The Practical Realization of Quantum Repeaters: An Exploration

by

David Luong

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

Waterloo, Ontario, Canada, 2015

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 is an exploration of quantum repeaters from a practical point of view. Quantum repeaters are devices which help improve the quantum communication capacity of a lossy bosonic channel (which include photonic channels such as optical fiber) beyond what is possible using a *purely* lossy channel. The analyses in this thesis involve modeling the experimental imperfections inherent in the various devices which comprise a quantum repeater, then combining these models to calculate various quantities of interest.

Two systems are analyzed in this thesis. One is a simple quantum repeater, while the other is a potential building block for more complex quantum repeaters.

The simple quantum repeater scheme can be implemented with currently available technology. In it, two parties perform quantum key distribution (QKD) by exchanging photons with two quantum memories placed between them. Its secret key rate ideally scales as the square root of the transmittivity of the optical channel, which is superior to QKD schemes based on direct transmission because key rates for the latter scale at best linearly with transmittivity. Taking into account imperfections in the setup, such as detector efficiency and dark counts, we present parameter regimes in which our protocol outperforms protocols based on direct transmission. We find that implementing our scheme with trapped ions is a promising way to reach the necessary parameter regimes, and that the regimes are easier to reach if the optical channels are very lossy.

The creation of entanglement between two quantum memories is an important building block in some quantum repeater schemes. We consider a specific quantum memory consisting of an atom trapped in a cavity. The system allows a CNOT operation to be performed between an atom and a photon. We study three methods for taking advantage of this to entangle two atoms: *(1)* interacting a coherent pulse with each atom, then performing an entangling measurement on the pulses; *(2)* interacting a single coherent pulse with each atom sequentially; *(3)* emitting an entangled photon from one atom and interacting it with the other atom. The success probability of each method is compared, as well as the quality of the entangled states produced by each one, taking into account imperfections which appear in a specific experimental implementation of such memories. We find that there is a tradeoff between success probability and entangled state quality when coherent states are used, and that method 3 provides higher-quality entangled states than is possible with the other two methods.

Acknowledgements

If I were to properly acknowledge all the people who supported me, I would exhaust all the ink and paper on this planet. So, gentle reader, if I have omitted a deserving name, know that it was not my gratitude that was limited, but my page count.

I owe a great debt to my supervisor, Norbert Lütkenhaus. This thesis would be nothing without his support and guidance. His clear and deep understanding of everything related to his research, as well as his ability to cut straight to the heart of a problem, will always stand before me as unforgettable lessons. And what a joy it was to drink from the fountains of his wisdom! An exemplary teacher, his door was always open and his valuable advice easily obtained. Where would I be without him? Not in graduate school, certainly.

Similar sentiments can be expressed of Marco Piani, who taught me well during the regrettably short time that I spent with him.

I would like to thank Christopher Wilson and Thomas Jennewein for their support as part of my advisory committee, and Kyung Soo Choi for sitting on my defence committee. Thanks also to Electra Eleftheriadou and Filippo Miatti for their invaluable comments on earlier drafts of this thesis.

The Institute for Quantum Computing has brought me into contact with brilliant ideas and brilliant people. Special mention goes to my office mate, Sascha Agne, whose conversation is always fascinating and witty. I am forever willing to sing the *Coffee Cantata* for him. And of course, there are my fellow members of the OQCT group, past and present: William Stacey, Sumeet Khatri, Electra Eleftheriadou, Filippo Miatti, and many others. From them I have gained knowledge, wisdom, and friendship. I wish particularly to thank Ryo Namiki, Yanbao Zhang, and Patrick Coles, who so kindly tolerated me every time I invaded their office. And how could I omit Juan Miguel Arrazola, with whom I have had so many insightful conversations on those long drives to Toronto?

I must thank my friends outside of IQC, too. I wish I could include them all here, but, being studious of brevity, I will mention only those who have helped me in a direct academic sense. One is Ian Lam, who regularly travels all the way from Kingston to Toronto for no other purpose than to have hot pot with me and listen to me whine. The other is Kyunghoon Han, concerning whom I can but remain silent. For what can I say in appreciation of a friend who is willing to chat with me from sunset to sunrise about every topic under heaven?

Those who know me well, know that I always save the best for last. And so I have reserved the final paragraph for my family. Thank you, Henry, for sticking by me as I worked through this degree. I really appreciate it. And, finally, thank you, Mom and Dad, for supporting me in every way possible, through all my studies and through all the days of my life. 爸爸媽媽，謝謝您。

Edifying Quote

I am inclined to believe—without proof, it is true, but on the basis of extremely strong numerical evidence—that Confucius never knew what photons were, nor would he have considered them friends even if he did know. It is probable, also, that he would have balked at the idea of identifying quantum memories with gentlemen. Yet the words which open his *Analects* seem to fit the theme of this thesis well:

> 學而時習之，不亦説乎？有朋自遠方來，不亦樂乎？人不知而不愠，不亦君子乎？
>
> To learn and then have occasion to practice what you have learned—is this not satisfying? To have friends arrive from afar—is this not a joy? To be patient even when others do not understand—is this not the mark of the gentleman?
>
> — Confucius, *Analects* 1.1

Table of Contents

List of Figures

Chapter 1

Introduction

Among the various branches of quantum information theory, one of the most exciting is undoubtedly quantum key distribution (QKD). In 1984, Bennett and Brassard published a seminal paper [1] in which they outlined a very simple way to exploit the properties of quantum mechanics to generate a secret key of arbitrary length and securely transmit it to two parties who wish to communicate in secret. (By long-standing convention, we call these parties *Alice* and *Bob*.) When used in the one-time pad scheme, this protocol promises an extremely high level of security: given that certain conditions hold, the encryption cannot be broken using any method consistent with the laws of physics. This is a stronger level of security than was available up to that point; prior cryptographic schemes made the additional assumption that the computational power of any eavesdropper is bounded in some way. Since the publication of Bennett and Brassard's protocol, the field of QKD has grown at an impressive rate. Much work has been done in both theory and experiment, and even commercial QKD systems have made an appearance.

One of the outstanding problems of QKD is the question of how to distribute key over arbitrarily long distances. For practical reasons, photons are the only viable physical systems with which to perform QKD. Unfortunately, the transmittivity of an optical channel decreases rapidly as the length of the channel grows (exponentially, in the case of fiber). This imposes a strong limit on the rate at which secret key can be generated when photons are directly transmitted from Alice to Bob over long distances. Specifically, Takeoka, Guha, and Wilde have shown that, when multi-mode signals are sent through a pure-loss bosonic channel with transmittivity η, the quantum communication capacity of the channel is at most

$$R_{\mathrm{TGW}} = \log_2\left(\frac{1+\eta}{1-\eta}\right)$$

bits per mode per channel use [2]. In particular, this means that the secret key rate

of any QKD protocol performed over such a channel cannot exceed this bound. The Takeoka-Guha-Wilde (TGW) bound is proportional to η for small η, meaning that the key rate, too, must decrease rapidly with distance. The problem is exacerbated in practical implementations of QKD, where experimental imperfections invariably introduce errors. When the transmittivity becomes too low, these errors dominate the system and no key can be generated at all. In order to improve this key rate vs. transmittivity scaling behavior and achieve even a modest key rate at very long distances, it is necessary to look beyond direct transmission.

The simplest way to overcome the problem is to simply introduce a relay between Alice and Bob, who then separately use QKD to establish secret keys with it [3]. The relay could then generate a single secret key for Alice and Bob to use. Alternatively, messages could be routed through the relay, which encrypts and decrypts the messages using the two secret keys as appropriate. The idea can be immediately extended to multiple relay stations stretching over an arbitrary distance. However, all this requires that the relays be *trusted*. Is it possible to devise a scheme that can surpass the TGW bound without making additional trust assumptions?

The *quantum repeater* is one such scheme [4]. First described in [5], quantum repeaters are auxiliary quantum devices placed along the channel between Alice and Bob, effectively breaking it up into multiple low-loss channels. A full repeater scheme might involve the use of many stations, each containing multiple qubits [5, 6, 7, 8, 9, 10, 11, 12]. These resource requirements are too demanding for such a scheme to be practical at present. No experiment has been performed that beats the TGW bound over any distance.

The aim of this thesis is to lay the groundwork for an experimental demonstration of a quantum repeater—that is, an experiment in which the key rate exceeds the TGW bound without trusting any device in the channel between Alice and Bob. We attack the problem on two fronts. In one of them, we present a very simple quantum repeater scheme that requires only two qubits in a central station between Alice and Bob. The behavior of this scheme is analyzed in detail, taking into account a large number of experimental imperfections, and conditions are found under which the scheme can beat the TGW bound. This scheme can be implemented using currently available technology; however, it is not immediately extendable to multiple stations and arbitrary distances. The second front of attack relates to the implementation of extendable quantum repeater schemes. In many of them, the establishment of entanglement between neighboring stations is an important step (see, for example, [5, 6, 7, 8, 10]). We therefore compare and contrast three different schemes for entangling two trapped-atom qubits; such an analysis should be helpful when evaluating a given quantum repeater scheme in the presence of experimental imperfections.

This thesis is organized on the following plan. In Chapter 2, some background information on quantum mechanics, QKD, and quantum repeaters is presented. Chapter 3 concerns the

simple quantum repeater scheme alluded to above, together with an analysis of its behavior when imperfections are taken into account. In chapter 4, we consider three different schemes for establishing entanglement between two spatially separated qubits. Finally, Chapter 5 contains some brief concluding remarks.

Chapter 2

Background

In this chapter, some essential concepts from quantum mechanics and quantum key distribution, necessary to understand the remainder of this thesis, are briefly presented.

2.1 Fundamentals of quantum mechanics

Almost all of the material in this section is derived from [13], to which the reader is referred for more details.

In quantum mechanics, the state of any physical system is completely specified by a linear operator acting upon a complex Hilbert space; the latter is called the *state space* of the system. The dimension of the state space is equal to the number of degrees of freedom possessed by the physical system, and may be either finite or infinite. Systems with two degrees of freedom play a special role in quantum information theory, and are called *qubits*.

Density operators

Not all linear operators are valid descriptions of a physical state; only so-called *density operators* are admissible. Conversely, any density operator is a valid description of some physical state.

Definition 1. A *density operator* (or *density matrix*) is a positive semidefinite Hermitian operator with unit trace.

Density operators of the form $|\psi\rangle\langle\psi|$, where $|\psi\rangle$ is a unit vector in the state space, represent what are called *pure states*. Pure states may naturally be identified with elements of the state space according to the correspondence $|\psi\rangle\langle\psi| \leftrightarrow |\psi\rangle$. (This correspondence only

specifies $|\psi\rangle$ up to a phase factor, which may be arbitrarily chosen.) It is often convenient, when the state of a system is pure, to specify it by giving the corresponding vector. States that are not pure are called *mixed*.

Any density operator ρ can be written as a convex combination of pure states—that is, in the form

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{2.1}$$

where the p_i are positive real numbers satisfying $\sum_i p_i = 1$ and the $|\psi_i\rangle$ are unit vectors. The spectral theorem proves that such a decomposition always exists, but it is not necessarily unique unless the state is pure.

Another important state of any physical system is the one described by the density operator $\mathbb{1}/n$, where n is the dimension of the state space. The state is called the *maximally mixed state*, and can be thought of as being a state of maximum "indeterminateness": nothing is known about the system other than its dimension. It corresponds to the uniform distribution in probability theory.

Composite systems: tensor products and the partial trace

It is often of interest to consider not only one physical system in isolation, but two or more of them jointly. The state space of a composite system is represented by the *tensor product* of the state spaces of the subsystems. (When working with matrices, this corresponds to the Kronecker product.) Systems consisting of two subsystems are called *bipartite*, and in general, systems consisting of more than one subsystem are called *multipartite*.

A common convention, followed in this thesis, is to omit the tensor product sign $\otimes$ when its presence is implied by context.

One may also proceed in the other direction—that is, discard one of the subsystems of a multipartite system and consider only the remainder. To model this, it is necessary to introduce the *partial trace* operation.

Definition 2. Let $A \in \mathcal{H}_A$ and $B \in \mathcal{H}_B$ be any two linear operators. The *partial trace* over $\mathcal{H}_B$ of $A \otimes B$ is defined as

$$\mathrm{tr}_{\mathcal{H}_B}(A \otimes B) := A \,\mathrm{tr}(B). \tag{2.2}$$

(An analogous definition holds for $\mathrm{tr}_{\mathcal{H}_A}$.) We extend this definition to *arbitrary* operators in $\mathcal{H}_A \otimes \mathcal{H}_B$ by defining the partial trace to be linear.

The partial trace may easily be stated in terms of matrix elements. Let T be a linear operator on the tensor product of two finite-dimensional Hilbert spaces. We can decompose

it in terms of orthonormal basis vectors as follows:

$$T = \sum_{ijmn} T_{ij,mn} |i\rangle\langle m| \otimes |j\rangle\langle n|. \tag{2.3}$$

Then by applying the definition above, we find that tracing out the second subsystem gives

$$\mathrm{tr}_2(T) = \sum_{im} \left(\sum_j T_{ij,mj} \right) |i\rangle\langle m|. \tag{2.4}$$

The coefficients $\sum_j T_{ij,mj}$ are the desired matrix elements. A formal similarity between this expression and the operation of index contraction in tensor analysis may be noted.

Given a system described by the bipartite density operator ρ^{AB}, the act of discarding subsystem B is sometimes referred to as "tracing out" system B. The resulting state $\rho^A = \mathrm{tr}_B(\rho^{AB})$ is called the *reduced density operator* for system A.

Measurements

Having modeled the state of a quantum mechanical system, it is natural to ask how a measurement on the system is modeled. In quantum mechanics, each measurement is represented by a set of *measurement operators* which, like density operators, act on the state space. Each operator corresponds to a possible outcome of the measurement.

When a system in the state ρ undergoes a measurement represented by the set $\{M_n\}$, the nth measurement outcome is obtained with probability

$$p_n = \mathrm{tr}(M_n \rho M_n^\dagger). \tag{2.5}$$

In order to guarantee that the probabilities sum to unity, we require the measurement operators to satisfy the equation

$$\sum_n M_n^\dagger M_n = \mathbb{1}. \tag{2.6}$$

After the measurement, the state of the system changes from ρ to

$$\rho_n = \frac{M_n \rho M_n^\dagger}{\mathrm{tr}(M_n \rho M_n^\dagger)}. \tag{2.7}$$

Notice that the state of the system after the measurement depends on the measurement outcome. According to some schools of thought, this change of state is responsible for an effect called *wavefunction collapse*.

In some situations, it is more convenient to work in terms of an alternative set of operators called a *POVM*[1] than with measurement operators directly.

Definition 3. A *POVM* is a set of positive semidefinite Hermitian operators which sum to the identity operator.

In the simplest case, the elements E_n of a POVM correspond to the measurement operators M_n by $E_n = M_n^\dagger M_n$, so each element corresponds to a measurement outcome. More generally, it is possible to perform "coarse-graining" by associating several measurement outcomes to one POVM element. In this case we have $E_n = \sum_i M_i^\dagger M_i$, where the summation is over the subset of measurement operators to be associated with E_n.

The probability of obtaining the measurement outcome associated with the POVM element E_n (or one of the outcomes, in the case of coarse-graining) is

$$p_n = \mathrm{tr}(E_n \rho). \tag{2.8}$$

If the post-measurement state is not important, it is sufficient to characterize a measurement by giving its POVM.

Given an orthonormal basis $\{|i\rangle\}$ of a state space, the projectors $\{|i\rangle\langle i|\}$ form a set of measurement operators (as well as a POVM). Measurements of this form are called *projective measurements*, and the act of performing such a measurement is referred to as "measuring in the $\{|i\rangle\}$ basis". A projective measurement performed on a pure state always results in a pure state.

Quantum channels

We now turn to the question of how physical operations upon a system are to be modeled. This is done using *completely positive, trace-preserving maps*, which are linear "superoperators" whose properties guarantee that they map density operators to density operators. Such maps are called *quantum channels* or *quantum operations*.

Definition 4. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces, and let $L(\,\cdot\,)$ denote the set of all linear operators on the specified space. A linear mapping $\Phi : L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ is called a *quantum channel* or *quantum operation* if it satisfies the following properties:

1. (Complete positivity) For all natural numbers n and all $\rho \in L(\mathcal{H}_A \otimes \mathbb{C}^n)$,

$$\rho \geq 0 \implies (\Phi \otimes \mathrm{id}_n)(\rho) \geq 0. \tag{2.9}$$

   Here id_n is the identity map on $L(\mathbb{C}^n)$.

[1] *POVM* is an abbreviation of *positive operator-valued measure*, though the term is very rarely written out in full.

2. (Trace preservation) For all $\rho \in L(\mathcal{H}_A)$, $\mathrm{tr}(\rho) = \mathrm{tr}[\Phi(\rho)]$.

The partial trace operation is an important example of a quantum channel.

