## Ultrafast and Fault-Tolerant Quantum Communication across Long Distances

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters

### Citation

### Published Version
doi:10.1103/PhysRevLett.112.250501

### Citable link
http://nrs.harvard.edu/urn-3:HUL.InstRepos:16883008

### Terms of Use
This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA
Ultrafast and Fault-Tolerant Quantum Communication across Long Distances

Sreraman Muralidharan,1 Jungsang Kim,2 Norbert Lütkenhaus,3 Mikhail D. Lukin,4 and Liang Jiang5,*

1Department of Electrical Engineering, Yale University, New Haven, Connecticut 06511, USA
2Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA
3Institute of Quantum computing, University of Waterloo, N2L 3G1 Waterloo, Canada
4Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA
5Department of Applied Physics, Yale University, New Haven, Connecticut 06511, USA
*(Received 8 July 2013; revised manuscript received 19 October 2013; published 27 June 2014)

Quantum repeaters (QRs) provide a way of enabling long distance quantum communication by establishing entangled qubits between remote locations. In this Letter, we investigate a new approach to QRs in which quantum information can be faithfully transmitted via a noisy channel without the use of long distance teleportation, thus eliminating the need to establish remote entangled links. Our approach makes use of small encoding blocks to fault-tolerantly correct both operational and photon loss errors. We describe a way to optimize the resource requirement for these QRs with the aim of the generation of a secure key. Numerical calculations indicate that the number of quantum memory bits at each repeater station required for the generation of one secure key has favorable polylogarithmic scaling with the distance across which the communication is desired.

DOI: 10.1103/PhysRevLett.112.250501

Quantum communication across long distances ($10^3$–$10^4$ km) can significantly extend the applications of quantum information protocols such as quantum cryptography [1] and quantum secret sharing [2,3] which can be used for the creation of a secure quantum internet [4]. Quantum communication can be carried out by first establishing a remote entangled pair between the sender and the receiver and using teleportation to transmit information faithfully. However, there are two main challenges that have to be overcome. First, fiber attenuation during transmission leads to an exponential decrease in the entangled pair generation rate. Second, several operational errors such as channel errors, gate errors, measurement errors, and quantum memory errors severely degrade the quality of entanglement used for secure key generation. In addition, quantum states cannot be amplified or duplicated deterministically in contrast to classical information [5]. Establishing quantum repeater (QR) stations based on entanglement distribution is the only currently known approach to long-distance quantum communication using conventional optical fibers without exponential penalty in time and resources.

A number of schemes have been proposed for long distance quantum communication using QRs [6–12], most of which could be broadly classified into three classes. The first class of QRs [6–9] reduces the exponential scaling of fiber loss to polynomial scaling by introducing intermediate QR nodes. However, this scheme for long distance quantum communication is relatively slow [13], even after optimization [14], limited by the time associated with two-way classical communication between remote stations required for the entanglement purification process needed to correct operational errors [15]. In contrast, the second class of QRs introduces quantum encoding and classical error correction to replace the entanglement purification with classical error correction, handling all operational errors [10,16]. As a consequence, the entanglement generation rate further improves from $1/O(\log(L_{tot}))$ to $1/O(\log(\log(L_{tot}))$ where $L_{tot}$ is the total distance of communication. Recently, the approach to a third type of QRs was proposed, which uses quantum encoding to deterministically correct photon losses [11,12]. By entirely eliminating two-way classical communication between all repeater stations, the third class of QRs promise extremely high key generation rates that can be close to classical communication rates, limited only by the speed of local operations.

Besides the high key generation rate, it is very important to consider the resource requirement and fault-tolerant implementation of QRs. Cluster states can be used for achieving fault-tolerant quantum computation [17–19] and long-range entanglement [20] in the presence of both loss and operation errors. Cluster state based protocols [20] naturally belong to second class of QRs because the preparation of a large cluster state shared by many QR stations uses two-way communications between neighboring stations. In the fault-tolerant surface-code proposal by Fowler et al. [11] (which belongs to the third class QRs), the resource for each station was estimated to scale logarithmically with the distance, while the exact resource overhead was found to be sensitive to the parameters for various imperfections. The proposal by Munro et al. [12] focused on the correction of photon loss errors using quantum parity code (QPC) [21], but did not consider fault tolerance, as perfect gate operations were assumed in their analysis.
To design the fault-tolerant third class of QRs, where a teleportation-based error correction (TEC) protocol [22,23] is employed within each repeater station to correct both operational and photon loss errors using Calderbank-Shor-Steane (CSS) encoding. We quantitatively investigate the optimum resource requirements using a cost function and optimize it for different repeater parameters. A schematic view of the proposed architecture of the third class of QRs is presented in Fig. 1.

