Rate-distance tradeoff and resource costs for all-optical quantum repeaters

Mihir Pant,[1,2] Hari Krovi,[2] Dirk Englund,[1] and Saikat Guha[2]

[1] *Dept. of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139, USA*
[2] *Quantum Information Processing group, Raytheon BBN Technologies, 10 Moulton Street, Cambridge, MA 02138, USA*

Over a direct-transmission link, the maximum key rate achievable by any Quantum Key Distribution (QKD) protocol must decay linearly with the channel's transmissivity η when the channel is lossy ($\eta \ll 1$), which in turn decays exponentially with the end-to-end range L in optical fiber, i.e., $\eta = e^{-\alpha L}$, thereby making the key rate unusable quickly as the distance between the communicating parties grows. Over a direct point-to-point link, the exact expression for the maximum key rate attainable is given by $R_{\text{direct}}(\eta) = -\log_2(1-\eta)$ bits/mode [1], which $\approx 1.44\eta$, when $\eta \ll 1$. The bits/s key rate is obtained by multiplying the bits/mode rate by the modes/sec (governed by the spatio-temporal optical bandwidth leveraged by the QKD protocol). Quantum repeaters, proposed in [2], are devices which when inserted along the length of the optical channel, can help generate shared secret at a bits/mode rate that surpasses $R_{\text{direct}}(\eta)$. Quantum repeaters need not be trusted or physically secured in order to ensure the security of the keys generated. Despite a lot of theoretical research on quantum repeaters starting from the original proposal of the concept in 1998, most of which involve some form of quantum memory, sources of entanglement, and limited quantum processing on the qubits held in the memories, there has yet to be an experimental demonstration of QKD using repeaters that outperforms the aforesaid best repeaterless rate performance. Therefore, it is very important to understand rigorously and quantitatively the tradeoff between resource requirements (to build a repeater "node") and the end-to-end key rates achieved using any specific repeater architecture, with all sources of device imperfections properly taken into account.

If n quantum repeaters are inserted along the length of the channel connecting the communicating parties Alice and Bob, and if there are absolutely no physical constraints placed on the repeater nodes (i.e., the repeaters are assumed to be lossless, error-corrected, general purpose quantum computers), then the maximum key rate achievable by Alice and Bob is given by $R_{\text{direct}}(\eta_{\min}) = -\log_2(1-\eta_{\min})$ bits/mode, where $\eta_{\min} \equiv \min(\eta_1, \eta_2, \ldots, \eta_{n+1})$ is the transmissivity of the lossiest segment between successive repeater nodes (with $\eta = \eta_1 \ldots \eta_{n+1}$) [3, 4]. Given n repeater nodes, their optimal placement is to lay them equally-spaced. Therefore, the maximum rate is given by $-\log_2(1-\eta^{1/(n+1)})$ bits/mode. As $n \to \infty$, this rate is clearly unbounded. However, assuming repeaters to be lossless error-corrected quantum computers is not practical. A more practically relevant question to ask is if the repeater nodes have finite resources with lossy and imperfect components (where 'resources' may be different physical entities depending upon the type of quantum repeater and the protocol employed), then what rate can Alice and Bob achieve, and more importantly what would it take to build repeater nodes so as to be able to significantly outperform $R_{\text{direct}}(\eta)$ bits/mode where η is the end-to-end transmissivity between the communicating parties. This is the topic addressed in this abstract and the accompanying long paper [5], for repeaters that are built solely using photonic components—single-photon sources, detectors, electro-optic feedforward, but no matter-based quantum memories. As we will see later in this abstract, that given physical constraints on a repeater node, placing more repeaters (higher n) between Alice and Bob may not always improve the rate, i.e., depending upon the total distance L (or equivalently, the transmissivity η) between Alice and Bob, and given the physical device constraints in a repeater node, there may be an optimal number $n^*(\eta)$ of nodes, which achieves the highest end-to-end rate.