Quantum channels which can be written in the form $\Phi(\rho) = U\rho U^\dagger$, where U is a unitary operator, are called *unitary channels*. When a unitary channel is applied to a pure state like $|\psi\rangle\langle\psi|$, the resultant state is again pure and corresponds to the vector $U|\psi\rangle$. A unitary channel, in essence, acts as a change of basis on the state space.

An important result about quantum channels states that they can always be simulated using unitary channels. One can do this by attaching an auxiliary system to the system of interest, performing a unitary channel on the joint system, then discarding some part of it. This result is called the *Stinespring dilation theorem* [13]. For simplicity, we present a special case of this theorem where the quantum channel maps between spaces of the same dimension.

Theorem 1. *Let $\Phi : L(\mathcal{H}) \to L(\mathcal{H})$ be a quantum channel. Then there exists a Hilbert space $\mathcal{K}$, a unit vector $|0\rangle \in \mathcal{K}$, and a unitary operator U on $\mathcal{H} \otimes \mathcal{K}$ such that*

$$\Phi(\rho) = \mathrm{tr}_{\mathcal{K}}[U(\rho \otimes |0\rangle\langle 0|)U^\dagger] \tag{2.10}$$

for any density operator ρ in $L(\mathcal{H})$.

By introducing an orthonormal basis on the auxiliary system $\mathcal{K}$ and explicitly evaluating the partial trace in terms of the basis vectors, we can rewrite (2.10) without introducing an auxiliary system. This representation of a quantum channel is called the *Kraus* or *operator-sum representation*. (This time, we will not restrict the domain and range of the quantum channel to be the same.)

Theorem 2. *Let $\Phi : L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ be a quantum channel. Then there exists a set of operators $\{K_n\}$, each mapping from $\mathcal{H}_A$ to $\mathcal{H}_B$, such that*

$$\Phi(\rho) = \sum_n K_n \rho K_n^\dagger \tag{2.11}$$

for any density operator ρ in $L(\mathcal{H}_\mathcal{A})$. Moreover, the K_n satisfy

$$\sum_n K_n^\dagger K_n = \mathbb{1}. \tag{2.12}$$

Note the similarity between the Kraus operators K_n and the measurement operators M_n described above. Measuring a system is the same as applying a quantum channel.

2.1.1 Entanglement

It was stated earlier that the state space of a composite system is the tensor product of the state spaces of its subsystems. However, not all states of the composite system can be represented as a tensor product of density operators on each of the subsystems, or even as a convex combination of such products. Such states, which are not "compatible" with the tensor product structure of the composite system, are called *entangled*.

To formalize this, we introduce the notion of a *separable state*. These are nothing but convex combinations of *product states*, which are of the form $\rho^A \otimes \rho^B$.

Definition 5. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. A density operator $\rho^{AB} \in L(\mathcal{H}_A \otimes \mathcal{H}_B)$ represents a *separable state* if it can be written in the form

$$\sum_i p_i \rho_i^A \otimes \rho_i^B, \tag{2.13}$$

where $p_i \geq 0$ for all i, $\sum_i p_i = 1$, and the $\rho_i^A \in L(\mathcal{H}_A)$ and $\rho_i^B \in L(\mathcal{H}_B)$ are themselves density operators.

Note that all separable *pure* states are product states.

Definition 6. Any state that is not a separable state is an *entangled state*.

Some of the most simple examples of entangled states are the four *Bell states*, which are pure states of a system consisting of two qubits. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis for the state space of a single-qubit system. Then the vectors which correspond to the Bell states are defined as follows:

$$\begin{aligned} |\Phi^+\rangle &:= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &:= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &:= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle &:= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{2.14}$$

For clarity and brevity, we have written (for example) $|00\rangle$ for $|0\rangle \otimes |0\rangle$.

Note that these four vectors form an orthonormal basis for the state space of two qubits. A measurement in this basis is called a *Bell state measurement* (BSM).

The Bell states have this very important property: if one takes a system whose state is described by $|\Phi^+\rangle$ and performs any projective measurement on one of the qubits, *both* qubits will be in the same state after the measurement. This is true of the other Bell states as well, up to a unitary channel on one of the qubits. Hence, in some sense, the Bell states are perfectly correlated.

It is possible to define *entanglement measures* which quantify "how entangled" a given bipartite state is. All entanglement measures are minimized by separable states; they are also nonincreasing under *local operations and classical communication* (LOCC).[2]

Many entanglement measures are difficult to compute for a given bipartite state. The *logarithmic negativity*, however, is quite easy to compute.

Definition 7. The *logarithmic negativity* of any bipartite density operator ρ^{AB} is defined to be

$$LN(\rho^{AB}) := \log_2 \|(T \otimes \mathrm{id})(\rho^{AB})\|_1 \tag{2.15}$$

where T is the transpose operation and $\|\cdot\|_1$ denotes the *trace norm* (sum of singular values).

The logarithmic negativity is zero for separable states. For two-qubit systems, the Bell states maximize the logarithmic negativity, achieving a value of 1.

For more details on entanglement measures, the reader is referred to [14].

2.1.2 Quantum optics

In classical physics, electromagnetic waves are described by solutions of Maxwell's equations. These solutions can be decomposed into a linear combination of orthonormal basis functions, each of which is called an *optical mode*. These modes may correspond, for example, to waves of various different frequencies and polarizations. When the Hamiltonian of the electromagnetic field is written in terms of these modes, it is mathematically equivalent to the Hamiltonian of a set of uncoupled simple harmonic oscillators, each one corresponding to a mode. In the quantum mechanical treatment of the electromagnetic field, one simply replaces these simple harmonic oscillators with quantum harmonic oscillators.

The state space of a quantum harmonic oscillator is spanned by a countably infinite set of orthonormal vectors $\{|n\rangle\}_{n=0}^{\infty}$. The quantum states that correspond to these vectors are

[2]Informally, LOCC may be defined as follows. Suppose Alice and Bob each hold a part of the bipartite state. They apply quantum operations only to their parts of the state, but can exchange classical information which they use in deciding what quantum operations to perform. There is no limit to the number of times they can exchange classical information or apply local quantum operations. Any quantum operation which can be implemented by Alice and Bob in this way is LOCC.

called *Fock states* or *number states*. In the context of quantum optics, the Fock state $|n\rangle$ is the state in which there are n photons in a given optical mode.[3]

There are two important operators that act on the state space of a quantum harmonic oscillator: the *annihilation operator* a and its adjoint, the *creation operator* $a^\dagger$. Their action on Fock states is as follows:

$$a|n\rangle = \sqrt{n}|n-1\rangle \tag{2.16}$$

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{2.17}$$

It can be seen that a decreases the number of photons by one, while $a^\dagger$ increases it by one, hence the names of the operators. The creation and annihilation operators satisfy the commutation relation

$$[a, a^\dagger] = 1. \tag{2.18}$$

Note that the creation and annihilation operators of two different modes always commute, since they act on different subspaces of the tensor product space of the two modes.

Another important operator is $N := a^\dagger a$. This is called the *number operator*, and takes its name from the fact that the nth Fock state is an eigenvector of N with eigenvalue n: $N|n\rangle = n|n\rangle$. In other words, it counts the number of photons in a mode.

States which are described by eigenvectors of the annihilation operator are called *coherent states*. One reason why they are important is that, in most cases, they accurately model the pulses of light emitted from a laser. In fact, we will assume throughout this thesis that all laser pulses are coherent states. A coherent state is completely characterized by its corresponding eigenvalue, which can be any complex number; this eigenvalue is called the *amplitude* of the state. In terms of Fock states, coherent states can be written in the form

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{2.19}$$

where α is the eigenvalue corresponding to $|\alpha\rangle$.

If a coherent state is measured in the Fock state basis, the probability of obtaining the nth Fock state is

$$P(n|\mu) = e^{-\mu}\frac{\mu^n}{n!} \tag{2.20}$$

where $\mu := |\alpha|^2$. This is a Poisson distribution with mean μ. Because Fock states contain a definite number of photons, we may interpret this as meaning that the number of photons in a coherent state has a Poisson distribution with mean photon number μ.

[3]Note that symbols like $|0\rangle$ or $|1\rangle$ are often used to represent states other than Fock states. The context should make it clear what the appropriate interpretation of them are.

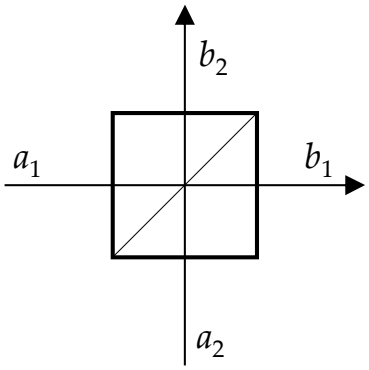

Figure 2.1: Diagram of a beamsplitter. The input and output light beams are labeled by their respective annihilation operators.

Unsurprisingly, coherent states involving multiple modes are described in terms of tensor products of single-mode coherent states.

Beamsplitters

One of the most important devices used to manipulate photons is the *beamsplitter*. Abstractly, it can be thought of as a device having two input and two output ports, each port corresponding to an optical mode. If a beam of light is sent through one input port, with nothing entering the other one, the action of a beamsplitter is that of a half-silvered mirror placed at an angle to the incident light: the beam is split into two beams which leave through the output ports. Indeed, beamsplitters are sometimes implemented using such mirrors.

Let a_1 and a_2 denote the annihilation operators for the two input modes and b_1 and b_2 be the annihilation operators for the two output modes, as illustrated in Fig. 2.1. Then the action of a beamsplitter is such that these operators are related as follows:

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} t & r \\ -r^* & t^* \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}. \tag{2.21}$$

The coefficients t and r are complex numbers that are constrained to satisfy

$$|t|^2 + |r|^2 = 1. \tag{2.22}$$

Note that (2.21), together with the constraint (2.22), implies that b_1 and b_2 satisfy the commutation relation (2.18) if a_1 and a_2 do. It may also be shown that $a_1^\dagger a_1 + a_2^\dagger a_2 =$

$b_1^\dagger b_1 + b_2^\dagger b_2$, meaning that the number of photons entering the beamsplitter is the same as the number that exit it.

It is worth pointing out that, if two coherent states are incident on a beamsplitter, the output states are also coherent states. Moreover, the amplitudes of the input and output coherent states are related in exactly the same way as the annihilation operators are in (2.21). Thus, if $|\alpha_1\rangle$ and $|\alpha_2\rangle$ were coherent states incident on a beamsplitter,

$$|\alpha_1\rangle|\alpha_2\rangle \to |t\alpha_1 + r\alpha_2\rangle|-r^*\alpha_1 + t^*\alpha_2\rangle. \tag{2.23}$$

In the case of a 50/50 beamsplitter, in which the half-silvered mirror (or its equivalent) reflects 50% of incoming light and transmits the rest, one may choose $t = r = 1/\sqrt{2}$.

When photons are sent through a lossy optical channel, such as an optical fiber or the atmosphere, some of them may be lost. This loss is usually modeled as a beamsplitter, with one input and one output port representing the channel and the other output port representing the outside environment into which photons are leaking. The other input port is assumed to be in the Fock state $|0\rangle$, since no light enters it. If the transmittivity of the channel (the probability that a photon traverses the channel without being lost) is η, then choosing $t = \sqrt{\eta}$ and $r = \sqrt{1-\eta}$ in (2.21) results in the correct probability for photon loss.

2.2 Quantum key distribution

Suppose Alice wants to send a message to Bob, but does not wish her message to be read by Eve the eavesdropper. For simplicity, assume that her message is a string of bits. The following is one scheme she could use to encrypt her message:

1. Create a *secret key*, a string of random bits that is as long as the message, and securely send it to Bob.

2. Combine the message and the secret key using the bitwise XOR operation.

3. Send the resulting encrypted message to Bob, who decrypts it by combining it with the secret key using bitwise XOR.

This scheme is called the *one-time pad*, and has been proved to be *information-theoretically secure*; this means that the scheme cannot be broken even if Eve has unlimited computing power. This very attractive property sets it apart from schemes such as the well-known Advanced Encryption Standard (AES) [15], which is secure in the *practical* sense that Eve requires more computational power to break it than is available in the present day—though she could do it with unlimited computing power. Despite its simplicity, however, the

one-time pad is difficult to use in practice. One key requirement is that the secret key needs to be sent to Bob securely, which is not always easy to arrange. One can think of the one-time pad, then, not as solving the problem of sending a message securely, but as reducing this problem to that of sending a random string securely.

The BB84 protocol

In 1984, Bennett and Brassard [1] devised a protocol for sending a random string securely by exploiting the principles of quantum mechanics. In their protocol, Alice has an apparatus that can send qubits in one of four states:

$$|0\rangle, \quad |1\rangle, \quad |+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.24}$$

The set $\{|0\rangle, |1\rangle\}$ is an orthonormal basis for the state space of a qubit; we will call it the Z basis. The set $\{|+\rangle, |-\rangle\}$ is another such basis, which we will call the X basis. Bob has a measurement device than can measure qubits in one of these two bases. Alice and Bob also share an *authenticated* communication channel. Messages sent over it are public, but cannot be changed or forged.

Bennett and Brassard's protocol, now known as *BB84*, is as follows.

1. Alice randomly chooses a bit value, either 0 or 1, and a basis in which to encode that bit value, either Z or X. She then sends a qubit to Bob, the state of which she chooses according to the following scheme:

	Z	X
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

2. Bob randomly chooses either Z or X, measures the incoming qubit in that basis, and records the bit value that corresponds to his measurement result (again according to the above scheme).

3. Steps 1 and 2 are repeated a large number of times. Alice and Bob each end up with a random bit string called their *raw key*.

4. Using the authenticated channel, Alice and Bob reveal to each other the bases they used to send and measure each qubit. Whenever Alice and Bob used different bases to send and measure a qubit, they discard the corresponding bit from their raw keys. The resulting strings are called their *sifted keys*.

5. Alice and Bob reveal a portion of their sifted keys to each other to estimate the number of errors between them. If this is too high, they abort the protocol. Otherwise, they perform processes called *error correction* and *privacy amplification* to resolve discrepancies between the sifted keys and eliminate any information Eve may have about them. Alice and Bob end up with identical, random bit strings about which Eve has no information. This is their secret key, which they can use in the one-time pad scheme.

We will not describe the processes of error correction and privacy amplification in detail, contenting ourselves with the knowledge that such processes exist.

The security of this protocol relies on the fact that, if Eve wishes to obtain any information on the key, she needs to make measurements on the qubits that Alice sends. In order for her to correctly determine what bit value is being encoded by a given qubit, she must measure in the same basis as the one in which Alice sent it in. If Eve measures in the other basis, it can easily be calculated that she obtains the correct bit value only with probability 1/2. If she then passes on the post-measurement qubit to Bob, he also obtains the correct bit value with probability 1/2 even if he did measure in the correct basis. In this way, Eve introduces errors into the communication (with some probability) whenever she tries to eavesdrop.

BB84 represents one method for performing *quantum key distribution* (QKD). Many other QKD protocols now exist; they all solve the problem of securely distributing a secret key to Alice and Bob by relying, like BB84, on the properties of quantum systems.

We should mention here that, in practice, QKD is always implemented using photons [16]. It is true that photons are easily lost and that optical channels with near-unit transmittivities are impractical; in fact, these problems form the core motivation for this thesis. However, there is simply no other practical, reliable way to send qubits over long distances. In BB84, the qubit states could be realized using photon polarization states (in which $|0\rangle$ and $|1\rangle$ represent horizontal and vertical polarization, respectively), by time bin states (where $|0\rangle$ and $|1\rangle$ represent early and late arrival of photons), or in some other manner.

In this thesis, we will focus on a variant of BB84 called *efficient BB84* [17]. It is almost exactly the same as BB84, except that Alice and Bob choose to send and receive qubits in the Z basis much more often than in the X basis. The result is that much fewer bits are discarded in the sifting process (step 4). (This does come at a price: Alice and Bob are required to perform a more sophisticated error analysis in step 5. But we need not concern ourselves with that.) In the limit of infinitely long secret keys, the probability of choosing the X basis may be made arbitrarily low, so that essentially no bits are discarded in the sifting process.

It can be shown that BB84 (in both its regular and efficient variants) is equivalent to one in which the two qubits of the Bell state $|\Phi^+\rangle$ are distributed to Alice and Bob, who both measure them in the same way Bob does in step 2 above [18]. Alice and Bob then discard those bits where they measured in different bases. This equivalence will be of extreme importance in the following chapter of the thesis, where Alice and Bob extend the range at which they can perform BB84 using a "central station" that (ideally) distributes Bell states.

Secret key rate

The most important figure of merit used to evaluate a QKD protocol is the *secret key rate* (often shortened to *key rate*). Here we state the definition in terms of channel uses, but one may analogously define secret key rates per unit time.

Definition 8. For a given QKD protocol, the *secret key rate* per channel use is the number of bits of secret key that can be generated each time the quantum channel is used, in the limit of infinitely long secret keys.