Fault-tolerant architecture.—Analogous to fault-tolerant quantum computers [26], fault-tolerant QRs should reliably relay quantum information from one repeater station to another in the presence of various imperfections. Unlike quantum computers, QRs do not require a universal gate set and it is sufficient to have CNOT gates, state initialization and measurement associated with the complementary basis of \{0,1\} and \{+,−\}. However, QRs are confronted by an important challenge from transmission loss, which is less severe in most models of quantum computation. To design the fault-tolerant third class of QRs, we consider the CSS codes for their fault-tolerant properties [26], in particular the compatibility with the TEC protocol that can efficiently correct not only operational errors, but also photon loss errors [22,23]. The \((n,m)\)-QPC [21] is a class of CSS codes with encoded qubits \(|0\rangle_L = \frac{1}{\sqrt{2}}(|+\rangle_L + |−\rangle_L)\) and \(|1\rangle_L = \frac{1}{\sqrt{2}}(|+\rangle_L − |−\rangle_L)\), where \(|±\rangle_L\) are given by

\[
|+\rangle_L = \frac{1}{2^{n/2}} (|00\ldots0\rangle_{12…m} + |11\ldots1\rangle_{12…m})^\otimes n, \\
|−\rangle_L = \frac{1}{2^{n/2}} (|00\ldots0\rangle_{12…m} − |11\ldots1\rangle_{12…m})^\otimes n. 
\]

The \((n,m)\)-QPC consists of \(n\) subblocks, and each subblock has \(m\) physical qubits. First, we define the Pauli operators, \(X_{ij}, Y_{ij}, Z_{ij}\) associated with the \((i,j)\)th qubit, where \(i = 1, \ldots, n\) is the row (subblock) label and \(j = 1, \ldots, m\) is the column label for the qubit. There is one logical qubit encoded in the \((n,m)\)-QPC, with logical operators \(\tilde{X} \equiv \prod_{i=1}^n Z_{ij}\) and \(\tilde{X} \equiv \prod_{j=1}^m X_{ij}\), where we may choose any \(j = 1, \ldots, m\) for \(\tilde{X}\) and any \(i = 1, \ldots, n\) for \(\tilde{X}\) [26]. The encoded states \(|0\rangle_L, |1\rangle_L, |+\rangle_L, |−\rangle_L\) can be prepared fault-tolerantly with suppressed correlated errors [25,27–29]. The encoded state is transmitted via an optical fiber to the neighboring repeater station followed by error correction and transmission to the next repeater station (Fig. 1).

Suppose that each transmitted physical qubit can reach the next QR station with probability \(\eta\), meanwhile suffering from depolarization errors. We apply TEC [22,23] to correct both photon loss and depolarization errors. The TEC procedure consists of Bell state preparation and Bell measurement at the encoded level [Fig. 1(b)], and both operations can be achieved fault-tolerantly without propagating errors within each encoding block [26]. The Bell measurement of two encoded blocks (received block \(R\) and local block \(S\)) can be achieved by an encoded CNOT gate followed by measurement of logical operators \(\tilde{X} \otimes \tilde{Z}\). More specifically, it consists of \(nm\) pairwise CNOT gates between \(R_{ij}\) and \(S_{ij}\), followed by \(2nm\) individual qubit measurements. Besides erasure errors, TEC can also correct operational errors from qubit depolarization (\(e_d\)), imperfect measurement (\(e_m\)), and noisy quantum gates (\(e_g\)), which can be captured by an effective error probability \(e = e_d + e_g/2 + 2e_m + O(e_{2,g,m}^2)\) acting on a single qubit for our fault-tolerant circuit designs [25].

In the presence of photon loss errors, each measurement may have three possible outcomes \(+1,−1,0\). Each qubit \(R_{ij}\) in the \(R\) block is measured in the \(X\) basis with outcome \(X_{ij}^R\) taking value \(+1\) for qubit state \(|+\rangle\), \(−1\) for qubit state \(|−\rangle\), and \(0\) if the qubit is erased due to transmission loss. Similarly, each qubit \(S_{ij}\) from the \(S\) block is measured in the \(Z\) basis with outcome \(Z_{ij}^S\) taking value \(+1\) for qubit state \(|0\rangle\), \(−1\) for qubit \(|1\rangle\), and \(0\) if the corresponding qubit in the \(R\) block \(R_{ij}\) is erased. The logical measurement outcomes depend on individual qubit measurement outcomes

\[
\tilde{M}_X^R = \text{sgn} \left[ \sum_{i=1}^n \left( \prod_{j=1}^m X_{ij}^R \right) \right], \quad \tilde{M}_Z^S = \prod_{i=1}^n \left( \text{sgn} \left[ \sum_{j=1}^m Z_{ij}^S \right] \right).
\]