A recent proposal by Azuma et al. [6] did away with quantum memories and leveraged ideas from all-optical quantum computing to protect photons against loss by attaching to them many redundant photons in a locally prepared entangled (tree-) cluster state [7]. This loss protection mimics the role of a quantum memory, yet only uses "flying qubits", linear optics and single photon detectors locally at repeater nodes, arguably making the design of a repeater more feasible compared to ones that employ quantum memories. In this paper, we address in great detail the resource requirements to implement an all-optical repeater architecture that could substantially outperform $R_{\text{direct}}(\eta)$, the best possible end-to-end key rates achievable without quantum repeaters. We propose several improvements to Azuma et al.'s protocol, reducing the resource requirements (viz., number of single photon sources needed locally at each repeater node) by five orders of magnitude. Our detailed study, which accounts for losses everywhere in the system, including coupling losses, source and detection inefficiencies, loss in fiber, loss in a photon being stored in a Silicon waveguide, develops a clear analytic expression, as a function of all the aforesaid losses, for how the key rate scales with the end-to-end channel transmissivity η, and the optimal spacing between successive repeater nodes that maximizes the rate-loss envelope (the device parameters assumed in our paper are shown in table I). Our results also provide clear insight on how such a repeater scheme's rate performance improves with progressively more resources (such as photon sources and detectors) being made available at each repeater node.

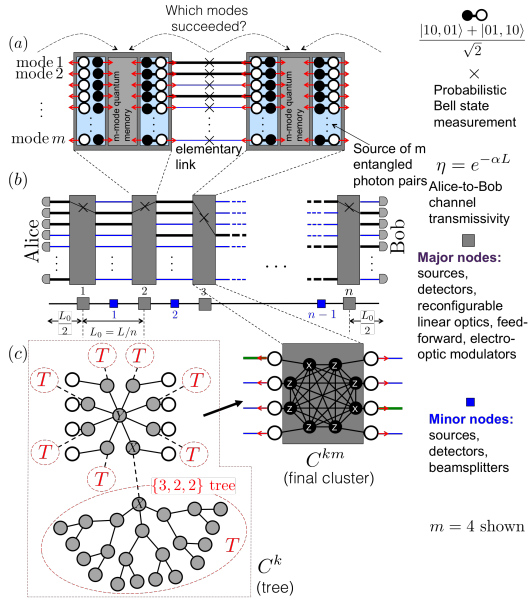

FIG. 1. (a), (b) show the schematics of an elementary link, and a chain of them connecting Alice and Bob, respectively, for a repeater architecture that employs quantum memories, Bell pair sources, probabilistic BSMs, and multiplexing over m orthogonal qubit modes (parallel channels). (c) shows the construction of a photonic cluster state that can subsume the roles of the quantum memory and pair sources, thereby resulting in a quantum repeater architecture based solely on 'flying' qubits. The outer (white) photonic qubits are transmitted on the fiber channels, and the inner (black) qubits are held locally in a (lossy) waveguide at the repeater node.

Relatively small ($\sim$ 100 photon) entangled photonic cluster states are already a useful quantum resource for long-distance secure communication, even though they may be too small a resource to build a truly useful general-purpose quantum computer. In Fig. 2, we plot the bits/mode rate of our improved repeater scheme. We find that a repeater station using a 130 photon entangled cluster state (which requires $k = 7$ fusion steps to prepare starting from unentangled single photons processed via a passive linear-optical interferometer) can surpass $R_{\text{direct}}(\eta)$ at a range slightly greater than 150 km. The number of repeaters n is chosen optimally at any given total range. As a specific performance point, our scheme—with repeater nodes that can generate 210-photon cluster states every time period—could generate keys at 10 kHz at a 400 km range, whereas an ideal repeater-less scheme will achieve less than 0.02 Hz. Given that continuous variable entangled optical clusters of $\sim$ 10000 modes were recently created experimentally, our results appear promising.