The key rate for efficient BB84, implemented using single photons, is [17, 16]

$$R = Y_1[1 - h(e_1) - fh(e_1)]. \tag{2.25}$$

Here Y_1 is the *yield*: the probability of Bob successfully detecting a photon given that Alice sent a single photon. The parameter e_1 is the *quantum bit error rate* (QBER): the fraction of Alice and Bob's sifted keys that do not match, as estimated in step 5 above. (The subscript 1 refers to the fact that single photons are being used.) The factor f is an error correction inefficiency factor. An ideal error correction scheme—one that results in the longest secret key for a given length of raw key—would correspond to $f = 1$; non-ideal schemes have $f > 1$. Finally, the function h is the *binary entropy function*, defined as

$$h(x) := -x \log_2(x) - (1 - x) \log_2(1 - x). \tag{2.26}$$

Whenever the expression $0 \log_2 0$ occurs, we will set it equal to 0. Lastly, it should be mentioned that, whenever R is not positive, it is conventionally taken to be 0.

In a practical implementation of QKD, it is almost always the case that errors between Alice and Bob arise that are not attributable to eavesdropping. In principle, if the behavior of a QKD system is known, it could be possible to take such errors into account. However, this kind of analysis turns out to be impractical. We need not mention, too, that it is dangerous to attribute any error to experimental imperfections without extremely strong justification. For this reason, we will attribute *all* errors to eavesdropping, no matter the

source. (These errors, of course, are corrected along with any errors caused by eavesdropping in the error correction step.) This may decrease the key rate, but that is a small price to pay for security.

2.2.1 Decoy states

The BB84 protocol, when implemented with single photons, is somewhat impractical: sources of light that reliably emit single photons are difficult to build. It is much easier to use lasers. However, lasers have one defect when used for QKD: they emit coherent states, which do not contain a definite number of photons. This creates a vulnerability: if a particular laser pulse is found to have at least two photons, Eve could split off one of the photons and send the remainder to Bob. She then waits until Bob announces the bases he used to measure his photons (step 4), then measures her photon in the same basis that Bob did. She thus obtains information on Bob's raw key without inducing any error between Alice and Bob. This is problematic, of course: Alice and Bob rely on errors to detect eavesdropping.

It appears necessary, then, to assume that *all* pulses containing two or more photons leak information to Eve. This means that the laser intensity must be set quite low to reduce the chance of emitting a pulse containing multiple photons. If Alice sends photons over a lossy optical channel with transmittivity η, then the key rate is optimized when the mean photon number of the laser pulses is on the order of η. Even then the key rate is low, on the order of η^2. But perhaps that assumption is unduly pessimistic. Is it possible to obtain a better characterization of the information leakage?

The solution is provided by the concept of *decoy states* [19, 20]. By sending laser pulses with different laser intensities and recording statistics for each intensity setting, Alice and Bob can infer whether Eve has been tampering with their channel. It is important that these decoy pulses be interspersed randomly among the signals used for generating the secret key, so that Eve cannot determine which pulses are decoys and which are true signals. The key[4] to this approach is the expression

$$Q_\mu = \sum_{n=0}^{\infty} P(n|\mu) Y_n. \tag{2.27}$$

Here Q_μ is the probability that Bob detects a signal given that Alice's laser pulses have mean photon number μ, $P(n|\mu)$ is as given in (2.20), and Y_n is the yield of n-photon states: the probability that Bob detects a signal given that Alice sent a pulse containing n photons. Eavesdropping would affect the yields Y_n. Now, Alice and Bob can determine Q_μ from their

[4] Pun intended.

data, but not the Y_n directly. If Alice and Bob could determine Q_μ for all values of μ, then it is reasonable to think (though not proven) that they can solve for the Y_n. But even by using two or three settings for μ, they can determine bounds on the possible values of Y_n. In this way, they can find out whether Eve has been eavesdropping and determine what fraction of their signals derive from pulses containing single photons (and can be safely used to create a secret key).

A similar analysis can be performed for the error rate using the expression

$$E_\mu = \sum_{n=0}^{\infty} P(n|\mu) Y_n e_n, \tag{2.28}$$

where e_n is the error rate for the bits of the raw key that derive from n-photon signals.

The key rate for BB84, implemented using laser pulses and decoy states, is [19]

$$R_{\text{decoy}} = Y_1 \mu e^{-\mu}[1 - h(e_1)] - f Q_\mu h(E_\mu) \tag{2.29}$$

where μ is the average photon number for *signal states* (laser pulses from which the secret key is to be generated) and f is the error correction inefficiency. Y_1 and e_1, the yield and QBER for single-photon states respectively, are estimated as outlined above.

Note that, using decoy states, it is no longer necessary to keep the mean photon number very low. The key rate in this case is proportional to the channel transmittivity η, which is a significant improvement.

2.3 Quantum repeaters

It has been pointed out that photons are the only practical physical systems with which to perform QKD. They have one great fault, however: they can get lost! This of course affects the secret key rate. In (2.25), for example, Y_1 heavily depends on the *transmittivity* of the channel between Alice and Bob—the probability that a photon can get from one end of the channel to the other. In fact, Y_1 is *equal* to the transmittivity if there are no background photons or other spurious detection events. The key rate, then, is proportional to the transmittivity.

This specific example is a manifestation of the fact that channel loss places a fundamental bound on the amount of quantum information that can be sent through the channel each time it is used. Takeoka, Guha, and Wilde have shown in [2] that, when light signals (which may, in general, involve multiple modes) are sent through a pure-loss optical channel with transmittivity η, the quantum communication capacity of the channel is upper bounded by

$$R_{\text{TGW}} = \log_2\left(\frac{1+\eta}{1-\eta}\right) \tag{2.30}$$

bits per mode per channel use [2]. Here, *pure-loss* means that the channel acts like a beamsplitter, as described in Sec. 2.1.2; it contains no components which affect the quantum state of the signals in any other way. For ease of reference, we will call this result the *TGW bound*.

As a result of the TGW bound, the secret key rate that can be achieved using a pure-loss optical channel cannot be higher than R_{TGW}. There is no QKD protocol whose key rate exceeds this bound, no matter whether single photons, coherent states, or more exotic photonic states are used to send signals, so long as a pure-loss channel is used.

When η is small, the TGW bound reduces to $R_{\mathrm{TGW}} \approx (2/\ln 2)\eta \approx 2.89\eta$. This limit is no mere mathematical curiosity, but has a practical importance. The transmittivity of an optical fiber of length L has the functional form

$$\eta = e^{-L/L_{\mathrm{att}}}, \tag{2.31}$$

where L_{att} is a characteristic quantity called the *attenuation length*. The exponential decrease means that when $L > L_{\mathrm{att}}$, transmittivities are quite low. A reasonable value for L_{att} is on the order of 22 km, so loss in fiber is significant even at moderate distances.

We see, then, that the $R \propto \eta$ scaling exhibited by BB84 cannot be improved upon, no matter what QKD protocol is used, so long as the assumptions leading to the TGW bound hold and transmittivities are low. In order to transcend the scaling behavior imposed by the TGW bound, Alice and Bob need to be connected using a channel that does not simply behave like a beamsplitter. This is where *quantum repeaters* enter the picture. Abstractly speaking, we might define them as follows.

Definition 9. A *quantum repeater* (QR) is any device that allows quantum communication over an optical channel to be performed at a rate exceeding the TGW bound.

This definition draws a very clear dividing line between true QR schemes, whose performance exceeds anything that is theoretically possible using a pure-loss channel, and schemes which show an improvement over *existing* protocols over pure-loss channels, but could nevertheless be emulated using a scheme over a pure-loss channel.

QRs are most commonly envisaged as auxiliary quantum devices placed along the channel between Alice and Bob, effectively breaking it up into multiple low-loss channels. The original quantum repeater scheme by Briegel *et al.* [5] fits this description, as do all of the QR schemes described in this thesis.

We are particularly interested in quantum repeaters that allow QKD to be performed at secret key rates exceeding the TGW bound. Moreover, we will confine our attention to devices that do not require the trust of Alice and Bob. This precludes such schemes as having Alice and Bob share separate secret keys with some relay station, which uses the keys to decrypt and re-encrypt messages routed through it.

Before we can obtain a more concrete idea of what a quantum repeater might look like, let us review some of the basic tools and techniques used by many quantum repeater schemes.

2.3.1 Tools for QRs

Quantum memories

In almost all quantum repeaters schemes, the auxiliary devices placed between Alice and Bob contain one or more *quantum memories*. A quantum memory (QM) is a physical system in which a quantum state (usually a qubit) can be stored, manipulated, and read out at will. They can be implemented, for example, using trapped ions [21, 22, 23], atomic ensembles [7], or atoms in cavities [24].

We will be particularly interested in QMs that can be entangled with single photons. (This can be done with both ions and atoms; see [25] and [24] respectively.) The reason for this is because two QMs can be entangled using such entangled photons as intermediaries. This might be done, for example, by entangling one QM with a photon and causing it to interact with another QM, or by entangling each QM with a photon and performing a Bell state measurement on the photons (an instance of entanglement swapping, a technique described below).

Quantum teleportation and entanglement swapping

Quantum teleportation, originally described in [26], is a technique for transmitting an arbitrary quantum state from one position to another without having to move a physical system containing the state through the intervening space. This is achieved with the help of an auxiliary bipartite entangled state, one subsystem of which is near the state to be teleported; the other subsystem will hold the quantum state after the teleportation is complete. For simplicity, we describe the method for teleporting a pure qubit state; the same steps apply to teleporting a mixed state. (Qubit teleportation will be sufficient for our purposes.)

Let $|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$ be the qubit that Alice wishes to teleport to Bob, and suppose that Alice and Bob share the Bell state $|\Phi^+\rangle_{A'B}$. In order to perform the teleportation, they proceed as follows.

1. Alice performs a Bell measurement between the qubit $|\psi\rangle_A$ and subsystem A' of the Bell state. Subsystem B collapses into one of the following states, depending on the result of Alice's measurement:

Result	State of system B
$\|\Phi^+\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
$\|\Phi^-\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

Result	State of system B
$\|\Psi^+\rangle$	$\beta\|0\rangle + \alpha\|1\rangle$
$\|\Psi^-\rangle$	$\beta\|0\rangle - \alpha\|1\rangle$

2. Alice sends her measurement outcome to Bob.

3. Depending on what Alice sends him, Bob sends system B through a unitary channel described by one of the following operators:

Result	Unitary
$\|\Phi^+\rangle$	$\mathbb{1}$
$\|\Phi^-\rangle$	Z
$\|\Psi^+\rangle$	X
$\|\Psi^-\rangle$	XZ

   Here X and Z are Pauli matrices. After this correction, system B ends up in the state $|\psi\rangle_B = \alpha|0\rangle + \beta|1\rangle$.

Several properties of quantum teleportation are to be noted. First, Alice does not need to know what $|\psi\rangle_A$ is. In order to teleport it, all that is necessary is that she measure it jointly with one subsystem of a Bell state. Second, after the teleportation is finished, Alice only has a random Bell state; she no longer has a copy of $|\psi\rangle_A$. Third, Bob cannot construct $|\psi\rangle_B$ without receiving Alice's measurement result. Conversely, the information sent from Alice to Bob is, by itself, not sufficient to reconstruct the state $|\psi\rangle_A$.

Entanglement swapping is a special application of quantum teleportation; it causes two distant quantum systems to become entangled without the need for preparing an entangled state and physically moving the subsystems to the desired locations. Essentially, it works by teleporting a subsystem of an entangled state. More explicitly, suppose that Alice and Bob each share a copy of the state $|\Phi^+\rangle$ with some central station CC', so that the total system is in the state $|\Phi^+\rangle_{AC}|\Phi^+\rangle_{C'B}$. Then by using $|\Phi^+\rangle_{C'B}$ to teleport subsystem C to B, Alice and Bob end up sharing a Bell state.

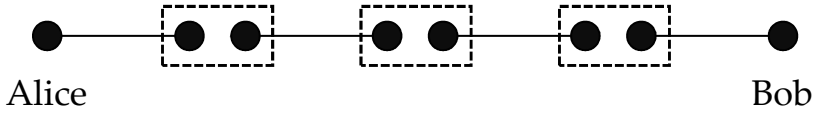

Figure 2.2: A quantum repeater scheme. Dots represent quantum memories, lines indicate entanglement, and dashed boxes indicate Bell state measurements.

Quantum teleportation can be performed using states other than $|\Phi^+\rangle$. If the auxiliary entangled state used for teleportation is *close* to $|\Phi^+\rangle_{AB}$ but contains some error, the final teleported state will contain some error. Similarly, entanglement swapping using imperfect Bell states will induce errors in the final entangled state. These facts, together with the fact that the information communicated by Alice during teleportation is insufficient to reconstruct the initial state, are crucial when applied to QKD. They mean that quantum teleportation is secure against eavesdroppers if Alice communicates her measurement result over an authenticated channel, and that Eve introduces errors whenever she tries to tamper with the auxiliary entangled state.

Finally, it should be mentioned that the correction in step 3 above is not always strictly necessary. Suppose Alice teleports one of the states in (2.24) to Bob, who immediately measures it in the X or Z basis. He can obtain the correct measurement outcome without performing step 3 if he instead applies an appropriate bit flip to his measurement result. If he measured in the X basis, then he flips his result if the Bell measurement yielded $|\Psi^+\rangle$ or $|\Psi^-\rangle$; similarly, if he measured in the X basis, he applies a bit flip if the Bell measurement yielded $|\Phi^-\rangle$ or $|\Psi^-\rangle$. The ability to "reinterpret" his measurement result is important in experiments because it removes a potential source of error.

2.3.2 A concrete QR scheme

We are now ready to look at a concrete QR scheme. Fig. 2.2 illustrates a simplified version of the scheme described in [5]. A number of stations, each containing two QMs, are placed at regular intervals between Alice and Bob. The two of them each have a station as well, with one QM each. Each station is connected to its neighbors with optical channels.

When Alice wishes to send a quantum signal to Bob, each QM is caused to be entangled with a QM in a neighboring station, so that a series of entangled pairs stretches from Alice to Bob. Finally, a Bell measurement is performed at each station, and all the measurement results sent to Bob. Essentially, this is nothing but entanglement swapping writ large. The end result is that Alice and Bob share an entangled state, which can be used to teleport a quantum signal from Alice to Bob.

The benefit of this scheme over the direct transmission of signals from Alice to Bob

lies in the fact that the success of entangling a given pair of QMs is independent of the success of entangling any other pair. Once a pair is successfully entangled, it can store its entangled state until all the other links are ready. The effect is that, if QKD were to be performed using this repeater system, the key rate would scale as the transmittivity of the individual links and not as the transmittivity of the whole channel from Alice to Bob. More explicitly, assume that the repeater stations are connected using optical fiber. If a direct connection from Alice to Bob would have transmittivity η, then the QR-assisted key rate goes as $\eta^{1/N}$ where N is the number of links between stations.

Recall that the TGW bound constrains the key rate to scale at best as $R \propto \eta$ (assuming $\eta \ll 1$). However, the scheme we have presented here scales as $R \propto \eta^{1/N}$, which is superior. We see, then, that this scheme really is a quantum repeater in the sense of Definition 9 above.

There are a number of factors that stand in the way of experimentally implementing such a scheme, however. Chief among them is the fact that, in practice, QMs do not perfectly retain a stored quantum state: in a process called *dephasing*, the stored state decays over time [10]. This introduces errors in the Bell states used for entanglement swapping, inducing potentially large errors in the final entangled state and in any state subsequently teleported from Alice to Bob. Another factor is the greater number of inefficiencies and sources of loss which are introduced by the repeater stations. If too severe, such losses may negate the benefit of introducing the stations.

Different QR schemes overcome such errors in different ways. The first QR proposal [5], a simplified version of which was presented above, places multiple pairs of quantum memories in each station. Multiple entanglement links are produced between each of the stations, and these imperfectly entangled states are used in a process called *entanglement distillation* to produce a single high-quality entangled state between Alice and Bob. Another approach, described in [8], is basically the same as the scheme presented above except that instead of producing Bell states between single QMs, *encoded* Bell states are produced between banks of QMs. Because of the redundancy involved in encoding a single Bell state in multiple pairs of QMs, this scheme is more tolerant of error. Yet another scheme [9] does away with entanglement swapping altogether, instead encoding every signal sent by Alice into a number of photons and sending them towards Bob. Along the way, the photons encounter repeater stations at which *quantum error correction* is performed. If a sufficient number of photons reach each station, the error correction regenerates the original signal.

