Assessing the Practicality of a Simple Multi-node Quantum Repeater

by

Christian Mastromattei

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics

Waterloo, Ontario, Canada, 2017

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

This thesis assesses the theoretical performance of a realistic multi-node quantum repeater that is implementable with current technology. A quantum repeater, by definition, allows for communication rates in a channel to be larger than what is fundamentally possible over a loss only channel.

We consider a simple, one-way, multi-node quantum repeater that utilizes entanglement swapping in the absence of any quantum error correction or entanglement purification. We create a theoretical model of the quantum repeater, incorporating the imperfections of each component within the system, to get an accurate key rate using current, viable state-of-the-art experimental parameters. Our main goal is to benchmark the performance of this specific multi-node quantum repeater. We compare the performance of this multi-node system to that of a single node repeater, which has been previously analysed for this architecture. We are interested to see if there is an advantage for introducing more nodes in this type of system. We also provide some suggestions for improving the key rate performance.

This thesis is structured as follows: Chapter 1 introduces the problem and provides motivation for this thesis. Chapter 2 provides relevant background information pertaining to this thesis. Chapter 3 is a comprehensive analysis of our theoretical model and discusses the results. Chapter 4 concludes the thesis.

Acknowledgements

There are many people I would like to thank but, for the sake of brevity, I will keep this short. First, I would like to thank my supervisor Norbert Lütkenhaus for all of the support and insightful discussions over the past two years. I owe many thanks to my officemate Filippo Miatto for the many helpful discussions and clarifications. As well, a thanks to all the members in the OQCT group and IQC community that I have had the pleasure of meeting. Being surrounded by so many talented individuals has made my time here very enjoyable. Lastly and without a doubt most importantly, I would like to thank my parents. Without their love and support, I certainly would not be where I am today.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The recent advances in the field of quantum information have produced many fascinating and novel technologies. While many of these technologies are still in their infancy, having yet to be physically implemented, some quantum technologies, mainly *quantum key distribution* (QKD), have already been commercialized [43].

Despite QKD being a more mature technology compared to its quantum counterparts, it still faces a menacing problem. Long distance communication has not been realized, with current records on the order of a few hundred kilometers [17]. This limitation is a consequence of the loss experienced by photons as they travel through media. It has recently been shown by Pirandola, Laurenza, Ottaviani, and Banchi that there is a fundamental upper bound on the quantum communication capacity of a pure-loss bosonic channel. For a channel with transmissivity η, it is given by

$$R_{PLOB} = -\log_2 [1 - \eta] \tag{1.1}$$

bits per channel use per mode [38]. For high channel losses, as is the case for long communication lengths, this rate scales linearly with η. This fundamental bound implies that any QKD protocol using only direct transmission is limited in performance and cannot generate a key rate per mode higher than this bound. There needs to be some solution to overcoming this bound for QKD to ever be implemented on an intercontinental scale.

A proposed solution for extending QKD distance is to implement a *trusted node network* [14]. Nodes can be implemented in a mesh network, allowing end parties to be connected via some path in the network. Key transport from end-to-end users can be done using a one-time pad with established keys generated between relays. Encryption and decryption is performed at each relay, allowing a key to be effectively transported from end-to-end in the network. The issue with this system is the fact that these stations must be trusted, as to not leak information to any potential eavesdropper. This solution is not ideal, since this poses a serious security risk. Ultimately, we want to avoid this issue of having to trust each station.

A proposed solution to overcoming this problem is to implement a *quantum repeater* [12]. A quantum repeater, by definition, allows for communication at a rate higher than what is fundamentally achievable over direct transmission via a loss only channel. There have been a wide variety of proposed quantum repeater schemes in literature. Some schemes are based on entanglement swapping, entanglement purification, or error correcting codes [12, 10, 22].

This thesis investigates and analyses a specific simple, multi-node quantum repeater scheme that can be implemented with current technologies. It is based on a one-way entanglement swapping scheme with no quantum error correction. In the absence of entanglement purification it is similar to the scheme in [12]. This multi-node quantum repeater is an extension of the single-node system recently analysed in [30]. We provide benchmarking for this proposed system to see if it is a viable solution for a practical quantum repeater. We also compare its performance to that of a similar single-node quantum repeater to see if it is advantageous to introduce additional nodes. It should be noted that to date, no one has yet experimentally achieved a key rate higher than R_{PLOB}. The following chapters provide relevant background information, description and analysis of the system, and concluding remarks.

Chapter 2

Background

In this chapter we discuss some of the basic ideas of quantum mechanics, quantum key distribution and quantum repeaters.

2.1 Quantum mechanics

The majority of this section is derived from [35] and [23], two standard introductory textbooks on quantum information theory.

Quantum states and operators

A *quantum state* or *state vector* in an isolated system is described by a unit vector in a complex Hilbert space, often referred to as the *state space*, denoted by $\mathcal{H}$. In quantum mechanics it is often convenient to work with the *Dirac notation*, where quantum states are denoted by *kets* $|\psi\rangle$. *Dual vectors* are obtained by the complex-conjugation of kets and are denoted by *bras* $\langle\psi|$.

In a closed system, an *evolution operator* evolves a state vector to another state vector in the same state space. To be a valid physical evolution operator, it must *unitary* and must be *Hermitian*. By definition a *unitary operator* U must satisfy the condition $U^\dagger U = 1$. A *Hermitian operator* satisfies the property $U^\dagger = U$. Any *observable* satisfies these two properties and must be positive semi-definite to ensures eigenvalues are real and positive. Mathematically, a natural description of an operator is a matrix.

Measurements

A measurement is described by a set of *Kraus operators*, denoted by $\{M_i\}$. If a system is in the state $|\psi\rangle$ prior to measurement, the probability of measuring the i-th outcome is given by

$$p_i = \langle\psi|M_i^\dagger M_i|\psi\rangle. \tag{2.1}$$

After the measurement outcome i is known to an observer, the final state becomes

$$|\psi\rangle_i = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}. \tag{2.2}$$

Any set of measurement operators must satisfy the *completeness relation*, given by

$$\sum_i M_i^\dagger M_i = I. \tag{2.3}$$

The completeness relation ensures the probabilities p_i sum to 1. The simplest measurement operators we can define are *projective measurements* or *von Neumann measurements.* Projectors are self-adjoint operators satisfying the property $M_i^2 = M_i$. By definition projective measurement elements are orthogonal, projecting quantum states into orthogonal subspaces. At most the set $\{M_i\}$ can contain d elements, where d is the dimension of the Hilbert space being measured. We can generalize the measurement operators by defining a set $\{F_m\}$, such that $F_m = M_m^\dagger M_m$. We call this set a *positive value-operator measure (POVM)*. POVM elements are not necessarily orthogonal, implying there can be more elements in the set set $\{F_m\}$ than the size of the original Hilbert space.

Qubits

The *qubit* is commonly used in quantum information. It can be thought of as the quantum analogue of the classical bit. Abstractly, it is a quantum state in a two-dimensional Hilbert space. In general, any qubit can be described by the following mathematical representation

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.4}$$

where $|0\rangle$ and $|1\rangle$ form any[1] orthonormal basis in the state space, and α and β are complex numbers, called *amplitudes*, associated with the basis states. Since the qubit state vector

[1] Not to be confused with the explicit representation of $|0\rangle$ and $|1\rangle$ in the computational basis.

must have unit norm, $|\alpha|^2 + |\beta|^2 = 1$ must always hold. We define the *computational basis* or *Z basis* by the two basis vectors

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.5}$$

The *diagonal basis* or *X basis* is defined by the two bases vectors

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), |-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right). \tag{2.6}$$

These two bases will be used throughout this thesis. The *Pauli matrices* are defined as

$$\hat{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \hat{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \text{ and } \hat{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.7}$$

which, along with the two-dimensional identity matrix I_2, form a basis for any operator in the two-dimensional Hilbert space.

Density matrix

It is often convenient to work with the *density matrix* formalism for quantum states. So far we have only described quantum states as ket vectors. In the density matrix formalism, quantum states are described by density matrices ρ. A ket vector is written as a density matrix by taking the outer product with the dual bra vector

$$\rho = |\psi\rangle\langle\psi|. \tag{2.8}$$

All of the quantum states we have considered so far are *pure states.* A pure quantum state can be described with a single ket vector. However, it is possible to have a statistical mixture of pure states, known as a *mixed state.* Mixed states are defined mathematically as

$$\bar{\rho} = \sum_i p_i |\psi\rangle_i \langle\psi|_i, \tag{2.9}$$

where the pure states $|\psi\rangle_i$ have some probability distribution denoted by p_i. In the density matrix representation of a quantum state, pure states have the property $\rho^2 = \rho$, whereas for mixed states $\bar{\rho}^2 \neq \bar{\rho}$ holds. Also in this formalism, the probability of measurement outcome i with POVM element F_i is given by

$$p_i = \mathrm{Tr}[\rho F_i], \tag{2.10}$$

where the operator Tr[*] is the *trace* of a matrix. For a square matrix, the trace is calculated as the sum of the diagonal elements of a matrix and is independent of basis choice.

Composite systems

Suppose we have multiple quantum states residing in different Hilbert spaces. The Hilbert spaces can be combined with the *tensor product*, a mathematical tool which acts on the Hilbert spaces as $\mathcal{H}_A \otimes \mathcal{H}_B$ to create a composite system $\mathcal{H}_{AB}$. The dimension of the combined Hilbert space N_{AB} is $N_{AB} = |N_A| * |N_B|$, the product of the dimensions of the original spaces.

A natural question to ask now is, how do we write the composition of quantum states? First consider what are called *product states*, states that can be written in a tensor product form. As an example, consider two general qubit states $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$ and $|\psi\rangle_B = a|0\rangle_B + b|1\rangle_B$. The product state of these two qubits is given by[2]

$$|\psi\rangle_A \otimes |\psi\rangle_B = (\alpha|0\rangle_A + \beta|1\rangle_A) \otimes (a|0\rangle_B + b|1\rangle_B), \tag{2.11}$$

which can be expanded with the tensor product as

$$|\psi\rangle_{AB} = \alpha a|0\rangle_A|0\rangle_B + \alpha b|0\rangle_A|1\rangle_B + \beta a|1\rangle_A|0\rangle_B + \beta b|1\rangle_A|1\rangle_B. \tag{2.12}$$

For a product state, any local measurement or operation on system A (B) does not effect system B (A), due to the factorability of states. Each system is completely uncorrelated from the other, meaning system A (B) cannot learn any information about the system B (A) solely based on local operations or measurements.

If states are not isolated and interact, they may become *entangled*. States that cannot be factored into a tensor product form are considered entangled. Entangled states are a more generalized combined state, in the sense that there are no restrictions on the factorability

[2] It is common to drop the system subscript and combine kets. For example, $|0\rangle_A|0\rangle_B$ and $|00\rangle$ are equivalent and may be often interchanged in this thesis.

of the coefficients in (2.12) to form a product state. A key property of entangled states is the shared correlations between sub-states. For example, consider the state

$$|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right). \tag{2.13}$$

If the same local measurement is performed on both qubits in system A and B, the outcomes will be perfectly correlated. This is easy to see if we perform a projective measurement in the computational basis[3]. This bipartite state is an example of a *maximally entangled* state. In a maximally entangled state, no information is known about sub-states. This may seem counter-intuitive, since we are able to describe the composite state fully, but we cannot describe the sub-states individually at all. We can verify this claim using a mathematical tool known as the *partial trace*. The partial trace is a mathematical tool to map a composite system into sub-systems. Given two sub-systems, A and B, in some bases, $\{|i\rangle_A\}$ and $\{|k\rangle_B\}$, respectively, the composite system can be written in general by the density matrix

$$\rho_{A,B} = \sum_{ijkl} \alpha_{ijlk}|i\rangle_A\langle j|_A \otimes |k\rangle_B\langle l|_B. \tag{2.14}$$

The state corresponding to sub-system A can be found by taking the partial trace or *tracing out* sub-system B. It is calculated by

$$\rho_A = Tr_B[\rho_{A,B}] = \sum_{ijkl} \alpha_{ijlk}|i\rangle_A\langle j|_A\langle l|_B|k\rangle_B. \tag{2.15}$$

Constructing a density matrix with the example in (2.13) and tracing out system B, the state corresponding to A is given by

$$\rho_A = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}, \tag{2.16}$$

which is the normalized two-dimensional identity matrix. This corroborates our initial claim that one cannot describe the sub-states in the maximally state, as Alice's state is described by a completely mixed state.

[3] Or any basis for that matter.

Bell states

The *Bell states* are four maximally entangled bipartite states. Mathematically they are described as

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) && (2.17) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right) && (2.18) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right) && (2.19) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right). && (2.20) \end{aligned}$$

The Bell states form an orthonormal basis in the four-dimensional Hilbert space and are an important tool in quantum information. Any measurement performed in this basis is known as a *Bell state measurement*.

2.2 Quantum key distribution

The one-time pad is a symmetric-key cryptographic protocol where encryption (decryption) is done with an XOR operation between the plaintext (cyphertext) and a private key. The private key must be randomly chosen with a length equal to the plaintext (cyphertext) and it can only be used once, hence its name. The one-time pad is proven to be *information-theoretically secure* under these conditions [45]. Practical implementations of the one-time pad are limited because it requires the key length to be at least the size of the message to be encrypted and it requires the two parties to exchange this key privately.

The idea of using quantum mechanical properties for cryptography was first introduced in 1984 by Bennett and Brassard [4]. Their seminal paper spawned the field of QKD. In it, they devised the BB84 protocol, which allows two spatially separated parties to generate a one-time pad cypher. The two parties, traditionally called Alice and Bob, have to be connected by a quantum channel, which allows quantum information to be transmitted, and a classical channel to allow them to communicate. The classical channel does not have to be private (i.e. anyone can listen in) but it must be authenticated to ensure no eavesdropper is tampering with the communication. The quantum channel is not authenticated and can be manipulated by an adversary, typically referred to as Eve. The protocol requires use of two mutually unbiased bases, for example, the computational and diagonal bases.

While any qubit implementation can be used, photons are the logical choice owing to their ability to travel through media rather quickly and with relatively low decoherence, compared to other potential candidates like atoms. Information is typically encoded in photon polarization or in time-bins. In time-bin encoding an interferometer is used to introduce delays in photon arrival time at Bob's detector. The different path lengths taken by the photon correspond to the two orthogonal encoding states [8]. Mathematically, both of these encoding schemes are equivalent. The differences in encoding variations manifest themselves in physical implementations.

The BB84 protocol operates as follows:

1) Alice randomly chooses one of the two bases and encodes a random bit to a corresponding state in that basis via a key map (see Table 2.1). Alice sends the state over the quantum channel to Bob and he randomly chooses to measure it in one of the two bases. This is repeated n-times.

2) For each round, Bob compares his measurement basis choice with the basis choice of Alice. Any rounds in which Bob measured in the wrong basis relative to the sent state by Alice are discarded. After this process, called *sifting*, they now share a *raw key*.

3) Random samples of the remaining key are compared to see if the state sent by Alice corresponds to the one measured by Bob. In the absence of errors, Alice and Bob should have perfect correlations between raw keys. If Eve has tried to measure or manipulate the transmitted states, they will manifest themselves in errors in the key correlation. Even if there are errors due to the transmission, they are associated to Eve's manipulation because this is the worst-case situation from a security point-of-view.

4) Classical *error correction* and *privacy amplification* protocols can resolve the issue of errors between Alice and Bob's raw key, provided error rates are sufficiently small. After these protocols, Alice and Bob will now share a *secure key*. They can then use this key as a one-time pad to encode a message and send it over the classical channel. An example of the protocol is summarized in Table 2.2.

The BB84 protocol has been proven to be information-theoretically secure in the presence of an eavesdropper [28, 46], provided error rates are small enough. However, practical implementations of BB84, or any QKD protocol, poses a security problem. Actual physical implementations may not match the theoretical models, opening up the possibility of side-channel exploitations [32, 42]. Although we will not discuss this in detail, it is worth noting. Efforts to produce device and measurement independent security proofs are a recent research topic of interest to overcome this. As well, finite-size effects need to be

Basis	Logical Bit	Qubit State
Z	0	$\lvert 0\rangle$
Z	1	$\lvert 1\rangle$
X	0	$\lvert +\rangle$
X	1	$\lvert -\rangle$

Table 2.1: BB84 key map

Round	1	2	3	4	5	6	7	8	9	10	11
Alice's Key	0	1	1	0	1	1	0	0	1	1	1
Alice's Basis Choice	x	x	z	x	z	z	z	x	x	x	z
Alice's State	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$
Bob's Basis Choice	z	x	z	z	x	z	z	z	x	z	z
Bob's Measured State	$\lvert 1\rangle$	$\lvert -\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert -\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert +\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$
Discard?	yes	no	no	yes	yes	no	no	yes	no	yes	no
Correct?		yes	no			yes	yes		no		no

Table 2.2: BB84 protocol example.

accounted for in security proofs [43], as many security proofs rely on the infinite key exchange limit, where the protocol is repeated an infinite number of times. For the analysis of our quantum repeater, we assume the infinite key limit. In this limit the BB84 key rate is lower bounded by [29]

$$R_\infty = Y(1 - 2h[e]), \tag{2.21}$$

where Y is the *yield*, defined as the probability Alice and Bob detect a signal per round. The parameter e denote the *quantum bit error rate* (QBER), the fraction of sifted key that is incorrect. The classical error correction and privacy amplification are denoted by the $1 - 2h[e]$ term. This term assumes perfect error correction efficiency in the Shannon limit, but this will not be the case for practical implementation. The function $h[x]$ is the *binary entropy function*, defined as

$$h[x] = -x \log_2[x] - (1 - x)\log_2[1 - x]. \tag{2.22}$$

For our quantum repeater, we implement the efficient BB84 protocol [29], a slight variation on the traditional BB84 protocol, where signals in the Z basis are sent more frequently, resulting in less discarded bits during the sifting process.

2.3 Quantum optics

A *photon* is the smallest excitation of the electromagnetic field [26]. In classical electrodynamics, solutions to the Helmholtz equation arising from the vector potential in Maxwell's equations can be expanded in an orthogonal basis of functions. These basis functions are how we define optical *modes*. Cannonically quantizating these field amplitudes of the modes results in the mode operators [51]. We use the *creation* and *annihilation* operators to describe the absorption and emission of photons. These operators act on the *Fock basis*[4] as

$$\hat{a}_j|n\rangle = \sqrt{n}|n-1\rangle_j \text{ and } \hat{a}_j^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle_j, \tag{2.23}$$

where the subscript j denotes the mode of the photon. We can also define the *number operator* as

$$\hat{n}_j|n\rangle = n|n\rangle_j, \tag{2.24}$$

where $\hat{n}_j = \hat{a}_j^\dagger \hat{a}_j$. The commutation relationship between the creation and annihilation operators are given by

$$[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{i,j}, \tag{2.25}$$

where δ is the Kronecker delta.

