PHY372: Numerical Simulations of All Photonics Quantum Repeaters

QiLin Xue

Contents

I. INTRODUCTION

Modern cryptography make the fundamental assumption involving the hardness of certain mathematical problems. Challenges related to factoring large numbers or resolving discrete logarithms serve as the basis for security in traditional cryptography - a foundation which, admittedly, has functioned well for many years. However, with the advent of quantum computing and the potential for exponentially increased computational power, many of these classical systems could be cracked. While research into post-quantum cryptography is being made, their security cannot be proven.

Quantum cryptography works on principles that are fundamentally different from their classical counterparts. One key aspect where they differ is that quantum cryptography uses the features of quantum systems, specifically superposition, and the fact that these states cannot be cloned, protecting them against potential eavesdroppers. Techniques such as the decoy state protocol are unique to quantum cryptography and promise to unlock a higher level of safeguarding information. A basic method within this field is the use of the BB84 protocol with Einstein-Podolsky-Rosen (EPR) pairs, which offers fundamentally secure encryption, as any attempt to intercept communication disturbs the system and reveals the eavesdropper.

The strength of quantum cryptographic systems also rests on their ability to distribute EPR pairs across large distances - a capability that becomes a technical challenge due to channel loss and noise that increases with distance. This problem, for classical signals, is typically resolved using classical repeaters that amplify the signals to overcome loss and degradation in the transmission medium. Yet, this approach fails when applied to quantum signals due to the no cloning theorem that prevents the replication of quantum states, making the traditional signal-boosting methodology impossible for quantum information transmission.

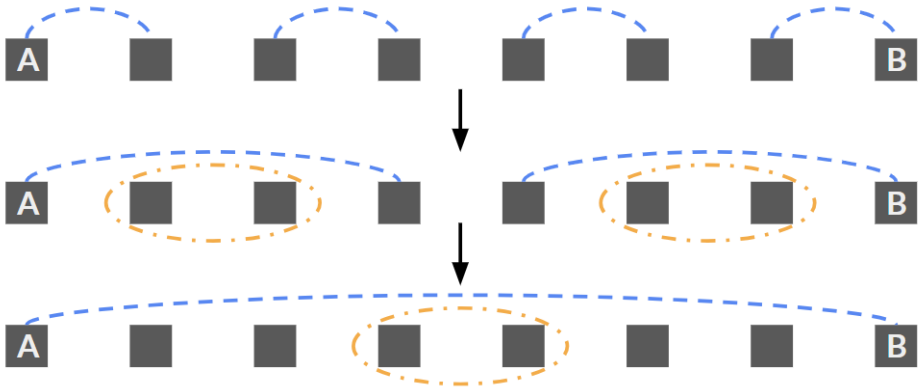


FIG. 1: A schematic of the quantum repeater with 8 repeater stations. The dashed blue lines show entangled pairs. When a bell state measurement (BSM) are done, shown in orange, entanglement swapping occurs.

This is where quantum repeaters come into play. Quantum repeaters, unlike their classical counterparts, do not amplify the quantum signal, but instead, creates long-distance entanglement linking distant nodes through a process known as entanglement swapping, as shown in figure 1. Repeater stations are distributed between Alice and Bob (labeled A and B) and entanglement is created between adjacent repeater stations. When a BSM is performed between adjacent repeater stations that aren't entangled together, the two qubits at these stations collapse into its basis states, but the two other qubits they were entangled to, are now entangled to each other. This process is known as entanglement swapping[1].

A. Motivation

The standard repeater protocol is impractical for two major reasons. First, it requires a quantum memory, as each repeater node needs to wait for nearby nodes to be finished before performing the bell state measurements. Second, it requires the ability to convert between stationary qubits (where one can apply quantum operations) and flying qubits (where one can send from one physical location to another). This is because the stationary qubits at the nodes need to be sent to the same location in order to perform the BSMs.

While there are suggestions for how to create a quantum memory, such as in the DLCZ protocol[1], the second

problem is very hard. In fact, it is listed as part of DiVencenzo's two extra conditions for a quantum computer[2]. Therefore, building a successful quantum repeater may be just as hard as building a quantum computer.

Luckily, there are methods to get around this by modifying the repeater architecture using photonics to avoid the problems associated with quantum memory. Similar techniques are also employed in photonics-based quantum computing.