Unfortunately, all of these schemes are impractical because they require the use of many QMs. It can be difficult to implement even two QMs in a lab, let alone the long string of them required by even the simple QR scheme presented at the beginning of this subsection. Although simpler QM schemes have been proposed [27], *no experiment to date has ever beat the TGW bound.*

Chapter 3

Beating the TGW bound using a single quantum repeater node

3.1 Introduction

In this chapter, we analyze a simplified quantum repeater scheme, containing only one node, which has the potential to beat the Takeoka-Guha-Wilde (TGW) bound. In it, two parties perform QKD by measuring photons sent from a central station containing two quantum memories (Fig. 3.1). If the station is placed midway between the parties, each photon need only travel half the distance between them. Moreover, the presence of the memories means that the probability of one party successfully measuring a photon is independent of the success of the other party. Together, these imply that the secret key rate for our protocol is expected to scale as $\sqrt{\eta_{\text{ch}}}$, where η_{ch} is the transmittivity of an optical fiber stretching between the parties. Such scaling would be a fundamental improvement over any scheme relying on direct transmission, and gives it the potential to surpass the TGW bound. Here, we study whether this scheme can beat the TGW bound in practice, taking into account

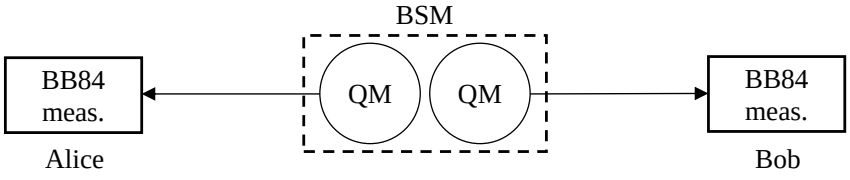

Figure 3.1: Schematic of the proposed protocol. One quantum memory (QM) sends entangled photons to Alice, the other to Bob. Once both parties successfully measure photons using BB84 measurements, a Bell measurement is performed on the QMs.

experimental imperfections.

One of the merits of this scheme is that it can be implemented using currently available technology. Though not directly scalable to multiple repeater stations, it represents a step towards a fuller implementation of quantum repeaters such as the ones alluded to in Sec. 2.3.2 of the previous chapter. It is similar in spirit to the protocol described in [27], except that in their proposal single photons or weak laser pulses are sent *toward* the central station instead of being emitted *from* the quantum memories (QMs). Our protocol thus simplifies the experimental requirements, at the cost of introducing wait times due to classical communication.

3.2 Description of the protocol

The protocol we consider in this chapter is illustrated in Fig. 3.1. It uses two quantum memories in a central station placed between Alice and Bob, who wish to establish a secret key via QKD. We do not assume a particular implementation of the QMs, but we do require that each QM can be entangled with a single photon (as in, for example, ion-photon entanglement [25] or the DLCZ scheme [6]). The photonic degree of freedom used to encode qubits can be freely chosen; examples include polarization or time-bin encoding. We further assume that the two QMs can be jointly measured in the Bell basis, either by applying the appropriate quantum channels and then directly measuring them or by mapping the memory states onto photons and performing an optical Bell measurement. Alice and Bob are connected to the central station by lossy optical channels, and each have measurement apparatuses that allow them to measure incoming photons in one of two settings which correspond to mutually unbiased bases of the qubit subspace (as in BB84). As in Sec. 2.2 of Ch. 2, we will call the bases X and Z.

The procedure to produce one bit of raw key is as follows:

1. An entangled memory-photon state is prepared in one of the QMs and the photon sent to Alice, who performs a BB84 measurement on the photon. (See the chart given in Ch. 2, Sec. 2.2.) This is repeated until she successfully detects a photon.

2. Same as the previous step, but with Bob and the other QM.

3. A Bell measurement is performed on the two QMs and the result announced to Bob.

4. If Bob measured in the Z basis, he applies a bit flip to his BB84 measurement if the Bell measurement yielded $|\Psi^+\rangle$ or $|\Psi^-\rangle$. Similarly, if he measured in the X basis, he applies a bit flip if the Bell measurement yielded $|\Phi^-\rangle$ or $|\Psi^-\rangle$.

This procedure is repeated until a sufficient amount of raw key is obtained. The rest of the protocol is the same as in efficient BB84.

The protocol described here admits of a few variations: the QMs could be *simultaneously* or *sequentially loaded* by performing steps 1 and 2 either at the same time or in sequence, and the position of the central station can be changed. In Sec. 3.6, we will explore the difference between simultaneous and sequential loading as well as the effect of changing the position of the central station.

3.3 Benchmarks

In comparing our protocol to schemes based on the direct transmission of photons from Alice to Bob, the TGW bound is the most stringent standard of comparison. We will, however, compare our protocol to other scenarios as well; this will make it easier to see how well it matches up to concrete schemes that can be performed in a lab. The direct transmission benchmarks with which we will compare our protocol are as follows:

1. The TGW bound on the secret key rate per mode,

$$R_{\mathrm{TGW}} = \log_2\left(\frac{1+\eta_{\mathrm{ch}}}{1-\eta_{\mathrm{ch}}}\right), \tag{3.1}$$

   where η_{ch} is the channel transmittivity. For small η_{ch}, this reduces to $R_{\mathrm{TGW}} \approx (2/\ln 2)\eta_{\mathrm{ch}} \approx 2.89\eta_{\mathrm{ch}}$.

2. BB84 with an ideal single-photon source and an ideal detector setup (no errors and no losses other than channel loss).

3. BB84 with an ideal single-photon source and a realistic detector setup (nonzero misalignment error and dark counts, imperfect detector efficiency).

4. Decoy-state BB84 with a laser and a realistic detector setup.

5. BB84 using a quantum memory as a single photon source and a realistic detector setup.

The figure of merit to be considered in this chapter is the key rate *per mode*. Because BB84 requires two optical modes when implemented with the usual polarization or time-bin encoding, its key rate expression takes on a factor of 1/2. We may compare the key rate per mode of our protocol to those of the benchmarks above either on a per time unit or a per channel use basis. In this chapter we will compare key rates per channel use only,

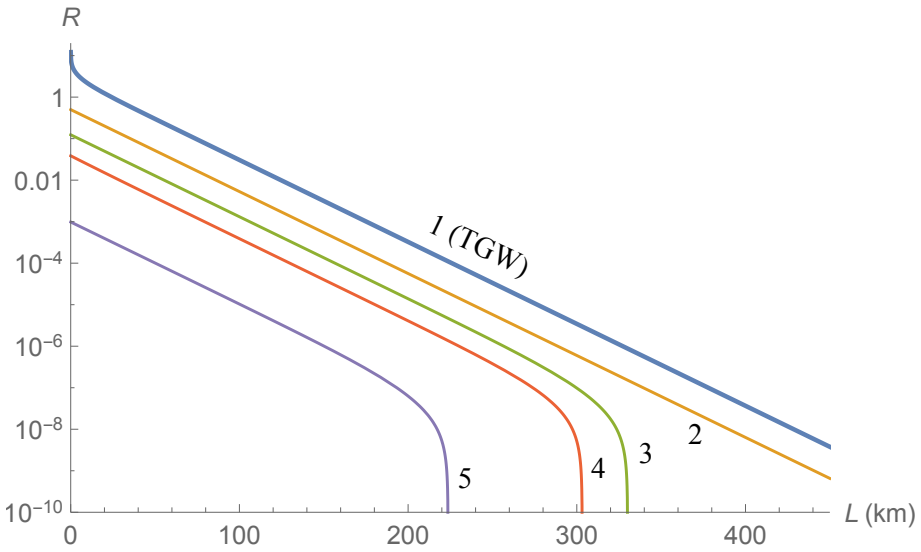

Figure 3.2: Key rate per channel use per mode vs. distance for the benchmarks listed in Sec. 3.3. The thick curve corresponds to the TGW bound (benchmark 1). Parameter values are as given in Sec. 3.6.

though in future work it is of course desirable to compete on a per time unit basis. Any reference to "key rates" in the remainder of this chapter, then, should be taken to mean "key rates per mode per channel use". Expressions for the key rates of benchmarks 2–5 are given in Appendix A.

Fig. 3.2 shows plots of key rates as a function of the distance between Alice and Bob. Note that all of these benchmarks are proportional to η_{ch} (within certain limits, depending on the benchmark).

3.4 Component modeling

In this section, we present a simple model of the experimental behavior of each component in the setup described in Sec. 3.2 in the absence of eavesdropping.

3.4.1 Quantum memories

In this chapter, we consider QMs that are adequately described by the following model. A photon-memory entangled state can be generated in a QM with probability η_p; each attempt to do so requires a preparation time of T_p. When a photon is successfully generated, it

is *maximally entangled* with the QM; without loss of generality, we may take the initial memory-photon state to be the Bell state $|\Phi^+\rangle$.

The memory-channel photon coupling efficiency is η_c. This includes not only the probability of a photon entering the optical channel, but the success probability of any process that occurs between the memory and the channel. For example, it contains the probability of successfully performing a wavelength conversion (if such is necessary).

Dephasing refers to the degradation of the state stored in a QM over time, and is characterized by a dephasing time T_2. We will model dephasing using the following map [10], which takes as input the initial state ρ of the QM and returns the state of the QM after it has dephased for time t:

$$\Gamma_t(\rho) := [1 - \lambda_{\text{dp}}(t)]\rho + \lambda_{\text{dp}}(t) Z\rho Z \tag{3.2}$$

where

$$\lambda_{\text{dp}}(t) := \frac{1 - e^{-t/T_2}}{2} \tag{3.3}$$

and Z is the Pauli Z operator. Notice that, in this model, the off-diagonal elements of ρ go to zero as $t \to \infty$.

3.4.2 Channels

Alice and Bob are connected to the central station by optical channels of lengths L_A and L_B respectively; the length of the total channel is therefore $L = L_A + L_B$. The speed of light through these channels is c. The transmittivity of a channel of length l is

$$\eta_{\text{ch}}(l) = e^{-l/L_{\text{att}}} \tag{3.4}$$

where L_{att} is the attenuation length.

The probability of error due to setup misalignment between Alice and the central station is e_{mA}. Setup misalignment is a discrepancy between the coordinate system that Alice imposes on the photon's state space and the one that the central station imposes; in the case of polarization encoding, this means Alice's detector is physically rotated relative to the central station. Misalignment results in an effective rotation of the qubit state of the photon. If we assume the rotation angle to be random and symmetrically distributed about 0, the initial memory-photon state $|\Phi^+\rangle$ becomes

$$(1 - e_{mA})|\Phi^+\rangle\langle\Phi^+| + e_{mA}|\Psi^-\rangle\langle\Psi^-| \tag{3.5}$$

when the photon reaches a detector. This holds for Bob as well, with misalignment error e_{mB}.

3.4.3 Detectors

For their BB84 measurements, Alice and Bob each use a detector setup consisting of an optical element that can distinguish photonic qubit states in the X and Z bases (such as a polarizing beam splitter for polarization qubits) and two threshold detectors which signal the presence or absence of photons, but do not count the number of photons in a given pulse. We assume that Alice and Bob actively choose the basis in which to measure. Each detector has a dark count probability of p_d; each setup has efficiency η_d.

If a photon heading towards one of the setups is in the state ρ, the effect of dark counts can be mimicked by photons which are effectively in the modified state

$$\alpha(\eta)\rho + [1 - \alpha(\eta)]\frac{\mathbb{1}}{2}, \tag{3.6}$$

where

$$\alpha(\eta) := \frac{\eta(1 - p_d)}{1 - (1 - \eta)(1 - p_d)^2} \tag{3.7}$$

and η is the probability that the photon reaches the detector setup. This assumes the use of a squashing map [28] which randomly assigns a measurement outcome to events in which both detectors click, reflected by ρ being mapped into the maximally mixed state. (The squashing map eliminates the need to consider higher-dimensional state spaces by mapping two-photon events into one-photon events according to the preceding prescription.)

3.4.4 Bell state measurement

The probability of successfully performing a Bell state measurement on the two QMs is p_{BSM}.

We model errors in the BSM by applying the depolarizing channel

$$\Delta_{\lambda_{\text{BSM}}}(\rho) = \lambda_{\text{BSM}}\rho + (1 - \lambda_{\text{BSM}})\frac{\mathbb{1}}{4} \tag{3.8}$$

to the QMs before a perfect BSM. The parameter λ_{BSM} indicates how close the actual BSM is to an ideal BSM.

3.5 Key rate analysis

The secret key rate is lower bounded by [17, 16]

$$R = \frac{Y}{2}[1 - h(e_X) - fh(e_Z)]. \tag{3.9}$$

Here, the yield Y is the probability per channel use that Alice and Bob's measurements, as well as the BSM, were successful. $h(e)$ is the binary entropy function, e_X and e_Z are the quantum bit error rates (QBERs) between Alice and Bob in the X and Z bases, and f is the error correction inefficiency. The factor of $1/2$ comes from the fact that our protocol requires the use of two optical modes.

Because the total channel between Alice and Bob is divided in two by the central station and because the number of signals sent over each segment of the channel may in general be different, it is not immediately obvious how to count channel uses. To be conservative, we define the number of channel uses required to produce one bit of raw key to be the *greater* of the number of times Alice or Bob used their segments of the channel during the production of that bit. (Note that this is not the *sum* of the number of times Alice and Bob used their segments of the channel, even in the case of sequential loading.)

3.5.1 Yield

The probability that a photon emitted from the central station is detected by Alice is

$$\eta_A := \eta_{\text{tot}} e^{-L_A/L_{\text{att}}}. \tag{3.10}$$

where we have defined

$$\eta_{\text{tot}} := \eta_p \eta_c \eta_d. \tag{3.11}$$

Due to the effect of dark counts, the probability that her detector clicks is

$$\eta'_A := 1 - (1 - \eta_A)(1 - p_d)^2. \tag{3.12}$$

Let N_A denote the number of photons that need to be sent to Alice so that her detector clicks once; it is a geometrically distributed random variable with success probability η'_A. Expressions similar to the above apply for Bob.

The average number of channel uses required for both Alice and Bob's detectors to click is $\mathbb{E}[\max(N_A, N_B)]$ where $\mathbb{E}$ is the expected value operator. The yield is therefore

$$\begin{aligned} Y &= \frac{p_{\text{BSM}}}{\mathbb{E}[\max(N_A, N_B)]} \\ &= p_{\text{BSM}} \left(\frac{1}{\eta'_A} + \frac{1}{\eta'_B} - \frac{1}{\eta'_A + \eta'_B - \eta'_A \eta'_B} \right)^{-1}. \end{aligned} \tag{3.13}$$

In evaluating the expectation value, we have used a result in [27].

3.5.2 Quantum bit error rates

Taking into account all the parameters listed in Sec. 3.4, we find (in the absence of eavesdropping) that

$$e_X = \lambda_{\mathrm{BSM}}\alpha(\eta_A)\alpha(\eta_B)[\varepsilon_m(1-\varepsilon_{\mathrm{dp}}) + (1-\varepsilon_m)\varepsilon_{\mathrm{dp}}] + \frac{1}{2}[1 - \lambda_{\mathrm{BSM}}\alpha(\eta_A)\alpha(\eta_B)] \tag{3.14}$$

$$e_Z = \lambda_{\mathrm{BSM}}\alpha(\eta_A)\alpha(\eta_B)\varepsilon_m + \frac{1}{2}[1 - \lambda_{\mathrm{BSM}}\alpha(\eta_A)\alpha(\eta_B)] \tag{3.15}$$

where

$$\varepsilon_m = e_{mA}(1-e_{mB}) + (1-e_{mA})e_{mB} \tag{3.16}$$

$$\varepsilon_{\mathrm{dp}} = \mathbb{E}\big[\lambda_{\mathrm{dp}}(t_A)[1-\lambda_{\mathrm{dp}}(t_B)] + [1-\lambda_{\mathrm{dp}}(t_A)]\lambda_{\mathrm{dp}}(t_B)\big]. \tag{3.17}$$

We may interpret ε_m and $\varepsilon_{\mathrm{dp}}$ as the total misalignment and dephasing errors, respectively, between Alice and Bob. Here t_A and t_B are the times that Alice and Bob's QMs are left to dephase for.

At this point, we have fully determined e_Z in terms of the parameters set out in Sec. 3.4. In order to evaluate e_X, we need only two more quantities: the dephasing time intervals t_A and t_B. These are the subject of the following subsection.

Dephasing

Each time a QM emits a photon towards Alice, she must signal whether or not she successfully measured her photon before the QM prepares another one. This constrains the amount of time that elapses between photons to be at least

$$\tau_A = T_p + \frac{2L_A}{c}. \tag{3.18}$$

Similar remarks apply to Bob.

If it happens that $L_A \neq L_B$, then (3.18) allows the QMs to run at different rates. Throughout this chapter, we will assume that each QM runs at the maximum rate allowed by (3.18). It is possible to choose the rates to be the same, but we will not do so here.