with three possible values \(+1,−1,0\). Here \(\text{sgn}[\ldots]\) is associated with majority voting between \(\{±1\}\), and \(\prod\ldots\) is associated with the product of trinary outcomes. Ideally, in
the absence of errors, the outcomes should be \( \hat{M}_x^R = \tilde{X}^R \) and \( \hat{M}_z^R = \tilde{Z}^R \), which determine the Pauli frame \([22,23]\) of the encoded block after teleportation. In the presence of errors, however, the outcomes become \( \hat{M}_x^R = \alpha X^R \) and \( \hat{M}_z^R = \beta Z^R \), with \( \alpha, \beta = +1 \) for correct measurement, \(-1\) for incorrect measurement, and 0 for heralded failure of measurement. We obtain the probability distribution \([see \ Fig. 2(a)]\) \([25]\)
\[
p_{a,b} \equiv \text{Pr}[\hat{M}_x^R = \alpha X^R, \hat{M}_z^R = \beta Z^R],
\]
which can be used to evaluate the QR performance.

Quantum bit error rate and success probability.—We use the probability distribution to compute the success probability and quantum bit error rate (QBER) that characterizes the QR. Since the encoded qubit passes through \( N \) repeater stations, there are \( N \) pairs of measurement outcomes \((\hat{M}_x, \hat{M}_z)\). The success probability with no heralded failure of measurements is
\[
P_{\text{succ}} = (p_{1,1} + p_{1,-1} + p_{-1,1} + p_{-1,-1})^N.
\]

Given that all measurement outcomes have no heralded failure, there might be an odd number of incorrect measurements of \( \hat{M}_x \) (or \( \hat{M}_z \)), which induces an error if the receiver decodes the information by measuring \( \tilde{X} \) (or \( \tilde{Z} \)) of the received block. We define the QBER at the encoded level of the QR as the ratio of the probability of having an odd number of incorrect measurements of \( \hat{M}_x \) (or \( \hat{M}_z \)) to the probability of having no heralded failure. The QBER for \( \tilde{X} \) (or \( \tilde{Z} \)) measurement by the receiver is
\[
Q_{X/Z} = \frac{1}{2} \left[ 1 - \left( p_{1,1} + p_{1,-1} + p_{-1,1} + p_{-1,-1} \right)^N \right].
\]

Key generation rate.—For our QR, the raw key generation rate is \( 1/t_0 \), where \( t_0 \) is the time taken for TEC. For simplicity, we may use \( t_0 \) as a time unit in our analysis. The raw keys can be converted to secure keys through classical communication protocols involving error correction and privacy amplification \([1]\). Because of finite success probability and nonvanishing QBER, the asymptotic secure key generation rate is given by
\[\text{[30,31]}\]
\[
R = \max_{t_0} \left[ \frac{1}{t_0} P_{\text{succ}} \left( 1 - 2h(Q) \right), 0 \right],
\]
where \( Q = (Q_X + Q_Y)/2 \) and \( h(Q) = -Q \log_2(Q) - (1 - Q) \log_2(1 - Q) \) is the binary entropy function. In Fig. 2, we show that \( R \) can approach \( 1/t_0 \) for reasonable encoding size \((n \times m)\) with an appropriate repeater spacing \((L_0)\), because it is possible to achieve high \( P_{\text{succ}} \) and low \( Q \). The range of \((n, m)\) that yields a high key generation rate varies with \( L_0 \) and the total distance of communication \( L_{\text{tot}} = (N \times L_0) \). Hence, we need to optimize the repeater parameters, including the size of encoding block, repeater spacing, and secure key generation rate.

For each secret bit generated by the QR, we should consider the cost of both time and qubit resources \([32]\): (1) the average time to generate a secret bit is \( 1/R \), and (2) the total number of memory qubits needed for the QR scheme is \( 2nm \times L_{\text{tot}}/L_0 \) \([33]\). We introduce the cost function \( C \) to be the product of these two factors \( 2nm/R \times L_{\text{tot}}/L_0 \), in units of \( \text{[qubits/t bit]} \). Here the rate \( R \) implicitly depends on the control parameters of \((n, m, L_0)\). For given \( L_{\text{tot}} \), we can achieve the minimum cost:
\[
C(L_{\text{tot}}) \equiv \min_{n,m,L_0} \frac{2nm}{R} \times \frac{L_{\text{tot}}}{L_0},
\]

among all possible choices of \((n, m)\)-QPC and repeater spacing \(L_0\). We assume the following imperfections as we search for the optimal scheme: (1) operation error with probability \( e \), and (2) finite photon transmission with probability \( \eta = (1 - p_c)e^{-L_0/L_{\text{att}}} \) due to fiber attenuation \((L_{\text{att}} = 20 \text{ km})\) and coupling loss \( (p_c) \).