II. ALL-PHOTONICS QUANTUM REPEATER

A. Brief Overview

The all photonics quantum repeater makes several improvements from the basic quantum repeater. First, it makes use of several channels for creating entanglement. Since creating these EPR pairs is probabilistic, using several channels ensures a higher chance of success. Failure only occurs if the photon gets lost in all the channels. Error correction techniques, which are discussed in detail later, are able to still guarantee successful entanglement even if only one of the channels at each repeater station successfully receive a photon. Most importantly though, the method

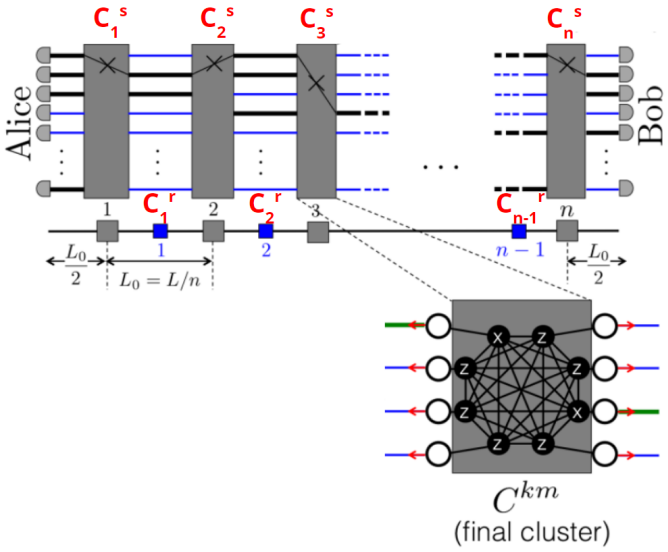


FIG. 2: A schematic of the all-photonics quantum repeater. Each of the n repeater stations is labeled as C_i^s where $1 \leq i \leq n$. These stations send entangled photons to the receiver stations C_i^r where $1 \leq i \leq n-1$ located between adjacent repeater stations. In the above diagram, a total of $m = 4$ parallel channels are used in the final cluster[3][4]

of creating entangled pairs do not require memory at all. Borrowing inspiration from the time-reversed EPR protocol (which ultimately leads to material-device-independent QKD), the intuition is that BSMs are performed by first creating entanglement and then performing measurements. However, the same result can be achieved by first creating all the necessary entanglements and then performing the basis measurements[3]. Figure 2 also shows a schematic of what each repeater source station looks like. Two X measurements are done to two successful modes, and $2m-2$ Z measurements are done to the rest. Z measurements have the effect of removing the node, so it acts as a clean up.

In between each of the n repeater nodes (receiver nodes) lie source nodes, as shown in figure 2. All of Alice, Bob, and the $n-1$ source nodes prepares EPR pairs and sends a photon from each pair to the nearest receiver nodes. For Alice and Bob, they only send one photon from each pair and keep the other. The photons that they keep will eventually be maximally entangled with each other[3].

B. Constructing a Graph

A photonic cluster state is a graph $G(V, E)$ that is prepared by initializing each vertex with a photon prepared in the $|+\rangle$ state and preparing the controlled edge operation of

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_Z \tag{1}$$

For example, a fully connected clique of three nodes will become

$$\frac{1}{\sqrt{8}} \cdot (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \tag{2}$$
$$\mapsto (|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle) \quad \text{qubit 2-3} \tag{3}$$
$$\mapsto (|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle + |111\rangle) \quad \text{qubit 1-3} \tag{4}$$
$$\mapsto (|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle) \quad \text{qubit 1-2} \tag{5}$$

where the most significant bit is marked as qubit 1. The advantage of this process is that the state is invariant under the operator

$$\mathcal{O}_i = X_i \prod_{j \in \mathcal{N}(i)} Z_j, \tag{6}$$

where $\mathcal{N}(i)$ is the set of neighbours of qubit i. In the 3-qubit example, we can WLOG take $i = 1$ and compute,

$$(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle) \tag{7}$$
$$\mapsto (|000\rangle - |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle) \tag{8}$$
$$\mapsto (|100\rangle - |101\rangle - |110\rangle - |111\rangle + |000\rangle + |001\rangle + |010\rangle - |011\rangle), \tag{9}$$

where we can verify is equal to the original state by simple term matching. This invariance property allows *indirect* measurement. If any node $n \in \mathcal{N}(i)$ was lost, we can still infer the result of Z_n by performing the operation $X_i \prod_{j \in \mathcal{N}(i), j \neq n} Z_j$. This gives a lot of potential for error correction by creating several correlations between qubits.[5]

In fact, it can be shown that these are two equivalent definitions. That is, any graph $G = (V, E)$ that satisfies

$$\mathcal{O}_i |G\rangle = |G\rangle, \forall i \in V \tag{10}$$

can be prepared in the method described above.