Beam splitter

Physically, a *beam splitter* is a device which reflects a fraction r of incident light and transmits a fraction t. The parameters r and t are often referred to as the *reflection* and *transmission coefficients*, respectively. The square of the modulus of these parameters are the probability of light reflecting or transmitting through the beam splitter. We can think of a beam splitter as having two input ports and two output ports, which can mathematically be described by *spatial modes* with some creation operators. The input spatial modes $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are related to the output spatial modes $\hat{c}^\dagger$ and $\hat{d}^\dagger$ by a unitary U, described by the following equation

$$\begin{bmatrix} \hat{c}^\dagger \\ \hat{d}^\dagger \end{bmatrix} = \begin{bmatrix} t & r \\ -r & t \end{bmatrix} \begin{bmatrix} \hat{a}^\dagger \\ \hat{b}^\dagger \end{bmatrix}. \tag{2.26}$$

An equal amount of light is transmitted and reflected through a 50/50 beam splitter, implying the transmission and reflection coefficients are the same. As a result

[4] The Fock basis describes the number of particle in a mode.

$$U = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \tag{2.27}$$

is a valid unitary[5] for (2.26). The input spatial mode creation operators then evolve as

$$\hat{a}_j^\dagger \to \frac{1}{\sqrt{2}}\left(\hat{c}_j^\dagger - \hat{d}_j^\dagger\right) \text{ and } \hat{b}_j^\dagger \to \frac{1}{\sqrt{2}}\left(\hat{c}_j^\dagger + \hat{d}_j^\dagger\right), \tag{2.28}$$

where the subscript j denotes a photon mode, other than spatial which is explicitly denoted by the operator symbol. If two distinguishable photons are incident on the two input spatial modes of the beam splitter ($i \neq j$), the output of the beam splitter can be calculated by applying the creation operators onto the vacuum and evolving the operators according to (2.28)

$$\begin{aligned} \hat{a}_j^\dagger \hat{b}_i^\dagger |vac\rangle &= \frac{1}{2}\left(\hat{c}_j^\dagger - \hat{d}_j^\dagger\right)\left(\hat{c}_i^\dagger + \hat{d}_i^\dagger\right)|vac\rangle & (2.29) \\ &= \frac{1}{2}\left(\hat{c}_j^\dagger \hat{c}_i^\dagger + \hat{c}_j^\dagger \hat{d}_i^\dagger - \hat{d}_j^\dagger \hat{c}_i^\dagger - \hat{d}_j^\dagger \hat{d}_i^\dagger\right)|vac\rangle & (2.30) \\ &= \frac{1}{2}\left(|1,1,0,0\rangle + |1,0,0,1\rangle - |0,1,1,0\rangle - |0,0,1,1\rangle\right). & (2.31) \end{aligned}$$

The kets represent the number of photons in each spatial and i, j modes, in general written as $|c_j, c_i, d_j, d_i\rangle$. For example, $|1,1,0,0\rangle$ implies there are two photons in the spatial mode c, but they are in different modes i and j, and no photons in the spatial mode d. The modes i and j denote another mode, for example polarization. It is clear from (2.31) that 50% of the time both photons will exit the same port and 50% of the time they will exit different ports. This is exactly what we would expect in classical physics.

Hong-Ou-Mandel interference

Let us consider the state $i = j$, which corresponds to two indistinguishable photons incident on the two input ports of a beam splitter. The middle terms in (2.30) cancel each other out, reducing the output state to[6]

$$\begin{aligned} |\Psi\rangle_{out} &= \frac{1}{2}\left(\hat{c}_j^\dagger \hat{c}_j^\dagger - \hat{d}_j^\dagger \hat{d}_j^\dagger\right)|vac\rangle & (2.32) \\ &= \frac{1}{\sqrt{2}}\left(|2,0\rangle - |0,2\rangle\right). & (2.33) \end{aligned}$$

[5] This matrix is not a unique solution for a 50/50 beam splitter unitary.

[6] The kets are two-dimensional in this case, compared to the four-dimensional kets in (2.31), because we assume both photons are in the *j-th* mode so there is no other distinguishing mode.

The two indistinguishable photons always exit the same port of the beam splitter, something not predicted or observed in classical physics. This quantum effect, known as the *photon bunching* or the Hong-Ou-Mandel (HOM) interference, is useful for quantum operations and a hallmark for linear optical quantum computing [25]. As photons become more distinguishable, one can see an increase in the coincidence counts between the two output ports. This is often refered to as the *HOM dip* [20]. The *visibility* of the HOM dip is given by

$$V = \frac{n_{max} - n_{min}}{n_{max} + n_{min}}, \tag{2.34}$$

where n denotes the coincidence counts between the beam splitter output modes. The visibility is a parameter that can easily be determined experimentally. It can be calculated by varying a photon mode corresponding to distinguishably, for example, rotating the polarization of one of the input photons, and comparing coincidence counts. If the two input photons are pure and completely indistinguishable, then the visibility of the HOM dip is unity, as no coincidences will occur. Due to non-ideal detectors and mode-mismatching of photons, it is not possible to achieve unit visibility, although using spectral filtering techniques [15] can improve visibility. A visibility of 97% has been demonstrated [18] using such filtering techniques. The visibility can be used as way of quantifying the mode-mismatch of photons. Assuming perfect photon detectors, the overlap of two photons γ can be related to the visibility of the HOM dip [40] as

$$\gamma = \frac{2V}{1+V}. \tag{2.35}$$

In general, the overlap of two quantum states is given by the *fidelity*. The fidelity between two quantum states ρ and σ is given by [35]

$$F(\rho, \sigma) = Tr[\sqrt{\rho^{1/2}\sigma\rho^{1/2}}]. \tag{2.36}$$

Although the fidelity and γ both refer to the overlap of quantum states, they are defined differently. These two quantities are related by $\gamma = F(\rho, \sigma)^2$.

Polarizing beam splitter

A *polarizing beam splitter* spatially separates photons into orthogonal polarizations. Using the same spatial mode convention as the beam splitter, the input modes are mapped as

$$\hat{a}_h^\dagger \rightarrow \hat{d}_h^\dagger, \quad \hat{a}_v^\dagger \rightarrow \hat{c}_v^\dagger, \quad \hat{b}_h^\dagger \rightarrow \hat{c}_h^\dagger, \text{ and } \hat{b}_v^\dagger \rightarrow \hat{d}_v^\dagger, \tag{2.37}$$

where the subscripts h and v denote horizontal and vertical polarization states, respectively. This mapping is illustrated in Figure 2.1.

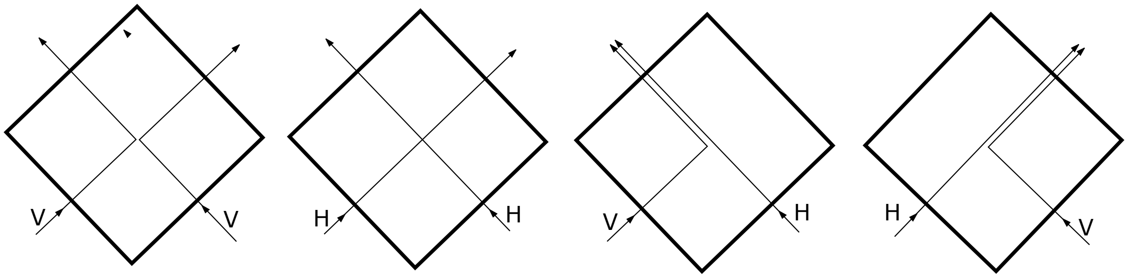

Figure 2.1: Visual representation of a polarizing beam splitter with two photons incident on the two input ports. Horizontal photons pass through the device and vertically polarized photons reflect.

Optical Bell state measurement

A Bell state measurement is a joint measurement on two qubits, which projects the qubits onto one of the Bell states in (2.17). Using a single beam splitter and two polarizing beam splitters, as in Figure 2.2, a *non-deterministic* Bell state measurement can be optically performed on two photons. The measured Bell state can be inferred based on the detection pattern in the four detectors, according to Table 2.3. Only the $|\Psi^+\rangle$ and $|\Psi^-\rangle$ states can be discriminated from the detection pattern. Using this scheme, or any scheme that involves linear optics and vacuum ancillae only, one can have a success probability at best of 50% [9]. If additional resources and ancilla qubits are used, that success probability can asymptotically reach unity [25]. Events that do not result in a successful measurement are simply discarded. It should be noted that other simple schemes exist to perform an optical Bell state measurement, such as the *double heralding* method [26]. Although, the double heralding method does not use polarization encoding. Rather, it encodes a qubit state by occupational number, where the state $|0\rangle$ corresponds to the vacuum state and the state $|1\rangle$ corresponds to one photon in the mode.

Detection Events	Bell State
{1},{2},{3} or {4}	$\|\Phi^+\rangle$
{1},{2},{3} or {4}	$\|\Phi^-\rangle$
{1,2} or {3,4}	$\|\Psi^+\rangle$
{1,4} or {2,3}	$\|\Psi^-\rangle$

Table 2.3: Bell state measurement outcomes from the setup in Figure 2.2. States $|\Phi^+\rangle$ and $|\Phi^-\rangle$ cannot be distinguished from one another based on the detection events.

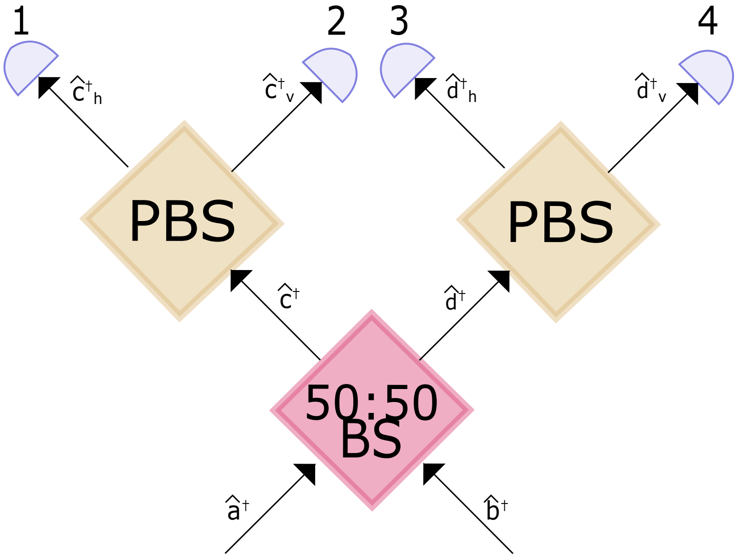

Figure 2.2: Optical Bell state measurement scheme using only linear optic components and four photon threshold detectors. Arrows represent direction of photon propagation. Spatial and polarization modes $\hat{c}_h^\dagger$, $\hat{c}_v^\dagger$, $\hat{d}_h^\dagger$, and $\hat{d}_v^\dagger$ are explicitly labelled with corresponding detector numbers to be consistent with Table 2.3.

2.4 Quantum repeaters

We define a *quantum repeater* as any device capable of transmitting information at a rate (in bits per mode per channel use) exceeding the quantum capacity of a total channel. The basic idea of most quantum repeater schemes is to divide the overall channel into N smaller channel segments. Throughout this thesis, we often refer to these smaller channel segments as *links*. We have already seen the fundamental upper bound on the quantum communication capacity of a lossy channel scales linearly with transmissivity η, the ratio of the amplitude of the electromagnetic radiation that passes through the medium. Dividing the channel into N smaller segments will allow the key rate to scale as $\eta^{1/N}$, as photons will experience loss only in a fraction of the total channel. Of course, there must be some additional auxiliary device between channel segments for the quantum repeater to function as intended. We refer to these intermediary devices as *nodes*. For this thesis, a node consist of two *quantum memories* (QMs). The system will utilize an entanglement swapping scheme at each node, effectively "connecting" the segments together. The following sections describes these principles in more detail.

Direct transmission

It has been shown that there is an upper bound on the amount of quantum information that can be sent over a lossy bosonic channel. This upper bound, known as the PLOB bound, is given by

$$R_{PLOB} = -\log_2 [1 - \eta] \tag{2.38}$$

bits per channel use per mode [38], where η is the channel transmissivity. For high-loss channels

$$R_{PLOB} \approx \frac{\eta}{\log[2]}, \tag{2.39}$$

which is also a lower bound on R_{PLOB}. Prior to the discovery of the PLOB bound, the fundamental upper bound on the capacity of a lossy bosonic channel was

$$R_{TGW} = \log_2 \left[\frac{1+\eta}{1-\eta}\right] \tag{2.40}$$

bits per channel use per mode. This bound, derived by Takeoka, Guha, and Wilde [49], is often referred to as the *TGW bound* and is looser than the PLOB bound.

Direct transmission of photons is limited due to the exponential increase of loss in a medium, as well as other decoherence effects. One can naively try to circumvent the exponential loss by sending more photonic qubits, but the exponential decay implies one would need to send an exponential amount of photons. This results in an exponential number of channel uses, which is a futile attempt for beating the PLOB bound, by definition.

Quantum memory

Quantum memories play an integral role in many quantum repeater schemes, as they are needed to store intermediate quantum states between links. We will define a quantum memory as any physical system that can write, store, and read-out a quantum state [16]. Physical implementations often include a light-matter interface, as photonic states are read-in, stored in matter, and read-out as photonic states. While there are many variations of QMs, each with their own nuances, the specific QMs we consider for our quantum repeater do not require the ability to read-in photonic states. We require a QM that can generate a photonic state entangled with a state stored in the QM via some controlled mechanism, like optical pumping.

Some figures of merit we consider for QM performance are the preparation efficiency and preparation time of generating a memory-photon entangled state, the wavelength of emitted photons, the efficiency of coupling the photon into fiber, and the decoherence time of the stored state. If QMs are implemented in a communication channel, decoherence times need to be sufficiently longer than communication times in order to reduce errors. As well, the wavelength of emitted photons becomes important, as the attenuation and dispersion of photons in fiber is dependent on wavelength. The lowest fiber attenuation occurs around 1550 nm [33], making it an ideal wavelength for telecommunications. Different QM implementation will emit photons at different wavelengths. Photon emission from ionic and atomic QMs are limited by their energy-level structures. For example, photons emitted from Yb^+ ions via the $^2\mathrm{P}_{1/2}$ to $^2\mathrm{S}_{1/2}$ energy level transition occur at a wavelength of 369.5 nm [34]. Engineerable QM sources, like quantum dots, have demonstrated photon emission around 1500nm [6]. If the photons generated by the QMs are not at a suitable wavelength for low-loss in a fiber, a wavelength conversion must be performed before transmission.

There have been a number of proposed and demonstrated physical implementations for QMs, including but not limited to trapped atoms [7, 52], atoms in optical cavities [48], atomic ensembles [11], and nitrogen-vacancy (NV) centers [10, 50]. For our system, we will consider trapped ions as our QMs, although the analysis is generalized for any implementation. Trapped ions have been demontrated to have decoherence times on the order of seconds [37, 27, 19]. Coupling emitted photons into fiber is often challenging for trapped ionic systems, resulting in low coupling efficiencies of about 0.03%-0.05% [36, 34]. However, using an optical cavity can potentially increase to the coupling efficiencies to over 30% [24]. Bell state measurements can be perfomed between neighbouring ions deterministically [47] or by optically reading-out and entangling photonic states. In the next chapter, we model these realistic imperfections for any general QM implementation.

Quantum teleportation and entanglement swapping

If Alice and Bob share an entangled state, then Alice (Bob) can transfer an unknown quantum state to Bob (Alice) without physically transferring the unknown state via a process called *quantum teleportation* [5]. Suppose Alice holds the qubit state $|\psi\rangle_C = \alpha|0\rangle + \beta|1\rangle$, and her and Bob share any Bell state $|\psi\rangle_{AB}$[7]. The total composite system is then described by

$$\begin{aligned} |\psi\rangle_{AB}|\psi\rangle_C &= |\Phi^+\rangle_{AB}\left(\alpha|0\rangle + \beta|1\rangle\right) && (2.41)\\ |\psi\rangle_{ABC} &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\left(\alpha|0\rangle + \beta|1\rangle\right) && (2.42)\\ &= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|110\rangle + \beta|001\rangle + \beta|111\rangle\right). && (2.43) \end{aligned}$$

It is easy to see that if Alice performs a Bell state measurement on the two qubits in her possession, then conditional on Alice's measurement outcome Bob effectively gets one of the following states:

$$\begin{aligned} \langle\Phi^+_{AC}|\psi_{ABC}\rangle &\rightarrow \alpha|0\rangle_B + \beta|1\rangle_B, && (2.44)\\ \langle\Phi^-_{AC}|\psi_{ABC}\rangle &\rightarrow \alpha|0\rangle_B - \beta|1\rangle_B, && (2.45)\\ \langle\Psi^+_{AC}|\psi_{ABC}\rangle &\rightarrow \beta|0\rangle_B + \alpha|1\rangle_B, && (2.46)\\ \langle\Psi^-_{AC}|\psi_{ABC}\rangle &\rightarrow \beta|0\rangle_B - \alpha|1\rangle_B, && (2.47) \end{aligned}$$

where each state occurs with a probability of 1/4. Depending on the measurement result of the Bell state measurement from Alice, Bob can apply a phase flip and/or a bit flip to correct his state, as described in 2.4. Bob then possesses a state that is identical to $|\psi\rangle_c$ original held by Alice.

Entanglement swapping uses the same principle as quantum teleportation [21]. Suppose there is an intermediate party, called Charlie, between Alice and Bob. If Alice and Charlie, and Bob and Charlie, each share an entangled state, for example a maximally entangled

[7] We chose the Bell state $|\Phi^+\rangle$ state for this example

Bell state measurement outcome	Bob's operation
$\vert\Phi^+\rangle$	Do nothing
$\vert\Phi^-\rangle$	Phase flip
$\vert\Psi^+\rangle$	Bit flip
$\vert\Psi^-\rangle$	Bit and phase flip

Table 2.4: Bob's correctional operation on his qubit, depending on the Bell state measurement outcome.

Bell state $|\Phi^+\rangle$, then Charlie can perform a Bell state measurement on his two qubit states, resulting in Alice and Bob sharing an entangled bipartite state. After Charlie performs a Bell state measurement, he communicates his measurement outcome to Bob (or Alice). Bob (or Alice) can then correct their state with the same operations as the quantum teleportation scheme utilized in in Table 2.4. This is a key principle used for many quantum repeater schemes, allowing for generation of entanglement between two spatially separated parties.

With respect to our quantum repeater, a node effectively acts as Charlie. Since we consider multiple nodes, each node operates in the same manner and this entanglement swapping effect cascades. Each node must relay their respective Bell state measurement outcome to Bob (or Alice), so the state can be properly adjusted. If there are an even amount of bit flips or phase flips to apply, Bob does not have to do anything since they effectively cancel each other out.

2.5 One-node quantum repeater

Analysis and benchmarking for a one-node quantum repeater similar to the system we consider in this thesis has been previously done in [30]. The performance of a single-node quantum repeater utilizing entanglement swapping was compared to some fundamental communication bounds and QKD protocols. At the time of the work in [30], the PLOB bound was not known yet. The TGW bound was used as a benchmark for the quantum communication capacity. To have an equitable comparison to a multi-node quantum repeater, we recalculate the results of this work with the PLOB bound as a benchmark. Much of the component modelling is similar to that used in [30], as we are extending the system. In fact, the key rate formula we derive in the following section is a generalized form of that in [30], which now depends on the number of nodes in the quantum repeater. Improvements to the protocol in [30] have already been proposed in [41]. They consider a six-state protocol with advantage distillation, as well as altering the protocol to abort if the QMs store states beyond a given threshold time.

Chapter 3

Analysis

3.1 System model

Before we describe the system model for an n-node quantum repeater, we briefly describe the one-node quantum repeater in [30]. This quantum repeater consists of two QMs in the single node, each capable of emitting entangled memory-photon states on demand with some probability. The emitted photons are sent through a fiber to Alice and Bob, where they are detected in the computational or diagonal bases. The protocol they consider operates sequentially: once Alice (Bob) heralds a successful detection, then photons are sent to Bob (Alice). Once both parties have heralded a successful detection, a Bell state measurement is performed on the two states stored in the QMs. The outcome is communicated via a classical channel to Bob (or Alice) so the proper operation can be performed on their measurements according to (2.4). The architecture of this quantum repeater is depicted in Figure 3.1.

To extend this system, we simply introduce more nodes in succession along the communication channel. Between neighbouring nodes, not connected to Alice or Bob, there is an optical Bell state measurement performed on the emitted photons. This allows for entanglement to be generated between these successive nodes. We also required a classical channel connecting Alice, Bob, all of the nodes, and optical Bell states together, so that entanglement swapping can be done. Figure 3.2 is an example of a three-node scheme.