For both sequential and simultaneous loading, we may assume without loss of generality that Bob signals a successful measurement later than Alice does. The BSM is performed as soon as he does, so the QM that sends him photons dephases for a time

$$t_B = \frac{2L_B}{c}. \tag{3.19}$$

The QM that sends photons to Alice dephases for a longer period of time because it must wait for Bob to make a successful measurement. If the QMs are sequentially loaded, Alice's QM dephases for

$$t_A^{\text{seq}} = N_B \tau_B + \frac{2L_A}{c}. \tag{3.20}$$

If they are loaded simultaneously, then it dephases for

$$t_A^{\text{sim}} = |N_B - N_A| \tau_B + \frac{2L_A}{c}. \tag{3.21}$$

In (3.17), because of the linearity of the expectation value operator $\mathbb{E}$, we need only evaluate $\mathbb{E}[e^{-t_A/T_2}]$. For sequential loading,

$$\mathbb{E}\left[e^{-t_A^{\text{seq}}/T_2}\right] = \frac{\eta_B' \exp\left(-\frac{2L_A}{cT_2}\right)}{e^{\tau_B/T_2} + \eta_B' - 1}. \tag{3.22}$$

For simultaneous loading, a result from [27] gives

$$\mathbb{E}\left[e^{-t_A^{\text{sim}}/T_2}\right] = \frac{\eta_A' \eta_B' \exp\left(-\frac{2L_A}{cT_2}\right)}{\eta_A' + \eta_B' - \eta_A' \eta_B'} \left[\frac{1}{1 - e^{-\tau_B/T_2}(1 - \eta_A')} + \frac{1}{1 - e^{-\tau_B/T_2}(1 - \eta_B')} - 1 \right]. \tag{3.23}$$

3.6 Results

Unless otherwise noted, the following parameter values were used for the results in this section. They are plausible values for an implementation of our protocol using trapped-ion quantum memories connected to Alice and Bob via optical fiber. A single ion fluorescence collection efficiency of 4.2% has been demonstrated in [29], a trapped-ion qubit was measured to have a dephasing time of 2.5 s in [21], and a two-qubit gate was used to entangle two ions with a fidelity of 99.3% (corresponding to $\lambda_{\text{BSM}} = 0.99$) in [22].

- η_p (preparation efficiency) $= 0.66$
- T_p (preparation time) $= 2\ \mu$s
- η_c (photon-fiber coupling efficiency $\times$ wavelength conversion) $= 0.04 \times 0.3$
- T_2 (dephasing time) $= 1$ s
- c (speed of light in optical fiber) $= 2 \times 10^8$ m/s
- L_{att} (attenuation length) $= 22$ km
- e_{mA} (misalignment error) $= e_{mB} = 0.01$

- p_d (dark count probability per detector) $= 10^{-8}$
- η_d (detector efficiency) $= 0.3$
- p_{BSM} (BSM success probability) $= 1$
- λ_{BSM} (BSM ideality parameter) $= 0.97$
- f (error correction inefficiency) $= 1.16$

For decoy-state BB84 (benchmark 4), we will set the mean photon number of the signal states equal to 1. For the above numbers, we find that $\eta_{\text{tot}} = \eta_p \eta_c \eta_d = 0.0024$.

3.6.1 Protocol variations

Simultaneous vs. sequential loading

For this comparison, the central station is located halfway between Alice and Bob.

We have found, for the parameter values given above, that simultaneous and sequential loading of QMs in our protocol yield almost indistinguishable key rates per channel use over all values of L for which the rates are nonzero (Fig. 3.3). A rough comparison of the dephasing time intervals t_A^{seq} and t_A^{sim} suggests that this holds whenever $\tau_B/(T_2\eta_{\text{tot}})$ is small over all values of L for which the key rates are nonzero. The parameters we have used are

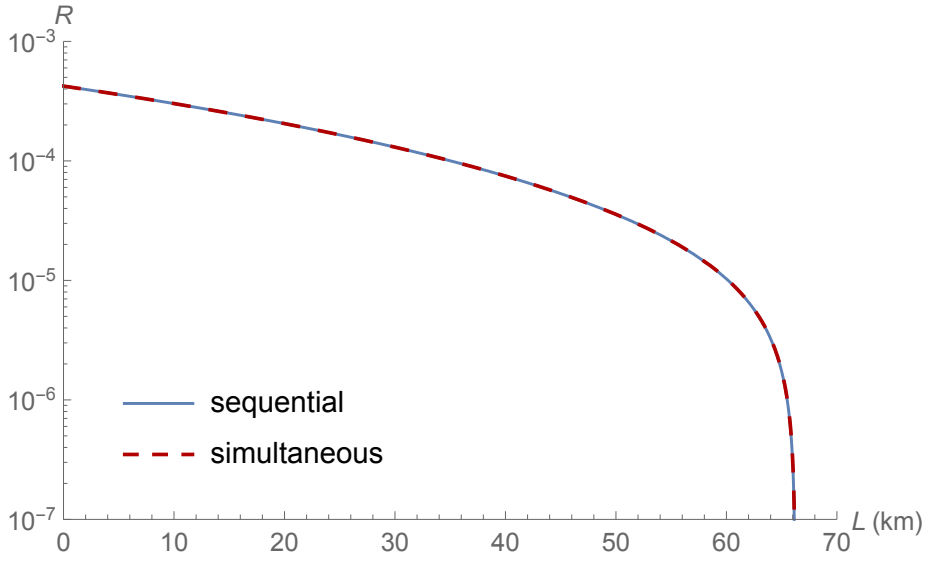

Figure 3.3: Key rate per channel use vs. distance for simultaneous and sequential loading. The two curves are virtually indistinguishable.

within this regime: $\tau_B/(T_2\eta_{\text{tot}}) = 0.140$ at $L = 66$ km. Outside of it, however, the difference can be dramatic: there are cases where the key rate is nonzero for simultaneous loading but not for sequential loading.

One might expect to see, at least in the ideal case where the dephasing time T_2 is very long, that the key rate for simultaneous loading is twice that of sequential loading. The reason this factor of two does not appear is because we count channel uses for both sequential and simultaneous loading in the same way. (Recall that we are considering key rates in terms of channel uses, not time.)

Because we will always be well within the parameter regime where simultaneous and sequential loading give nearly the same key rate, we will consider only sequential loading in the remainder of this chapter.

Optimization of central station position

When the QMs are sequentially loaded, it need not be true that placing the central station halfway between Alice and Bob will yield the maximum key rate. This is because there is an inherent asymmetry in our protocol in this case: Bob only begins making measurements after Alice has finished hers.

Fig. 3.4 shows the behavior of the key rate (per channel use) as a function of L when the central station is placed at $L/2$ and when it is placed at the position that maximizes the key rate. For small L, both key rates are approximately the same, and scale proportionally to $\sqrt{\eta_{\text{ch}}} = e^{-L/(2L_{\text{att}})}$. When L becomes large enough for memory dephasing to become significant, the unoptimized key rate drops to zero. Around that same point, the optimized key rate transitions from $e^{-L/(2L_{\text{att}})}$ scaling to $\eta_{\text{ch}} = e^{-L/L_{\text{att}}}$ scaling—which is the same as for direct transmission—and continues thus until L is so large that detector dark counts become significant, at which it too drops to zero.

For greater insight into this behavior, consider Fig. 3.5, which shows the optimal central station position as a fraction of L as L is varied. For lower values of L, the station remains near the middle. Once dephasing becomes significant, the optimal position moves closer to Bob. This keeps dephasing errors low because Bob's link runs quicker, giving Alice's QM less time to dephase. At longer distances, the optimal position is a fixed distance away from Bob, just far enough away that the dephasing in Alice's QM does not overwhelm the system with errors. The price of suppressing dephasing errors in this way is that the key rate scales with the transmittivity of the longer link in the setup, so the key rate scaling is degraded.

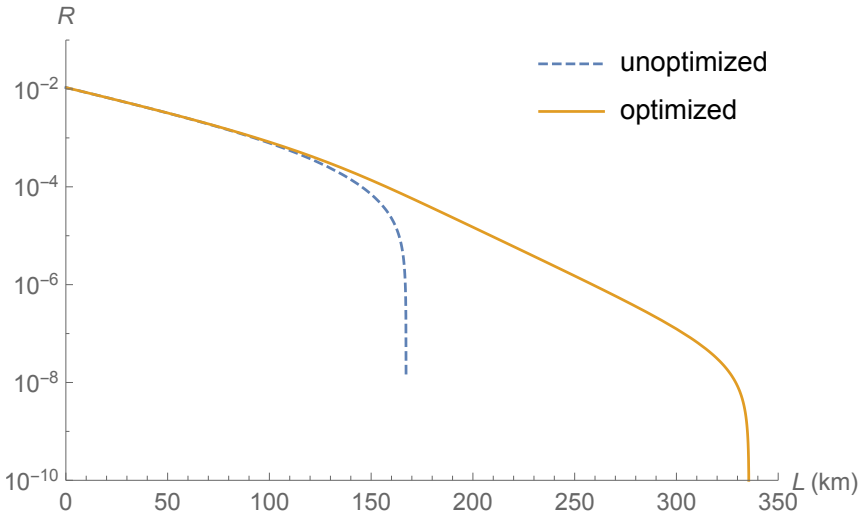

Figure 3.4: Key rate vs. distance when the central station is at $L/2$ and when its position is optimized. (η_c was increased to 0.3 to better show the features of the curves.) Near 150 km, the unoptimized key rate begins to drop to 0 and the optimized key rate transitions from $e^{-L/(2L_{\text{att}})}$ scaling to $e^{-L/L_{\text{att}}}$ scaling.

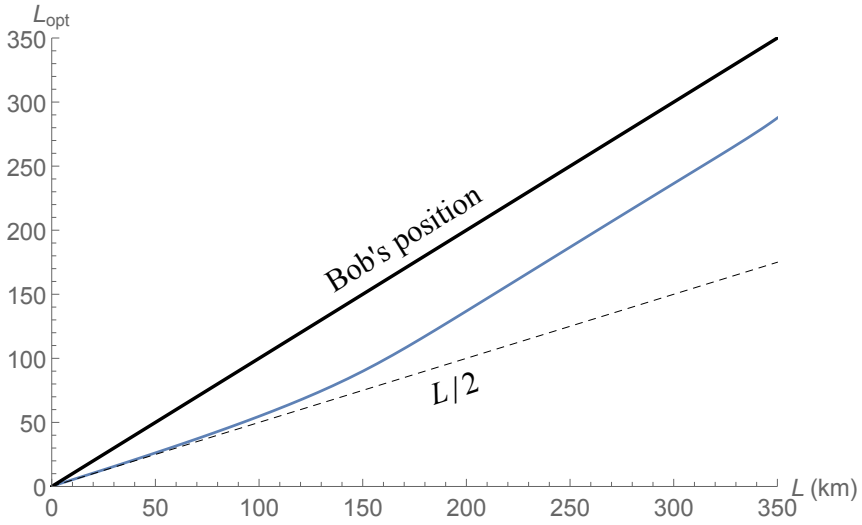

Figure 3.5: Optimal central station position as a function of the total distance L. (Alice's position is taken to be at $L = 0$.) Near where the scaling changes from $e^{-L/(2L_{\text{att}})}$ to $e^{-L/L_{\text{att}}}$, around $L = 150$ km, the optimal position moves away from $L/2$ and remains a fixed distance away from Bob.

3.6.2 Beating direct transmission

We are now in a position to determine the conditions under which our protocol can beat the direct transmission benchmarks listed in Sec. 3.3. First, note that at $L = 0$ the performance of our protocol may be worse than that of the benchmarks because the central station introduces additional sources of loss. However, because the key rate for our protocol scales better with distance than the benchmark key rates when L is not too large, *crossover* with one or more of them is possible at some $L > 0$.

When the central station position is optimized, crossover can only occur in the $e^{-L/(2L_{\text{att}})}$ regime (excluding marginal cases)—that is, when the optimal position is near the midpoint between Alice and Bob. Equivalently, crossover can only occur when the unoptimized key rate is nonzero. For this reason, we will fix the central station at $L/2$ for the remainder of this section instead of optimizing its position. It is worth mentioning that crossover with a certain benchmark does not mean that our protocol beats it for *all* L beyond the crossover point; the interval over which our protocol is superior may be quite small. But optimizing the central station position can potentially increase the range of distances over which our protocol beats the benchmark compared to the leaving the station at $L/2$.

We identify two parameters, the combined efficiency η_{tot} and the dephasing time T_2, which are crucial in determining whether crossover occurs with any of the benchmarks and which can be improved from the values given at the beginning of this section. For example, the photon-fiber coupling efficiency in η_c could be pushed from 0.04 to as high as 0.3 [30] (leading to $\eta_{\text{tot}} = 0.0178$), while a T_2 of 50 s has already been demonstrated [23]. Fig. 3.6 shows the regions in η_{tot}-T_2 space in which we can beat each of the benchmarks. It is clear from the figure that we cannot beat any of the benchmarks with the parameters given at the beginning of the section. From our perspective, improving η_{tot} is preferable to improving T_2. If η_{tot} were fixed at a low value, the T_2 required to beat the benchmarks would be unreasonably long. In such a case, the experiment itself may run so slowly that it is infeasible to accumulate a significant amount of secret key.[1]

Each region may be explained in the following way. When L is small enough for errors to be negligible, the key rate of our protocol is $R \approx R_0 e^{-L/(2L_{\text{att}})}$ while that of the benchmark of interest is $R_b \approx R_{b,0} e^{-L/L_{\text{att}}}$, where R_0 and $R_{b,0}$ are the key rates at $L = 0$ of our protocol and of the benchmark respectively.[2] These curves intersect at a distance L_{int}. If L_{int} is smaller than some characteristic distance L_{dp} beyond which dephasing becomes significant,

[1] Recall, from Definition 8 of the previous chapter, that secret key rate is defined in the limit of *infinitely long* keys. We have implicitly assumed throughout the chapter that so-called *finite-size effects* are negligible. But this is not true if the experiment cannot produce a large amount of key in a reasonable amount of time.

[2] This does not quite apply to the TGW bound, which goes to infinity as $L \to 0$. In this case, one must continue the $e^{-L/L_{\text{att}}}$ behavior all the way to $L = 0$, so that $R_{b,0} = 2/\ln 2$.

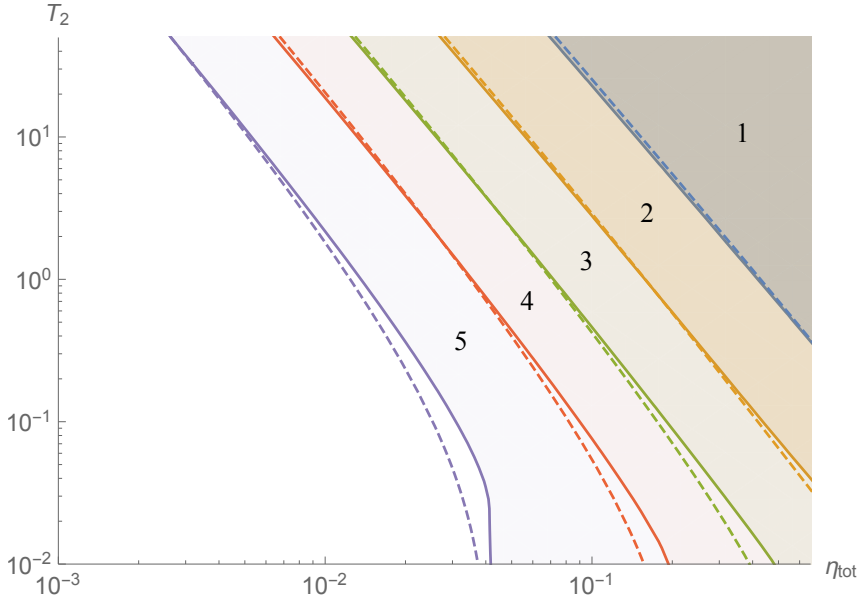

Figure 3.6: Regions in η_{tot}-T_2 space where our protocol beats each of the benchmarks listed in Sec. 3.3, together with approximations of their boundaries obtained using (3.24) (dashed lines). For benchmark 5 (quantum memory as single photon source), we have fixed $\eta_c = 0.3 \times 0.3$.

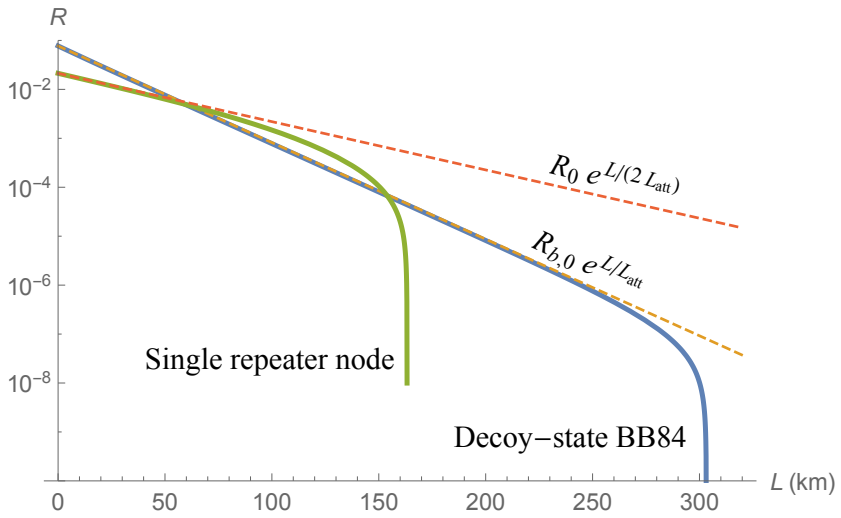

Figure 3.7: Approximating the crossover point using the scaling behavior of the key rates. Note that the intersection point of the approximating curves coincides with the crossover point of the key rate curves, and that the intersection occurs before dephasing becomes significant and the key rate of our protocol goes to 0. (We have set $\eta_c = 0.3$.)

then there is a crossover. The boundary of the crossover region corresponds to $L_{\text{int}} = L_{\text{dp}}$. These ideas are illustrated in Fig. 3.7.