C. Photonic Tree

One major challenge of an all photonics quantum repeater is to construct these trees. Specifically, to protect against loss via error correction, we wish to construct figure 3[4] where the attached tree has a branching vector of $\vec{b} = [b_0, b_1, \ldots, b_d]$. Here, d is the depth of the tree. It turns out that the optimal depth is $d = 2$, as depicted in figure 3. After this is set up, X-measurements are done on the $2m$ qubits surrounding the central qubit and the $2m$ qubits that form the head of the error correcting trees. Finally, a Y-measurement is done on the central qubit, turning the graph into a cluster state[4]. The specific setup of how this can be done is discussed in [6].

This report will discuss and analyze two different ways of constructing such a graph. One using a naive method and one using an improved version.

D. Building a Cluster State

The general idea is to create the needed GHZ states, and combine them to create intermediate states. The states are combined using Fusion II gates which removes two photons in the process[6]. That is, combining two states of x photons will result in a state with $2x - 2$ photons. That is, if $N(\ell)$ is the number of photons in each cluster tree at the feed-forward stage ℓ, then it satisfies the recursive relationship

$$N(\ell) = 2N(\ell - 1) - 2. \tag{11}$$

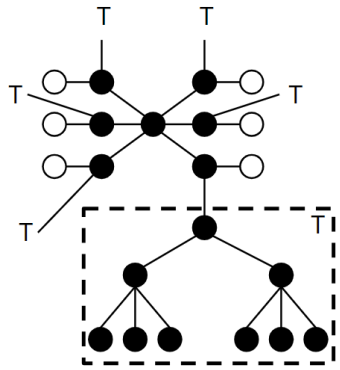


FIG. 3: The quantum tree that needs to be constructed at each repeater node. It consists of a central node in the middle connected to $2m$ nodes. Each of these nodes are connected to a tree T and an outer node (which is the qubit that is transmitted between stations). The tree depicted in this figure has a branching vector of $\vec{b} = [2, 3]$ and a depth of $d = 2$.

Using the initial condition of $N(0) = 3$, we obtain the maximum possible number of photons in the final stage, after k feed-forward steps, as

$$N(k) = 2^k + 2, \tag{12}$$

which can be verified via induction. Note that this is the maximum number because additional measurements can be done in the Z-basis which will destroy photons. If a $\vec{b} = [b_0, b_1]$ tree is attached to the central cluster, then the total number of photons is given by

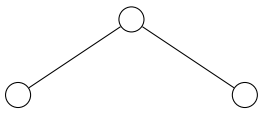
$$2m(b_0 b_1 + b_0 + 1) + (1 + 4m) \tag{13}$$

where $b_0 b_1 + b_0 + 1$ is the number of photons on each tree and $1 + 4m$ is the number of photons in the central cluster. This gives us a restriction relating b_0, b_1, m, k together,

$$2^k + 2 \geq 2m(b_0 b_1 + b_0 + 1) + (1 + 4m). \tag{14}$$

E. Basic Mechanisms

The fundamental building block of creating these cluster states is with Greenberger-Horne-Zeilinger (GHZ) states, is typically given by the maximally entangled state[6],



represented by the graph $G(V = 3, E = 2)$, i.e. a linear chain of three qubits. The probability of successfully generating a GHZ state is[4]

$$P_{\text{GHZ}} = \frac{1}{32}\left[\eta_s \eta_d (2 - \eta_s \eta_d)^3\right]^3 \tag{15}$$

where $\eta_s \eta_d$ characterizes the efficiency of the source detector, and should be close to unity. The transmittance of these GHZ states are is given by

$$\eta_{\text{GHZ}} = \frac{\eta_s \eta_d}{2 - \eta_s \eta_d}. \tag{16}$$

The probability that the photons survive on the chip in a given clock cycle is given by

$$P_{\text{chip}} = e^{-\beta \tau_s c_{\text{ch}}} \tag{17}$$

where c_{ch} is the speed of light on the chip, τ_s is the feed-forward time on the chip, and β is the on-chip loss coefficient. These parameters can be picked such that the probability the phootn survives in the fiber in one clock cycle, $P_{\text{chip}} = e^{-\alpha \tau_f c_f}$, is the same. Here, α is another loss coefficient and τ_f, c_f are the feed-forward time and speed of light in the fiber, respectively.