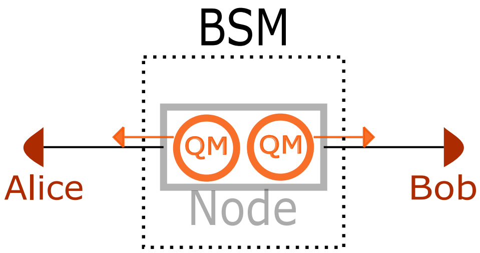

Figure 3.1: The one-node quantum repeater setup analysed in [30].

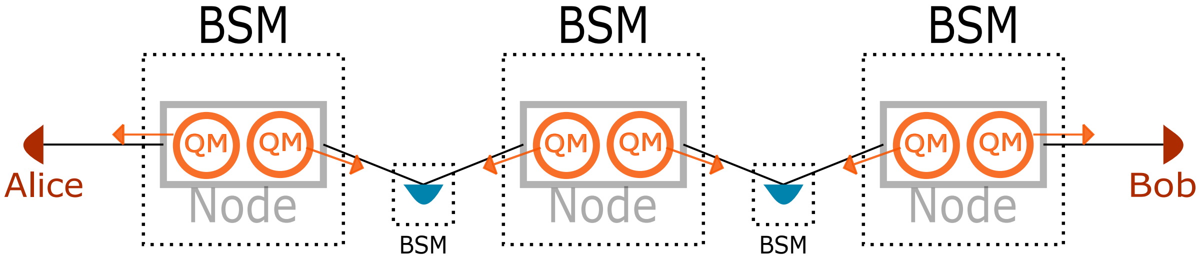

Figure 3.2: The architecture of a three-node quantum repeater. Each node contains two QMs. Orange arrows indicate direction of photon propagation. The dashed black boxes indicated Bell state measurements. The optical Bell state measurements are depicted by the blue detectors.

3.2 Component modelling

To provide an accurate performance of this system, we must model the imperfections in each component. In the following section we discuss the component models. We use the same error models from [30] except for the optical Bell state measurement, which we derived. We assume information is encoded in photon polarization, although this can be generalized to any other qubit encoding, like time-bin encoding. However, a time-bin encoding would require using a different scheme for the optical Bell state measurement.

Detectors

Detectors are modelled as threshold detectors, where a click indicates at least one photon or a dark count is detected and no click indicates no photon or no dark count is detected. Each detector has a detection efficiency, denoted by η_d, and a probability of a dark count occurring, denoted by p_{dark}. We assume all detectors in this system have identical parameters. The POVM elements for Alice and Bob's detectors are modelled by $\{F_{vac}, F_{click}\}$, which are found by extending the basic detector model in [31] to include η_d and p_{dark}. The POVM elements are explicitly given as

$$F_{vac} = (1 - p_{dark}) \sum_{n=0}^{\infty} (1 - \eta_d)^n |n\rangle\langle n| \tag{3.1}$$

and

$$F_{click} = \sum_{n=0}^{\infty} (1 - (1 - p_{dark})(1 - \eta_d)^n) |n\rangle\langle n|. \tag{3.2}$$

Alice and Bob each have two detectors that can distinguish photon polarization with the capability to measure in either the Z or X basis. We use the squashing map [2] to map double-detection events to a randomly chosen outcome, reducing the Fock state to a finite dimensional space with at most a single photon received. Vacuum events, where there are no detections from either detector, are easily flagged and discarded. This effectively maps the state ρ to

$$\Gamma(\rho) = \alpha\rho + (1 - \alpha)\frac{\mathbb{I}}{2}, \tag{3.3}$$

where

$$\alpha = \frac{\eta_d(1 - p_{dark})}{1 - (1 - \eta_d)(1 - p_{dark})^2}. \tag{3.4}$$

For the inner link detectors, contained in the optical Bell state measurement, we assume at most two photons can be detected per event per detector. Any detection patterns that do not herald a distinguishable Bell state given in Table 2.3 are discarded. Since we account for mode-mismatch in the optical Bell state measurement, we modify the detector POVM elements in (3.1) and (3.2). We assume each of the four detectors in the optical Bell state measurement can distinguish between any general mode-mismatch of the photons incident on the detectors. We can abstractly think of this as some device within the detector that is able to separate photons based on their distinguishing modes (as a polarizing beam splitter does for polarization modes). To account for this, we model each of the four physical threshold detectors as two "virtual" detectors with the ability to separate mismatched modes (see Figure 3.3). Since there is only one detector physically, the observer does not have access to this information regarding mode-mismatch. A click in the matched or mismatch detector (or both) is simply seen as a click in the physical detector for an observer. Based on this model, the POVM elements for the detectors in the optical Bell state measurement can be expressed as

$$\bar{F}_{vac} = \frac{1}{1 - p_{dark}} F_{vac,1} \otimes F_{vac,2} \tag{3.5}$$

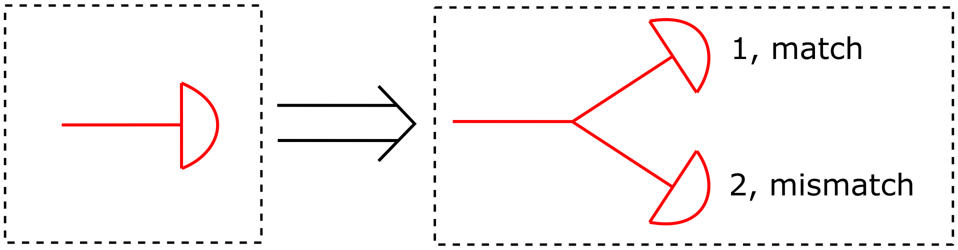

Figure 3.3: Detector model for detectors in an optical Bell state measurement (see Figure 2.2). Single detectors can distinguish between two modes corresponding to matched or mismatched photons, although an observer may not have access to this distinguishing information.

and

$$\bar{F}_{click} = \mathbb{I} - \bar{F}_{vac}, \tag{3.6}$$

where $F_{vac,1}$ and $F_{vac,2}$ are defined in (3.1). Here the subscripts 1 and 2 denote different modes, other than polarization. We assume mode 1 corresponds to the matched mode and mode 2 corresponds to the mismatched mode. Taking the tensor product of (3.1) with itself results in a prefactor of $(1 - p_{dark})^2$, which implies both "virtual" detectors can experience dark counts. In reality there is only one physical detector which can detect at most one dark count per time slot, so we must include a factor $1/(1 - p_{dark})$ in (3.5).

Quantum memories

A memory-photon entangled state can be generated with some probability η_P, requiring some preparation time T_{prep}. We assume the QMs and emitted photons share a maximally entangled bipartite state. Without loss of generality, we assume it to be the $|\Phi^+\rangle$ state. Associated to each quantum memory is a *dephasing time*, commonly referred to as the T_2 time. We model decoherence in the QMs using a general model that covers many physical implementations [39]. A state ρ that is stored in the memory for a time t becomes

$$\Lambda(\rho) = g(t)\rho + (1 - g(t))\hat{Z}\rho\hat{Z}, \tag{3.7}$$

where $g(t) = (1 + e^{-t/T_2})/2$ and $\hat{Z}$ is the Pauli-Z operator. In this simple model we ignore the T_1 relaxation times in the QMs, as the time scale is usually much loner than T_2.

Channels

The physical channel we consider for our scheme is a fiber. The emitted photons from the quantum memories are coupled into a fiber and transmitted through the links. We denote the coupling efficiency by η_c. The transmission efficiency of light in a fiber decreases exponentially with length and can be modelled by

$$\eta_{ch}(L) = e^{-L/L_{att}}. \tag{3.8}$$

The attenuation length L_{att} for fiber depends on the wavelength of the propagating light and is approximately 22 km at 1550 nm. If the emitted photons are not at this wavelength, we consider a photon wavelength conversion efficiency, denoted by η_λ.

Since only linear optic components are used in our quantum repeater and all of the detectors are assumed to have the same parameters, the detector losses can be combined with the losses in the channels. In fact, from this same argument, all of the efficiencies we have introduced can be combined into one term, denoted by η_{tot}, where $\eta_{tot} = \eta_p \eta_\lambda \eta_c \eta_d$. The total efficiency η_{tot} will be used as a figure of merit for analysis in the following section.

Polarization encoded photons are used in our quantum repeater, which will introduce some misalignment error as photons propagate through the channels. Misalignment error occurs when the detectors are physically rotated relative to the coordinate system of the emitted photon's polarization. The probability that a photon is misaligned is given by the *misalignment parameter*, denoted by e_M. We assume polarization misalignment is the same in each fiber. The shared Bell states between the QMs and photons at the detectors are now modelled by the mixed state [30]

$$\rho = (1 - e_M)|\Phi^+\rangle\langle\Phi^+| + e_M|\Psi^-\rangle\langle\Psi^-|. \tag{3.9}$$

Geometric spacing

In the next chapter we will see that the distance of nodes relative to one another will affect the key rate. Given a total separation length L between Alice and Bob, the nodes effectively divide the channel into segments. We denote the lengths of these segments by $L_a, L_1, L_2, ...L_{n-1}$, and L_b. In the case of a symmetric setup, the channels connecting Alice and Bob to their neighbouring nodes are defined by the *spacing parameter*, denoted by x, where

$$x = L_a/L = L_b/L. \tag{3.10}$$

From this definition, we can express the inner length segments as

$$L_i = \frac{(1-2x)}{(n-1)}L. \tag{3.11}$$

In our analysis we will also consider an asymmetric setup, where L_a and L_b are different. For this asymmetric setup, we define another spacing parameter y, where

$$y = L_b/L. \tag{3.12}$$

For the asymmetric setup, the spacing parameter x still holds in (3.10) for L_a. All of the results and figured in this thesis will be assuming the symmetric setup, unless otherwise stated. Figures 3.4 and 3.5 illustrate the two different spacings and naming conventions.

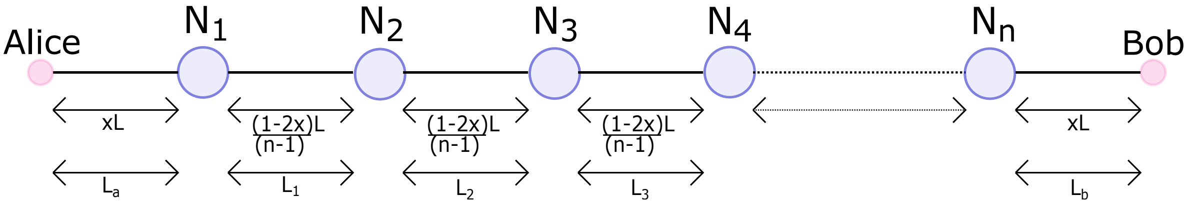

Figure 3.4: The symmetric geometric spacing setup with the channel lengths labelled in terms of the spacing parameter x, the number of nodes n and total repeater lengths L. The channel length labels L_i are indicated for clarity.

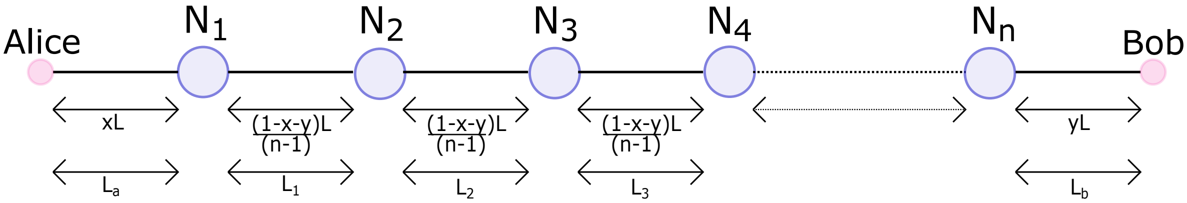

Figure 3.5: The asymmetric geometric spacing setup with the channel lengths labelled in terms of the two spacing parameters x and y, the number of nodes n and total repeater lengths L. The channel length labels L_i are indicated for clarity.

Quantum memory Bell state measurements

We model the Bell state measurement between QMs in each node with a general depolarizing channel, which maps the two QMs states, denoted by ρ, to

$$\Delta(\rho) = \lambda_{BSM}\rho + (1-\lambda_{BSM})\frac{\mathbb{I}}{4}. \tag{3.13}$$

The parameter $1-\lambda_{BSM}$ is the noise introduced in the Bell state measurement. Each QM Bell state measurement has some success probability, denoted by p_{BSM}. For our specific implementation, the QM Bell state measurement is deterministic so p_{BSM} is unity. This is of course not the case for non-deterministic Bell state measurements like the optical one we consider between nodes.

Optical Bell state measurement

In this subsection, we show how we derive the optical Bell state measurement success probability by including a general mode-mismatch. Photons incident on the two input ports of 50/50 beam splitter in Figure 2.2 may not interfere if there is some temporal, frequency, or other mode-mismatch[1]. To account for this general mode-mismatch in the optical Bell state measurement, let us consider the two pure states generated by two adjacent QMs[2]

$$|\Psi\rangle_a = \frac{|H\rangle|0\rangle + |V\rangle|1\rangle}{\sqrt{2}} \tag{3.14}$$

and

$$|\Psi\rangle_b = \sqrt{\gamma}\left(\frac{|H\rangle|0\rangle + |V\rangle|1\rangle}{\sqrt{2}}\right) + \sqrt{1-\gamma}\left(\frac{|\bar{H}\rangle|0\rangle + |\bar{V}\rangle|1\rangle}{\sqrt{2}}\right), \tag{3.15}$$

where the subscripts a and b refer to the different spatial modes of the beam splitter. The kets H and V denote horizontal and vertical polarization modes, respectively. The bar indicates another photon mode that is distinguishable, besides polarization, and corresponds to a mismatched mode. The states $|0\rangle$ and $|1\rangle$ denote qubit states stored within the QMs. The overlap of these two states is given by

$$|\langle\Psi|_a|\Psi\rangle_b|^2 = \gamma, \tag{3.16}$$

[1] We do not consider polarization mismatch, we explicitly model the polarization mismatch in the misalignment parameter in (3.9).

[2] Since we assume the QMs are capable of generating a $|\Phi^+\rangle$, we use this example.

which corresponds to the degree of matching between two input states. Given these two pure states, the input state at the optical Bell state measurement is given by

$$|\Psi\rangle_{input} = |\Psi\rangle_a \otimes |\Psi\rangle_b, \tag{3.17}$$

which can be written explicitly as

$$\begin{aligned}|\Psi\rangle_{input} = \frac{\sqrt{\gamma}}{2}\left(|HH\rangle|00\rangle + |HV\rangle|01\rangle + |VH\rangle|10\rangle + |VV\rangle|11\rangle\right) + \\ \frac{\sqrt{1-\gamma}}{2}\left(|H\bar{H}\rangle|00\rangle + |H\bar{V}\rangle|01\rangle + |V\bar{H}\rangle|10\rangle + |V\bar{V}\rangle|11\rangle\right).\end{aligned} \tag{3.18}$$

If we construct a density matrix from $|\Psi\rangle_{input}$ and apply the operation of the 50/50 beam splitter (2.28), polarizing beam splitter (2.37), and measure the photons using the POVM in (3.5, 3.6), the off-diagonal terms arising from the outer product of matched and mismatched photon modes will not contribute to the measurement outcome, due to the diagonal structure of the POVM elements (see Appendix A.1 for a more detailed calculation). Therefore, we only have to consider the following mixed state at the input

$$\begin{aligned}\rho_{input} = \frac{\gamma}{4}\left(|HH\rangle|00\rangle + |HV\rangle|01\rangle + |VH\rangle|10\rangle + |VV\rangle|11\rangle\right) \\ \left(\langle HH|\langle 00| + \langle HV|\langle 01| + \langle VH|\langle 10| + \langle VV|\langle 11|\right) + \\ \frac{1-\gamma}{4}\left(|H\bar{H}\rangle|00\rangle + |H\bar{V}\rangle|01\rangle + |V\bar{H}\rangle|10\rangle + |V\bar{V}\rangle|11\rangle\right) \\ \left(\langle H\bar{H}|\langle 00| + \langle H\bar{V}|\langle 01| + \langle V\bar{H}|\langle 10| + \langle V\bar{V}|\langle 11|\right)\end{aligned} \tag{3.19}$$

or more compactly as

$$\rho_{input} = \gamma\rho_{match} + (1-\gamma)\rho_{mismatch}. \tag{3.20}$$

The photonic states that arrive at the optical Bell state measurement are given by the mixed state in (3.9), due to the polarization misalignment. We can still use an input state of the form in (3.20), where we now define ρ_{match} and $\rho_{mismatch}$ as

$$\begin{aligned}\rho_{match} = (1-e_M)^2|\Phi^+\rangle_a\langle\Phi^+|_a \otimes |\Phi^+\rangle_b\langle\Phi^+|_b + \\ e_M(1-e_M)|\Phi^+\rangle_a\langle\Phi^+|_a \otimes |\Psi^-\rangle_b\langle\Psi^-|_b + \\ e_M(1-e_M)|\Psi^-\rangle_a\langle\Psi^-|_a \otimes |\Phi^+\rangle_b\langle\Phi^+|_b + \\ e_M^2|\Psi^-\rangle_a\langle\Psi^-|_a \otimes |\Psi^-\rangle_b\langle\Psi^-|_b\end{aligned} \tag{3.21}$$

and

$$\begin{aligned}\rho_{mismatch} = (1-e_M)^2 |\Phi^+\rangle_a\langle\Phi^+|_a \otimes |\bar{\Phi}^+\rangle_b\langle\bar{\Phi^+}|_b + \\ e_M(1-e_M)|\Phi^+\rangle_a\langle\Phi^+|_a \otimes |\bar{\Psi}^-\rangle_b\langle\bar{\Psi^-}|_b + \\ e_M(1-e_M)|\Psi^-\rangle_a\langle\Psi^-|_a \otimes |\bar{\Phi}^+\rangle_b\langle\bar{\Phi^+}|_b + \\ e_M^2|\Psi^-\rangle_a\langle\Psi^-|_a \otimes |\bar{\Psi}^-\rangle_b\langle\bar{\Psi^-}|_b.\end{aligned} \tag{3.22}$$

To find the success probability of the optical Bell state measurement, we must apply the operations of the 50/50 beam splitter and polarizing beam splitters to the input state in (3.20) to find the corresponding output state at the detectors. Tracing out the QM states in (3.20) and conditioning on measuring a successful detection pattern according to Table 2.3, we can determine the success probability of the optical Bell state measurement. We note that the misalignment error will not affect the success probability since tracing out the QM states leaves the input state in the maximally mixed state, regardless of e_M. In Appendix A.1 we calculate the probability of success for the optical Bell state measurement to be

$$p_{OBSM} = \frac{1}{2}(1-p_{dark})^2(\eta_{inner}^2 + 8p_{dark}^2(1-\eta_{inner})^2 + p_{dark}\eta_{inner}(8-(7-\gamma)\eta_{inner})), \tag{3.23}$$

where $\eta_{inner} = \eta_{tot}e^{L_i/(2L_{att})}$. The factor of two in the exponent comes from the fact that the optical Bell state measurement is halfway between nodes, dividing L_i in half. If there is no mode-mismatch ($\gamma = 1$), then this result agrees with that in [1]. In the absence of dark counts, the success probability becomes

$$p_{OBSM} = \frac{1}{2}\eta_{inner}^2. \tag{3.24}$$

We denote the probability of an error occurring in the optical Bell state measurement by $e_{obsm,x}$ and $e_{obsm,z}$, where the x and z subscripts indicate the error in the X and Z bases, respectively. The parameters $e_{obsm,z}$ and $e_{obsm,x}$ are derived by calculating each situation where the optical Bell state measurement yields an incorrect measurement outcome, given the input photonic states. For example, if two perfectly matched horizontally polarized photons are incident on the two input ports of the optical Bell state measurement, then a single click should be observed in either detector 1 or 3. If these two photons yield any successful measurement event according to Table 2.3, then an error has occurred. This ultimately leads to incorrect correlations between the states stored in the QMs entangled with the input photons. When we calculate the general QBERs in the following section, it will be convenient to define the parameter μ such that $\mu = 1 - 2e_{obsm}$, which holds for both bases. In Appendix A.1 we give a detailed calculation of μ_x and μ_z. We find these parameters to be

$$\mu_z = \frac{(1-p_{dark})^2(1-(\gamma+1)p_{dark})\eta_{inner}^2}{2p_{OBSM}} \tag{3.25}$$

and

$$\mu_x = \frac{(1-p_{dark})^2\eta_{inner}^2\gamma}{2p_{OBSM}}. \tag{3.26}$$

The misalignment error e_M is not accounted for in μ_x and μ_z because of the way the QBERs are defined in (3.31) and (3.32). A factor of $(1-2e_M)^2$ should appear in both μ_x and μ_z but we opt to factor the misalignment errors caused in each fiber into one term in the QBERs.