Based on this explanation, we can derive an approximate formula for the boundary of the region in which crossover occurs with a given benchmark with key rate R_b:

$$T_2 = K\left[\frac{QT_p}{\eta_{\text{tot}}^2} + \frac{2L_{\text{att}}\ln(Q/\eta_{\text{tot}})}{c}\left(1 + \frac{Q}{\eta_{\text{tot}}^2}\right)\right]. \tag{3.24}$$

Here

$$Q = \frac{3R_{b,0}}{2R_0^{\eta_{\text{tot}}=1}}, \tag{3.25}$$

$R_0^{\eta_{\text{tot}}=1}$ denotes the key rate of our protocol when $L = 0$ and $\eta_{\text{tot}} = 1$, and K is a fitting parameter characterizing how long the QMs must dephase for, as a fraction of T_2, before dephasing becomes significant. It needs to be chosen to fit the exact crossover region boundary; empirically, $K = 14$ gives a good fit. This approximation is valid when $T_p \ll T_2$ and $p_d \ll \eta_{\text{tot}}^2/Q$. A derivation is given in Appendix B.

The dashed lines in Fig. 3.6 are the boundary approximations given by (3.24).

Attenuation length; the high-loss limit

Let us now consider the *high-loss limit*, where the attenuation length L_{att} is very small. This limit is interesting in the context of hybrid quantum-classical networks. In passive optical networks, where multiple users are connected to a source, each user is effectively connected to the source via a high-loss channel. The limit is also applicable when the wavelength of the photons emitted by the QMs happens to be greatly attenuated by the optical channel.

The effect of reducing the attenuation length is to make it easier to beat the benchmarks, as shown in Fig. 3.8 and predicted in (3.24). This is because the photons cannot travel as far, so there is less dephasing. However, because of the nonzero preparation time T_p, beating the benchmarks is still nontrivial in the $L_{\text{att}} \to 0$ limit. The high-loss limit thus represents a regime in which experimental requirements are relaxed, yet the benchmarks can still meaningfully be beaten.

Fig. 3.9 shows the effect of changing the preparation time T_p and the dark count probability p_d on the η_{tot}-T_2 regions in which our protocol can beat the TGW bound. As expected from (3.24), the benchmarks become easier to beat as T_p goes down. (This is true whatever the value of L_{att}.) We also see that when $T_p = 0$ and $L_{\text{att}} \to 0$, they can be beat for any value of T_2. Because there is no dephasing at all in this case, T_2 plays no role in determining whether there is a crossover.

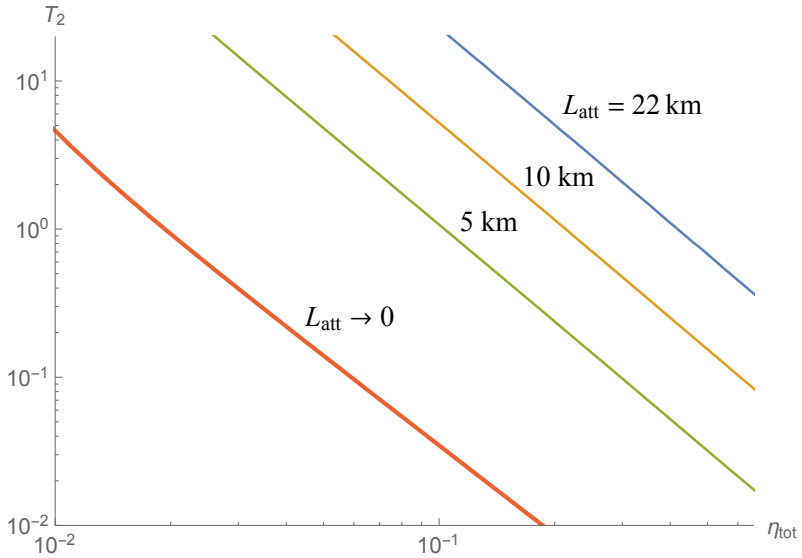

Figure 3.8: Boundaries of regions in η_{tot}-T_2 space where our protocol beats the TGW bound for various attenuation lengths.

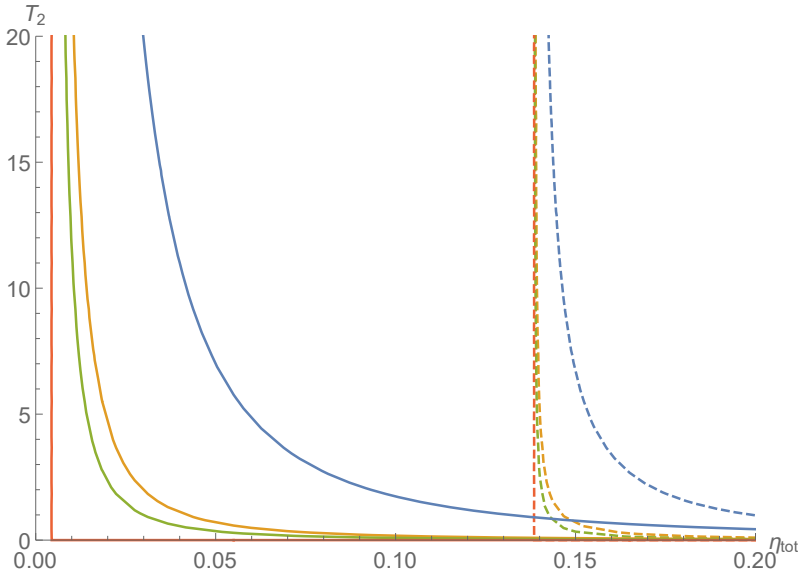

Figure 3.9: Boundaries of regions in η_{tot}-T_2 space where our protocol beats the TGW bound in the limit $L_{\text{att}} \to 0$. Solid lines indicate $p_d = 10^{-8}$, dashed lines $p_d = 10^{-5}$. Blue, orange, green, and red lines indicate $T_p = 100$, 10, 5, and 0 μs respectively.

Eq. (3.24) suggests that when $T_p = 0$ and $L_{\text{att}} \to 0$, crossover can happen for any value of η_{tot}. However, Fig. 3.9 shows that crossover can happen only when η_{tot} is sufficiently large. There is no contradiction: when η_{tot} is too low, the condition $p_d \ll \eta_{\text{tot}}^2/Q$ is violated and (3.24) no longer holds. It turns out that there is no crossover when η_{tot} is small because dark counts become significant. Using reasoning similar to that employed in deriving (3.24) (with the characteristic dephasing length L_{dp} replaced with a characteristic dark count length L_d), we can obtain the following approximation to the minimum η_{tot} necessary for our protocol to beat a given benchmark:

$$\eta_{\text{tot}}^{\text{min}} = \sqrt{\frac{Qp_d(2-p_d)(1-\xi)}{(1-p_d)(p_d+\xi-p_d\xi)}}. \tag{3.26}$$

The quotient of key rates at zero distance, Q, is as defined in (3.25), and depends on the choice of benchmark. The fitting parameter ξ is a measure of how much error due to dark counts our system can tolerate before the key rate drops to zero. For the parameter values given at the beginning of the section, $\xi = 0.012$ fits well. This equation is valid when $T_p \ll T_2$ and $p_d \ll \eta_{\text{tot}}$. The derivation is in Appendix B.

3.7 Conclusion

In this chapter, we have analyzed a QKD protocol in which Alice and Bob exchange signals with a central station consisting of two quantum memories: a rudimentary quantum repeater node. We have also introduced a number of benchmarks to which our protocol can be compared, the most important of them being the Takeoka-Guha-Wilde bound on the secret key rate. We showed that our protocol can, in principle, beat the benchmarks because of its improved rate-vs.-distance scaling: the key rate of all protocols relying on direct transmission between Alice and Bob scales at best with $e^{-L/L_{\text{att}}}$, while our protocol scales as $e^{-L/(2L_{\text{att}})}$. In effect, our protocol doubles the attenuation length. Finally, we explored the conditions under which we can beat the benchmarks in practice.

Our protocol cannot be scaled up to arbitrary lengths in the same way as the one described in Sec. 2.3.2 of Ch. 2. One cannot simply string together multiple copies of the central station without introducing some method for entangling two of these stations. This could be done, for example, using an optical Bell measurement. But the introduction of such a measurement would be a nontrivial change in the protocol, necessitating additional analysis. Because our protocol is so simple, it is feasible to implement using currently available technology while still exhibiting the rate improvement of a full quantum repeater scheme and the ability to beat the TGW bound. Beating the bound would, in and of itself,

be a fundamental experimental achievement—an achievement which we have shown to be within reach, particularly in the high-loss limit. Our protocol, then, is a first step towards the experimental implementation of quantum repeaters.

Chapter 4

Entangling two spatially separated quantum memories

4.1 Introduction

The generation of entanglement between two spatially separated quantum memories (QMs) is an important step in many quantum repeater schemes [5, 6, 7, 8, 10]. From a practical point of view, this is one of the most difficult and error-prone aspects of implementing a quantum repeater.

In this chapter, we focus on a specific experimental implementation of a QM and explore three different methods for how two of them can be entangled. Two of them involve coherent states, while the third relies on entangled single photons (much like in the previous chapter). We will compare the probability that each method successfully produces an entangled state, as well as the quality of the entanglement. In the analysis, we will show that there is a tradeoff between success probability and quality of entanglement in the first two schemes, controlled by the amplitude of the coherent states. But neither of them can generate states that are as entangled as those produced by the third scheme.

The QM of interest is a single atom trapped in a cavity, as described in [31, 32, 33]. Certain tasks expected of a QM have already been experimentally demonstrated with this system. For example, a research team headed by Rempe has demonstrated the processes of "writing" the state of a photonic qubit into an atom and "reading" it out into a photon again [32]. In [31], it was verified that an atom could be entangled with a photon. This was achieved by means of an atom-photon interaction which is equivalent to the so-called *controlled-NOT* (CNOT) operation, as we will now describe.

4.1.1 The atom-photon interaction

Qubit basis states are encoded as two hyperfine ground states of the atom, though we will denote them abstractly as $\{|0\rangle, |1\rangle\}$. The cavity is resonant with a transition between $|1\rangle$ and an excited state which is mediated by right circularly polarized photons. It is not resonant with any transition from $|0\rangle$, nor with any transition involving left circularly polarized photons. This structure gives rise to an interesting interaction between the trapped atom and a photon that is reflected off the cavity. In the ideal case, the interaction can be described as follows. Let $|L\rangle$ and $|R\rangle$ denote states in which a single photon is left and right circularly polarized, respectively. Then the effect of reflecting a single photon off of the cavity is that of a quantum operation known as the *controlled π phase gate*:

$$\begin{aligned} |0\rangle|L\rangle &\rightarrow |0\rangle|L\rangle \\ |0\rangle|R\rangle &\rightarrow |0\rangle|R\rangle \\ |1\rangle|L\rangle &\rightarrow |1\rangle|L\rangle \\ |1\rangle|R\rangle &\rightarrow -|1\rangle|R\rangle. \end{aligned} \tag{4.1}$$

When applied to a right polarized *coherent state*, this operation has the effect of inducing a sign change in the coherent state amplitude: $|\alpha\rangle \rightarrow |-\alpha\rangle$. (Note that in the Fock state expansion of $|\alpha\rangle$, only the terms with odd photon number receive a sign change under this interaction.) It has no effect on left polarized photonic states.

If we write the interaction (4.1) in terms of the horizontal/vertical polarization states

$$|H\rangle := \frac{|L\rangle + |R\rangle}{\sqrt{2}}, \quad |V\rangle := \frac{|L\rangle - |R\rangle}{\sqrt{2}}, \tag{4.2}$$

we find that it is equivalent to the *CNOT operation*:

$$\begin{aligned} |0\rangle|H\rangle &\rightarrow |0\rangle|H\rangle \\ |0\rangle|V\rangle &\rightarrow |0\rangle|V\rangle \\ |1\rangle|H\rangle &\rightarrow |1\rangle|V\rangle \\ |1\rangle|V\rangle &\rightarrow |1\rangle|H\rangle. \end{aligned} \tag{4.3}$$

Note the interchange between horizontal and vertical polarizations when the atom is in the state $|1\rangle$. This interchange occurs with coherent states, too: $|1\rangle|\alpha, \beta\rangle \rightarrow |1\rangle|\beta, \alpha\rangle$, where the first and second modes correspond to horizontal and vertical polarization, respectively.

CNOT is well known to be an *entangling* operation: it can transform a separable state into an entangled state [13]. As mentioned above, it was used to produce atom-photon entanglement in [31]. We will now explore its use as a building block for creating entanglement between two atoms.

4.2 Three schemes for entangling two QMs

We here describe three possible schemes for entangling two trapped atoms. They are illustrated in Fig. 4.1. The first two were inspired by work done in [34, 35], which give schemes for entangling two QMs using coherent states and controlled phase gates. The third has actually been realized; see [36].

Scheme 1. Initialize each atom to the state $|+\rangle$ (where, as in Ch. 2, we define $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$). Reflect a right circularly polarized coherent state $|\alpha\rangle$ off of each cavity, then perform a "pseudo-Bell state measurement" on the two coherent states by sending

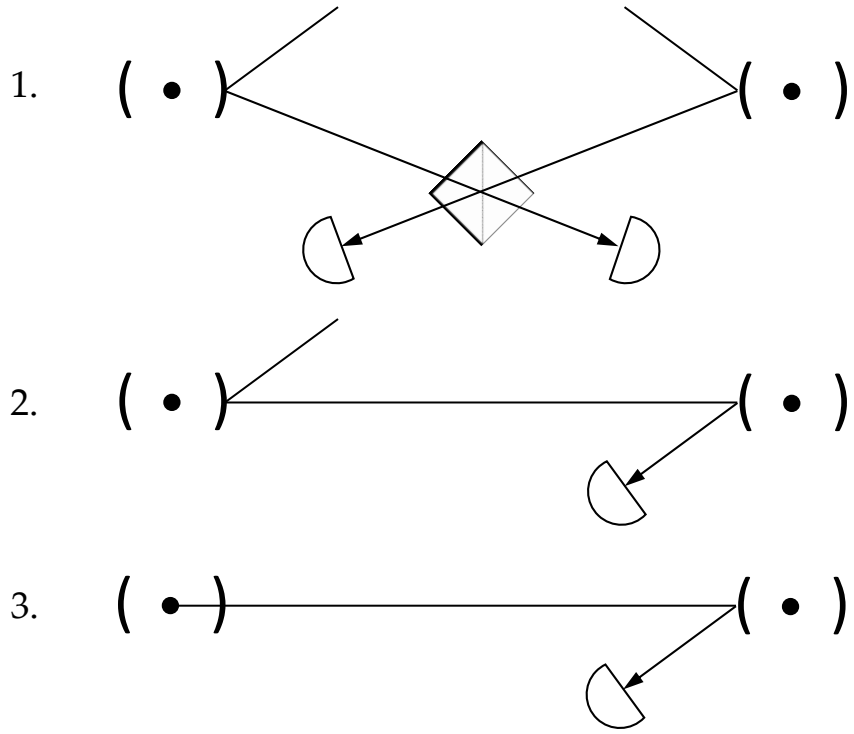

Figure 4.1: Three schemes for creating entanglement between two trapped atoms. Scheme 1: Reflect a coherent state off of each cavity, send them through a beamsplitter, then measure them. Scheme 2: Reflect a coherent state off of both cavities sequentially, then measure it. Scheme 3: Generate an atom-photon entangled state in one cavity, reflect the photon off of the other cavity, then measure the photon.

them into a 50/50 beamsplitter and making a measurement on the output. (Note that the two coherent states must have the same phase.) The atoms are then left in an entangled state which depends on the measurement outcome.

Scheme 2. Initialize each atom to the state $|+\rangle$. Interact one atom with the horizontally polarized coherent state $|\sqrt{2}\alpha\rangle$, then interact the resultant state with the other atom.[1] Finally, make a measurement to find whether the polarization of the coherent state was horizontal or vertical. This decouples the optical modes from the system and leaves behind an entangled state, conditioned on the measurement outcome.