III. NAIVE APPROACH

A. Probability Computation

The general idea is to create the needed GHZ states, and combine them to create intermediate states. The states are combined using Fusion II gates which removes two photons in the process[6]. That is, combining two states of m photons will result in a state with $2m-2$ photons.

However, because creating GHZ states and performing fusion operations are probabilistic, we may need to attempt these operations with multiple copies at each stage. That is, if n_{GHZ} GHZ states are attempted, the probability that at least one of them is successful is given by

$$P_0 = 1 - (1 - P_{\text{GHZ}})^{n_{\text{GHZ}}}$$

where $1 - P_{\text{GHZ}}$ is the probability that creating a GHZ state fails, so $(1 - P_{\text{GHZ}})^{n_{\text{GHZ}}}$ is the probability that all the GHZ state creation attempts fails. The probability of fusion being successful is given by

$$Q_\ell = \frac{1}{2} \cdot (\eta_{\text{GHZ}} P_{\text{chip}}^\ell)^2 \tag{18}$$

where $\frac{1}{2}$ is the probability under ideal circumstances, and P_{chip}^ℓ is the probability a photon survives on the chip through ℓ feed-forward steps. Because we need two photons at this stage, this is squared. The probability of creating the cluster C_i^ℓ is given by the recursive formula

$$P_\ell = 1 - (1 - P_{\ell-1}^2 Q_\ell)^{n_B}, \tag{19}$$

where n_B is the number of attempts to create that cluster. For each attempt, the success probability is given by $P_{\ell-1}^2 Q_\ell$ because we need both previous cluster states to be available, and the fusion needs to be successful.

In the final stage, a total of $4m+1$ measurements are made, and the probability of those measurements succeeding is given by

$$P' = (\eta_{\text{GHZ}} P_{chip}^{k+1})^{4m+1} \tag{20}$$

since each photon needs to survive $\ell = k+1$ feed-forward cycles. Because these measurements are done on several copies (specifically n_{meas} copies), the probability that at least one of them succeeds is given by

$$P_{c1} = 1 - (1 - P_k P')^{n_{\text{meas}}}. \tag{21}$$

Note that in the original paper, the probability was written as $P_{\text{c1}} = 1 - (Q_k P')^{n_{\text{meas}}}$. This is a typo. Because there are n repeater stations, the total probability of all of them succeeding is given by

$$P_{\text{cn}} = P_{\text{c1}}^n. \tag{22}$$

B. Optimization

A total of $6n_{\text{GHZ}}$ photons are needed to create the GHZ states. In each of the k stages, we need 2 ancillary photons for each of the n_B attempts. A total of n_{meas} clusters are attempted, so the total number of photon sources needed at each repeater node is given by

$$N_s = 6 n_{\text{GHZ}} n_{\text{meas}} \cdot (2n_B)^k$$

photons. Given a specific N_s, we can find the optimal probability P_{cn} by optimizing the three user parameters: $n_B, n_{\text{meas}}, n_{\text{GHZ}}$. The probability computations are straightforward to do, so this can be done via a grid search. The result of the optimization is shown in figure 4.

IV. IMPROVED APPROACH

The major drawback of the naive approach is that there is a lot of wasted clusters. For example, if there were three successful intermediate clusters created, only one would go towards the next step. The other two would be wasted,