3.3 Protocol

Different protocols will affect the key rate generated by our quantum repeater. These variations manifest themselves in altering the yield and/or QBERs in the system. Since we have not explicitly defined the key rate for our quantum repeater in detail yet, we will discuss the affect on key rate various protocols can have in more depth in Section 3.4. For now, we take at face value that it is imperative the protocol be defined explicitly prior to any analysis. Before we define a protocol, Figure 3.6 below illustrates the numbering convention we will use for our system.

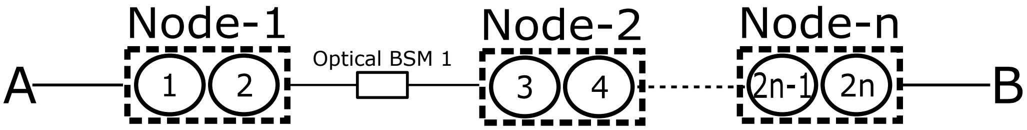

Figure 3.6: Numbering convention for quantum memories, denoted by circles, and nodes, denoted by dashed boxes. Our numbering convention always has numeric label values increasing from Alice to Bob. As well, we always assume Alice to be on the left and Bob to be on the right.

We define the following protocol, which we refer to as the *sequential protocol*:

1) QM-1 attempts to generate an entangled memory-photon state and transmit the photon to Alice. Alice randomly chooses between the Z or X basis for measurement. This

process is repeated until Alice heralds a successful detection. Alice then sends a classical signal to node 1 and node 2 indicating a successful event.

2) QM-2 (node 1) and QM-3 (node 2) attempt to generate memory-photon states and transmit the photons through the first inner link, to the first optical Bell state measurement. This is repeated until the optical Bell state measurement successfully detects a Bell state according to the detection pattern in Table 2.3. A classical signal is sent to node 1, node 2, and node 3 to indicate a successful detection.

3) A Bell state measurement is performed on the two QMs in node-1. If this Bell state measurement fails, then the protocol is aborted and restarted.

4) QM-4 (node 2) and QM-5 (node 3) repeat steps 2) and 3) and this continues in succession until node n is signalled that the previous optical Bell state measurement was successful.

5) QM-2n (node n) performs step 1) with Bob. Upon a successful detection, Bob signals back to node-n and step 3) is performed on node n.

6) The measurement outcomes from all of the Bell state measurements are sent to Bob (or Alice). Depending on which basis their photons were measured in, the proper bit or phase flips can be applied to their measurement outcome according to Table 2.4. This can be done classically, after the measurement is performed, which is more ideal than having to store a quantum state and then implement a quantum gate. Alice and Bob can then perform the rest of the efficient BB84 protocol [29].

All of the analysis presented in this thesis is done using this sequential protocol. A simultaneous protocol was initially considered as well, where all of the QMs attempt to generate a memory-photon state simultaneously, instead of in succession. Deriving an analytic expression for the key rate of such a protocol proved to be difficult, due to the various geometric spacing between in the inner and outer links and the expectation value that appears in the QBER. We did, however, derive an analytic expression of a *semi-simultaneous* protocol, where the inner links attempt to create an entangled pair simultaneously and then the outer links attempt to create an entangled pair sequentially. We were able to do this because all of the inner links are assumed to have the same length and success probabilities, reducing the complexity of the functions appearing in the key rate. This semi-simultaneous protocol did not appear to offer significant advantage in the key rate, compared to the sequential protocol. We will discus this in more detail in the following section, once we introduce the explicit expression for the key rate. For practical implementations, we expect that the sequential protocol would have a disadvantage in running time versus a simultaneous protocol. However, the metric of interest is the throughput per channel use, so there is no concern of total protocol run time in our analysis. For some physical implementations, a sequential protocol may be necessary. For example, if only one physical QM is used in each node containing two internal qubits states that cannot be simultaneously addressed, as in the broker-client method [3]. As well, some physical experimental setups may consist of a light-matter coupling device capable of being addressed by one photon at a time [41].

3.4 Key rate

We implement the efficient BB84 protocol [29] for our quantum repeater. The secret key rate is lower bounded by

$$R_\infty = \frac{Y}{2}(1 - h[e_x] - fh[e_z]) \tag{3.27}$$

bits per channel use per mode[3]. Often in literature the secret key rate of QKD protocols is defined as bits per unit time. We are interested in the amount of resources required for communication to compare with the fundamental bound on the quantum communication capacity of the channel. We are not concerned with the overall repetition rate (bits per unit time) of the protocol[4]. The fundamental PLOB bound is defined as bits per channel use, hence, we define the key rate in this fashion. The term Y is the yield, defined as bits per channel use and represents the number of bits of raw key that can be generated per channel use. The factor of 1/2 comes from the fact that the protocol uses two polarization modes. The $1 - h[e_x] - fh[e_z]$ term represents the classical error correction and privacy amplification protocols. The variables e_x and e_z denote the QBER in the X and Z bases respectively. The factor f represents the realistic inefficiency in error correction. For ideal error correction schemes $f = 1$ and for non-ideal schemes $f \geq 1$.

Yield

By our definition the number of channel uses is accounted for in the yield, which is inversely proportional to the number of channel uses. The number of channel uses is not so straightforward to calculate, given that each link divides up the total channel. The number of channel uses is simply not the sum of the total channel uses per link. For example, if there are two links and one requires one channel use to succeed, and the other requires two channel uses, then the total number of channel uses is two, not three. From this simple

[3] The definition of the key rate is different than in (2.21); the yield in (2.21) does not account for the number of channel uses or modes used.

[4] Although, for practical implementation this is certainly important.

example, we intuitively see that the overall number of channel uses will be limited by the link that requires the most channel uses.

We know the expected number of channel uses is dependent on the probability of success for each link. For clarity, a "success" is indicated by a successful detection in the link. Each link can be modelled by an independent geometric distribution with some success probability p. For a geometric random variable, the expected number of trials Q until a successful event occurs is given by $Q = 1/p$. Since we have multiple links, we are not concerned with the number of trials for a single link to succeed, but the maximum number of trials needed for all of links to succeed.

For our quantum repeater, we have three different probabilistic events to consider: the probability of success in Alice's outer link, denoted by p_a, the probability of success in Bob's outer link, denoted by p_b, and the probability of success in the inner links, denoted by p_i (see Figure 3.7). The p_i denoted in this figure are equal to p_{OBSM}, given in (3.23). Accounting for detector dark counts, the probability that Alice (Bob) herald a successful detection is given by

$$p_{a,b} = 1 - (1 - \eta_{a,b})(1 - p_{dark})^2, \tag{3.28}$$

where $\eta_{a,b} = \eta_{tot} e^{-L_{a,b}/L_{att}}$. These success probabilities depend on the length of the respective links. If we consider the symmetric setup, where the first and last link lengths are equal, and all of the inner links are the same length, then p_a and p_b are equal and all p_i are equal[5].

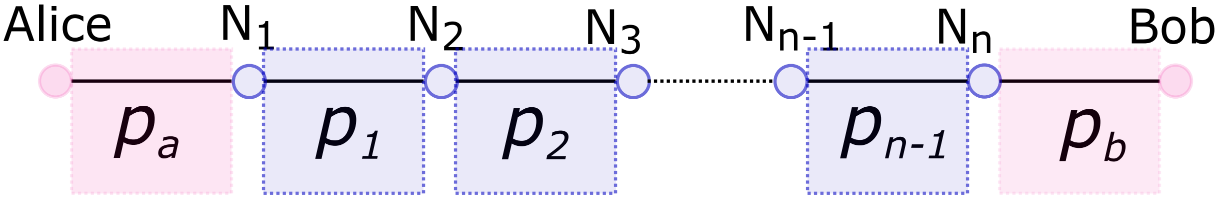

Figure 3.7: Each link has an associated success probability, denoted by p_i. N_i denotes node #i.

The maximum expected number of channel uses is given by

$$\mathbb{E}[\#channel\ uses] = \sum_{k=0}^{\infty} \left(1 - (1 - (1 - p_a)^k)(1 - (1 - p_b)^k) \prod_{i=1}^{n-1} (1 - (1 - p_i)^k) \right), \tag{3.29}$$

[5] Later we will consider the asymmetric setup, where Alice and Bob have different lengths, changing their success probabilities. The inner links will always have the same length and thus, same probabilities.

which is derived in Appendix A.2. In order for the protocol not to abort, all of the QM Bell state measurements in each node must succeed. This event occurs with probability p^n_{BSM}. Thus, the yield can explicitly be written as

$$\begin{aligned} Y &= \frac{p^n_{BSM}}{\mathbb{E}[\#channel\ uses]} \\ Y &= \frac{p^n_{BSM}}{\sum_{k=0}^{k=\infty}\big(1-(1-(1-p_a)^k)(1-(1-p_b)^k)\prod_{i=1}^{n-1}(1-(1-p_i)^k)\big)}. \end{aligned} \tag{3.30}$$

Assuming the total repeater length is $L = 0$ and given that p_i is at best $1/2$, it can easily be shown from (3.30) that the yield will decrease as n increases due to the power relation with p_{BSM} and the increase in expected number of channel uses. This indicates there is an initial price to pay in the yield for adding more repeater stations. When we consider the effects of link length on p_a, p_b and p_i, we will see that our yield will scale differently, depending on how many repeaters we have and how they are geometrically spaced. It is important to highlight that in an ideal scenario, where there is no error introduced in the quantum system, the key rate can reach arbitrarily low values without going to zero, since the yield term is always positive for non-zero success probabilities. In the absence of errors and by choosing appropriate geometric spacing of the repeaters, we show we can always beat the fundamental PLOB bound in Section 3.4.1.

Quantum bit error rate

Each component in the system introduces some error, which accumulates in the communication channel between Alice and Bob. Since an error event is a binary outcome in each component, it is possible for multiple errors to cancel out. For example, if there are an even number of bit-flip or phase errors in a channel, there will be no overall bit-flip error or phase error.

The general QBERs in (3.31) and (3.32) can be derived by analysing the error each component introduces in each basis. An effective bit error between Alice and Bob occurs only for an odd number of errors from the components. Summing over all of the possible situations when this occurs gives a total effective error rate per basis between Alice and Bob. The general QBER can also be found with a similar derivation used in [41], yielding the same result. The general QBERs for an n-node repeater scheme in the Z and X bases can be expressed as

$$e_z = \frac{1}{2} - \frac{(1-2e_M)^{2n}\lambda^n_{BSM}\alpha^2\mu_z^{n-1}}{2} \tag{3.31}$$

and

$$e_x \quad = \quad \frac{1}{2} - \frac{(1-2e_M)^{2n}\lambda_{BSM}^n \alpha^2 \mu_x^{n-1} f_{dp}[n]}{2}. \tag{3.32}$$

The parameter $f_{dp}[n]$ in (3.32), referred to as the *dephasing parameter*, is related to the error caused by dephasing in the QMs. In general, regardless of protocol, it is given by

$$f_{dp}[n] = \mathbb{E}\left[e^{-\sum_{i=1}^{i=2n} t_i/T_2}\right] \tag{3.33}$$

and depends on the sum of the overall storage times of states in each QM. For the sequential protocol considered in our analysis, we can derive an explicit equation for this expression. Using the QM numbering convention in Figure 3.6 and assuming the protocol operates from Alice to Bob, the odd numbered QMs in each node store their states longer than the even numbered QMs. This is a result of the odd numbered QMs having to wait for the successive link to successfully herald a detection before a Bell state measurement can be performed on the two QMs in a node, while the even numbered QMs only have to wait for the classical communication time from the heralding signals. This implies that the states stored in the even numbered QMs will have a smaller waiting time, and thus a lower dephasing error. As an example, Table 3.1 explicitly shows the waiting time of the QMs in a three-node quantum repeater. The link time constants τ_i represent the repetition rate of a trial per link, and are given by

$$\tau_p = L_i/c + T_{prep} \tag{3.34}$$

for the inner links and

$$\tau_b = 2L_b/c + T_{prep} \tag{3.35}$$

for the outer link (Bob). There is no factor of two in (3.34) because the optical Bell state measurement occurs in the middle of L_i. Hence, the total distance a photon travels from the QM to optical Bell state measurement and an optical signal travels from the optical Bell state measurement back to the node is L_i.

Generalizing the storage times from Table 3.1 for an arbitrary number of nodes, the dephasing parameter in (3.33) for the sequential protocol evaluates to

$$f_{dp}[n] = e^{\dfrac{-(3-2x)L}{cT_2}} \left(\frac{p_{OBSM}}{e^{\tau_p/T2} + p_{OBSM} - 1}\right)^{n-1} \left(\frac{p_b}{e^{\tau_b/T2} + p_b - 1}\right), \tag{3.36}$$

which we derive in Appendix A.3. We can easily verify that as $T2 \to \infty$, (3.36) approaches unity, implying the error causes by dephasing vanishes, as expected.

Node	QM	Time
1	1	$2L_a/c + L_i/c + \tau_p Q_1$
1	2	L_i/c
2	3	$2L_i/c + \tau_p Q_2$
2	4	L_i/c
3	5	$2L_i/c + \tau_b Q_b$
3	6	$2L_b/c$

Table 3.1: QM waiting times for a three-node quantum repeater. The parameter Q_i denotes the number of trials the successive link requires.

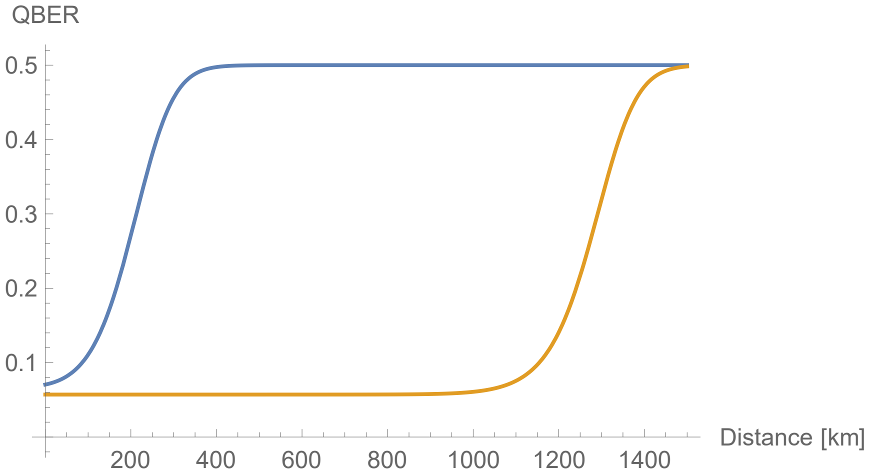

Figure 3.8: QBER in the X basis (blue curve) (3.32) and the Z basis (yellow curve) (3.31) of a two-node system, as a function of total communication distance, with $x = 0.35$.

Since the QBERs are essential in determining if any key can be distilled between Alice and Bob, we are interested in how the QBERs scale with length. Comparing (3.31) and (3.32), we notice that e_x and e_z are similar, except for the μ terms and the dephasing factor; although, μ_x and μ_z have the same length dependence. Figure 3.8 illustrates the difference between the QBER in the two bases using the parameters in Table 3.2. The QBER in the Z basis appears to be independent of length for approximately $L \leq 1000$ km for these parameters. This is not the case for the QBER in the X basis. The variation in length dependence between e_x and e_z is a result of the dephasing error. For low T_2, this dephasing parameter dominates the length dependence of e_x. We can conclude that dephasing error will limit the performance of our quantum repeater.

Protocol influence on key rate

We will not derive any explicit expressions in this subsection. Instead, we aim to provide some intuition for protocol affects on the key rate. The benefit to a simultaneous protocol mentioned in Section 3.3 manifests itself in the reduction of expected storage time within the QMs. The yield is unaffected, since the number of channel uses will not change. It is difficult to analytically calculate (3.33) for a simultaneous protocol, due to the different link spacing. Although, we did derive this function for the semi-simultaneous protocol mentioned in Section 3.3, where all of the inner links run simultaneously and the two outer links run sequentially, but we did not notice a significant benefit in this key rate with respect to the sequential protocol key rate. Figure 3.9 compares the key rates of these two protocols for some parameter set given in the figure caption. The key rates both depend on the geometric spacing, but the spacing can be chosen such that there is a marginal difference between the two key rates.

One may also conceive a protocol which aborts if some conditions are not met, for example, if a QM dephases for longer than a certain threshold time. Intuitively, this would decrease dephasing errors in the QMs as the total expected storage time would be limited, but this does not come without a price. The yield decreases in such situations owing to the decrease in probability that Alice and Bob share a bit of key. In [41] they show this trade-off between yield and dephasing error can be beneficial in some situations, albeit modest. We find a similar modest beneficial trade-off in the key rate performance when we introduce asymmetries to the geometric spacing in Section 3.6.1.

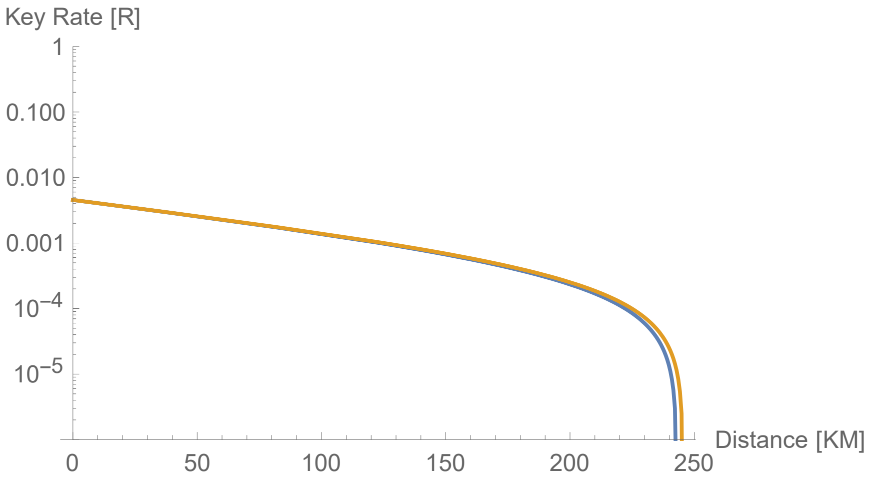

Figure 3.9: Comparing sequential protocol (blue curve) to the simultaneous (yellow curve), with parameters: $\eta_{tot} = 0.5$, $T_2 = 1s$, $n = 3$, $x = 0.25$ and those in Table 3.2.

3.4.1 Key rate scaling

From Equation (2.39), we observe the PLOB bound has a linear scaling with channel transmittance η_{ch}. Given the exponential behaviour of η_{ch} with respect to the length of fiber (3.8), the PLOB bound scales as

$$R_{PLOB} \approx \frac{1}{\log[2]} e^{-L/(L_{att})} \tag{3.37}$$

with respect to channel length. For the quantum repeater, the key rate scaling is determined from the yield, which, as we have already established at the beginning of this section, is inversely proportional to the number of channel uses. The key rate for a one-node system with the node directly in between Alice and Bob scales as

$$R \approx R_0 e^{-L/(2L_{att})}, \tag{3.38}$$

where R_0 represents the key rate at $L = 0$. Equation (3.38) can also be used as an upper bound on the key rate, since the error correction and privacy amplification term in the key rate (3.27) will act as an envelope.