We also develop and analyze a specific method to create photonic clusters required at each repeater node using passive linear optics, single photon sources and photon detectors, again including losses in each component. In Fig. 3, we plot the number of photon sources available

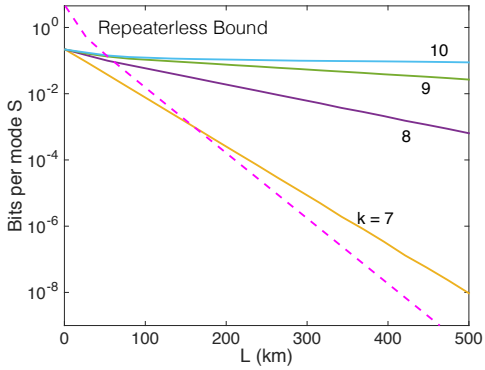

FIG. 2. Key rate in bits per mode as a function of distance L for different numbers of fusion steps k. The size (in number of photons) of the cluster at a repeater node, $Q = 2^k + 2$. $R_{\text{direct}}(\eta)$ is plotted using the pink dashed line.

at each repeater node versus the success probability of simultaneously creating a cluster requiring 7 fusion steps (130 photon states) at 250 repeater nodes with and without our improvements.

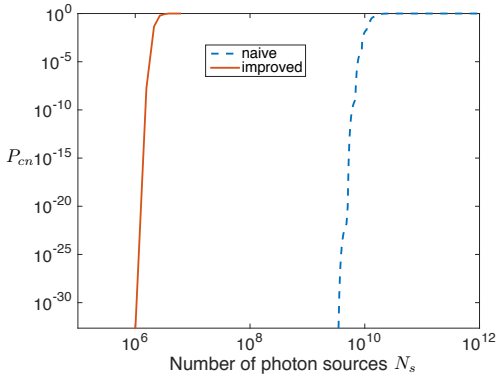

FIG. 3. The probability that all $n = 250$ major nodes simultaneously succeed in creating 130 photon clusters ($k = 7$ fusion steps), using the naive and improved multiplexing schemes.

We find that with the naive scheme, it would require $\sim 10^{10}$ single-photon sources at each repeater station to create this 130 photon cluster at each repeater station with 90% probability. With our improvements, the number of photon sources required at each repeater station to achieve the same success probability is reduced to 3×10^6. Furthermore, our improved architecture also leads to better performance for the same cluster size. Combining these effects, our improvements reduce the number of photon sources required to outperform $R_{\text{direct}}(\eta)$ by five orders of magnitude. We show that the number of sources required could be further reduced by 3 orders of magnitude if one could find a way to create good-quality three-photon-entangled (GHZ) states directly, perhaps using a non-linear optical medium, and be reduced even further by incorporating yet-undiscovered novel quantum-error-correction techniques tailored for error mechanisms

that naturally occur in optical qubits. Assuming a 1 MHz repetition rate, as per our calculation, a 954-photon cluster can allow for QKD at 144 kHz over 5000 km, a useful distance measure for long distance terrestrial communication given the size of the earth. The key rate without repeaters with the same parameters would be less than 10^{-92} Hz. Creating the 954 photon cluster for QKD at 5000 km will require, based on our cluster-generation scheme (which to our knowledge is the best-known one) about 100 million single photon sources at each node. The recent upward trend in the scalable realization of programmable linear-optical interferometers and research on scalable fabrication of single photon sources and detectors in integrated photonic chips are important enablers to eventually realize photonic quantum repeaters for long-distance QKD at practically-useful rates.

