0 + \log_2 d_1) + 2f(\varepsilon) \}, \]  

\[ \leq \varepsilon \log_2 d + f(\varepsilon), \]  

where \( d = |ABC| \). Thus we complete the proof for all partitions. \( \blacksquare \)

Now we are ready to prove the theorem. Let \( \mathcal{P}_\rho = (\mathcal{P}_\rho) \) and \( X_\sigma = (X_\sigma) \) be the optimal partitioning and permutation for \( \rho \) \( (\sigma) \), respectively, such that \( E_{\text{rem}}(\rho) = \)
\( E_\rho(\mathcal{P}_\rho, X_\rho) \) (\( E_{\text{rcm}}(\sigma) = E_\sigma(\mathcal{P}_\sigma, X_\sigma) \)) holds. Without loss of generality, we can assume that \( E_{\text{rcm}}(\rho) = E_\rho(\mathcal{P}_\rho, X_\rho) \leq E_{\text{rcm}}(\sigma) \). Lemma 16 implies
\[
\left| E_\rho(\mathcal{P}_\rho, X_\rho) - E_\sigma(\mathcal{P}_\sigma, X_\rho) \right| \leq \varepsilon \log d + f(\varepsilon). \tag{B41}
\]
Since \( E_\rho(\mathcal{P}_\rho, X_\rho) \leq E_\sigma(\mathcal{P}_\sigma, X_\sigma) \), we get
\[
\left| E_\rho(\mathcal{P}_\rho, X_\rho) - E_\sigma(\mathcal{P}_\sigma, X_\rho) \right| \leq \varepsilon \log d + f(\varepsilon). \tag{B42}
\]
which completes the proof. ■

Appendix C: Detailed proof of Theorem 2

Consider the \( M \)-partite product of bipartite states, \( \rho_{A_1 \cdots A_M} = \bigotimes_{i,j \geq 1} \rho_{A_i,A_j} \), where \( i,j \in \{1, \cdots M\} \).

**Theorem 2** Distillable GHZ entanglement of \( \rho_{A_1 \cdots A_M} \) is bounded as
\[
\min_{\mathcal{P}} \frac{1}{|\mathcal{P}|-1} \sum_i I_C(A_j;A_k)_{\rho_{A_i,A_k}} \leq E_{\text{GHZ}}^D(\rho)
\]
\[
\leq \min_{\mathcal{P}} \frac{1}{|\mathcal{P}|-1} \sum_i E_R(A_j;A_k)_{\rho_{A_i,A_k}}, \tag{C1}
\]
where \( \mathcal{P} \) is the partitioning of \( M \)-partite system and the sum is taken over all states \( \rho_{A_i,A_k} \) across the groups of partition. \( E_R(A_j;A_k)_{\rho_{A_i,A_k}} \) is the relative entropy of entanglement (REE) for bipartite state \( \rho_{A_i,A_k} \), \( I_C(A_j;A_k)_{\rho_{A_i,A_k}} = \max\{I_C(A_j;A_k)_{\rho_{A_i,A_k}}, I_C(A_i,A_j)_{\rho_{A_i,A_k}}\} \), and \( I_C(A,B)_{\rho} \) is the coherent information of \( \rho_{AB} \).

**Proof.** To prove the first inequality (lower bound), we first describe a simple algorithm proving the following lemma

**Lemma 17** One tripartite GHZ qubit state can be obtained deterministically from two Bell states.

**Proof.** Consider the Hilbert space \( \mathcal{H}_{AB'BC} \) where one party has access to parts \( B \) and \( B' \). Consider also two Bell states
\[
|\Phi\rangle_{AB} \otimes |\Phi\rangle_{B'BC} = \frac{1}{4} (|0000\rangle_{AB'BC} + |0011\rangle_{AB'BC} \\
+ |1100\rangle_{AB'BC} + |1111\rangle_{AB'BC}). \tag{C2}
\]
The proof is given by an explicit protocol. It starts with applying \( \text{CNOT}_{BB'} = |0\rangle_0 \otimes I_{BC} + |1\rangle_0 \otimes \sigma^z_{BC} \), where \( I_{BC} \) is the identity and \( \sigma^z \) is the bit flip. After that, one applies the measurement in the basis of \( |0\rangle_{B'} \) and \( |1\rangle_{B'} \). Result 0 directly gives the GHZ state. Result 1 leads to the state that after the bit flip in \( C \) becomes the GHZ as well (see Fig. 5).

Note that in any network, one \( m \)-party GHZ state can be generated by concatenation of the above protocol if all the \( m \) nodes are connected via at least one Bell state. For example, replacing one of the Bell states in the above protocol with \( |\Phi^{(3)}\rangle_{B'BCD} \), one can generate \( |\Phi^{(4)}\rangle_{\text{GHZ}}_{ABCD} \) in the end.

We also require the following tree-packing theorem from graph theory:

**Theorem 18** (Tree-packing lemma [37, 38]) A graph \( G \) contains \( k \) pairwise edge-disjoint spanning trees if and only if for every partition \( \mathcal{P} \) of its vertices, the graph \( G/\mathcal{P} \) has at least \( k(|\mathcal{P}|-1) \) edges.