The scaling is a bit different for a multi-node system, due to the different success probabilities of inner and outer links. In the absence of dark counts, the probability of success for the outer links is

$$p_{a,b} = \eta_{tot} e^{-xL/L_{att}}, \tag{3.39}$$

whereas the success probability of the inner links is

$$p_{OBSM} = \frac{1}{2}\eta_{tot}^2 e^{-(1-2x)L/((n-1)L_{att})}. \tag{3.40}$$

The key rate scaling is dominated by the link with success probability that is the lowest, as this will require the most channel uses for success. When $L = 0$, clearly $p_{OBSM} < p_{a,b}$, implying the inner links will require more channel uses until a successful event than the outer links. This implies our yield is limited by this inner process and we can use this as a crude upper bound on our key rate since the expected number of channel uses will increase with length. Denoting $R_{0,n}$ as the key rate for an n-node repeater at $L = 0$, we can always upper bound the key rate R by the scaling of the inner link success probability. Consequently, the key rate is upper bounded by

$$R \leq R_{0,n} e^{-(1-2x)L/((n-1)L_{att})}. \tag{3.41}$$

Figure 3.10 shows key rates compared to the upper bound scaling for a single-node and three-node quantum repeater, where we have used some arbitrary parameters to generate the key rates.

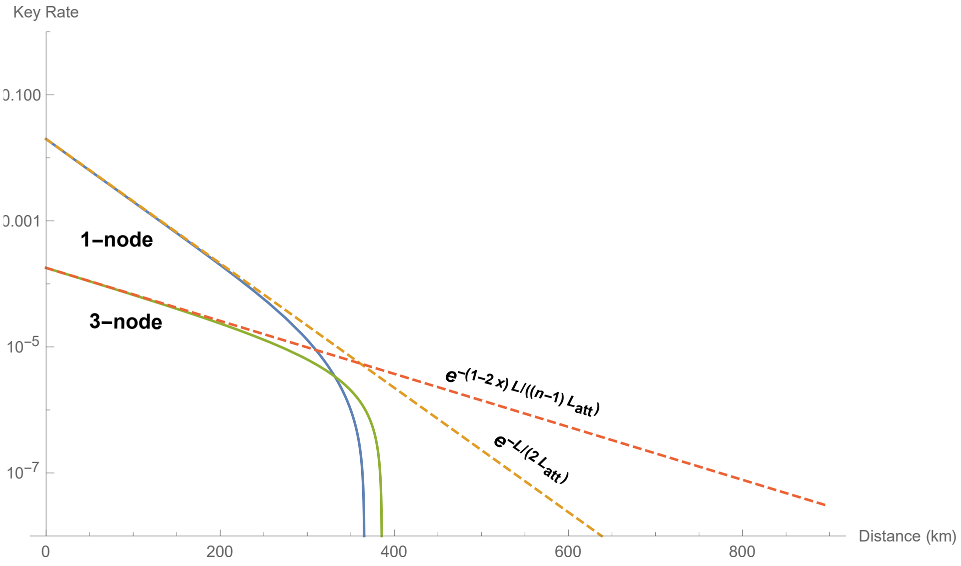

Figure 3.10: Key rates of a one-node (blue) and three-node (green) quantum repeater for arbitrarily chosen parameters. The key rate scalings (upper bounds) from (3.38) and (3.41) are indicated by the dashed curves.

If we consider a situation where there is no error in the system, we may observe two different scalings in the yield for the multi-node quantum repeater[6], depending on the geometric spacing. This situation occurs when the success probability of the outer links becomes larger than the inner links at some length, since the number of channel uses is limited by the link with the lowest probability. It is easy to verify from (3.39) and (3.40) that if $x = 1/(n+1)$, then the inner and outer link success probabilities have the same scaling with respect to length. Thus the channel use will still be dominated by the inner links. We can only observe this different scaling if $1/(n+1) \leq x \leq 0.5$ holds, as this can allow $p_{a,b} \leq p_{OBSM}$ at some arbitrary length. We observe the two different scaling behaviours in Figure 3.11. The intersection of these two curves, L_{sc}, occurs when

$$L_{sc} = L_{att}\left(\frac{n-1}{x(n+1)-1}\right)\log\left[\frac{R_{0,1}}{R_{0,n}}\right], \tag{3.42}$$

where $R_{0,1}$ is the key rate for $L = 0$ of the multi-node quantum repeater, assuming $p_{OBSM} = 1$. We can use the various key rate scalings for an improved upper bound than the one we previously stated in (3.41). In summary, the key rate is bounded by

$$R \leq \begin{cases} R_{0,n}e^{-(1-2x)L/((n-1)L_{att})} & 0 \leq x \leq 1/(n+1), \quad \forall L \\ R_{0,n}e^{-(1-2x)L/((n-1)L_{att})} & 1/(n+1) \leq x \leq 1/2, \quad L \leq L_{sc} \\ R_{0,1}e^{-xL/L_{att}} & 1/(n+1) \leq x \leq 1/2, \quad L \geq L_{sc}. \end{cases} \tag{3.43}$$

Although we cannot analytically solve at what length out key rate will cross the PLOB bound, we can use these key rate upper bounds to get an approximation. Solving the length at which (3.43) and (3.37) intersect, denoted by L_{int}, gives a lower bound on the crossover length on the crossover length L_{cross}. As a result, the crossover length is lower bounded by

$$L_{cross} \geq \begin{cases} -L_{att}\left(\dfrac{n-1}{n+2x-2}\right)\log[R_{0,n}\log[2]] & 0 \leq x \leq 1/(n+1), \quad \forall L \\ -L_{att}\left(\dfrac{n-1}{n+2x-2}\right)\log[R_{0,n}\log[2]] & 1/(n+1) \leq x \leq 1/2, \quad L_{int} \leq L_{sc} \\ -L_{att}\left(\dfrac{1}{1-x}\right)\log[R_{0,1}\log[2]] & 1/(n+1) \leq x \leq 1/2, \quad L_{int} \geq L_{sc} \end{cases} \tag{3.44}$$

Having these bounds on the crossover length will be needed for the approximate crossover regions calculated in the following section.

[6] We can include some error, but the key rate must be positive for lengths beyond L_{sc}, which is the length at which the scaling changes.

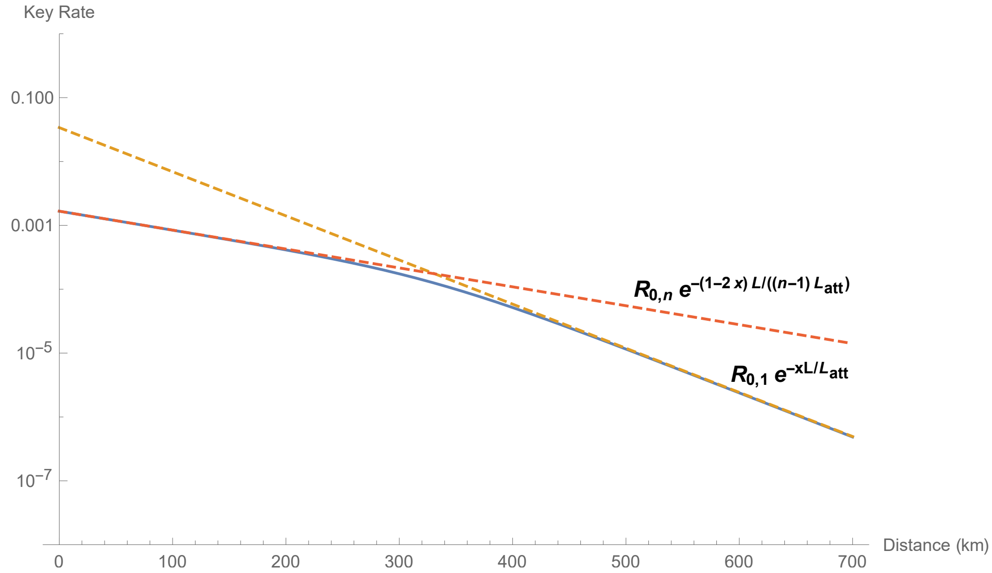

Figure 3.11: Observing different key rate scalings with parameters: x = 0.35, n = 3, η_{tot} = 0.1, and those in Table 3.2. The length at which the two dashed lines intersect is denoted by L_{sc}.

Optimal geometric spacing

We have established that the geometric spacing impacts the performance of the quantum repeater by affecting the yield and scaling. Since x is a free parameter, how should it be chosen such that the key rate beats the PLOB bound? From (3.43), we can argue that $1/(n+1) \leq x \leq 1/2$ should hold for optimal spacing, as the key rate scaling is better in this region than if $0 \leq x \leq 1/(n+1)$. Figure 3.12 corroborates this argument by showing plots of the optimal x value resulting in the maximum yield as a function of length for various number of nodes. As the length approaches infinity, the optimal x approaches $1/(n+1)$, indicated by the dashed lines.

There is also another factor we have to keep in mind when selecting x, since the geometric spacing will also affect the dephasing parameter in (3.36). As we discussed earlier in this section, the length dependence of e_x is predominantly dominated by the dephasing error, ultimately dictating the length at which the key rate reaches zero. We refer to this length as the cutoff length, denoted by L_{cutoff}. Varying x will causing L_{cutoff} to shift in a non-trivial way. Overall there are two effects to consider for the key rate dependence on x. We can choose x such that the key rate is optimized over length, or we can choose x to

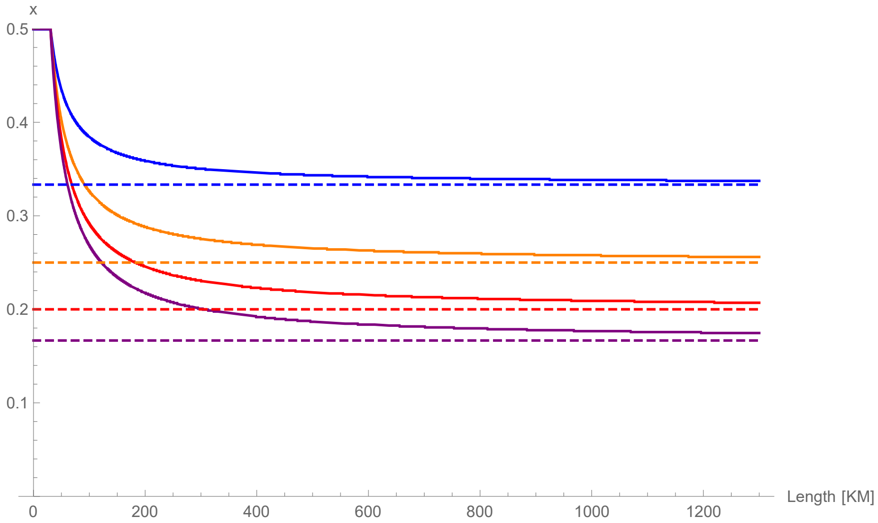

Figure 3.12: The optimal geometric spacing x as a function of length for $n = 2$, $n = 3$, $n = 4$, and $n = 5$ given by the blue, orange, red, and purple solid curves, respectively. The corresponding dashed lines indicate $1/(n+1)$. For this plot, we set $\eta_{tot} = 1$ and $p_{dark} = 0$.

optimize L_{cutoff}, allowing the key rate to extend to its maximum allowable length. Both of these effects need to be considered when optimizing our key rate to beat the PLOB bound. As a result, we have to numerically optimize over all possible x value when we look at beating the PLOB bound in the next section.

3.5 Positive key rate conditions

In all QKD protocols there exists a threshold error rate, denoted by e_{th}, such that no key can be distilled with a QBER in excess of e_{th}. We can use e_{th} to bound the QBERs, and consequently bound some of the system parameters contained in the QBERs expressions. The QBERs in the X (3.32) and Z (3.31) bases have an increasing dependence on length so to bound the QBERs we set $L = 0$. That is to say, at $L = 0$ the error rates are minimized as a function of length so we must satisfy these conditions to generate any key at all. We use this idea of bounding parameters based on threshold error rates. All of the calculations for this section are done assuming $L = 0$.

To solve e_{th}, we assume it to be the same in both the X and Z bases. From the key rate formula (3.27), we impose the condition

$$0 = 1 - h[e_{th}] - fh[e_{th}]. \tag{3.45}$$

Rearranging for e_{th} results in

$$e_{th} = h^{-1}\left[\frac{1}{1+f}\right], \tag{3.46}$$

where h^{-1} represents the inverse of the binary entropy function. Although there is not an analytic expression for this function, it can easily be computed numerically. We use an error correcting efficiency of $f = 1.16$, which results in $e_{th} \approx 9.81\%$.

3.5.1 Parameter bounds

We can use the threshold error rate to derive bounds on some of the parameters. For all of the following expressions, we assume the ideal case where $T_{prep} = 0$. This condition, in conjunction with assuming $L = 0$, will result in no dephasing error being introduced into the system. From (3.36), we can verify that $f_{dp}[n] = 1$. This results in a simplification of the QBER formulas, allowing us to find bounds on some of the parameters in the rest of this section.

Maximum number of nodes

If the photons are perfectly match, $\gamma = 1$, then we can verify that $e_z \geq e_x$[7]. We use e_x as our lower bound on the error in both bases. This implies $e_{th} \geq e_x$, or explicitly written out as

$$e_{th} \geq \frac{1}{2} - \frac{(1-2e_M)^{2n}\lambda_{BSM}^{n}\alpha^2\mu_x^{n-1}}{2} \tag{3.47}$$

Rearranging for n results in

$$n \leq \left\lfloor \frac{\log\left[\dfrac{(1-2e_{th})\mu_x}{\alpha^2}\right]}{\log[((1-2e_M)^2\lambda_{BSM}\mu_x)]} \right\rfloor, \tag{3.48}$$

[7] Although, they are nearly identical

which is an upper bound on the number of possible nodes for the quantum repeater. The function $\lfloor x \rfloor$ denotes the floor function, since n must be an integer. Substituting the appropriate variables into (3.48), we find an upper bound on the number of nodes as

$$n \leq \left\lfloor \frac{\log \left[\frac{(1-(1-\eta_{tot})(1-p_{dark})^2)^2(1-2e_{th})}{2p_{OBSM}} \right]}{\log \left[\frac{(1-2e_M)^2 \lambda_{BSM}(1-p_{dark})^2 \eta_{tot}^2}{2p_{OBSM}} \right]} \right\rfloor . \tag{3.49}$$

Any number of nodes exceeding this bound will introduce too much error into the system, resulting in no shared key between Alice and Bob. We will use this same idea for the remainder of parameter bounds in this section.

Maximum misalignment error

We can bound single parameters by assuming all other parameters are ideal. Setting all of the error parameters in (3.47) to ideal and rearranging for the misalignment error, we see that

$$e_M \leq \frac{1-(1-2e_{th})^{1/2n}}{2}. \tag{3.50}$$

QM Bell state measurement

Similarly, we can bound the noise from the QM Bell state measurement $1-\lambda_{BSM}$ by

$$1-\lambda_{BSM} \leq 1-(1-2e_{th})^{1/n} \tag{3.51}$$

3.5.2 One-node versus multi-node

Before we begin comparing the key rate of our quantum repeater to the PLOB bound, we first compare the key rate of a one-node quantum repeater to that of a multi-node quantum repeater. After all, we are interested to see if having more than one node to our quantum repeater is beneficial. Our goal in this section is to find conditions in the parameter space of η_{tot} and T_2 where a one-node quantum repeater will always have a higher key rate than a multi-node quantum repeater.

For any multi-node repeater, let us consider the case when $x = 0.5$. From (3.11), this implies that all of the inner link lengths L_i are equal to zero. Effectively, all of the nodes are bunched together in the center of the quantum repeater with no space between them. Intuitively, we can argue that this situation implies that a one-node repeater will always have a higher key rate. This is because the yield at $L = 0$ decreases as n increase and for $x = 0.5$, we see from (3.43) that the key rate scaling will be the same, regardless of node number. As well, the additional nodes will add more error into into the system causing the QBERs to increase and as a result L_{cutoff} will be lower. Figure 3.13 illustrates this situation, comparing a single-node to a two-node quantum repeater with $x = 0.5$.

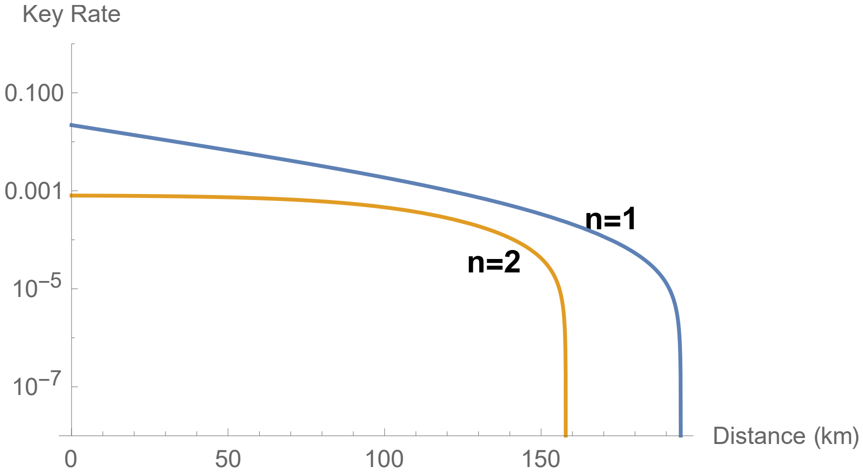

Figure 3.13: Key rates for a one-node (blue curve) and two-node (orange curve) quantum repeater with $x = 0.5$, $\eta_{tot} = 0.11$, $T_2 = 1s$, and the remaining parameters in Table 3.2.