Scheme 3. Stimulate one atom to emit a single photon whose state is entangled with the atomic qubit state. Interact the photon with the other atom, which is initialized in the state $|+\rangle$. Finally, measure the photon in the $\{|H\rangle, |V\rangle\}$ basis. Again, the entangled state depends on what outcome is measured.

Notice that while schemes 1 and 2 rely on coherent states, scheme 3 is fundamentally a single-photon scheme.

Before considering experimental imperfections, it is instructive to calculate the outcomes of the three schemes given above in the case where all processes are ideal.

4.2.1 Scheme 1

The joint state of the atoms and the coherent states just before the pseudo-BSM is

$$\frac{|00\rangle|\alpha\rangle|\alpha\rangle + |01\rangle|\alpha\rangle|-\alpha\rangle + |10\rangle|-\alpha\rangle|\alpha\rangle + |11\rangle|-\alpha\rangle|-\alpha\rangle}{2}. \tag{4.4}$$

Here, the first ket in each term refers to the two atoms, while the second and third refer to the two right circularly polarized coherent states. We may rewrite the state in the form

$$\frac{|\Phi^+\rangle|\widetilde{\Phi}^+_\alpha\rangle + |\Psi^+\rangle|\widetilde{\Psi}^+_\alpha\rangle}{\sqrt{8}N_+} + \frac{|\Phi^-\rangle|\widetilde{\Phi}^-_\alpha\rangle + |\Psi^-\rangle|\widetilde{\Psi}^-_\alpha\rangle}{\sqrt{8}N_-}, \tag{4.5}$$

[1] The factor of $\sqrt{2}$ is included so that the total number of photons used in this scheme and the previous one are the same. Note that when written in terms of left and right circularly polarized modes, the coherent state becomes $|\alpha, \alpha\rangle$.

where we have defined

$$N_\pm := (2 \pm 2e^{-4|\alpha|^2})^{-1/2} \tag{4.6}$$

$$|\widetilde{\Phi}_\alpha^\pm\rangle := N_\pm(|\alpha\rangle|\alpha\rangle \pm |-\alpha\rangle|-\alpha\rangle) \tag{4.7}$$

$$|\widetilde{\Psi}_\alpha^\pm\rangle := N_\pm(|\alpha\rangle|-\alpha\rangle \pm |-\alpha\rangle|\alpha\rangle) \tag{4.8}$$

In this form, we see that we can project the atoms into an entangled state if we had a measurement that could distinguish between the four states $\{|\widetilde{\Phi}_\alpha^\pm\rangle, |\widetilde{\Psi}_\alpha^\pm\rangle\}$. This cannot be done perfectly since this is not an orthonormal set: $\langle\widetilde{\Phi}_\alpha^+|\widetilde{\Psi}_\alpha^+\rangle = \mathrm{sech}(2|\alpha|^2)$ (though the set is otherwise pairwise orthogonal). There is, however, a simple way to distinguish them with some nonzero failure probability. If they were sent through the two input ports of a 50/50 beamsplitter, the states would be transformed as follows:

$$\begin{aligned} |\widetilde{\Phi}_\alpha^\pm\rangle &\to |\mathrm{cat}_\pm\rangle|0\rangle \\ |\widetilde{\Psi}_\alpha^\pm\rangle &\to |0\rangle|\mathrm{cat}_\pm\rangle \end{aligned} \tag{4.9}$$

where

$$\begin{aligned} |\mathrm{cat}_\pm\rangle &:= N_\pm\big(|\sqrt{2}\alpha\rangle \pm |-\sqrt{2}\alpha\rangle\big) \\ &= N_\pm e^{-|\alpha|^2} \sum_{n=0}^{\infty} \frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}[1 \pm (-1)^n]|n\rangle. \end{aligned} \tag{4.10}$$

The states $|\mathrm{cat}_\pm\rangle$ are commonly called *cat states* [37], a reference to Schrödinger's cat.

Note that in the Fock state expansion of $|\mathrm{cat}_+\rangle$, only even photon numbers appear; similarly, only odd photon numbers appear in $|\mathrm{cat}_-\rangle$. Therefore, by measuring the number of photons coming out of each beamsplitter output port (or, more precisely, the parity of the photon number), it is possible to distinguish the states $\{|\widetilde{\Phi}_\alpha^\pm\rangle, |\widetilde{\Psi}_\alpha^\pm\rangle\}$ and project the atoms into one of the Bell states. This is the "pseudo-BSM" alluded to above.

We emphasize that it is not possible to distinguish the original four states perfectly, even though the cat states are orthogonal. Note that $|\widetilde{\Phi}_\alpha^+\rangle$ and $|\widetilde{\Psi}_\alpha^+\rangle$, which we have shown to be non-orthogonal, both map to states containing a $|0\rangle|0\rangle$ component. This outcome, which corresponds to no photons being measured at all, means that the measurement failed. The success probability of the measurement is $p_{\mathrm{succ}} = 1 - e^{-2|\alpha|^2}$.

Although $|\mathrm{cat}_\pm\rangle$ could be distinguished if the photon number parity could be measured, it is difficult in practice to construct a photon number detector. Photon number *parity* detectors are no easier. Much more common are *threshold detectors*, which signal the presence or absence of a photon, but not how many photons there are. The POVM for such

a measurement is, in terms of Fock states,

$$\left\{ E_{\text{no click}} := |0\rangle\langle 0|, E_{\text{click}} := \sum_{n=1}^{\infty} |n\rangle\langle n| \right\}. \tag{4.11}$$

Threshold detectors appear at first sight to be useless for distinguishing between the states $\{|\widetilde{\Phi}_\alpha^\pm\rangle, |\widetilde{\Psi}_\alpha^\pm\rangle\}$, since each output port of the beamsplitter corresponds to two of the states. Suppose, however, that a photon comes out of the first output port. Even though this could have been triggered by either of the states $|\widetilde{\Phi}_\alpha^\pm\rangle$, the probability that the triggering state was $|\widetilde{\Phi}_\alpha^+\rangle$ is smaller than that of $|\widetilde{\Phi}_\alpha^-\rangle$ by a factor of approximately $|\alpha|^2$. This can be seen by an inspection of the leading terms of $E_{\text{click}}|\text{cat}_\pm\rangle$, which are

$$E_{\text{click}}|\text{cat}_+\rangle = \frac{2\alpha^2 e^{-|\alpha|^2}}{\sqrt{1+e^{-4|\alpha|^2}}}|2\rangle + \cdots \tag{4.12}$$

$$E_{\text{click}}|\text{cat}_-\rangle = \frac{2\alpha e^{-|\alpha|^2}}{\sqrt{1-e^{-4|\alpha|^2}}}|1\rangle + \cdots \tag{4.13}$$

The effect is that, if the photon number parity detectors were replaced with threshold detectors, the atoms would be left in a *mixed state* with a large contribution from $|\Phi^-\rangle\langle\Phi^-|$. A full calculation shows that, if the first detector clicked, the two atoms would be found in the state

$$(1-e_{\text{BSM}})|\Phi^-\rangle\langle\Phi^-| + e_{\text{BSM}}|\Phi^+\rangle\langle\Phi^+| \tag{4.14}$$

where

$$e_{\text{BSM}} := \frac{1-e^{-2|\alpha|^2}}{2}. \tag{4.15}$$

A similar result holds if the second detector clicked, but with $|\Psi^-\rangle$ and $|\Psi^+\rangle$.

Photon number detectors could be approximated using a large number of threshold detectors. The basic idea is to diffuse the incoming signal into multiple modes such that the probability of each mode containing more than one photon is small, then use threshold detectors to detect photons in each mode. This could be done using a series of beamsplitters [38], or by using beam-shaping optical components to spread out the incoming signal over an array of detectors (demonstrated in e.g. [39]). As for photon number parity detectors, one could in fact be constructed using the very cavity-atom system under consideration; see [33]. However, since threshold detectors are more practical than either photon number detectors or parity detectors (no matter how they are implemented), we will assume the use of threshold detectors throughout the remainder of this chapter. This allows for a possibly fairer comparison with schemes 2 and 3, too, since they require only threshold detectors.

Another fact that should be mentioned is that this scheme relies on the *phase* of the initial amplitude, $\arg(\alpha)$, being the same for the two coherent states. Experimentally, the mean photon number $|\alpha|^2$ is easy to control by changing the intensity of a laser, but coordinating the phases of two separate pulses is more difficult. Having noted this potential problem, however, we will not worry about it in the remainder of this chapter.

4.2.2 Scheme 2

Just before the polarization measurement, the system is in the state

$$\frac{|\Phi^+\rangle|\sqrt{2}\alpha, 0\rangle + |\Psi^+\rangle|0, \sqrt{2}\alpha\rangle}{\sqrt{2}} \tag{4.16}$$

where the first and second coherent state modes refer to horizontal and vertical polarization, respectively. It is clear that the polarization measurement is successful if at least one photon reaches the detector. Using (2.20), we find that the success probability is $p_{\text{succ}} = 1 - e^{-2|\alpha|^2}$. Given that the measurement is successful, the atoms are left in either $|\Phi^+\rangle$ or $|\Psi^+\rangle$, depending on the measurement outcome; both outcomes are equally likely.

4.2.3 Scheme 3

As described in [36], after an atom is stimulated to emit an entangled photon, the atom-photon state is

$$\frac{|0\rangle|L\rangle - |1\rangle|R\rangle}{\sqrt{2}}. \tag{4.17}$$

Note that this is essentially the same as $|\Psi^-\rangle$, but between the atom and the photon.

After the photon interacts with the second atom, the entire system is in the state

$$\frac{|0+\rangle|L\rangle - |1-\rangle|R\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left(\frac{|0+\rangle - |1-\rangle}{\sqrt{2}}|H\rangle + \frac{|0+\rangle + |1-\rangle}{\sqrt{2}}|V\rangle\right). \tag{4.18}$$

Upon measurement of the photon, the atoms are left in one of the states $(|0+\rangle \pm |1-\rangle)/\sqrt{2}$, depending on the measurement outcome; both states occur with equal probability. These entangled states are the same as $|\Phi^\pm\rangle$ except for a unitary on the second atom. Unlike the other schemes, this process is *deterministic*; it succeeds with probability 1.

4.3 Component modeling

In this chapter, we will not model the components of the setup as elaborately as was done in the previous chapter. In particular, we assume that our threshold detectors are perfect. Additionally, we assume that each cavity contains exactly one atom at all times. We will, however, take into account the following imperfections.

Note that, because of imperfections, there is a chance that both detectors click in scheme 1 and that photons of both polarizations are detected in scheme 2. These cases are treated as inconclusive, as if there had been no detection at all.

4.3.1 Loss

We assume that all losses can be modeled using beamsplitters, and that nonlinear optical effects can be neglected.

When photons interact with a cavity, they are lost with a probability that depends on the atom-photon state [31]. If the state was one of $|0\rangle|L\rangle$, $|0\rangle|R\rangle$, or $|1\rangle|L\rangle$, the photon is successfully reflected with probability η. If the state was $|1\rangle|R\rangle$, the photon is reflected with a different probability η'. Notice that this is the same state that picks up a negative sign in (4.1).

The effect is more striking when written in terms of right circularly polarized coherent states:

$$\begin{aligned} |0\rangle|\alpha\rangle|0\rangle_E &\to |0\rangle|\sqrt{\eta}\,\alpha\rangle|\sqrt{1-\eta}\,\alpha\rangle_E \\ |1\rangle|\alpha\rangle|0\rangle_E &\to |1\rangle|-\sqrt{\eta'}\,\alpha\rangle|-\sqrt{1-\eta'}\,\alpha\rangle_E. \end{aligned} \tag{4.19}$$

The subscript E refers to the environment into which photons get lost.

Apart from cavity losses, the optical channel between the cavities is also lossy, with transmittivity η_{ch}.

4.3.2 Mode mismatch

The optical mode functions within the cavities are not the same as for free space. This *mode mismatch* means that, with probability ξ, photons reflected off a cavity do not interact with it. If a coherent state $|\alpha\rangle$ were to impinge on a cavity, it could be rewritten in terms of a matched and a mismatched mode as

$$|\alpha\rangle = |\alpha'\rangle_{\text{matched}}|\alpha''\rangle_{\text{mismatched}}, \tag{4.20}$$

where α' and α'' are are such that the probability of measuring a photon in the mismatched mode is ξ. The conditional phase shift acts only on the matched mode. Because none of

the measurements involved in the three schemes distinguishes between the matched and mismatched modes, the resulting states are effectively the same as if the conditional phase shift were applied probabilistically. Specifically, if ρ is the photon-atom state before the interaction and CR_π is the controlled π phase gate, then spatial mismatch means that

$$\rho \to (1-\xi)\mathrm{CR}_\pi(\rho) + \xi\rho \tag{4.21}$$

after the interaction.

It may be of interest to note that, if the probability that a cavity did not contain an atom were nonzero, this case would be modeled using (4.21), as a probabilistic application of the conditional phase gate.

Note that if a photon reflects off a cavity without interacting, it does not suffer the cavity losses outlined in the previous subsection.

4.3.3 State preparation

All of the above schemes require at least one of the atoms to be initialized to the state $|+\rangle$. In practice, this initialization cannot be done perfectly; there is some probability of error. We will assume that the atoms are actually initialized to the state

$$(1-e_p)|+\rangle\langle+| + e_p|-\rangle\langle-| \tag{4.22}$$

where e_p is the error probability.

Additionally, scheme 3 requires that one of the atoms emit an entangled photon. This can be done with probability η_{ent}.

4.4 Results

Unlike last chapter, we are not interested in performing QR-assisted QKD using the trapped-atom system considered in this chapter—though this is a goal for future work. For this reason, we cannot use the secret key rate as a figure of merit. Because our task is to entangle two atoms, it makes sense to consider the probability that the entanglement can be established, as well as how strongly entangled the resulting state is (given that the operation was successful). The first of these two requires no further explanation. The second we will quantify using the logarithmic negativity function defined in (2.15): the higher this quantity, the better the entanglement. Note, however, that each of the schemes generate different entangled states depending on the measurement outcome. We will deal with this by averaging their logarithmic negativities, weighted by the probability of the

corresponding measurement outcomes. (These probabilities, of course, are conditioned on a successful measurement.) The two figures of merit that we will consider in this chapter, then, are the *success probability* and the *average logarithmic negativity*.

For all of the plots in this section, the following parameter values were used. They are taken from [31], except for η_{ent} which was taken from [36].

- η (cavity reflectivity) $= 0.7$
- η' (cavity reflectivity for $|1\rangle|R\rangle$) $= 0.66$
- ξ (mode mismatch) $= 0.08$
- e_p (state preparation error) $= 0.05$
- η_{ent} (entangled photon emission probability) $= 0.4$

4.4.1 Pseudo-BSM location (scheme 1)

In scheme 1, we have not specified the location at which the pseudo-BSM is to be performed. In the ideal case, the location does not matter. However, when channel loss is taken into account, the final atom-atom state does indeed change as a function of the pseudo-BSM location.

Because the amount of channel loss undergone by the two coherent states will differ if the pseudo-BSM is not performed at the midpoint between the atoms, it is necessary to make one point clear: we require the mean photon numbers of the coherent states to be the same *at the beamsplitter*. The success of the pseudo-BSM depends on this. The effect seen in (4.10), where the photons leave the beamsplitter through only one of the two output ports, could not occur if the mean photon numbers of the input pulses were not the same. Naturally, this requirement means that the mean photon numbers of the *initial* coherent states are not the same. They need to be changed to adapt to the loss, and are related by $\sqrt{\eta_{\text{ch},1}}\,\alpha_1 = \sqrt{\eta_{\text{ch},2}}\,\alpha_2$, where the subscripts 1 and 2 refer to the two coherent states and the segments of optical channel through which they travel.

Given that requirement, numerical evidence suggests that the midpoint between the two atoms is the optimum point in the following sense. If the probability p_{succ} that one of the detectors successfully detects a photon is held fixed (so the coherent state amplitudes vary with the pseudo-BSM location), then the average logarithmic negativity is maximized when the beamsplitter is placed midway between the atoms. An example of this can be seen in Fig. 4.2. Similar plots were made with varying parameter values, and all are optimized at the midpoint.

In what follows, we will assume that the pseudo-BSM is performed at the midpoint. Note that, in this case, the initial amplitudes of both coherent states are equal.