The lower bound is then shown as follows: First, \( n \) copies of each bipartite state \( \rho_{A_i,A_k}^{A_i,A_k} \) are used to generate Bell states between \( A_j \) and \( A_k \). This is possible at least with the rate of \( I_C(A_j;A_k) \) [36]. That is, the number of Bell pairs \( m_{jk} \) shared between \( A_j \) and \( A_k \) is greater than \( n I_C(A_j;A_k) \). Then we use the protocol in Lemma 17 to generate GHZ states. To generate a GHZ state over all parties, one has to choose a set of Bell states connecting all parties. Furthermore, these connections should be carefully chosen such that one can maximize the amount of GHZ states to be generated.

Consider the mapping of the above network to the following undirected graph. We can think of each party as a node. The number of edges connecting two nodes are the number of Bell states that are shared between the pair of nodes. Now, we want to count the number of GHZ states that can be created from these sets of Bell states. Observing Lemma 17 and its note, we see that this is equivalent to finding the number of edge-disjoint spanning trees in the generated graph. With this, we have mapped the problem of finding the number of generated GHZ states to the tree-packing lemma stated above.

The tree-packing lemma implies that the maximum number of edge-disjoint spanning tree \( k_s \) is given by
\[
k_s = \min_{\mathcal{P}} \frac{k_p}{|\mathcal{P}|-1}, \tag{C3}
\]
where \( k_p \) is the number of edges in partitioned graph \( G/\mathcal{P} \). Now \( k_p \) is equal to the number of Bell pairs across the elements of the partition, which is greater than \( n \sum_{j,k} I_C(A_j;A_k) \), where \( A_j \) are the parties in the one element of the partitions and \( A_k \) are the parties in the
other elements of the partition. Then,
\[
E_D^\text{GHZ}(\rho) = \frac{k_s}{n} \sum_p \frac{k_p}{|P| - 1} \geq \min_p \frac{1}{|P| - 1} \sum_i I_C(A_j; A_k)_{\rho_i}. \tag{C4}
\]
This concludes the proof of the lower bound. Note that the Steiner tree approach to the entanglement and key distribution over a quantum network is also discussed in [26–28] where the more general case, i.e., the tree packing among a subgraph is mainly considered.

The upper bound follows from a direct application of Theorem 1, i.e., the RCM bound, to a tensor multipartite state. As an example, consider the following tripartite system:
\[
\rho_{A_1, A_2, B_1, B_2, C_1, C_2} = \sigma_{A_1, B_1} \otimes \tau_{A_2, C_1} \otimes \nu_{B_2, C_2}, \tag{C5}
\]
where $A_i$ corresponds to the system being with the $A$ party and the same for $B$ and $C$. We have four partitions: $P_1 = \{A_1, A_2; B_1, B_2, C_1, C_2\}$ and its permutations $P_2$ and $P_3$, and $P_4 = \{A_1, A_2; B_1, B_2, C_1, C_2\}$. For partition $P_1$, we observe
\[
E^\text{rcm}(P_1) = E_R(A_1; B_1)_{\sigma} + E_R(A_2; C_1)_{\tau}, \tag{C6}
\]
Similar results are obtained for the other permutations. Consider $E^\text{rcm}(P_4)$. This implicitly has a minimization over all permutations. However, without loss of generality, we can assume that the following permutation gives the minimum:
\[
E^\text{rcm}(P_4) = \frac{1}{2} \left( E_R(A_1; B_2; B_1; C_2)_{\rho} + \bar{E}_R(B_1; B_2; C_1; C_2)_{\bar{\rho}} \right), \tag{C7}
\]
where
\[
\bar{\rho} = U_{B_1, B_2, C_1, C_2} \left( \sigma_{B_1, B_1} \otimes |00\rangle_1 \otimes \tau_{C_2, C_1} \otimes \nu_{B_2, B_2} \otimes \nu_{B_2, C_2} \right), \tag{C8}
\]
and $U$ is a unitary operation. Then we have the following:
\[
\bar{E}_R(B_1; B_2; C_1; C_2)_{\bar{\rho}} = \min_{\bar{\rho}} E_R(B_1; B_2; B_1; B_2; C_1; C_2; C_1; C_2)_{\bar{\rho}} \leq E_R(B_1; B_2; C_1; C_2)_{\nu}. \tag{C9}
\]
The last equation follows by choosing $U_{B_1, B_2, C_1, C_2}$ to be an identity operation. We then obtain
\[
E^\text{rcm}(P_4) \leq \frac{1}{2} \left( E_R(A_1; B_1)_{\sigma} + E_R(A_2; C_1)_{\tau} + E_R(B_1; B_2; C_1; C_2)_{\nu} \right). \tag{C10}
\]
Combining all of them, we get the desired result. Generalization of the above example to the multipartite scenario completes the proof.

**Appendix D: Distillable GHZ entanglement for a product of bipartite states**

Here we apply Theorem 2 into $|\phi\rangle_{A_B C} = |\Phi\rangle_{A_B} \otimes |\Phi\rangle_{A_C} \otimes |\Phi\rangle_{B_C}$, where $m_1, m_2,$ and $m_3$ are some positive integers. This is a special case of (C9) (for simplicity, we only put the party labels). Consider three parties sharing $n$ copies of $|\phi\rangle_{A_B C}$.