The advantage gained by adding multiple nodes manifests itself in an improved key rate scaling over length. This scaling is a function of x, the geometric spacing. As we vary x from 0.5 to 0 we expect a multi-node system to achieve a higher key rate than the one-node system, at some distance. In order to achieve a better key rate, this implies that the cut-off length of the multi-mode system must increase, since the scaling will decrease with decreasing x. Here, we aim to find conditions such that varying x from 0.5 to 0 only decreases L_{cutoff} for the multi-mode quantum repeater. In other words, we want to find the conditions such that L_{cutoff} is maximized when $x = 0.5$. We have already established that the e_x dominates e_z and determines L_{cutoff}. The main contributor to this is the dephasing parameter, defined in (3.36) for the sequential protocol. This parameter is composed of a product of three terms, all depending on x. It is obvious that the first term is maximized when $x = 0.5$. It is the last two terms that significantly contribute to the cut-off, which

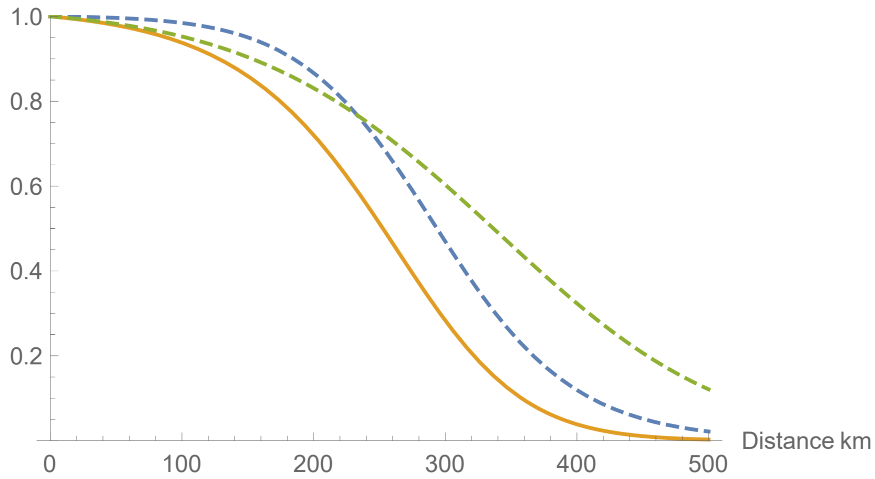

Figure 3.14: Comparing $F_b[L, x]$ (blue curve) and $F_p[L, x, n]$ (green curve) with $n = 3$, $x = 0.35$ and other parameters given in Table 3.2. The yellow curve is $f_{dp}[n]$ (3.33).

we define as the functions

$$F_p[L, x, n] = \left(\frac{p_{OBSM}}{e^{\tau_p/T2} + p_{OBSM} - 1} \right)^{n-1} \tag{3.52}$$

and

$$F_b[L, x] = \left(\frac{p_b}{e^{\tau_b/T2} + p_b - 1} \right). \tag{3.53}$$

For this calculation, we assume an ideal case where $p_{dark} = 0$, resulting in p_b and p_{OBSM} given by (3.39) and (3.40), respectively. We also assume $T_{prep} = 0$ to simplify some of the calculations and achieve an analytic solution. If $x = 0.5$, then (3.52) is independent of length and is equal to unity. Similarly, if $x = 0$, then (3.53) is independent of length and is equal unity. Since both functions have a range between zero and one, the smaller valued function will dominate the product of the two. Hence,

$$f_{dp}[n] \leq \min\{F_p[L, x, n], F_b[L, x]\}. \tag{3.54}$$

Figure 3.14 illustrates this, as we see that the dephasing parameter, $f_{dp}[n]$, is upper-bounded by the minimum of the two functions. We also see that both of these functions are sigmoid functions with an inflection point. Since the function $F_p[L, x, n]$ does not appear for a one-node repeater, the idea is to find conditions on $F_p[L, x, n]$ such that decreasing x

from 0.5 to 0 causes L_{cutoff} to decrease. Although not mathematically rigorous, this can be approximately done by setting the inflection point of $F_p[L, x, n]$ such that it occurs at $L = 0$. This means for $L \geq 0$ and $0 \leq x < 0.5$, the function is always concave up, with concavity increasing as x decreases. This will cause the product of $F_p[L, x, n]$ and $F_b[L, x]$ to have the same form and should cause L_{cutoff} to decrease as x decreases. We provide a detailed calculation of this in Appendix A.5 and find that for our multi-node quantum repeater and sequential protocol one-node is optimal, unless

$$\eta_{tot} \gtrapprox \sqrt{\frac{4L_{att}}{L_{att} + 2cT_2}} \tag{3.55}$$

holds. Rearranging for T_2, we find

$$T_2 \gtrapprox \left(\frac{4}{\eta_{tot}^2} - 1\right)\frac{L_{att}}{2c}, \tag{3.56}$$

which is shown graphically in Figure 3.15. The grid region represents conditions where a single-node quantum repeater is optimal. This region is not a strict bound and we should caution is only valid for the sequential protocol we have described.

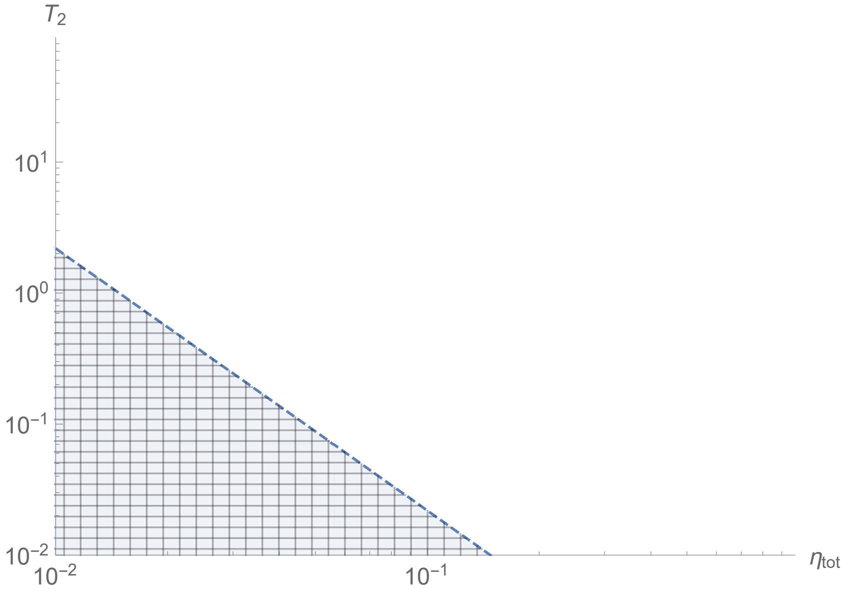

Figure 3.15: Region in η_{tot}-T_2 space where a single node repeater out performs a multi-node repeater for the sequential protocol.

3.6 Beating the PLOB bound

Since we have derived a general key rate for this protocol, we can now determine what parameters are needed to beat the PLOB bound. Keep in mind, we are not concerned with at what length our key rate beats the PLOB bound, we simply want to know if it is possible at any length. Since the parameter space is so large, we focus on two main experimental parameters of interested: η_{tot} and T_2 as these two parameters are often a focal point for experimental improvement. For benchmarking, we will look at the resources needed in the η_{tot}-T_2 space for beating the PLOB. First we will consider every other parameter to be ideal besides η_{tot} and T_2. This allows us to benchmark what is possible with a system only consisting of only inefficiencies and dephasing errors. Then we will consider other realistic parameters for imperfect implementations, which we have modelled in previous sections. We also provide and explore ideas for improving crossover regions.

Ideal crossover

First, we consider the situation where the only imperfections in the system model are the total inefficiencies and dephasing errors caused by the QMs. This allows us to observe what the best case situation is for our quantum repeater, as including other imperfections will only hinder the key rate performance and ultimately, reduce the crossover region in the η_{tot}-T_2 space. Figure 3.16 illustrates the boundaries for beating the PLOB bound for an increasing number of nodes. We observe from this figure that increasing the number of nodes in the quantum repeater does in fact decrease the resources needed in the η_{tot}-T_2 space to beat the PLOB bound. As well, we observe that the decrease in resources marginally improves with increasing node number. Does this imply that increasing n indefinitely will allow crossover of the PLOB bound to always be with less resources in this space? Not necessarily. In fact, this cannot be true for the sequential protocol. Consider the bound on T_2 in (3.56). If T_2 is below this, then the one-node repeater is optimal, but we see in Figure 3.17, a one-node repeater cannot beat the PLOB bound in that regime. So increasing n indefinitely cannot reach this limit, or else we have a contradiction where a one-node repeater can out perform the n-node repeater, yet the n-node repeater can beat the PLOB bound but the one-node repeater cannot. Although this is not a strict bound, we expect it to hold for large n and conclude that as n approaches infinitely, it must asymptotically reach a limit in the η_{tot}-T_2 space that satisfies (3.56). Unfortunately, the maximum number of nodes that we can numerically calculate the key rate for is about 50. Numerical error begins to dominate the key rates above this threshold so we cannot test the limit as n gets very large.

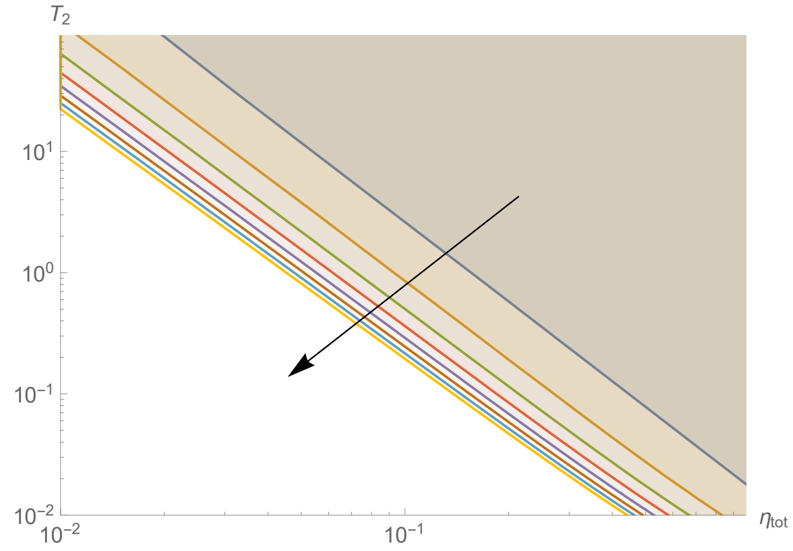

Figure 3.16: Regions in the η_{tot}-T_2 space where our quantum repeater beats the PLOB bound with perfect implementation, aside from efficiencies and dephasing errors. The different curves correspond to different node numbers. The upper, blue curve corresponds to a one-node quantum repeater. The arrow indicates increasing node number. Each successive region has n increasing by 1.

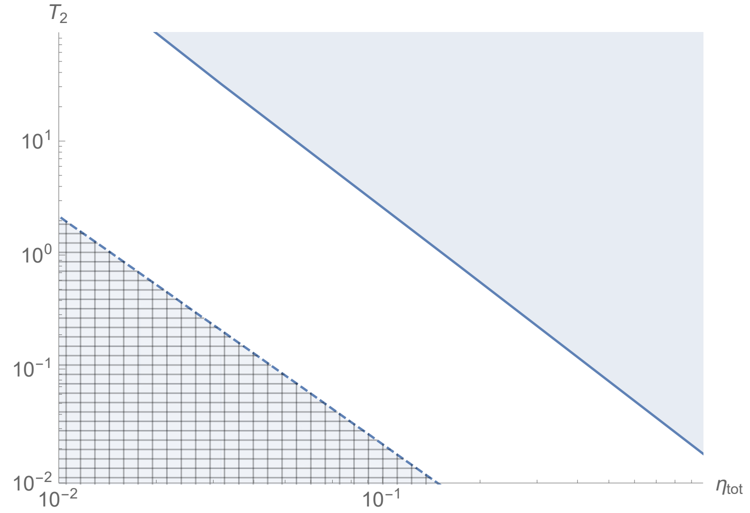

Figure 3.17: The grid area indicates where one-node is optimal, over n-nodes. The solid blue area indicates where a one-node repeater can beat the PLOB bound.

Realistic crossover

For a useful, realistic benchmark we must consider including other experimental imperfections. We use state-of-the-art experimental parameters for our system model, which are summarized in Table 3.2.

Parameter	Experimental Value
η_p (QM-Photon preparation efficiency)	2/3
T_p (QM-Photon preparation time)	$2\ \mu s$
η_c (QM-Photon coupling efficiency)	0.05
η_λ (Wavelength conversion efficiency)	0.5
T_2 (QM dephasing time)	2 s
c (Speed of light in fiber)	2×10^8 m/s
L_{att} (Fiber attenuation length)	22 km
e_M (Misalignment parameter)	0.01
p_{dark} (Dark count probability per detector)	1.8×10^{-11}
η_d (Detector efficiency)	0.7
p_{BSM} (BSM success probability)	1
λ_{BSM} (BSM ideality factor)	0.98
f (Error correction inefficiency)	1.16
V (HOM dip visibility)	0.95

Table 3.2: Current parameters used for analysis of this quantum repeater system. QMs are implemented with an ion trap scheme.

Figure 3.18 shows the region in η_{tot}-T_2 space where our quantum repeater will beat the PLOB bound. We observe from this figure that with the current parameters listed in Table 3.2, the one-node repeater beats the PLOB bound with the least resources in the η_{tot}-T_2 space. We also observe that for $n \geq 4$, there is no PLOB crossover. This can be predicted from (3.49), where $n \leq 3$ must hold for the given parameters[8]. Included on this plot is a point identifying the current η_{tot} and T_2 parameters. We observe that these current parameters are each about an order of magnitude off from satisfying the region where the quantum repeater beats the PLOB bound, implying the PLOB bound cannot be beaten with current state-of-the-art parameters.

[8] We use $\eta_{tot} = 1$, to get a best case situation, although there is not a strong dependence on η_{tot} in (3.49).

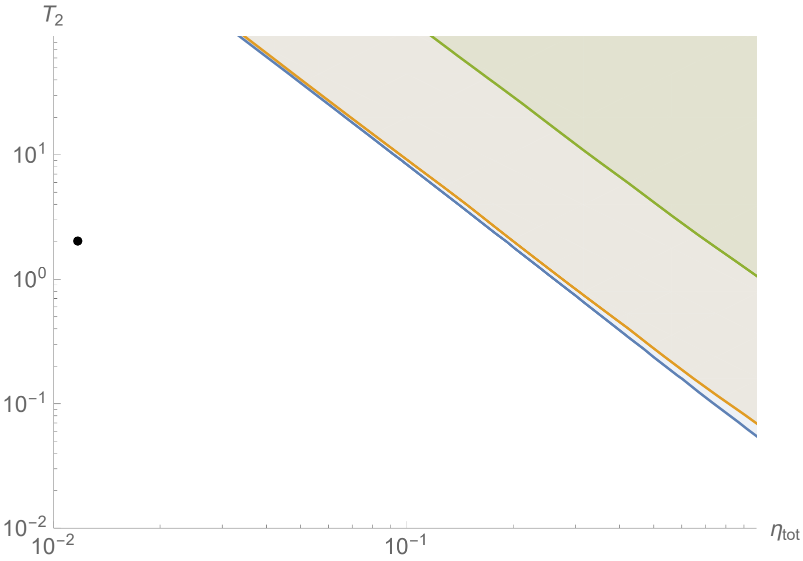

Figure 3.18: Regions in the η_{tot}-T_2 space where our quantum repeater beats the PLOB bound. The blue, orange, and green curves indicate a one, two, and three-node quantum repeater, respectively. The black dot indicates current η_{tot} and T_2 parameters, given in Table 3.2.

Approximating crossover

Solving an exact algebraic solution for when the key rate beats the PLOB bound is not possible due to the complexity of the functions and solving the crossover numerically is cumbersome, given that any change in parameter requires resolving the numerical crossover. The goal of this subsection is to find an equation to approximate crossover region in the η_{tot}-T_2 space. All of the equations in this subsection are derived in more detail in Appendix A.6.

Using a similar technique as [30], we find the fraction of total time the memories dephase to the T_2 time of the QMs, which is given by

$$\frac{1}{K} = \frac{\mathbb{E}\left[\sum_{i=1}^{i=2n} t_i\right]}{T_2}. \tag{3.57}$$

Instead of arbitrarily choosing K as a fit parameter that needs to be chosen to fit the numerics for each parameter set, as done in [30], we define K from the following equation

$$K = \frac{-1}{\log\left[\dfrac{1-2h^{-1}[1-fh[e_z]]}{(1-2e_M)^{2n}\lambda_{BSM}^{n}\alpha^2\mu_x^{n-1}}\right]}. \tag{3.58}$$

The main advantage of defining K this manner is that there is no need to numerically compute the crossover curves first, and then determine the arbitrary fitting parameter, which is done in [30]. One can simply get an approximate of the crossover region in η_{tot}-T_2 space by using this formula. Rearranging (3.57) for T_2 and solving the expectation value for the sequential protocol, we get

$$T_2 = K\left(\frac{2(n-1)\tau_P}{p_{OBSM}} + \frac{\tau_B}{p_b} + \frac{L_o(3-2x)}{c}\right), \tag{3.59}$$

where τ_p and τ_b are defined in (3.34) and (3.35), respectively. The length L_o is equal to the cutoff length, under the assumption that the key rate beats the PLOB bound. This means $L_o \geq L_{cross}$, since the key rate cutoff length must be larger than the crossover length.

To solve for T_2, the cutoff length L_o must be known, since it appears directly in (3.59) and since p_{OBSM}, p_b, τ_p and τ_b all depend on the total quantum repeater length. Despite not being able to solve L_{cross} analytically (and hence we cannot solve which L_o are valid), we do have a lower bound on L_{cross} from (3.44). Since $L_o \geq L_{cross}$, we set L_o equal to this lower bound, implying $L_o = L_{int}$. Using L_{int}, instead of the actual crossover length, will give a lower bound on the T_2 time as a function of η_{tot}. However, to get an approximation of the L_o required for actual crossover to occur, we add an arbitrarily chosen distance to L_{int}, so that $L_{int} \approx L_o$. For the calculation, adding a factor of 70 km gives a good fit for all of the curves analysed. While this is simply an arbitrarily chosen number, it seems robust for arbitrary parameter choices for the quantum repeater. Figure 3.19 compares the approximate crossover regions from (3.59) to the numerically calculated crossover regions.

3.6.1 Improving crossover

Improving parameters

One naive way to reduce resources in η_{tot}-T_2 space is to improve other parameters. Of course, this would be the goal for any experimentalist, but it is interesting to point out from (3.32) and (3.31) that decreasing the misalignment error e_M has a similar impact as decreasing the noise in the Bell state measurement. Both scale exponentially with the

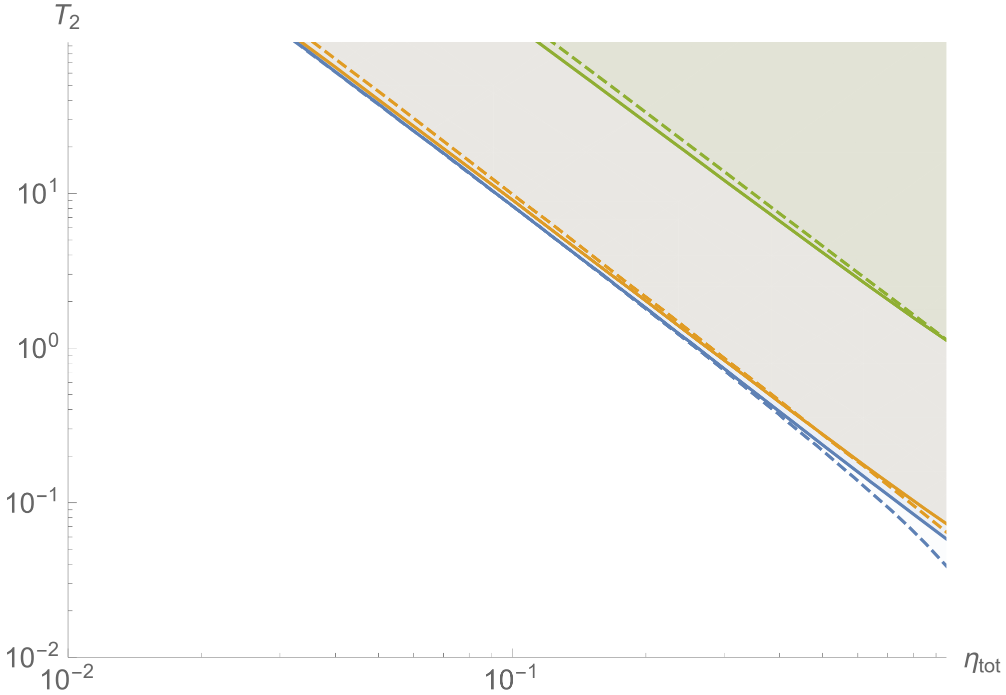

Figure 3.19: Regions in the η_{tot}-T_2 showing numerically calculated crossover regions (solid curves) and the approximate crossover regions (dashed curves) calculated from (3.59). The blue, yellow and green curves are for $n = 1$, $n = 2$ and $n = 3$.

number of nodes, so any hope in reducing these errors will be necessary to introduce more nodes.

Another avenue to explore is if the optical Bell state success probability is increased from at best 50% to 100%. Practically implementing improvements to the success probability would require much more additional resources, but it is worth investigating how it would affect the crossover regions. We did a heuristic calculation, changing the factor in (3.23) from 1/2 to 1 but keeping the error rates the same. There is a marginal improvement, as seen in Figure 3.20. We expect this effect to increase with increasing numbers of node, owing to the exponential dependence on n. Of course it is not possible to achieve unity success probability in practice so perhaps the efforts to increase this probability may not be worth in resources for implementation.