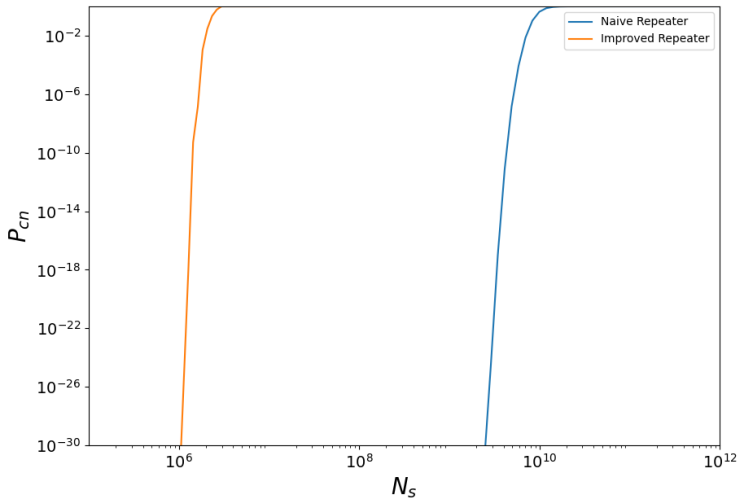


FIG. 4: A plot of P_{cn}, the probability of successfully generating the cluster states in all n repeater stations. Typical parameter values of $k = 7, m = 4$ were used. Note that the naive repeater uses almost 10^4 times more photon sources than the improved repeater architecture.

even if it might be needed somewhere else. The improved approach addresses this problem by creating a bank of intermediate cluster states, and fusion steps can choose between any of them.

Additionally, another major improvement was to move the $4m + 1$ basis measurements to be much earlier on, as switching the order of basis measurements and fusion II operations do not matter[4].

If we start off with N_s photons, then we're attempting to create $\lfloor N_s/6 \rfloor$ GHZ states, each with a probability of P_{GHZ}. Since these probabilities are identical and independent, the distribution of GHZ states follow a binomial distribution,

$$B(x, \lfloor N_s/6 \rfloor, P_{\text{GHZ}}) \tag{23}$$

These GHZ states are distributed into 2^k banks $C^0_{i_1,\ldots,i_k}$. These banks are then paired up, and fusion II operations are done to create the 2^{k-1} possible different $C^1_{i_1,\ldots,i_{k-1}}$ cluster states, which are then placed in their respective banks, and this process is continued.

Mathematically, the total number of $C^{\ell m}$ states can be approximated by the recursive relation:

$$B(\min(y_1, y_2), \lfloor N_s/6 \rfloor, P_{\text{GHZ}}) \tag{24}$$

where y_1, y_2 are the number of states in the bank for the previous two cluster states, which follows the same distribution. This can be simulated with a Monte Carlo simulation.

Note however that even in the Monte Carlo simulation, there are a few simplifications. Since the $4m + 1$ basis measurements are done on the GHZ states before any fusion gates are applied, so the banks that contain them will have fewer photons since measurements are also probabilistic. Therefore, the banks that will be measured should be provided with $1/(P_{\text{chip}}\eta_{\text{GHZ}})$ more GHZ states, to counteract this effect. However, because $P_{\text{chip}}\eta_{\text{GHZ}}$ is near unity, we can get the same results as the paper without making this adjustment.

V. RATE CALCULATIONS

The key rate, in terms of bits per mode, can be computed as[4]

$$R = \frac{P_{\text{cn}} P_{\text{meas}}}{N_{\text{parallel}}} \tag{25}$$

where N_{parallel} is the number of parallel fiber links between adjacent repeater noes. For the improved scheme, which is what this section will cover, we have $N_{\text{parallel}} = 2m$. The reason it is per mode is because while increasing the number

of parallel channels could seemingly increase the key rate without bound, a repeaterless architecture could also increase its key rate with access to several channels, so this allows the key rate to be normalized. The value of N_{parallel} is computed differently for the naive scheme, as well as other things, which will be discussed later. Additionally, P_{meas}