Then, for $P_1$,
\[
\frac{1}{|P_1| - 1} E_D(A; BC)_{\phi} = H(A)_{\phi} = m_1 + m_2, \tag{D1}
\]
and similarly,
\[
\frac{1}{|P_2| - 1} E_D(B; AC)_{\phi} = m_1 + m_3 \quad \text{and} \quad \frac{1}{|P_3| - 1} E_D(C; AB)_{\phi} = m_2 + m_3. \tag{D2}
\]
Thus, plugging them into Theorem 2, we get
\[
E_D^\text{GHZ}(\phi) = \min \{m_1 + m_2, m_1 + m_3, m_2 + m_3, \frac{1}{2}(m_1 + m_2 + m_3) \}. \tag{D3}
\]

**Appendix E: Proof of Theorem 5**

Theorem 5 states the following: suppose in the teleportation simulable quantum network $N$ with $M$ nodes, $\{A_1, \ldots, A_M\}$, GHZ states are distributed over only part of the nodes $\{A_1, \ldots, A_N\}$, where $N < M$. Let $P$ be the partitioning of these $N$ nodes where the other $M - N$ nodes are included in some of these partitions. Then, $Q_{*+}^\text{GHZ}(N; A_1, \ldots, A_N) \leq \min_p \frac{1}{|P| - 1} \sum_i E_R(A_j; A_k)_{\sigma_i},$ \tag{E1}
where $P$ is the partitioning of $N$-partite system and the sum is taken over all states $\rho_i$ across the groups of partition.

**Proof.** Let us choose a particular partitioning $P^*$. Then consider a modified scenario where, in each partition, one allows arbitrary global quantum operations among all nodes in the partition. In other words, each partition is regarded as one big node. Suppose $Q_{*+}^*(P^*)$ is the GHZ entanglement distribution capacity of this particular modified scenario. Then clearly
\[
Q_{*+}^\text{GHZ}(N; A_1, \ldots, A_N) \leq Q_{*+}^*(P^*), \tag{E2}
\]
since any possible operation in the original scenario can be realized in this modified scenario. In addition, from Theorem 3, we observe that
\[
Q_{*+}^*(P^*) \leq \frac{1}{|P^*| - 1} \sum_i E_R(A_j; A_k)_{\sigma_i}. \tag{E3}
\]
Thus plugging them, we get
\[
Q^\text{GHZ}_{\varepsilon}(N; A_1, \ldots, A_N) \leq \frac{1}{|\mathcal{P}|} - 1 \sum_i E_R(A_j; A_k)_{\sigma_1}.
\]
Since this holds for any partitioning, we obtain the desired result. ■

Appendix F: Common key distribution

Here we show that the RCM bound is an upper bound not only for the distillable GHZ entanglement, but also for the distillable common keys from multipartite quantum systems. The is done by considering the distillation of private states [47, 48]. The multipartite private state is defined as [35],
\[
\gamma^{(M)} = U^\dagger \rho^{(M)} U \otimes \tau_{A_1 \cdots A_M} U^t,
\]
\[
\tau_{A_1 \cdots A_M} \text{ is an arbitrary state on } A_1 \cdots A_M, \quad (F1)
\]
\[
U^t = \sum_{i,j=1}^{d-1} |i_1 \cdots i_M \rangle \langle i_1 \cdots i_M | A_1 \cdots A_M \otimes U_{A_1 \cdots A_M},
\]
\[
(\text{F2})
\]
is a twisting unitary operator, and \(l = \log_2 d\). System \(A_1 \cdots A_M\) are called the shield system. For infinite dimensional systems, such as bosonic systems, the shield system’s dimension is also unbounded which could be problematic on upper bounding the distillable key rate. This can be circumvented by using the hypothesis testing relative entropy approach which allows one to derive a dimension-independent bound.

Let \(\rho_{A_1 \cdots A_M}\) be a multipartite quantum state. Then a triple \((n, P, \varepsilon)\) for common-key generation consists of \(n\) uses of the state \(\rho_{A_1 \cdots A_M}\), the rate \(P\), and the error \(\varepsilon \in [0, 1]\). Such a triple is achievable if there exists a LOCC protocol \(\Lambda\) such that \(l/n \geq P\)
\[
F(\gamma^{(M)}_{\Lambda}, \omega_{A_1 A_2 A_3 \cdots A_M A_M}) \geq \varepsilon,
\]
\[
(\text{F3})
\]
where \(\omega_{A_1 A_2 A_3 \cdots A_M A_M} = \Lambda(\rho_{A_1 \cdots A_M})\), and \(\Lambda\) is a LOCC protocol. In what follows, \(D^\text{rcm}(\rho||\sigma)\) is the hypothesis testing relative entropy defined as
\[
D^\text{rcm}_H(\rho||\sigma) = -\log_2 \inf_{\Lambda} \{ \text{Tr}[\Lambda \sigma] : 0 \leq \Lambda \leq I \wedge \text{Tr}[\Lambda \sigma] \geq 1 - \varepsilon \}.
\]
\[
(\text{F4})
\]
We first prove the following bound:

**Theorem 19** The one-shot common key distillation of \(\rho_{A_1 \cdots A_M}\) is bounded from above by
\[
P(1, \varepsilon, \rho_{A_1 \cdots A_M}) \leq E^\varepsilon_{\text{rcm}}(\rho),
\]
where \(E^\varepsilon_{\text{rcm}}(\rho)\) is defined analogous to \(E_{\text{rcm}}(\rho)\) with \(E_R(\rho)\) replaced with \(E^\varepsilon_R(\rho)\), and \(E^\varepsilon_R(\rho) = \min_{\sigma \in \mathcal{SEP}} D^\varepsilon_H(\rho||\sigma).
\]
**Proof.** We prove the above theorem for tripartite state; the proof for multipartite state follows. For tripartite state, we have four partitions, therefore we need to prove the following statement
\[
P(1, \varepsilon, \rho_{ABC}) \leq \min \{ E^\varepsilon_{\text{rcm}}(P_1), E^\varepsilon_{\text{rcm}}(P_2), E^\varepsilon_{\text{rcm}}(P_3), E^\varepsilon_{\text{rcm}}(P_4) \}.
\]
The proof for \(E^\varepsilon_{\text{rcm}}(P_1), E^\varepsilon_{\text{rcm}}(P_2), \) and \(E^\varepsilon_{\text{rcm}}(P_3)\) follows from Sec. IVB and C of [21]. We need to prove that
\[
P(1, \varepsilon, \rho_{ABC}) \leq E^\varepsilon_{\text{rcm}}(P_4).
\]
For this we need to prove that
\[
P(1, \varepsilon, \rho_{ABC}) \leq E^\varepsilon_{\text{rcm}}(BB'CB'CC'),
\]
where \(\tilde{\rho}\) is the cut-and-merge of \(\rho\) on \(BC\).

For a common key distillation protocol, we know that \(F(\gamma_{\text{ABC}\bar{A}\bar{B}C}, \omega_{\text{ABC}\bar{A}\bar{B}C}) \geq 1 - \varepsilon\), where \(\gamma_{\text{ABC}\bar{A}\bar{B}C}\) is tri-partite private state and \(\omega_{\text{ABC}\bar{A}\bar{B}C}\) is the output of the protocol. Let \(\tilde{\omega}_{\text{BC}\bar{C}CB'\bar{C}'BC'}\) be a cut-and-merge of \(\omega_{\text{ABC}\bar{A}\bar{B}C}\) on \(BCB'\bar{C}\). Then we can always construct a cut-and-merge \(\tilde{\gamma}_{\text{BC}\bar{C}CB'\bar{C}'BC'}\) of \(\gamma_{\text{ABC}\bar{A}\bar{B}C}\) on \(BCB'\bar{C}\) such that
\[
F(\tilde{\gamma}_{\text{BC}\bar{C}CB'\bar{C}'BC'}, \tilde{\omega}_{\text{BC}\bar{C}CB'\bar{C}'BC'}) \geq 1 - \varepsilon.
\]
Now, we can construct the following dichotomic measurement
\[
\{ \tilde{\Pi}_{\text{BC}\bar{C}CB'\bar{C}'BC'}, 1 - \tilde{\Pi}_{\text{BC}\bar{C}CB'\bar{C}'BC'} \},
\]
where
\[
\tilde{\Pi}_{\text{BC}\bar{C}CB'\bar{C}'BC'} = V_{B'C'\bar{C}'\bar{C}} \Pi_{B'CB'\bar{C}} U^t_{B'CB'\bar{C}} V_{B'C'\bar{C}'\bar{C}}^\dagger.
\]
\[
(\text{F11})
\]
Here the unitary \(V\) is the same unitary that is used to define the cut-and-merge of \(\tilde{\gamma}\) and \(\tilde{\omega}\). Then we observe
\[
\text{Tr} \left[ \hat{\Pi}_\omega \right] = \text{Tr} \left[ V_{B'C'\bar{B}'\bar{C}'} \Pi_{B'B'C'C'} \otimes |00\rangle \langle 00|_{C'C'} V_{B'C'\bar{B}'\bar{C}'}^\dagger V_{B'C'\bar{B}'\bar{C}'} \omega_{B'B'C'C'} \otimes |00\rangle \langle 00|_{C'C'} V_{B'C'\bar{B}'\bar{C}'}^\dagger \right] = \text{Tr} [\hat{\Pi}_\omega] \geq 1 - \varepsilon.
\]

The first two equalities are rewritings, and the last inequality follows from (47)-(51) of [21]. Now, let us consider the following set of (in)equalities for a separable state \( \sigma \):

\[
\text{Tr} \left[ \hat{\Pi}_\sigma \right] = \text{Tr} \left[ V_{B'C'\bar{B}'\bar{C}'} U_{B'B'C'C'}^{t,t} (\Phi_{B'B'C'C'} \otimes I_{B'B'C'C'} \otimes |00\rangle \langle 00|_{C'C'}) U_{B'B'C'C'}^{t,t\dagger} \Phi_{B'B'\bar{B}'\bar{C}'\bar{C}'} \right] = \text{Tr} \left[ \Phi_{B'B'C' \bar{B}'\bar{C}'} \otimes |00\rangle \langle 00|_{C'C'} U_{B'B'C'C'}^{t,t\dagger} \Phi_{B'B'\bar{B}'\bar{C}'\bar{C}'} U_{B'B'C'C'}^{t,t} \right] \leq \frac{1}{d}.
\]