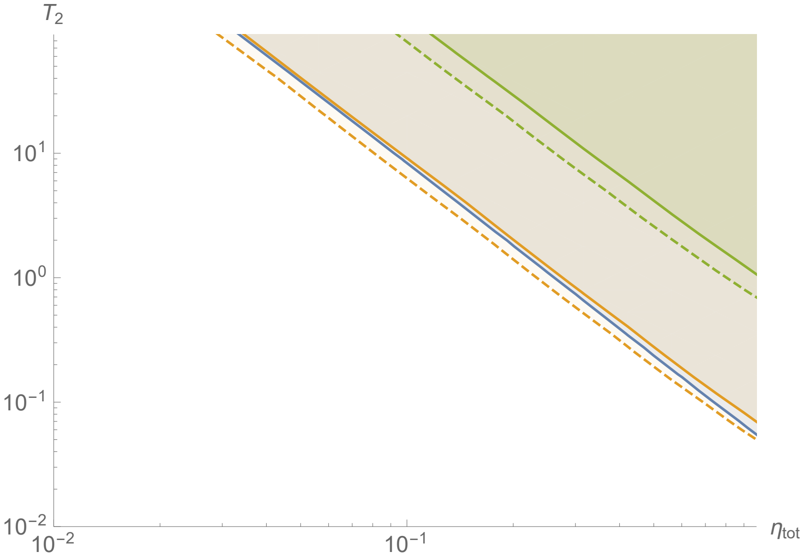

Figure 3.20: Comparing an optical Bell state measurement with at most unity success probability (dashed curves) to the at best 50% case (solid curves) for a two-node (orange) and three-node (green curve) quantum repeater.

Introducing asymmetries

A simple way to improve the crossover region is to introduce asymmetries into the geometry of the link lengths. For the sequential protocol, the expectation value of the total time the QMs store a state depends on the overall length of the setup, and the expected number of trials it takes for a successful event in the links. It is important to note that the overall expectation value for memory storage time in (3.36) is independent of the number of trials it takes for the first link to succeed (QM 1 to Alice) because QM 1 does not store a quantum state until it has heralded a successful measurement by Alice. This can be exploited to decrease the overall storage expectation time of the QMs, and ultimately decrease the error caused by dephasing, by making the first link L_a longer than the last link L_b. However, this exploitation does not come without a price, introducing this asymmetry results in an increase of the expected channel uses (see Section A.4.1), thus deceasing the yield. Despite this trade off, there is still an advantage when comparing key rates of this asymmetric setup to that of a symmetric setup. This can be seen in Figure 3.21. There is no benefit to introducing asymmetries in the inner links for the same reason of increasing channel uses and it will increase QM storage time (see Section A.4.2).

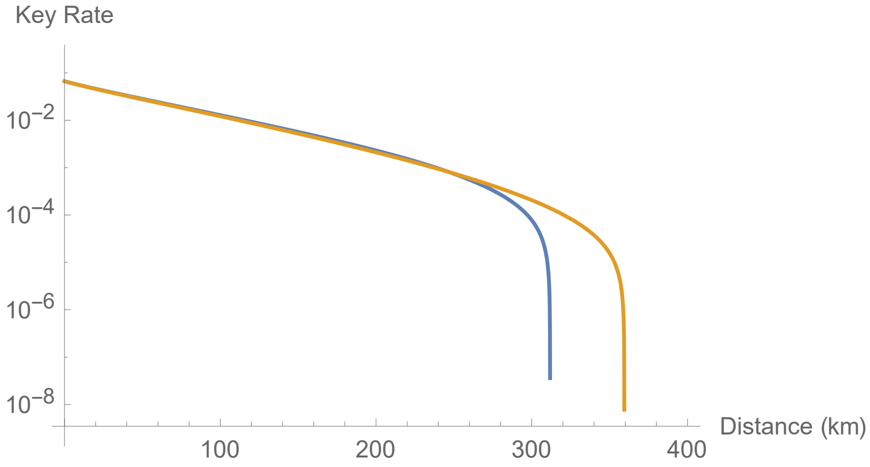

Figure 3.21: Comparing symmetric (blue) and asymmetric (yellow) key rates for $n = 2$. All other parameters used from Table 3.2, except $\eta_{tot} = 1$ to more clearly highlight the difference.

We see in Figure 3.22 that introducing asymmetries to the geometric spacing increase the η_{tot}-T_2 parameter space in which a crossover of the PLOB bound can occur. We also see that it becomes possible for a two-node repeater to crossover with fewer resources than a one-node repeater, albeit very minimally. Figures 3.23 and 3.24 also show crossover regions are possible for less ideal parameters in $x - y$ space when asymmetries are introduced. The symmetric space, where $x = y$, is denoted by the light blue line in both figures. It is clear that this line does not intersect the regions where our parameters are less ideal. From these two figures we observe that $x \approx 0.6$ and $y \approx 0.25$ are the optimal choices for a two-node

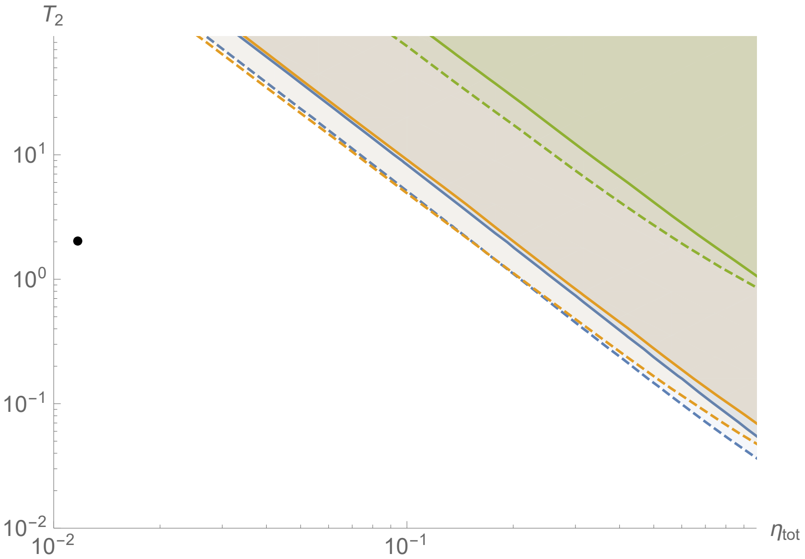

Figure 3.22: Regions in the η_{tot}-T_2 space where our quantum repeater beats the PLOB bound. The blue, orange and green curves indicate a one, two and three-node quantum repeater, respectively. The dashed (solid) curves indicate an asymmetric (symmetric) geometric spacing.

system.

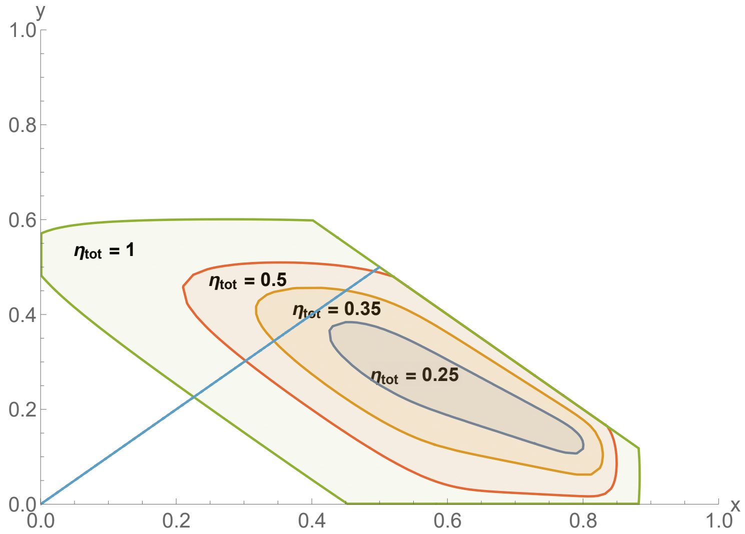

Figure 3.23: Regions in the x-y space where a two-node quantum repeater can beat the PLOB bound. Here η_{tot} is varied, with $T_2 = 1$ s. The straight blue line indicates the regime where a symmetric setup is possible.

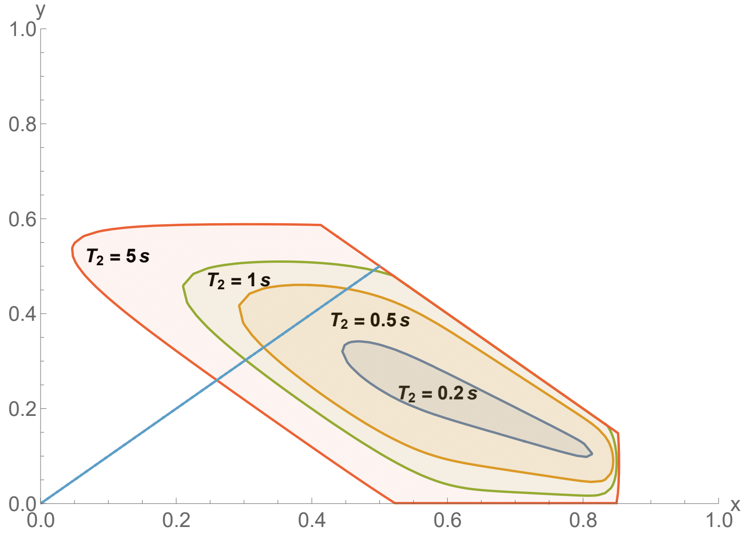

Figure 3.24: Regions in the x-y regime where a two-node quantum repeater can beat the PLOB bound. Here T_2 is varied, with $\eta_{tot} = 0.5$. The straight blue line indicates the regime where a symmetric setup is possible

Chapter 4

Conclusion

We have seen that there is potential for improving the performance of the quantum repeater in [30] by adding more nodes to the system. However, by incorporating realistic imperfections to our model, the marginal advantages gained by adding more nodes may be crippled by the accumulating errors each one introduces. Given current state-of-the-art experimental parameters, there does not appear to be any advantage in using more than one node for beating the PLOB bound with this quantum repeater examined.

We have explored different possibilities for improving the key rate performance. For the sequential protocol analysed, we can exploit asymmetries in the node spacing to reduce overall quantum memory storage times. This reduces the resources in η_{tot}-T_2 space needed for the repeater to beat the PLOB bound and appears to have the same beneficial outcome, regardless of node number. Efforts to implement a more efficient optical Bell state measurement between inner nodes will improve the repeaters performance, of course, but may not be too fruitful for realistic implementation. Improvements in other experimental parameters affecting error rates, especially with power n scaling, can drastically improve performance for multi-node repeaters and allow an increase in allowable nodes.

In summary, the addition efforts to implement a multi-node quantum repeater may be futile for experimentally beating the PLOB bound. For now, it seems a one-node quantum repeater is the most feasible experimental choice for beating the PLOB bound with this type of quantum repeater.

References

[1] S. Abruzzo, H. Kampermann, and D. Bruß. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A*, 89:012301, Jan 2014.

[2] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, Aug 2008.

[3] S. C. Benjamin, D. E. Browne, J. Fitzsimons, and J. J. L. Morton. Brokered graph-state quantum computation. *New Journal of Physics*, 8(8):141, 2006.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[6] M. Benyoucef, M. Yacob, J. P. Reithmaier, J. Kettler, and P. Michler. Telecom-wavelength (1.5m) single-photon emission from inp-based quantum dots. *Applied Physics Letters*, 103(16):162101, 2013.

[7] B. B. Blinov, D. L. Moehring, L.-M. Duan, and C. Monroe. Observation of entanglement between a single trapped atom and a single photon. *Nature*, 428(6979):153–157, Mar 2004.

[8] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.*, 82:2594–2597, Mar 1999.

[9] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72(1):67–71, Jan 2001.

[10] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin. Fault-tolerant quantum communication based on solid-state photon emitters. *Phys. Rev. Lett.*, 96:070504, Feb 2006.

[11] 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, Nov 2001.

[12] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *Phys. Rev. A*, 59:169–181, Jan 1999.

[13] B. Eisenberg. On the expectation of the maximum of iid geometric random variables. *Statistics & Probability Letters*, 78(2):135–143, 2008.

[14] C. Elliott. Building the quantum network. *New Journal of Physics*, 4(1):46, 2002.

[15] A. R. McMillan et al. Two-photon interference between disparate sources for quantum networking. *Sci Rep*, 3:2032, Jun 2013. 23783585[pmid].

[16] C. Simon et al. Quantum memories. *The European Physical Journal D*, 58(1):1–22, May 2010.

[17] H.-L. Yin et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[18] T. Gerrits, F. Marsili, V. B. Verma, L. K. Shalm, M. Shaw, R. P. Mirin, and S. W. Nam. Spectral correlation measurements at the hong-ou-mandel interference dip. *Phys. Rev. A*, 91:013830, Jan 2015.

[19] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas. High-fidelity preparation, gates, memory, and readout of a trapped-ion quantum bit. *Phys. Rev. Lett.*, 113:220501, Nov 2014.

[20] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987.

[21] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, Dec 1993.

[22] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin. Quantum repeater with encoding. *Phys. Rev. A*, 79:032325, Mar 2009.

[23] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing.* Oxford University Press, 2007.

[24] T. Kim, P. Maunz, and J. Kim. Efficient collection of single photons emitted from a trapped ion into a single-mode fiber for scalable quantum-information processing. *Phys. Rev. A*, 84:063423, Dec 2011.

[25] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, Jan 2001.

[26] P. Kok. *Five Lectures on Optical Quantum Computing*, pages 187–219. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[27] C. Langer, R. Ozeri, J. D. Jost, J. Chiaverini, B. DeMarco, A. Ben-Kish, R. B. Blakestad, J. Britton, D. B. Hume, W. M. Itano, D. Leibfried, R. Reichle, T. Rosenband, T. Schaetz, P. O. Schmidt, and D. J. Wineland. Long-lived qubit memory using atomic ions. *Phys. Rev. Lett.*, 95:060502, Aug 2005.

[28] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[29] H.-K. Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptology*, 18(2):133–165, 2005.

[30] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus. Overcoming lossy channel bounds using a single quantum repeater node. *Applied Physics B*, 122(4):96, Apr 2016.

[31] N. Lütkenhaus. Quantum key distribution. In E. Andersson and P. Öhberg, editors, *Quantum Information and Coherence*, pages 107–146. Springer Publishing Company, Incorporated, 2014.

[32] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4(10):686–689, Oct 2010.

[33] N. Massa. Fiber optic telecommunication. *Fundamentals of Photonics. University of Conneticut*, 2000.

[34] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.*, 100:150404, Apr 2008.

[35] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[36] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, and C. Monroe. Quantum teleportation between distant matter qubits. *Science*, 323(5913):486–489, 2009.

[37] S. Olmschenk, K. C. Younge, D. L. Moehring, D. N. Matsukevich, P. Maunz, and C. Monroe. Manipulation and detection of a trapped yb$^+$ hyperfine qubit. *Phys. Rev. A*, 76:052314, Nov 2007.

[38] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, Apr 2017.

[39] M. Razavi, M. Piani, and N. Lütkenhaus. Quantum repeaters with imperfect memories: Cost and scalability. *Phys. Rev. A*, 80:032301, Sep 2009.

[40] P. P. Rohde and T. C. Ralph. Error models for mode mismatch in linear optics quantum computing. *Phys. Rev. A*, 73:062312, Jun 2006.

[41] F. Rozpędek, K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss. Realistic parameter regimes for a single sequential quantum repeater. *ArXiv e-prints*, April 2017.

[42] S. Sajeed, A.i Huang, S.. Sun, F. Xu, V. Makarov, and M. Curty. Insecurity of detector-device-independent quantum key distribution. *Phys. Rev. Lett.*, 117:250505, Dec 2016.

[43] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[44] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[45] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, Oct 1949.

[46] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[47] E. Solano, R. L. de Matos Filho, and N. Zagury. Deterministic bell states and measurement of the motional state of two trapped ions. *Phys. Rev. A*, 59:R2539–R2543, Apr 1999.

[48] H. P. Specht, C. Nolleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe. A single-atom quantum memory. *Nature*, 473(7346):190–193, May 2011.

[49] M. Takeoka, S. Guha, and M. M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, Aug 2014.

[50] S. E. Vinay and P. Kok. Practical repeaters for ultralong-distance quantum communication. *Phys. Rev. A*, 95:052336, May 2017.

[51] W. Vogel, D.G. Welsch, and S. Wallentowitz. *Quantum Optics: An Introduction*. Wiley, 2001.

[52] J. Volz, M. Weber, D. Schlenk, W. Rosenfeld, J. Vrana, K. Saucke, C. Kurtsiefer, and H. Weinfurter. Observation of entanglement of a single photon with a trapped atom. *Phys. Rev. Lett.*, 96:030404, Jan 2006.

[53] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

APPENDICES

Appendix A

Derivations

A.1 Optical Bell state measurement

In this section we derive the success probability and error rates of the optical Bell state measurement in Figure 2.2. The photon states contained within the input state in (3.18) can be written in terms of the creation operators, resulting in

$$\begin{aligned}|\Psi\rangle_{input} = \frac{\sqrt{\gamma}}{2}\Big(\hat{a}_H\hat{b}_H|00\rangle + \hat{a}_H\hat{b}_V|01\rangle + \hat{a}_V\hat{b}_H|10\rangle + \hat{a}_V\hat{b}_V|11\rangle\Big)|vac\rangle + \\ \frac{\sqrt{1-\gamma}}{2}\Big(\hat{a}_H\hat{b}_{\bar{H}}|00\rangle + \hat{a}_H\hat{b}_{\bar{V}}|01\rangle + \hat{a}_V\hat{b}_{\bar{H}}|10\rangle + \hat{a}_V\hat{b}_{\bar{V}}|11\rangle\Big)|vac\rangle,\end{aligned} \tag{A.1}$$

where the kets $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ correspond to the qubit states stored in the two QMs entangled with the input photons. The 50/50 beam splitter causes the photon creation operators evolve according to (2.28), resulting in the state

$$
\begin{aligned}
|\Psi\rangle_{output} = \frac{\sqrt{\gamma}}{2}\Bigg(\Bigg(\frac{\hat{c}_H^2 - \hat{d}_H^2}{2}\Bigg)|00\rangle + \Bigg(\frac{\hat{c}_H\hat{c}_V + \hat{c}_H\hat{d}_V - \hat{d}_H\hat{c}_V - \hat{d}_H\hat{d}_V}{2}\Bigg)|01\rangle + \\
\Bigg(\frac{\hat{c}_V\hat{c}_H + \hat{c}_V\hat{d}_H - \hat{d}_V\hat{c}_H - \hat{d}_V\hat{d}_H}{2}\Bigg)|10\rangle + \Bigg(\frac{\hat{c}_V^2 - \hat{d}_V^2}{2}\Bigg)|11\rangle\Bigg)|vac\rangle + \\
\frac{\sqrt{1-\gamma}}{2}\Bigg(\Bigg(\frac{\hat{c}_H\hat{c}_{\bar{H}} + \hat{c}_H\hat{d}_{\bar{H}} - \hat{d}_H\hat{c}_{\bar{H}} - \hat{d}_H\hat{d}_{\bar{H}}}{2}\Bigg)|00\rangle + \\
\Bigg(\frac{\hat{c}_H\hat{c}_{\bar{V}} + \hat{c}_H\hat{d}_{\bar{V}} - \hat{d}_H\hat{c}_{\bar{V}} - \hat{d}_H\hat{d}_{\bar{V}}}{2}\Bigg)|01\rangle + \\
\Bigg(\frac{\hat{c}_V\hat{c}_{\bar{H}} + \hat{c}_V\hat{d}_{\bar{H}} - \hat{d}_V\hat{c}_{\bar{H}} - \hat{d}_V\hat{d}_{\bar{H}}}{2}\Bigg)|10\rangle + \\
\Bigg(\frac{\hat{c}_V\hat{c}_{\bar{V}} + \hat{c}_V\hat{d}_{\bar{V}} - \hat{d}_V\hat{c}_{\bar{V}} - \hat{d}_V\hat{d}_{\bar{V}}}{2}\Bigg)|11\rangle\Bigg)|vac\rangle
\end{aligned}
\tag{A.2}
$$

at the detectors. The creation operators act on the vacuum state to create photons in the four spatial modes indicated in Figure 2.2, which correspond to the four different detectors. Each detector contains two modes, corresponding to matched and mismatch photons (see Figure 3.3). To be consistent with our naming convention, we denote mode 1 as corresponding to the matched mode and mode 2 as corresponding to the mismatched mode. For clarity, we label the output photon ket vectors by its modes: polarization, spatial, and other mismatch. The vector labelling convention we use is $|c_{H,1},\ c_{H,2},\ c_{V,1},\ c_{V,2},\ d_{H,1},\ d_{H,2},\ d_{V,1},\ d_{V,2}\rangle$, where each vetor entry corresponds to the number of photons residing in each mode. We can explicitly write the output state in (A.2) as

$$\begin{aligned}
|\Psi\rangle_{output} = \frac{\sqrt{\gamma}}{2}\Bigg(\Bigg(\frac{|20000000\rangle - |00002000\rangle}{\sqrt{2}}\Bigg)|00\rangle + \\
\Bigg(\frac{|10100000\rangle + |10000010\rangle - |00101000\rangle - |00001010\rangle}{2}\Bigg)|01\rangle + \\
\Bigg(\frac{|10100000\rangle + |00101000\rangle - |10000010\rangle - |00001010\rangle}{2}\Bigg)|10\rangle + \\
\Bigg(\frac{|00200000\rangle - |0000020\rangle}{2}\Bigg)|11\rangle\Bigg) + \\
\frac{\sqrt{1-\gamma}}{2}\Bigg(\Bigg(\frac{|11000000\rangle + |10000100\rangle - |01001000\rangle - |00001100\rangle}{2}\Bigg)|00\rangle + \\
\Bigg(\frac{|10010000\rangle + |10000001\rangle - |00011000\rangle - |00001001\rangle}{2}\Bigg)|01\rangle + \\
\Bigg(\frac{|01100000\rangle + |00100100\rangle - |01000010\rangle - |00000110\rangle}{2}\Bigg)|10\rangle + \\
\Bigg(\frac{|00110000\rangle + |00100001\rangle - |00010010\rangle - |00000011\rangle}{2}\Bigg)|11\rangle\Bigg). \qquad \text{(A.3)}
\end{aligned}$$