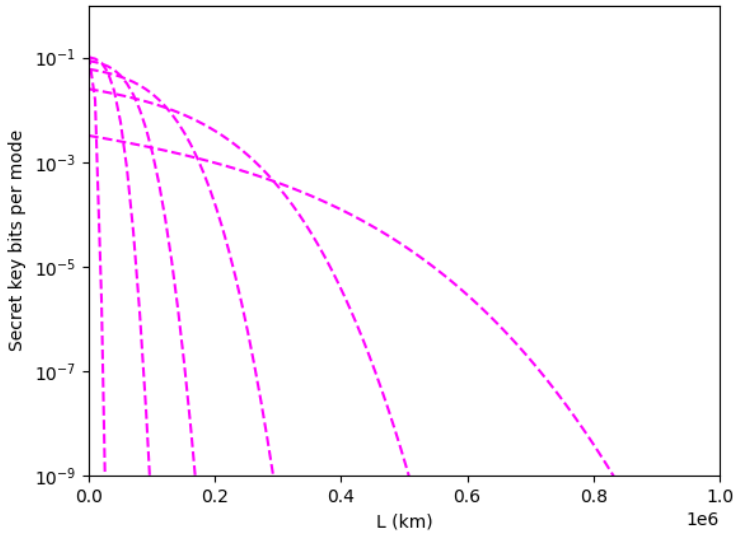


FIG. 5: They key rate as a function of distance for $n = 1, 10, 24, 56, 133, 314$, where $n = 1$ has the fastest drop off and $n = 314$ has the slowest drop off. Note that for each distance between Alice and Bob, there is a finite optimal value of the number of repeater stations n, characterized by an envelope function.

is the probability that Alice and Bob, who are located at opposite ends of the quantum repeater system, are all able to obtain a successful detection on at least one of the parallel channels. For each repeater station, a total of $2m-2$ Z-basis measurements are made, and a single X-basis measurement. These all need to be successful, and at least one of the m Bell state measurements in the $n-1$ sites between the repeater nodes also need to be successful, as well as the measurements at the two ends. This gives

$$P_{\text{meas}} = P_Z^{2(m-1)n} P_X^{2n} \left[1 - (1 - P_B)^m\right]^{n-1} P_{\text{end}}^2. \tag{26}$$

Finally, note that N_{parallel} is the number of modes, which is why we divide it. To characterize $P_Z, P_X, P_B, P_{\text{end}}$ we need to first determine the loss rate of qubits. They are different depending on whether they are outer qubits, where their loss rate is

$$\epsilon_{\text{trav}} = 1 - \eta^{1/(2n)} P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c$$

and the loss rate for inner qubits is given by

$$\epsilon_{\text{stat}} = 1 - \eta^{1/n} P_{\text{fib}} P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c.$$

Note that for outer qubits, the transmissivity is given by $\eta^{1/(2n)}$ instead of $\eta^{1/n}$. This is because the distance they need to travel is only to halfway between each repeater node, i.e. a distance of $L/(2n)$. Inner qubits on the other hand, are transmitted to nearby repeater stations using classical channels, so there is an additional delay characterized by P_{chip}. The probability of a successful X and Z measurements are different, and are given by

$$P_X = \xi_0 \tag{27}$$

$$P_Z = (1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}} \xi_1)^{b_0} \tag{28}$$

where ξ_i is given by the recursive relationship

$$\xi_i = 1 - \left[1 - (1 - \epsilon_{\text{stat}})(1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}} \xi_{i+2})^{b_{i+1}}\right]^{b_i} \tag{29}$$

for $i \leq \ell$ and $\xi_{\ell+1} = b_{\ell+1} = 0$. For a tree with a branching vector of $\vec{b} = [b_0, b_1]$, we can compute

$$\xi_0 = 1 - [1 - (1 - \epsilon_{\text{stat}})(1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}}\xi_2)^{b_1}]^{b_0} \tag{30}$$
$$= 1 - [1 - (1 - \epsilon_{\text{stat}})^{b_1+1}]^{b_0} \tag{31}$$

where we note that $\xi_2 = 0$ and we can also compute

$$\xi_1 = 1 - [1 - (1 - \epsilon_{\text{stat}})(1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}}\xi_3)^{b_2}]^{b_1} \tag{32}$$
$$= 1 - [1 - (1 - \epsilon_{\text{stat}})]^{b_1} \tag{33}$$
$$= 1 - \epsilon_{\text{stat}}^{b_1} \tag{34}$$

where we used the fact that $b_2 = 0$. Using these, we can write explicit formulas for P_X and P_Z. Specifically,

$$P_X = 1 - [1 - (1 - \epsilon_{\text{stat}})^{b_1+1}]^{b_0} \tag{35}$$
$$= 1 - [1 - (\eta^{1/n} P_{\text{fib}} P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c)^{b_1+1}]^{b_0} \tag{36}$$

and

$$P_Z = (1 - \epsilon_{\text{stat}} + \epsilon_{\text{stat}} - \epsilon_{\text{stat}}^{b_1+1})^{b_0} \tag{37}$$
$$= (1 - \epsilon_{\text{stat}}^{b_1+1})^{b_0} \tag{38}$$
$$= \left(1 - \left(1 - \eta^{1/n} P_{\text{fib}} P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c\right)^{b_1+1}\right)^{b_0}. \tag{39}$$