The last inequality is justified as follows. Assume that \( \sigma \) is a pure state. That is,

\[
\sigma_{B'B'\bar{B}'\bar{C}'\bar{C}'} = |\psi\rangle \langle \psi|_{B'B'\bar{B}'\bar{C}'\bar{C}'},
\]

where

\[
|\psi\rangle_{B'B'\bar{B}'\bar{C}'\bar{C}'\bar{C}'} = \sum_i \alpha_i |i\rangle_{B'} |\psi_i\rangle_{B'\bar{B}'\bar{C}'} \otimes \sum_j \beta_j |j\rangle_{C'} |\phi_j\rangle_{C'\bar{C}'},
\]

Then, we have,

\[
\text{Tr} \left[ \Phi_{B'B'C'C'} \otimes |00\rangle \langle 00|_{C'C'} U_{B'B'C'C'}^{i,j,k} (V_{B'C'\bar{B}'\bar{C}'\bar{C}'} \otimes |\psi\rangle \langle \psi|_{B'B'\bar{B}'\bar{C}'\bar{C}'\bar{C}'}) U_{B'B'C'C'}^{i,j,k\dagger} \right] = \text{Tr} \left[ \Phi_{B'B'C'C'} \otimes |00\rangle \langle 00|_{C'C'} U_{B'B'C'C'}^{i,j,k} (V_{B'C'\bar{B}'\bar{C}'\bar{C}'} \otimes |\psi\rangle \langle \psi|_{B'B'\bar{B}'\bar{C}'\bar{C}'\bar{C}'}) U_{B'B'C'C'}^{i,j,k\dagger} \right] = \frac{1}{d} \left\| \sum_i \langle 0 |_{B'C'} U_{B'B'C'C'}^{i,j,k} V_{B'C'\bar{B}'\bar{C}'\bar{C}'} \alpha_i |\psi_i\rangle_{B'\bar{B}'\bar{C}'} \otimes \beta_i |\phi_i\rangle_{C'\bar{C}'}, \right\|^2
\]

\[
= \left\| \sum_i \right\|^2 \left\| \frac{1}{d} \sum_i \alpha_i \beta_i |\xi_i\rangle_{B'B'C'C'} \right\|^2
\]

\[
= \left\| \sum_i \alpha_i \beta_i |\xi_i\rangle_{B'B'C'C'} \right\|^2 \leq \frac{1}{d} \left( \sum_i |\alpha_i| |\beta_i| \right)^2
\]

\[
\leq \frac{1}{d}.
\]

The bound for general separable states in (F13) follows because every such state can be written as a convex combination of pure product states.

Combining this with the definition of the hypothesis (F17),
testing relative entropy implies,
\[ D_H(\hat{\omega} \| \sigma) \geq \log_2 d. \] (F18)
Since this holds for any separable \( \sigma \), we obtain,
\[ P(1, \varepsilon, \rho_{ABC}) \leq E_{rcm}(BB'; CC')_\rho. \] (F19)
This concludes the proof. \( \blacksquare \)

The above theorem implies the RCM upper bound for the common key distillation:

**Theorem 20** The distillable common key of \( \rho_{A_1 \cdots A_M} \) is bounded as
\[ K_D(\rho_{A_1 \cdots A_M}) \leq E_{rcm}(\rho). \] (F20)

**Proof.** The above theorem immediately leads to the following bound:
\[ P(n, \varepsilon, \rho_{A_1 \cdots A_M}) \leq \frac{1}{n} E_{rcm}(\rho^\otimes n) \] (F21)
We can then use the following relation ([49], see also Appendix B of [50])
\[ D_H(\rho \| \sigma) \leq \frac{1}{1 - \varepsilon} (D(\rho \| \sigma) + h_2(\varepsilon)), \] (F22)
along with the definition of common key distillation capacity, and the subadditivity of the RCM bound to obtain
\[ K_D(\rho_{A_1 \cdots A_M}) \leq E_{rcm}(\rho). \] (F23)
This concludes the proof. \( \blacksquare \)

Now, we can consider the network scenario where one uses a teleportation-simulable network \( n \) times, with each use interleaved by local operations and classical communication (LOCC). The protocol can be bounded from above by the performance of a protocol with a much simpler form: the simplified protocol consists of a single round of LOCC acting on \( n \) copies of the resource state [39–41] as we have discussed for the GHZ entanglement distribution scenario in Theorem 3. Then we have the following theorem for the multipartite common private capacity \( P^c \):

**Theorem 22** The common private capacity of the teleportation simulable quantum network \( \mathcal{L} \) consisting of point-to-point pure-loss bosonic channels is given by
\[ P^c_{\leftrightarrow}(\mathcal{L}) = \min_p \frac{1}{|P| - 1} \sum_{jk} -\log_2(1 - \eta_{jk}), \] (F25)
where \( \eta_{jk} \) is the transmittance of the pure-loss bosonic channel connecting node \( j \) and \( k \), and the sum goes over pairs across the partitions.