We can express (A.3) as a density state, given by

$$\rho_{output} = |\Psi\rangle_{output}\langle\Psi|_{output}. \qquad \text{(A.4)}$$

To calculate the success probability of the optical Bell state measurement, we trace out the two QM qubit states in ρ_{output}, resulting in a reduced density matrix, denoted by $\hat{\rho}_{output}$. The POVM elements heralding a successful optical Bell state measurement, according to Table 2.3, can be constructed using the POVM elements in (3.5, 3.6). They are given by

$$\begin{aligned}
\bar{F}_{(1,4)} &= \bar{F}_{click} \otimes \bar{F}_{vac} \otimes \bar{F}_{vac} \otimes \bar{F}_{click}, && \text{(A.5)} \\
\bar{F}_{(1,2)} &= \bar{F}_{click} \otimes \bar{F}_{click} \otimes \bar{F}_{vac} \otimes \bar{F}_{vac}, && \text{(A.6)} \\
\bar{F}_{(3,4)} &= \bar{F}_{vac} \otimes \bar{F}_{vac} \otimes \bar{F}_{click} \otimes \bar{F}_{click}, && \text{(A.7)}
\end{aligned}$$

and

$$\bar{F}_{(2,3)} = \bar{F}_{vac} \otimes \bar{F}_{click} \otimes \bar{F}_{click} \otimes \bar{F}_{vac}. \qquad \text{(A.8)}$$

Owing to the diagonal structure of these POVM elements, the outer product terms of orthogonal photon states in ρ_{output} do not contribute to the measurement success probability or error rate. As a result, these orthogonal outer product photon states can be ignored. Matched and mismatched photon states are orthogonal before and after propagating through the linear optic components in the optical Bell state measurement and because of this, the input density matrix can be written as a mixed state of matched and mismatched photons, as in as in (3.20). The success probability of the optical Bell state measurement is calculated from

$$P_{OBSM} = Tr[(\bar{F}_{(1,4)} + \bar{F}_{(1,2)} + \bar{F}_{(3,4)} + \bar{F}_{(2,3)})\hat{\rho}_{output}], \tag{A.9}$$

which yields the equation in (3.23).

A similar calculation is done to determine the error introduced by optical Bell state measurement. An error occurs when the outcome of the optical Bell state measurement indicates an incorrect correlation between the qubit states in the two QMs. For example, a click in detectors 1 and 4 should yield anti-correlated qubits in the Z basis. We condition on all of the cases where a Bell state measurement outcome will yield incorrect correlations between the states in the two QMs. We use the output state described by ρ_{output} in (A.4), where we have not traced out the QM states. The POVM elements are modified to account for errors in correlations between QM states. In the Z basis, it is given by

$$\begin{aligned} \bar{F}_{e,z} \quad = \quad & \bar{F}_{(1,4)} \otimes |00\rangle\langle 00| + \bar{F}_{(1,4)}|11\rangle\langle 11| + \\ & \bar{F}_{(1,2)} \otimes |00\rangle\langle 00| + \bar{F}_{(1,2)}|11\rangle\langle 11| + \\ & \bar{F}_{(3,4)} \otimes |00\rangle\langle 00| + \bar{F}_{(3,4)}|11\rangle\langle 11| + \\ & \bar{F}_{(2,3)} \otimes |00\rangle\langle 00| + \bar{F}_{(2,3)}|11\rangle\langle 11|. \end{aligned} \tag{A.10}$$

The QBER in this basis can be calculated as

$$e_{obsm,z} = \frac{Tr[\bar{F}_{e,z}\rho_{output}]}{p_{OBSM}}, \tag{A.11}$$

yielding equation (3.25). Similarly for the X basis, the POVM is given by

$$\begin{aligned} \bar{F}_{e,x} \quad = \quad & \bar{F}_{(1,4)} \otimes |++\rangle\langle ++| + \bar{F}_{(1,4)}|--\rangle\langle --| + \\ & \bar{F}_{(1,2)} \otimes |+-\rangle\langle +-| + \bar{F}_{(1,2)}|-+\rangle\langle -+| + \\ & \bar{F}_{(3,4)} \otimes |+-\rangle\langle +-| + \bar{F}_{(3,4)}|-+\rangle\langle -+| + \\ & \bar{F}_{(2,3)} \otimes |++\rangle\langle ++| + \bar{F}_{(2,3)}|--\rangle\langle --| \end{aligned} \tag{A.12}$$

and the QBER is given by

$$e_{obsm,x} = \frac{Tr[\bar{F}_{e,x}\rho_{output}]}{p_{OBSM}}, \tag{A.13}$$

yielding equation (3.26).

A.2 Channel uses

We derive the maximum number of channel uses in (3.29) using a smiliar method given in [13]. Each link in Figure 3.7 is modelled as a discrete geometric random variable X_i with probability distribution

$$P[X_i = k] = (1 - p_i)^{k-1} p_i, \tag{A.14}$$

where $k \geq 1$ and denotes the number of trials until success, and p_i denotes the probability of success for each link. For each link the probability of succeeding in k or less trials is given by

$$P[X_i \leq k] = 1 - (1 - p_i)^k. \tag{A.15}$$

We combine all of the geometric random variables into a set $\mathbb{X}$, where

$$\mathbb{X} = \{X_a, X_1, X_2, ..., X_{n-1}, X_b\}. \tag{A.16}$$

For clarity, we denote Alice and Bob's link with the subscript a and b, in accordance with the labelling convention in Figure 3.7. We let $M = max\{\mathbb{X}\}$, so that the probability that all the events X_i succeed in k trials or less is given by

$$\begin{aligned} P[M \leq k] &= \prod_{a,b,i=1}^{n-1} (1 - (1 - p_i)^k) \\ P[M \leq k] &= (1 - (1 - p_a)^k)(1 - (1 - p_b)^k) \prod_{i=1}^{n-1} (1 - (1 - p_i)^k \end{aligned} \tag{A.17}$$

The expected number of trials is given by the sum of probabilities of not succeeding in less than k trials [13]. Thus, the expected number of channel uses is given by

$$\begin{aligned} \mathbb{E}[M] &= \sum_{k=0}^{k=\infty} P[M > k] \\ \mathbb{E}[M] &= \sum_{k=0}^{k=\infty} \left(1 - (1 - (1 - p_a)^k)(1 - (1 - p_b)^k) \prod_{i=1}^{n-1} (1 - (1 - p_i)^k)\right). \end{aligned} \tag{A.18}$$

A.3 Sequential dephasing parameter

We derive an explicit expression for the dephasing parameter for the case of the sequential protocol. Regardless of the chosen protocol, the dephasing parameter is given by

$$f_{dp}[n] = \mathbb{E}\left[e^{-\sum_{i=1}^{i=2n} t_i / T_2}\right], \tag{A.19}$$

which can be written as

$$f_{dp}[n] = \mathbb{E}\left[\prod_{i=1}^{i=2n} e^{-t_i/T_2}\right] \tag{A.20}$$

We can find explicit values for the wait times t_i by analysing the protocol. In Table 3.1 we show the wait times for the QMs of a three-node quantum repeater. Generalizing to an n-node system results in

$$f_{dp}[n] \;=\; \mathbb{E}\left[e^{-(3-2x)L/(cT_2)} \prod_{i=1}^{i=n-1} e^{-\tau_p Q_i/T_2} e^{-\tau_b Q_b/T_2}\right]. \tag{A.21}$$

We are able to factor out the variables from the expectation value that do not depend on the number of trials, Q_i or Q_b. Since the protocol runs sequentially, Q_i and Q_b are all independent random variables. This implies the expectation value of the product of random variables exponentiated can be factored into a product of expectation values of the exponent of random variables

$$f_{dp}[n] \;=\; e^{-(3-2x)L/(cT_2)} \prod_{i=1}^{i=n-1} \mathbb{E}\left[e^{-\tau_p Q_i/T_2}\right] \mathbb{E}\left[e^{-\tau_b Q_b/T_2}\right]. \tag{A.22}$$

For a geometric random variable Q with success probability p, the expectation value $\mathbb{E}\left[e^{-aQ}\right]$ can be evaluated as

$$\begin{aligned} \mathbb{E}\left[e^{-aQ}\right] &= \sum_{k=1}^{\infty} p(1-p)^{k-1} e^{-ak} \\ &= \left(\frac{p}{e^a + p - 1}\right), \end{aligned} \tag{A.23}$$

where a is a constant. Since the inner links have the same length, they have the same geometric probability distribution Q_i. Hence, the product of expectation values can be written as a power of $n-1$. The explicit expression for the dephasing parameter of the sequential protocol is evaluated to be

$$f_{dp}[n] = e^{\dfrac{-(3-2x)L}{cT_2}} \left(\frac{p_{OBSM}}{e^{\tau_p/T2} + p_{OBSM} - 1}\right)^{n-1} \left(\frac{p_b}{e^{\tau_b/T2} + p_b - 1}\right). \tag{A.24}$$

A.4 Two events: Symmetric versus asymmetric

In Figure 3.22 we observe that adding asymmetries to the system geometry allows for crossover of the PLOB bound to happen with less resources in the η_{tot}-T_2 space. Here we will aim to show two things: First, introducing asymmetries between similar links (either between Alice and Bob's links, or between any of the inner links) results in an increased number of channel uses. Second, we show that for the inner links, introducing asymmetries increases overall QM storage times. Note, this proof is only considering two links. We did not prove it for an arbitrary number of links, but it is believed to hold true.

Let us assume that we have two IID geometric random variables, both with success probabilities that depend on some parameter, which we denote by L (length), and scale exponentially, so $p[L] = e^{-L}$.

A.4.1 Channel use

First we show the minimum number of channel uses occurs when $L_n = L_m$. We define these lengths as $L_n = L + \epsilon$ and $L_m = L - \epsilon$. Using (3.29) for two events

$$\mathbb{E}[\#channel\ uses] = \frac{1}{p[L_m]} + \frac{1}{p[L_n]} - \frac{1}{p[L_m] + p[L_n] - p[L_m]p[L_n]}. \tag{A.25}$$

We aim to show that

$$\frac{1}{p[L_m]} + \frac{1}{p[L_n]} - \frac{1}{p[L_m] + p[L_n] - p[L_m]p[L_n]} \geq \frac{2}{p[L]} - \frac{1}{2p[L] - p[L]^2} \tag{A.26}$$

holds. We will show the first two terms on the left are greater than the first term on the right.

$$\begin{aligned} \frac{1}{p[L_m]} + \frac{1}{p[L_n]} &\geq \frac{2}{p[L]} \\ e^{L_n} + e^{L_m} &\geq 2e^L \\ e^{L+\epsilon} + e^{L-\epsilon} &\geq 2e^L \\ e^L\left(\frac{e^{\epsilon} - e^{-\epsilon}}{2}\right) &\geq e^L \\ \cosh[\epsilon] &\geq 1 \end{aligned} \tag{A.27}$$

Next we will show the rest of the inequality in A.25 is true.

$$\begin{aligned} -\frac{1}{p[L_m]+p[L_n]-p[L_m]p[L_n]} &\geq -\frac{1}{2p[L]-p[L]^2} \\ p[L_m]+p[L_n]-p[L_m]p[L_n] &\geq 2p[L]-p[L]^2 \end{aligned} \tag{A.28}$$

The first two terms on the LHS can be shown to be always larger than the first term on the RHS, from (A.27) since $p[L]$ is midpoint convex. Next we show

$$\begin{aligned} -p[L_m]p[L_n] &\geq -p[L]^2 \\ p[L_m]p[L_n] &\leq p[L]^2 \\ e^{L_m}e^{L_n} &\leq e^{2L} \\ e^{L+\epsilon}e^{L-\epsilon} &\leq e^{2L} \\ e^{2L} &\leq e^{2L} \end{aligned} \tag{A.29}$$

Thus, the minimal channel uses for two links with the same probability distribution is when they are the same length.

A.4.2 Minimum dephasing time

Next we will show that for two inner links, the minimum total expected time the QMs store their states is when the link lengths are the same. For two links we consider the overall storage time of the corresponding QMs. Since the dephasing time depends on the expectation value of the number of trials of each of the inner links for the sequential protocol. The general expression we want to minimize for L_m and L_n is

$$\begin{aligned} \mathbb{E}\left[\sum_{i=m,n} t_i\right] &= \mathbb{E}\left[g[L_m,L_n]+\tau_m Q_m+\tau_n Q_n\right] \\ &= g[L_m,L_n]+\frac{\tau_m}{P[L_m]}+\frac{\tau_n}{P[L_n]} \end{aligned} \tag{A.30}$$

The function $g[L_m, L_n]$ depends on L_m and L_n but is does not depend on the number of trials. For any general sequential protocol, when we consider all of the nodes

$$g[L_m,L_n] = -(3-2x)L/(cT_2), \tag{A.31}$$

which is a function of total length and x, not individual inner link lengths (see (3.36)). So we do not have to consider it for minimization as it will become a constant. We then have to minimize

$$\frac{\tau_m}{P[L_m]}+\frac{\tau_n}{P[L_n]}$$

with respect to L_m and L_n. Again, we define $L_n = L + \epsilon$ and $L_m = L - \epsilon$. We can easily show that

$$\frac{T_{prep} + L_m/c}{P[L_m]} + \frac{T_{prep} + L_n/c}{P[L_n]} \leq 2\left(\frac{T_{prep} + L/c}{P[L]}\right) \tag{A.32}$$

holds, from the same argument of midpoint convexity in Section A.4.1. Thus, the minimum storage time occurs when $L_m = L_n$.

A.5 One-node versus multi-node

We derive (3.55) by setting the inflection point of $F_p[L, x, n]$ to occur at $L = 0$. This is done by differentiating (3.52) twice with respect to length, and setting it equal to 0 for $L = 0$, resulting in

$$0 \;=\; \frac{2(1-2x)^2\left(L_{att}^2\left(2(n-1) - \eta_{tot}^2 + 2\right) - 2cT_2 L_{att}\eta_{tot}^2\right)}{c^2(n-1)T_2^2 L_{att}^2 \eta_{tot}^4}. \tag{A.33}$$

Rearranging for η_{tot} yields

$$\eta_{tot} \;\gtrapprox\; \sqrt{\frac{L_{att}2n}{L_{att} + 2cT_2}} \tag{A.34}$$

If we include the $\sqrt{n}$ factor this approximation does not seem to hold as well for large n. So we set $n = 2$, which will hold for $n \geq 2$ and will provide a more accurate lower bound for large n. This results in

$$\eta_{tot} \;\gtrapprox\; \sqrt{\frac{4L_{att}}{L_{att} + 2cT_2}} \tag{A.35}$$

All this equation tells us is that if this inequality does not hold, then the dephasing parameter is always concave up and as x decrease, the concavity increases. The $n-1$ power in (3.52) will increase the concavity as well, which is why we believe (A.35) will hold for large n.

A.6 Approximate crossover

To get an approximation of the when our quantum repeater key rate beats the PLOB bound, we first determine at what length this crossover should occur. Since we cannot solve for the crossover length algebraically, we will estimate it. For now, let us denote this approximate crossover length by L_{cross}. We introduce a new length L_o, which is the length at which the key rate goes to zero, assuming the key rate has beaten the PLOB bound at some length. We know $L_o \geq L_{cross}$ and for now assume we know L_o. We want to calculate what T_2 value will cause the key rate to drop to 0 at L_o. Setting the error correction and privacy amplification term to zero

$$0 \;=\; 1 - fh[e_z] - h[e_x], \tag{A.36}$$

we can rearrange for e_x, resulting in

$$e_x \;=\; h^{-1}[1 - fh[e_z]] \tag{A.37}$$

We cannot solve the inverse of $h[x]$ analytically, but this can easily be done numerically. Substituting the definition of e_x from (3.32) into (A.37) and isolating for the dephasing parameter, we find

$$f_{dp}[n] \;=\; \frac{1 - 2h^{-1}[1 - fh[e_z]]}{(1 - 2e_M)^{2n}\lambda_{BSM}^{n}\alpha^2\mu_x^{n-1}} \tag{A.38}$$

In general, the dephaing function $f_{dp}[n]$ is defined in (3.33), which is the expectation value of an exponentially decaying function. Since the exponential function is convex, we can use Jensen's inequality to shown that

$$\mathbb{E}\left[e^{-\sum_{i=1}^{i=2n} t_i/T_2}\right] \geq e^{-\mathbb{E}\left[\sum_{i=1}^{i=2n} t_i\right]/T_2}. \tag{A.39}$$

Therefore, we can use $e^{-\mathbb{E}\left[\sum_{i=1}^{i=2n} t_i\right]/T_2}$ as a lower bound on $f_{dp}[n]$. From this lower bound, we now assume that $f_{dp}[n]$ has the form of a decaying exponential function $e^{-1/K}$. The parameter K represents the fraction of the T_2 time to the total expected waiting time in the QMs. Substituting this function into (A.38) yields

$$e^{-1/K} = \frac{1 - 2h^{-1}[1 - fh[e_z]]}{(1 - 2e_M)^{2n}\lambda_{BSM}^{n}\alpha^2\mu_x^{n-1}}. \tag{A.40}$$

From this equation, we can analytically determine K as

$$K = \frac{-1}{\log\left[\dfrac{1 - 2h^{-1}[1 - fh[e_z]]}{(1 - 2e_M)^{2n}\lambda_{BSM}^{n}\alpha^2\mu_x^{n-1}}\right]}. \tag{A.41}$$