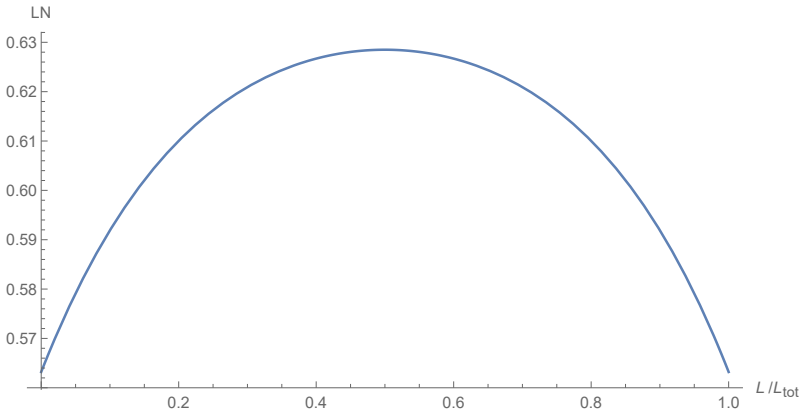

Figure 4.2: Average logarithmic negativity for scheme 1 as a function of the distance L of the pseudo-BSM from one atom (normalized to the total distance L_{tot} between the atoms). The success probability p_{succ} is fixed at 10^{-3}, and the coherent state amplitudes of the initial pulses are allowed to vary with L. We have used $\eta_{\text{ch}} = 0.01$.

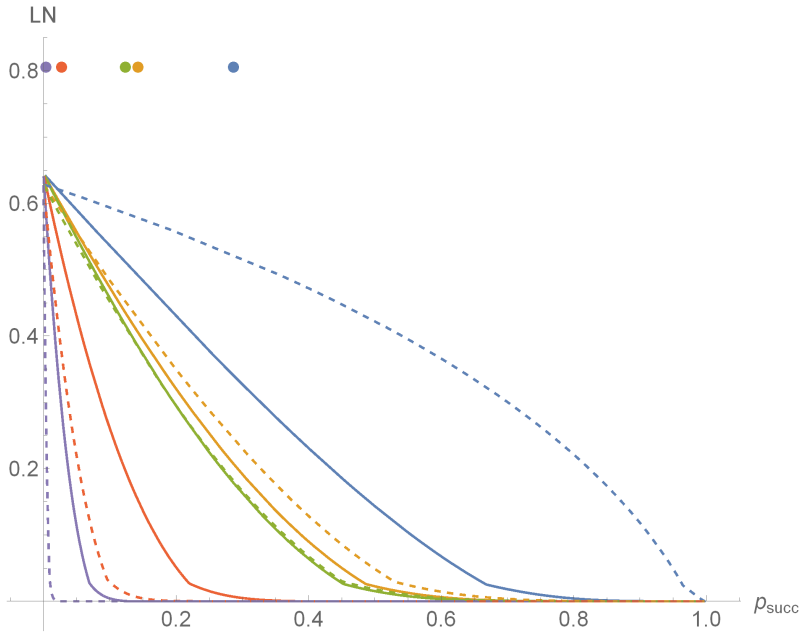

Figure 4.3: Average logarithmic negativity vs. success probability for schemes 1 (solid lines), 2 (dashed lines), and 3 (points). The lines for schemes 1 and 2 are parameterized by the coherent state parameter α; scheme 3 is only represented by points because it has no parameter to vary. Blue, orange, green, red, and purple correspond to $\eta_{\text{ch}} = 1$, 0.5, 0.43, 0.1, and 0.01 respectively.

4.4.2 Success probability and logarithmic negativity

When scheme 1 is implemented with threshold detectors, we see that, even in the ideal case, there is a tradeoff between the success probability and the amount of error in the resulting entangled state: as the success probability increases, so does the error. When imperfections are taken into account, it turns out that this type of tradeoff holds for scheme 2 as well. In both schemes, the success probability and the average logarithmic negativity depend on the coherent state amplitude α, so by tuning this parameter, it is possible to choose between a high success probability and a higher-quality entangled state. Fig. 4.3 shows what success probabilities and average logarithmic negativities can be achieved in these two schemes by tuning α. It is notable that, when the channel transmittivity is above 0.43, scheme 2 is superior to scheme 1 for almost all values of the success probability, but that this relationship is reversed when η_{ch} drops below 0.43. This value of 0.43 appears to depend on the cavity reflectivities η and η', but not on the other parameters.

Because scheme 3 is a single-photon scheme, the success probability and the quality of entanglement cannot be tuned; they depend entirely on the imperfections inherent in the components of the system. Fig. 4.3 shows the average logarithmic negativity vs. success probability for this scheme as discrete points on the plot. One can see that the average logarithmic negativity does not depend on channel loss, and that it is superior to the maximum value achievable with the other schemes. This can be attributed to the fact that channel loss does not degrade a single-photon signal in the same way it does a coherent state signal. Single photons are either lost or left unaffected by the optical channel; coherent states are attenuated rather than lost entirely. Moreover, in this scheme the signal is affected by imperfections in only one cavity, while in schemes 1 and 2 both cavities contribute errors.

4.5 Conclusion

Entangling two distant qubits is an essential step in many quantum repeater schemes, such as the one described in Sec. 2.3.2 of Ch. 2. In this chapter, we analyzed three possible schemes for entangling two trapped atoms of the type described in [31]. Taking into account a number of experimental imperfections, we compared the success probability of these schemes as well as the quality of the resulting entangled states. It is expected that analyses like the one presented in this chapter will lay the groundwork for the experimental implementation of a QR scheme which can, unlike the one in the previous chapter, be extended to arbitrary distances.

Chapter 5

Concluding remarks

The main theme of this thesis has been the exploration of quantum repeaters from an practical point of view. The emphasis, in all the research presented in this work, has been on mathematically modeling various imperfections and inefficiencies inherent in the components of a quantum repeater, and on assembling these models to obtain an idea of how well a given task can be done.

Chapter 3 describes an experiment that can be performed using currently available equipment. We analyzed in detail all the various components of a simple quantum repeater scheme and determined conditions under which it can beat the TGW bound. We have shown that high efficiencies and long memory dephasing times are required to do so. The parameter regions are not out of reach, though, and could likely be achieved with state-of-the-art trapped ion technology. It is hoped that the experiment will actually be performed in the near future. If the TGW bound is exceeded in such an experiment, it will be a notable achievement: the first implementation of a true quantum repeater.

Chapter 4 is a little more future-oriented. It is not concerned with a specific implementation of a quantum repeater, but grapples with one of the major building blocks of many quantum repeater schemes: the generation of entanglement between qubits. To that end, we compared three schemes for entangling two trapped-atom quantum memories, looking in particular at the success probability of each scheme and the logarithmic negativity of the generated entangled states. The analysis presented here is not entirely complete: imperfections in the detectors, for example, have yet to be considered. We have shown, however, that there is a clear tradeoff between success probability and logarithmic negativity when coherent states are used to establish the entanglement. We also found that, if we instead stimulate one atom to emit an entangled photon and use this photon to establish entanglement with the other atom, better entangled states are obtained. These conclusions are unlikely to change in a more detailed analysis.

One avenue for further work would be to analyze the behavior of a specific quantum repeater scheme that uses trapped atoms, in the style of the analysis in Chapter 3. The work in Chapter 4 could form the groundwork for such an analysis. This would be very helpful in determining whether a viable and fully scalable quantum repeater can be built using such atoms.

It is hoped that the results in this thesis will be helpful in understanding the behavior of quantum repeaters in the presence of experimental imperfections—an important endeavor, for theoretical perfection is somewhat difficult to come by in an imperfect universe. May this and similar work speed the day in which a quantum repeater is built in the laboratory.

APPENDICES

Appendix A

Benchmark key rates

In this appendix, we list the secret key rates per mode of benchmarks 2–5 in Sec. 3.3. We will do so by giving explicit expressions for the observables in (2.25) and (2.29) in terms of the experimental parameters in Sec. 3.4. We assume throughout that there is no eavesdropping activity.

For benchmarks 2, 3, and 5, Alice transmits single photons to Bob. In accordance with (2.25), the efficient BB84 key rate per mode is

$$R = \frac{Y_1}{2}[1 - h(e_1) - fh(e_1)]. \tag{A.1}$$

For benchmark 5, put

$$\begin{aligned} \eta &:= \eta_{\text{tot}} e^{-L/L_{\text{att}}} \\ Y_1 &:= 1 - (1-\eta)(1-p_d)^2 \\ e_1 Y_1 &:= Y_1/2 - (1/2 - e_m)\eta(1-p_d). \end{aligned} \tag{A.2}$$

Here Y_1 and e_1 are the yield and QBER for single photons, f is the error correction inefficiency, L is the length of the optical channel between Alice and Bob, and e_m is the setup misalignment error probability. The other variables are as defined in Sec. 3.4. The factor of $1/2$ comes from the fact that BB84 uses two optical modes.

For an ideal single photon source (benchmark 3), $\eta_p = \eta_c = 1$. For an ideal detector setup (benchmark 2), $\eta_d = 1$ and $p_d = e_m = 0$. This amounts to setting $e_1 = 0$ and $\eta_{\text{tot}} = 1$, and results in $R = e^{-L/L_{\text{att}}}/2 = \eta_{\text{ch}}/2$.

Based on (2.29), the key rate per mode for decoy-state BB84 with a laser (benchmark 4) is

$$R_{\text{decoy}} = \frac{1}{2}\big(Y_1 \mu e^{-\mu}[1 - h(e_1)] - fQ_\mu h(E_\mu)\big). \tag{A.3}$$

In terms of the experimental parameters in Sec. 3.4, we have

$$\begin{aligned} Q_\mu &:= 1 - e^{-\eta\mu}(1-p_d)^2 \\ E_\mu Q_\mu &:= Q_\mu/2 - (1/2 - e_m)(1 - e^{-\eta\mu})(1-p_d). \end{aligned} \tag{A.4}$$

Here μ is the average photon number for signal states; Y_1, e_1, f, and e_m are as defined above.

Appendix B

Approximation of crossover regions

In this appendix, we derive (3.24) and (3.26). We will assume that the QMs are loaded sequentially and that the central station is at $L/2$. Let R_b be the key rate for the benchmark whose crossover region we wish to approximate.

We will first derive (3.24). As outlined in the discussion leading up to that equation, our approach is to equate the intersection of the curves $R_0 e^{-L/(2L_{\text{att}})}$ and $R_{b,0} e^{-L/L_{\text{att}}}$ with some characteristic dephasing length L_{dp} in order to find the boundary of the crossover region. (R_0 and $R_{b,0}$ are the key rates at $L = 0$ of our protocol and of the benchmark, respectively.)

The first step is to find conditions under which

$$R_0 \propto \eta_{\text{tot}} R_0^{\eta_{\text{tot}}=1}. \tag{B.1}$$

If p_d is small and $T_p \ll T_2$, then e_X and e_Z are approximately independent of η_{tot}—see (3.7) and (3.22)—and R_0 only depends on η_{tot} through Y. If we further assume that $\eta'_A \approx \eta_A$, then

$$Y = p_{\text{BSM}} \frac{\eta_{\text{tot}}(2 - \eta_{\text{tot}})}{3 - 2\eta_{\text{tot}}} \approx \frac{2}{3} p_{\text{BSM}} \eta_{\text{tot}}. \tag{B.2}$$

to first order in η_{tot}. These conditions are therefore sufficient for the approximation in (B.1) to hold, with proportionality constant $2/3$.

Given this fact, the intersection of the two curves is at

$$L_{\text{int}} = 2L_{\text{att}} \ln\left(\frac{Q}{\eta_{\text{tot}}}\right) \tag{B.3}$$

where Q is defined in (3.25). Note that $T_p \ll T_2$ implies that Q is independent of T_2.

We now derive a characteristic dephasing length by determining the distance at which Alice's QM dephases for a significant fraction of T_2. (Recall that Alice's QM always dephases longer than Bob's.) That is, we put

$$\frac{T_2}{K} = \mathbb{E}(t_A^{\text{seq}}) = \frac{L_{\text{dp}}}{c} + \frac{T_p + L_{\text{dp}}/c}{\eta_{\text{tot}} e^{-L_{\text{dp}}/(2L_{\text{att}})}} \tag{B.4}$$

where we have again used $\eta_A' \approx \eta_A$. The fitting parameter K defines the fraction of T_2 at which dephasing becomes significant.

Equation (B.4) cannot be solved for the dephasing length L_{dp} using elementary functions, but this is unnecessary: to find the crossover boundary, we need only substitute L_{int} for L_{dp}. After a minor rearrangement of terms, this yields (3.24).

It may appear that a small p_d implies that $\eta_A' \approx \eta_A$. It is true that $p_d \ll 1$ implies $|\eta_A' - \eta_A| \ll 1$, but since $\eta_A \ll 1$ and $\eta_A' \ll 1$ in general, this is not strong enough to meaningfully say that $\eta_A' \approx \eta_A$. We require instead that $|\eta_A' - \eta_A|/\eta_A \ll 1$. Moreover, because we have used $\eta_A' \approx \eta_A$ in deriving (B.4), we require this to hold for all L up to L_{dp}—or, equivalently, up to L_{int}. By manipulating (3.12), we can write

$$\frac{|\eta_A' - \eta_A|}{\eta_A} = \left(\frac{1}{\eta_A} - 1\right)(2p_d - p_d^2) \approx \left(\frac{1}{\eta_A} - 1\right) p_d. \tag{B.5}$$

If η_A is close to 1, then $(1/\eta_A - 1)p_d$ is already small and the approximation holds. If $\eta_A \ll 1$, then $(1/\eta_A - 1)p_d \approx p_d/\eta_A$, which is small for all L up to L_{int} when $p_d \ll \eta_{\text{tot}}^2/Q$. This condition, then, together with $T_p \ll T_2$, guarantees the validity of (3.24).

Let us now derive (3.26). This time, we will compare L_{int} with a length L_d at which errors due to dark counts become significant.

The error due to dark counts is related to $\alpha(\eta_A)$, defined in (3.12). We will put $1 - \xi = \alpha(\eta_A)$ where ξ is a parameter indicating the amount of error the system can tolerate due to dark counts. Rearranging this equation, we obtain

$$L_d = 2L_{\text{att}} \ln\left(\frac{\eta_{\text{tot}}(1 - p_d)(p_d + \xi - p_d\xi)}{p_d(2 - p_d)(1 - \xi)}\right). \tag{B.6}$$

By equating L_d and L_{int}, we obtain (3.26).

In deriving this equation, we have made no assumptions beyond those required for (B.1). In particular, we do not require $\eta_A' \approx \eta_A$ for all L up to L_{int}, but only at $L = 0$. This means that the condition on p_d is less strict: $p_d \ll \eta_{\text{tot}}$.

Finally, we note that the condition $p_d \ll \eta_{\text{tot}}^2/Q$, required for (3.24), can be obtained from a linearization of the square of (3.26).

References

[1] 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, Bangalore, India*, pp. 175–179, New York, 1984, IEEE.

[2] M. Takeoka, S. Guha, and M. M. Wilde, IEEE Transactions on Information Theory **60**, 4987 (2014).

[3] C. Elliott, New Journal of Physics **4**, 46 (2002).

[4] S. Guha *et al.*, Rate-loss analysis of an efficient quantum repeater architecture, 2014, arXiv:1404.7183.

[5] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[7] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[8] L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009).

[9] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, Nature Photonics **6**, 777 (2012).

[10] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).

[11] A. G. Fowler *et al.*, Phys. Rev. Lett. **104**, 180503 (2010).

[12] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[14] M. B. Plenio and S. Virmani, Quant. Inf. Comput. **7**, 1 (2007).

[15] *Announcing the Advanced Encryption Standard (AES)* (United States National Institute of Standards and Technology, 2001).

[16] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[17] H. K. Lo, F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

[18] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[19] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[20] B. Ma, X.and Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[21] S. Olmschenk *et al.*, Phys. Rev. A **76**, 052314 (2007).

[22] J. Benhelm, G. Kirchmair, C. F. Roos, and R. Blatt, Nature Physics **4**, 463 (2008).

[23] T. P. Harty *et al.*, Phys. Rev. Lett. **113**, 220501 (2014).

[24] A. Reiserer and G. Rempe, arXiv:1412.2889 (2014).

[25] B. Blinov, D. Moehring, L.-M. Duan, and C. Monroe, Nature **428**, 153 (2004).

[26] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[27] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New Journal of Physics **16**, 043005 (2014).

[28] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[29] E. W. Streed, B. G. Norton, A. Jechow, T. J. Weinhold, and D. Kielpinski, Phys. Rev. Lett. **106**, 010502 (2011).

[30] T. Kim, P. Maunz, and J. Kim, Phys. Rev. A **84**, 063423 (2011).

[31] A. Reiserer, N. Kalb, G. Rempe, and S. Ritter, Nature **508**, 237 (2014).

[32] N. Kalb, A. Reiserer, S. Ritter, and G. Rempe, Phys. Rev. Lett. **114**, 220501 (2015).

[33] A. Reiserer, S. Ritter, and G. Rempe, Science **342**, 1349 (2013).

[34] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).

[35] K. Azuma *et al.*, Phys. Rev. A **80**, 060303 (2009).

[36] S. Ritter *et al.*, Nature **484**, 195 (2012).

[37] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, Phys. Rev. A **68**, 042319 (2003).

[38] P. Kok and B. W. Lovett, *Introduction to optical quantum information processing* (Cambridge University Press, 2010).

[39] L. A. Jiang, E. A. Dauler, and J. T. Chang, Phys. Rev. A **75**, 062325 (2007).