Numerical search for optimized strategy.—We search for optimized choices of \((n, m, L_0)\) for different values of \( L_{\text{tot}} \) with fixed imperfection parameters of \(\{e, p_c\}\). We run a numerical search for \(L_0\) and for a different number of qubits to obtain \(C(L_{\text{tot}})\), which should increase at least linearly with \(L_{\text{tot}}\). In Fig. 3, we show the variation of cost coefficient \((C = C(L_{\text{tot}}))\) with \(L_{\text{tot}}\), to illustrate the additional overhead associated with \(L_{\text{tot}}\). The cost coefficient can be interpreted as the resource overhead \((\text{qubits} \times t_0)\) for the creation of one secret bit over 1 km (with target distance \(L_{\text{tot}}\)).

For imperfection parameters of \(e = 10^{-3}\) and \(p_c = 0\), the algorithm picks only four different codes up to \(L_{\text{tot}} = 10000 \text{ km}\). When the code chosen by the algorithm changes (for example at 4500 km in Fig. 3), the product of \(L_0\) and \(R\) also jumps to an appropriate higher value, so that the cost coefficient varies continuously with \(L_{\text{tot}}\). In the presence of coupling loss \(p_c < 10\%\), the optimized values of \(L_0\) is within the range 1.4–2 km (Fig. 3) with total loss errors up to 20%; \(R_0\) is high \((0.6–0.85)\) because of the favorable QBER associated with the chosen codes.

The optimized cost coefficient for different operational error probabilities is shown in Fig. 3. When \( e \) decreases below \(10^{-3}\), the cost coefficient is dominated by photon
loss errors rather than operational errors, and does not decrease by a significant amount as $\epsilon$ decreases further. In a realistic scenario, photons are lost due to finite coupling losses besides fiber attenuation. In Fig. 3, we show that the QR scheme can tolerate coupling losses up to 10% for a reasonable overhead in the number of qubits. Numerical calculations indicate that the cost coefficient increases by $O(\text{poly} [\log(L_{\text{tot}})])$ [25]. Table I provide an estimate of the resource requirements of our code under different scenarios.

Experimental considerations.—To implement our QR scheme, it is crucial to fulfill the following two experimental requirements: (1) The coupling loss should be sufficiently low ($p_c \lesssim 10\%$), because if the transmission probability $\eta < 50\%$, then the probability that the receiver decoders the logical qubit will be exponentially small [34]. (2) The quantum repeater station should have hundreds of qubits with high fidelity operations. For ion trap systems, a single qubit gate error probability of $2 \times 10^{-5}$ [37], a two-qubit gate error probability of 0.007 [38], and a measurement error probability of $10^{-4}$ [39,40] have been demonstrated. There are also promising developments in NV centers [50,51], quantum dots [52,53], and Rydberg atoms [54,55] are also promising systems for quantum repeater implementations. Furthermore, with the advance of coherent conversion between optical and microwave photons [56], superconducting qubits may become an attractive candidate to realize our scheme as they can achieve both ultrafast quantum gates and high coupling efficiency.

Summary and outlook.—We have presented a new QR scheme belonging to the third class of QRs, which considers both fault tolerance and small encoding blocks. In comparison with the first and second classes of QR schemes, our QR scheme uses TEC within each QR station to correct both photon loss and operation errors. In particular, our QR scheme can tolerate finite coupling loss ($p_c \lesssim 10\%$) and achieve fault-tolerant operation with approximately hundreds of qubits per repeater station. This enables an improved key generation rate that is limited only by local gate operations. Our scheme requires smaller QR spacing compared to the previous classes of QRs and consequently the number of QR stations is higher by roughly an order of magnitude. But it is important to note that the key generation rate increases by more than 3 orders of magnitude, by eliminating the communication time between the repeater stations. In addition, we have
introduced a cost function to optimize the control parameters of our QR scheme, which can potentially be used as a criterion to compare all three classes of QRs as well as to search for more efficient quantum error correcting codes for quantum communication.

This work was supported by the DARPA (Quiness program), NSF, CUA, NBRPC (973 program), Packard Foundation, and Alfred P. Sloan Foundation. We thank Austin Fowler, Steven Girvin, Archana Kamal, Chris Monroe, Bill Munro, David Poulin, and Hong Tang for discussions.

*liang.jiang@yale.edu


[32] There is an overhead of ancillary qubits to enable the fault tolerant preparation of the encoded Bell pair. This overhead depends on the fault tolerant preparation scheme as discussed in Ref. [25]. To fix ideas, we will use the number of memory qubits $2mn$ in our calculations.
[33] Our repeater scheme is effectively a sequence of quantum erasure channels with forward-only communication between neighboring repeater stations, which has capacity $\max[0, 2\eta - 1]$ [35,36]. If $\eta < 1/2$, the channel capacity vanishes, which implies that the probability of faithful transmission between neighboring repeater stations cannot approach unity, and consequently the probability of faithful transmission over many repeater stations will decrease exponentially with the number of repeater stations.