Following Theorem 5 for the GHZ entanglement distribution, we also have,

**Theorem 23** Suppose in the teleportation simulable quantum network \( \mathcal{N} \) with \( M \) nodes, \( \{A_1, \cdots, A_M\} \), common keys are intended to be distributed over only part of the nodes \( \{A_1, \cdots, A_N\} \) where \( N < M \). Let \( \mathcal{P} \) be the partitioning of these \( N \) nodes where the other \( M - N \) nodes are included in some of these partitions. The common private capacity \( P^c_{\leftrightarrow}(\mathcal{N}; A_1, \cdots, A_N) \) is then bounded by
\[ P^c_{\leftrightarrow}(\mathcal{N}; A_1, \cdots, A_N) \leq \min_p \frac{1}{|P| - 1} \sum_{\sigma} E_R(A_j; A_k)_{\sigma_i}, \] (F26)
where \( \mathcal{P} \) is the partitioning of \( N \)-partite system and the sum is taken over all states \( \rho_i \) across the groups of partition.

Finally, we point that the above theorems hold not only for a full quantum network, where network nodes are supposed to operate coherently, but also for the trusted node based quantum key distribution (QKD) network, where QKD links are terminated at each node, which is assumed to be safe (trusted), and keys are classically relayed to reach arbitrary nodes. This is a realistic scenario of the QKD network deployment without quantum repeaters [30–33].

The statement is justified as follows: the lower bounds are derived by considering a classical version of the protocol in Theorem 3. For the upper bound, the key relay protocols in the trusted node scenario are usually classical but one can always interpret them as fully quantum key relays. Then since the rate of the full quantum version of the key relay (and QKD links) is upper bounded by the above theorems, the rate of the classical key relay with QKD links are also limited by the same bound.

**Appendix G: Network quantum repeater**

In this appendix, we discuss the details of the network quantum repeater in the quantum network illustrated in Fig. 3 of the main text. Figure 3(a) is a rectangular quantum network \( \mathcal{N}_{rec} \) without a network quantum repeater, where four nodes \( A_1 \) to \( A_4 \) intend to share GHZ states and are connected by six pure-loss channels (e.g. optical fibers) where \( l_0 \) and \( 2l_0 \) represents the distances of the channels and \( \eta_i \) is the loss parameter with \( \eta_1 = \eta_0^2 \) and
\(\eta_2 = \eta_0^{\sqrt{5}}\). Applying Theorem 4, we can calculate the GHZ entanglement distribution capacity of this network as

\[
Q_{\text{GHZ}}^{\text{rec}}(N_{\text{rec}}) = \begin{cases} 
2(f(\eta_1) + f(\eta_2)), & \eta_0 \leq 0.3257,
\frac{1}{2} f(\eta_0) + f(\eta_1) + f(\eta_2), & 0.0027 \leq \eta_0 \leq 0.6180,
\frac{1}{2} (2f(\eta_0) + 2f(\eta_1) + 3f(\eta_2)), & \text{otherwise},
\end{cases}
\]

where \(f(\eta) = -\log_2(1 - \eta)\). For a high loss network \((\eta_0 < 0.3257)\), it scales as \(2(f(\eta_1) + f(\eta_2)) \sim 2\eta_0^{\sqrt{5}/2}\) which gives the exponential rate improvement from the repeaterless case.

Figure 3(b) is the same quantum network with a quantum repeater node \(R\) at the center, which we denote as \(N_{\text{rec}}^R\). The repeater node and the other nodes are connected via a pure-loss channel with \(\tilde{\eta}_2 = \eta_0^{\sqrt{5}/2}\). Applying Theorem 5, we obtain the upper bound of the GHZ distribution capacity as

\[
Q_{\text{GHZ}}^{\text{rec}}(N_{\text{rec}}^R; A_1, A_2, A_3, A_4) \leq \begin{cases} 
2(f(\eta_1) + f(\tilde{\eta}_2)), & \eta_0 \leq 0.0027, \\
\frac{1}{2} f(\eta_0) + f(\eta_1) + f(\tilde{\eta}_2), & 0.0027 \leq \eta_0 \leq 0.6180, \\
\frac{1}{2} (2f(\eta_0) + 2f(\eta_1) + 3f(\tilde{\eta}_2)), & \text{otherwise}.
\end{cases}
\]

In our protocol 1, \(R\) simply acts as two point-to-point quantum repeaters: one connects channels \(A_1 R\) and \(A_3 R\) and the other connects \(A_2 R\) and \(A_4 R\). If \(R\) works as ideal repeaters, the whole network is effectively equivalent to a repeaterless network with the same configuration as Fig. 3(a) where the loss of channels \(A_1 A_3\) and \(A_2 A_4\) are replaced by \(\tilde{\eta}_2\). The maximum achievable rate of this network can be calculated from Theorem 4 and we get

\[
Q_{\text{GHZ}}^{\text{rec}}(N_{\text{rec}}^R; A_1, A_2, A_3, A_4) \geq \begin{cases} 
2(f(\eta_1) + f(\tilde{\eta}_2)), & \eta_0 \leq 0.0027, \\
\frac{1}{2} (2f(\eta_0) + 2f(\eta_1) + 3f(\tilde{\eta}_2)), & \text{otherwise}.
\end{cases}
\]

For a high loss network \((\eta_0 < 0.0027)\), it saturates the upper bound and scales as \(2(f(\eta_1) + f(\tilde{\eta}_2)) \sim 2\eta_0^{\sqrt{5}/2} \sim 2\eta_0^{1.1}\) which gives the exponential rate improvement from the repeaterless case.