Each bell state measurement has a success probability of

$$P_B = \left[\frac{1}{2}(\eta_s \eta_d)^2 + \frac{1}{4}(\eta_s \eta_d)^4\right] \cdot \left(P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c\right)^2 \cdot \eta^{1/n} \tag{40}$$

where the first factor evaluates to around $\frac{3}{4}$ which is the upper limit of the success probability of a bell state measurement, and the other parameters characterize the loss associated with transmitting two photons a distance of $L/(2n)$ through a lossy channel[4].

The probability of detecting a photon in one of the m channels is given by ϵ_{trav} so the probability of at least one successful detection at the end is given by

$$P_{\text{end}} = 1 - (1 - \eta^{1/(2n)} P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c). \tag{41}$$

This gives us a formula for the rate per mode[4]. For a given m, k, b_0, b_1, the number of repeater stations n can be optimized depending on the total distance of the repeater system. See figure 6. Notice that there is an envelope function. That is, the optimal n changes depending on the length. For a given k we can optimize m, b_0, b_1, n using grid search to obtain the maximum rate where condition 14 is imposed. The optimal parameters for both the naive approach and the improved approach is summarized in table I and the experimental values of device parameters are listed in reference [4].

Using these optimal parameters, we can plot the optimal key rate at various distances, for different k values. The magenta line gives the best-known key rate where no repeaters are used, given by[4]

$$R_{\text{PLOB}} = -\log_2(1 - \eta) \tag{42}$$

where η has the same dependence on L as in the repeater architecture. Note that in the improved scheme, a better key rate can be achieved for $k = 7, 8, 9, 10$ for sufficiently long distances.

A. Naive Approach

In the naive approach, there are a few changes.

- Instead of having $2m$ parallel channels, the number of parallel channels change to

$$N_{\text{parallel}} = 2m(b_0 b_1 + b_0 + 1). \tag{43}$$

That is, all the qubits part of the attached trees become outer qubits and form channels.

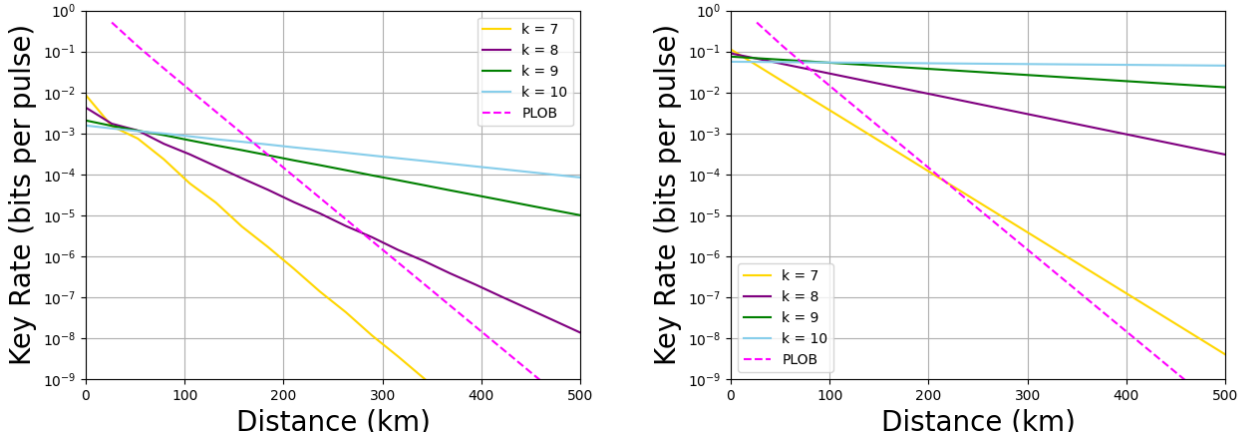


FIG. 6: Key rate as a function of distance at various values of k for the naive and improved repeater schemes. The magenta line shows the best known repeaterless architecture. Note that in both the naive and improved scheme, the slopes are smaller than the magenta slope. This means that at sufficiently large distances, the repeater architecture will beat the repeaterless one. However, the improved architecture is able to beat the repeaterless one much faster.