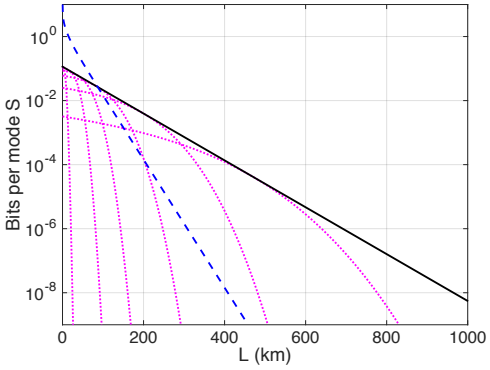

FIG. 4. The key rate (in bits per mode) $S_n(L)$ achieved by an n-node repeater chain shown as a function of range L, for $n = 1, 10, 24, 56, 133, 314$ (magenta dotted plots). The rate-distance envelope $S_{\rm LB}(L)$ is shown (black solid plot). We chose $m = 4$ parallel channels and $\vec{b} = \{7, 3\}$ error-protection trees (which translates to $k = 8$ clusters) for all plots. $R_{\rm direct}(\eta)$ is shown for comparison (blue dashed plot).

Finally, we find an analytical expression for the rate loss envelope for the all-optical repeater scheme (see black plot in Fig. 4). Our analytical expression shows that for fixed resources available at each repeater node, the rate loss envelope optimized over the number of repeater stations goes as $D\eta^s$ bits/s where D and $s < 1$ are constants depending on device parameters and size of clusters used at the repeater stations. Note that $\eta^s = e^{-\alpha s L}$. Hence, although the repeater protocol can outperform $R_{\rm direct}(\eta)$ (the dashed blue plot in Fig. 4) which $\propto \eta$ when $\eta \ll 1$), the key rate using this all-optical repeater scheme still scales exponentially with distance, but with a smaller exponent compared to $R_{\rm direct}(\eta)$. Another implication of our analytical results is that the distance between each repeater node is a constant that is a function of all the device losses, but independent of the total range L. In other words, given the device parameters and the choice of the major-node cluster size, there is an optimal gap L_0 with which repeaters should be placed—no more, and no less. For the numbers used for the plots in Fig. 4, $L_0 = 1.49$ km.

We believe that the theory of quantum error correction for photonic quantum processing is in its infancy, and the tree-cluster based loss protection method, which our all-optical repeater scheme relies upon, is far from optimal. For example, we found that the performance of our scheme cannot be improved indefinitely by making larger and larger tree clusters at each node. At some point, the additional losses incurred overshadows the additional error protection obtained from a larger cluster. This issue will plague larger general-purpose optical quantum computers designed using tree-cluster error correction.

Device parameter	symbol	value
fiber loss coefficient	α	0.046 km^{-1} (0.2 dB/km)
on-chip loss coefficient	β	0.62 m^{-1} (2.7 dB/m)
feed-forward time in fiber	τ_f	102.85 ns
feed-forward time on-chip	τ_s	20 ps
chip to fiber coupling efficiency	P_c	0.99
source detector efficiency product	$\eta_s\eta_d$	0.99
speed of light in fiber	c_f	$2 \times 10^8 m/s$
speed of light on chip	c_{ch}	$7.6 \times 10^7 m/s$

TABLE I. Assumed values for device performance parameters. The source detector efficiency product $\eta_s\eta_d$ is sufficient for our calculations, and need not be specified separately.

Significant research is needed in: (a) new theory on error correction for photonic quantum computing, and (b) efficient direct creation of multi-photon entangled states. We believe that our results will help inform the integrated photonics community about device requirements for making useful all-optical quantum repeaters, and will hopefully encourage other researchers developing quantum repeater technology carry out similar detailed resource-cost vs. rate-performance study of various other genres of quantum repeaters.

[1] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, (2015), arXiv:1510.08863.
[2] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, Physical Review Letters **81**, 5932 (1998).
[3] S. Pirandola, (2016), arXiv:1601.00966.
[4] K. Azuma, A. Mizutani, and H.-K. Lo, (2016), arXiv:1601.02933.
[5] M. Pant, H. Krovi, D. Englund, and S. Guha, (2016), arXiv:1603.01353.
[6] K. Azuma, K. Tamaki, and H.-K. Lo, Nature communications **6**, 6787 (2015).
[7] M. Varnava, D. Browne, and T. Rudolph, Physical Review Letters **97**, 120501 (2006).