In our protocol 2, we separate the whole network into two parts: one is a rectangular network consisting of 4 links, \(A_1 A_2, A_2 A_3, A_3 A_4, A_1 A_4\), and the other is a star network each \(A_i\) is connected to \(R\) via \(A_i R\). For the former network, the optimal GHZ distribution rate is calculated from Theorem 4. For the latter network, rate of \(f(\tilde{\eta}_2)\) is achievable by first each \(A_i R\) and \(R\) generate Bell states with rate \(f(\tilde{\eta}_2)\) and then generate GHZ states by concatenating them at \(R\). The total GHZ state generation rate is derived to be

\[
Q_{\text{GHZ}}^{\text{rec}}(N_{\text{rec}}^R; A_1, A_2, A_3, A_4) \geq \begin{cases} 
2(f(\eta_1) + f(\tilde{\eta}_2)), & \eta_0 \leq 0.618,
\frac{1}{2} (2f(\eta_0) + 2f(\eta_1) + 3f(\tilde{\eta}_2)), & \text{otherwise},
\end{cases}
\]

which shows better performance than the first protocol in a low loss region and saturates the upper bound for \(\eta_0 \geq 0.618\). However, there is still a gap between the lower bounds and the upper bound in the intermediate region, \(0.0027 \leq \eta_0 \leq 0.618\).

[1] H. J. Kimble. The quantum internet. Nature, 453(7198):1023–1030, June 2008.
[2] Stephanie Wehner, David Elkouss, and R Hanson. Quantum Internet: a vision for the road ahead. Science, 362(October):303, 2018.
[3] Daniel M Greenberger, Michael A Horne, and Anton Zeilinger. Bell’s Theorem, Quantum Theory, and Conceptions of the Universe, chapter Going Beyond Bell’s Theorem, pages 69–72. Klwer, Dordrecht, 1989.
[4] Michael Epping, Hermann Kampermann, Chiara Macchiavello, and Dagmar Bruß. Multi-party entanglement can speed up quantum key distribution in networks. New Journal of Physics, 19(9), 2017.
[5] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. Physical Review A - Atomic, Molecular, and Optical Physics, 59(3):1829–1834, 1999.
[6] P. Kómr, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. Nature Physics, 10(8):582–587, 2014.
[7] Ryszard Horodecki, Michal Horodecki, and Karol Horodecki. Quantum entanglement. Reviews of Modern Physics, 81(2):865–942, jun 2009.
[8] Jian-Wei Pan, Zeng-Bing Chen, Chao-Yang Lu, Harald Weinfurter, Anton Zeilinger, and Marek Żukowski. Multiphoton entanglement and interferometry. Reviews of Modern Physics, 84(2):777–838, may 2012.
[9] H. Aschauer, W. Dürr, and H. J. Briegel. Multiparticle entanglement purification for two-colorable graph states. Physical Review A - Atomic, Molecular, and Optical Physics, 71(1):1–20, 2005.
[10] Caroline Kruszynska, Simon Anders, Wolfgang Dürr, and Hans J. Briegel. Quantum communication cost of preparing multipartite entanglement. Physical Review A - Atomic, Molecular, and Optical Physics, 73(6):1–18, 2006.
[11] Martí Cuquet and John Calsamiglia. Growth of graph states in quantum networks. Physical Review A - Atomic, Molecular, and Optical Physics, 86(4):1–15, 2012.
[12] J. Wallnöfer, M. Zwerger, C. Muschik, N. Sangouard, and W. Dürr. Two-dimensional quantum repeaters. Physical Review A, 94(5):1–12, 2016.
[13] A. Pirker, J. Wallnöfer, and W. Dürr. Modular architectures for quantum networks. New Journal of Physics, 20(5), 2018.
[14] J. Wallnöfer, A. Pirker, M. Zwerger, and W. Dürr. Multiparticle state generation in quantum networks with optimal scaling. Scientific Reports, 9(1):1–18, 2019.
[15] John a. Smolin, Frank Verstraete, and Andreas Winter. Entanglement of assistance and multipartite state distillation. Physical Review A, 72(5):052317, nov 2005.
[16] A. Streltsov, C. Meignant, and J. Eisert. Rates of multi-partite entanglement transformations and applications in quantum networks. arXiv e-prints, page arXiv:1709.09693, Sep 2017.

[17] Peter Vrana and Matthias Christandl. Distillation of greenbergerhornezeilinger states by combinatorial methods. IEEE Transactions on Information Theory, 65(9):1–1, 2019.

[18] Masahiro Takeoka, Saikat Guha, and Mark M Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. Nature Communications, 5:5235, October 2014.

[19] Masahiro Takeoka, Saikat Guha, and Mark M Wilde. The squashed entanglement of a quantum channel. IEEE Transactions on Information Theory, 60(8):4987–4998, August 2014. arXiv:1310.0129.

[20] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. Nature Communications, 8:15043, 2017.

[21] Mark M Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. IEEE Transactions on Information Theory, 63(3):1792–1817, 2017.

[22] Masahiro Takeoka, Kausik P. Seshadreesan, and Mark M Wilde. Unconstrained Capacities of Quantum Key Distribution and Entanglement Distillation for Pure-Loos Bosonic Broadcast Channels. Physical Review Letters, 119:150501, 2017.