- Because the mentioned qubits become outer qubits, they are transmitted through quantum channels instead, so all instances of ϵ_{stat} can be replaced with ϵ_{trav}.
- Bell state measurements are done with less efficiency, and the success probability is given by

$$P_B = \frac{1}{2} \cdot \left(P_{\text{chip}}^{k+2} \eta_{\text{GHZ}} \eta_c \right)^2 \cdot \eta^{1/n} \tag{44}$$

instead.

k	m_{naive}	$\vec{b}_{\text{naive}}$	R_{naive}	m_{improved}	$\vec{b}_{\text{improved}}$	R_{improved}
7	5	$[3,2]$	1.91×10^{-8}	4	$[4,2]$	3.87×10^{-6}
8	8	$[4,2]$	6.13×10^{-6}	5	$[5,3]$	2.98×10^{-3}
9	11	$[5,3]$	5.77×10^{-4}	7	$[6,4]$	2.71×10^{-2}
10	13	$[7,4]$	7.42×10^{-4}	8	$[10,5]$	4.93×10^{-2}

TABLE I: A summary of the optimization results for both the naive and improved architecture at various values of k. A distance of $L = 300$ km is used.

The optimal parameters in table I mostly agree with the ones found by Pant et al.[4], with a few minor differences. In the naive scheme, for $k = 10$, the original authors found the optimal parameters to be $m_{\text{naive}} = 12$ while keeping the same $\vec{b}$. The rate using $m = 12$ is $R = 7.26 \times 10^{-4}$, which is only a 2% difference. Perhaps the extra resources needed for only a 2% improvement is not necessary, or the original authors did not consider this case.

For the improved scheme in the $k = 9$ case, the original authors found $m_{\text{improved}} = 6$ and $\vec{b}_{\text{improved}} = [7,4]$. This gives a rate of 2.70×10^{-2}, which is an even smaller percent difference of 0.4% from the one I computed. This difference could be attributed to different ways of optimizing the number of repeater stations n, i.e. computing the envelope function, as it is not exact. Furthermore, this small of an error will be practically not noticeable as uncertainties in device parameters would likely lead to larger percent errors.

VI. CONCLUSION

In conclusion, this report has discussed the concept of quantum repeaters, specifically focusing on the all-photonics quantum repeater. We have explored the motivation behind the development of quantum repeaters and the challenges they aim to address. We have also described the basic mechanisms and construction of the all-photonics quantum repeater, including the creation of cluster states and the use of fusion gates.

Two different approaches to constructing the all-photonics quantum repeater have been presented: a naive approach and an improved approach. The naive approach involves creating GHZ states and combining them to generate the necessary cluster states, while the improved approach optimizes the use of intermediate cluster states to minimize wastage. We have discussed the probability computations and optimization strategies for both approaches, as well as compared their key rates at different distances. It was found that the improved approach generally outperforms the naive approach, achieving higher key rates for a given distance.

It is important to note that this report has only scratched the surface of the topic of quantum repeaters. There are many other aspects and variations of quantum repeaters that have not been explored here, but have been investigated by the scientific community. Further research and development in this area are likely to lead to advancements in quantum communication and cryptography, which have the potential to revolutionize information security and enable secure communication over long distances. The study of quantum repeaters is vital in the quest for practical quantum communication networks.

VII. SPECIAL THANKS

I'd like to extend a special thanks to both Professor Hoi-Kwong Lo and Dr. Jie Lin for their time mentoring me through this course.

---

[1] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413–418, November 2001.
[2] David P. DiVincenzo and IBM. The physical implementation of quantum computation. 2000.
[3] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature Communications*, 6(1), April 2015.
[4] Mihir Pant, Hari Krovi, Dirk Englund, and Saikat Guha. Rate-distance tradeoff and resource costs for all-optical quantum repeaters. *Physical Review A*, 95(1), January 2017.
[5] Michael Varnava, Daniel E. Browne, and Terry Rudolph. Loss tolerance in one-way quantum computation via counterfactual error correction. *Physical Review Letters*, 97(12), September 2006.
[6] Ying Li, Peter C. Humphreys, Gabriel J. Mendoza, and Simon C. Benjamin. Resource costs for fault-tolerant linear optical quantum computing. *Physical Review X*, 5(4), October 2015.