[23] Koji Azuma, Akihiro Mizutani, and Hoi-kwong Lo. Fundamental rate-loss trade-off for the quantum internet. Nature Communications, 7:13523, 2016.

[24] Stefano Pirandola. End-to-end capacities of a quantum communication network. Communications Physics, 2(1):51, 2019.

[25] Kausik P Seshadreesan, Masahiro Takeoka, and Mark M Wilde. Bounds on Entanglement Distillation and Secret Key Agreement for Quantum Broadcast Channels. IEEE Transactions on Information Theory, 62(5):2849–2866, 2016.

[26] Stefan Bäuml and Koji Azuma. Fundamental limitation on quantum broadcast networks. Quantum Science and Technology, 2(2):024004, 2017.

[27] Stefan Bäuml, Koji Azuma, Go Kato, and David Elkouss. Linear programs for entanglement and key distribution in the quantum internet. arXiv e-prints, page arXiv:1809.03120, Sep 2018.

[28] Siddhartha Das, Stefan Buml, Marek Winczewski, and Karol Horodecki. Universal limitations on quantum key distribution over a network, 2019.

[29] Charles H Bennett, Sandu Popescu, Daniel Rohrlich, John A Smolin, and Ashish V Thapliyal. Exact and asymptotic measures of multipartite pure-state entanglement. Physical Review A - Atomic, Molecular, and Optical Physics, 63(1):012307, 2001.

[30] M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Broui, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The secoqc quantum key distribution network in vienna. New Journal of Physics, 11:075001, 2009.

[31] M Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Waki, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, K Yoshino, Y Nambu, S Takeahashi, A Tajima, A Tomita, T Domeki, T Hasegawa, Y Sakai, H Kobayashi, T Asai, K Shimizu, T Tokura, T Tsurumaru, M Matsui, T Honjo, K Tamaki, H Takesue, Y Tokura, J F Dynes, A R Dixon, A W Sharpe, Z L Yuan, A J Shields, S Uchikoga, M Legrè, S Robyr, P Trinkler, L Monat, J-B Page, G Ribordy, A Poppe, A Allacher, O Maurhart, T Länger, M Peev, and A Zeilinger. Field test of quantum key distribution in the tokyo qkd network. Optics Express, 19(11):10387–10409, 2011.

[32] D Stucki, M Legrè, F Buntschu, B Clausen, N Felber, N Gisin, L Helsen, P Junod, G Litzistorf, P Monbaron, L Monat, J B Page, D Perroud, G Ribordy, A Rochas, S Robyr, J Tavares, R Thew, P Trinkler, S Ventura, R Voirol, N Walenta, and H Zbinden. Long-term performance of the swissquantum quantum key distribution network in a field environment. New Journal of Physics, 13:123001, 2011.

[33] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Hong-Wei Li, De-Yong He, Yu-Hu Li, Zheng Zhou, Xiao-Tian Song, Fang-Yi Li, Dong Wang, Hua Chen, Yun-Guang Han, Jing-Zheng Huang, Jun-Fu Guo, Peng-Lei Hao, Mo Li, Chun-Mei Zhang, Dong Liu, Wen-Ye Liang, Chun-Hua Miao, Ping Wu, Guang-Can Guo, and Zheng-Fu Han. Field and long-term demonstration of a wide area quantum key distribution network. Optics Express, 22(18):21739, 2014.

[34] Dong Yang, Karol Horodecki, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Wei Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. IEEE Transactions on Information Theory, 55(7):3375–3387, July 2009.

[35] Remigiusz Augusiak and Pawel Horodecki. Multipartite secret key distillation and bound entanglement. Phys. Rev. A, 80:042307, Oct 2009.

[36] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 461:207–235, 2005.

[37] W. T. Tutte. On the problem of decomposing a graph into n connected factors. J. London Math. Soc., 36:221–230, 1961.

[38] C. St. J. A. Nash-Williams. Edge-disjoint spanning trees of finite graphs. J. London Math. Soc., 36:445–450, 1961.

[39] Charles H Bennett, David P. DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. Physical Review A, 54(5):3824, 1996.

[40] Julien Niset, Jaromir Fiurasek, and Nicolas Cerf. No-Go Theorem for Gaussian Quantum Error Correction. Physical Review Letters, 102(12):1–4, 2009.

[41] Alexander Müller-Hermes. Transposition in quantum information theory. Master’s thesis, 2012.

[42] Michał Horodecki, Pawel Horodecki, and Ryszard Horodecki. Limits for entanglement measures. Physics
Vlatko Vedral and Martin B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619–1633, March 1998. arXiv:quant-ph/9707035.

Michal Horodecki. Simplifying monotonicity conditions for entanglement measures. *Open Systems and Information Dynamics*, 12:231, dec 2005.

Matthew J. Donald and Michał Horodecki. Continuity of relative entropy of entanglement. *Physics Letters A*, 264(4):257 – 260, 1999.

Andreas Winter. Tight Uniform Continuity Bounds for Quantum Entropies: Conditional Entropy, Relative Entropy Distance and Energy Constraints. *Communications in Mathematical Physics*, 347:291–313, 2016.

Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. arXiv:quant-ph/0309110.

Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189.

Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456.

Eneet Kaur and Mark M Wilde. Upper bounds on secret-key agreement over lossy thermal bosonic channels. *Physical Review A*, 96:062318, 2017.