Design of Quantum Repeaters

by

Yi Li

A thesis submitted for the degree of

Doctor of Philosophy

of

The Australian National University
July 2017

THE
AUSTRALIAN
NATIONAL
UNIVERSITY

Statement of Originality

This work contains no material that has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of the thesis, when deposited in the University Library, being available for loan, photocopying and dissemination through the library digital thesis collection.

The author of this thesis acknowledges that copyright of published work contained within this thesis (as listed in the publications page) resides with the copyright holder(s) of that work.

Signed

Date

Publications

Paper published

[1] Y. Li, A. R. R. Carvalho, and M. R. James, "Continuous-mode operation of a noiseless linear amplifier," *Phys. Rev. A*, vol. 93, p. 052312, May 2016. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.93.052312

[2] Y. Li, "Generation of distributed w-states over long distances," *Optics Communications*, vol. 396, pp. 19 – 22, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0030401817301979

[3] Y. Li, "Single photon modulation," in *2016 35th Chinese Control Conference (CCC)*, July 2016, pp. 9124–9127.

[4] Y. Li and M. R. James, "Equalization for linear quantum channels," in *the 56th IEEE Conference on Decision and Control*, 2017.

Acknowledgments

First and foremost, I must recognize my principal supervisor Prof. Matthew James for his constant and patient guidance during the period of my PhD study. His meticulous approach to learning and tolerance towards others will influence me for the rest of my life. Talking with him not only in professional areas but also on other topics such as culture has always been enjoyable and beneficial.

I would also like to wholeheartedly thank my co-supervisors Dr. Andre Carvalho and my adviser Prof. Ping Koy Lam for providing valuable suggestions to my research.

Sincere thanks also to my classmates and colleagues in the Research School of Engineering for their unselfish help in extending my knowledge. They are Thien Nguyen, Oliver Thearle, James Dannatt, Shuangshuang Fu, Syed Assad, Jiayin Chen and Yu Pan.

I am indebted for the work done by the staff in the Research School of Engineering and the College of Engineering and Computer Science.

A very special gratitude goes out to my neighbours in Graduate House for their constant support and encouragement during my PhD studies.

Finally, my deepest thanks to my mother and brother, who always encourage and support me in my life.

Thanks for all your encouragement!

Yi Li (July 2017)

Abstract

Quantum communication holds the promise of achieving long-distance secure message transmission by exploiting quantum entanglement between remote locations. Quantum repeaters are indispensable to the realization of quantum networks for long-distance quantum communication. Similar to its classical analogue, a good quantum repeater should be able to compensate channel attenuation with a quantum amplifier, and to combat channel distortion through a quantum equaliser. This quantum repeater should also operate by an efficient and robust protocol.

The first part of this project researches the continuous mode operation of a noiseless linear amplifier (NLA). We develop a dynamical model to describe the operation of the nondeterministic NLA in the regime of continuous-mode inputs. Both the quantum scissor based NLA and the photon addition-subtraction based NLA are analysed. Simulation results are also presented to confirm theoretical analysis.

The second part proposes two quantum protocols. An atomic ensemble based quantum protocol is developed to generate distributed W-states. These generated distributed W-states could be considered as an entanglement resource between more than two distant nodes and would be useful in quantum communication and distributed quantum computation in the future. We also propose a protocol by which quantum key distribution can be achieved deterministically between multiple nodes. This deterministic quantum key distribution scheme may be used to guarantee secure communication for wireless sensor networks and Internet of Things.

The last project analyses distortion of quantum channels and develops physically realisable modules to combat it. The minimum phase channel and non-minimum phase all pass channel are discussed separately.

Contents

Conventions

Typesetting

This thesis is typeset using the LaTeX2e software.

The fonts used in this thesis are Times New Roman and Sans Serif.

Referencing

Referencing and citation style in this thesis are based on the Institute of Electrical and Electronics Engineers (IEEE) Transaction style [1].

For electronic references, the last accessed date is shown at the end of a reference.

Units

The units used in this thesis are based on the International System of Units (SI units) [2].

Spelling

The Australian English spelling is adopted in this thesis.

Abbreviations

BB84	Bennett Brassard 1984
BS	Beam Splitter
DFE	Decision Feedback Equalisation
DLA	Deterministic Linear Amplification
DLCZ	Duan–Lukin–Cirac–Zoller
FIR	Finite Impulse Response
GHZ	Greenberger–Horne–Zeilinger
IOT	Internet of Things
ISI	Intersymbol Interference
MMSE	Minimum Mean Square Error
MSZ	Mu-Seberry-Zheng
NLA	Noiseless Linear Amplification
PNS	Photon Number Splitting
QND	Quantum Nondemolition
QKD	Quantum Key Distribution
Qutip	Quantum Toolbox in Python
RF	Radio Frequency
SARG	Scarani-Acín-Ribordy-Gisin

SME Stochastic Master Equation

UAV Unmanned Aircraft Vehicle

WSN Wireless Sensor Network

List of Figures

Chapter 1

Introduction and Motivation

THIS chapter gives a brief introduction to three aspects of quantum communication systems. The original research contributions of this thesis are presented. Finally, the thesis structure is discussed and the contents of each chapter are summarized.

1.1 Research area

Ever since the development of quantum mechanics theory, scientists have been trying to harness the power of quantum mechanics to benefit mankind. Several approaches to applying quantum mechanics application have been proposed, of which the most promising and intensively researched are quantum computing and quantum communication.

With quantum computing, people may make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Unlike the binary digits based classical computing, quantum computing deals with quantum bits (qubits), which can be in superpositions of orthogonal states. With large-scale quantum computers, people may theoretically be able to solve certain problems much quicker than any classical computers [3–7].

Through optical fibres or free space [8,9], quantum communication benefits mankind by transmission of secret classical messages and faithful transfer of unknown quantum states. With quantum key distribution (QKD), cryptography could be implemented with unconditional security for classical messages transmission [10–19]. With the help of classical communication and previously shared quantum entanglement, quantum information can be transmitted over long distances through a process called quantum teleportation [20–22]. For example, people can teleport one or more qubits between two distant entangled atoms [23–25] without sending any particles.

For both quantum cryptography and quantum teleportation, the distribution of quantum states over long distances is essential. Almost all the QKD protocols [26–28] require reliable transmission of quantum states over long distances. In order to perform quantum teleportation, quantum entanglement pairs between two distant nodes need to be prepared. The transmission of quantum states is also needed during the process of entanglement distribution.

Quantum channels such as optical fibers and free space transmission are affected by loss and distortion. Therefore the direct distribution distance for quantum states is less than $200km$ [29]. In order to extend the distance of quantum communication, quantum repeaters are indispensable. Like its classical counterpart, a good quantum repeater should be able to compensate channel attenuation with a quantum amplifier, and to combat channel distortion through a quantum equaliser. This quantum repeater should also operate by an efficient and robust protocol.

As shown in Figure 1.1, this PhD thesis includes three projects, contributing to the three aspects of quantum repeaters design-quantum amplification, quantum communication protocol and quantum channel distortion.

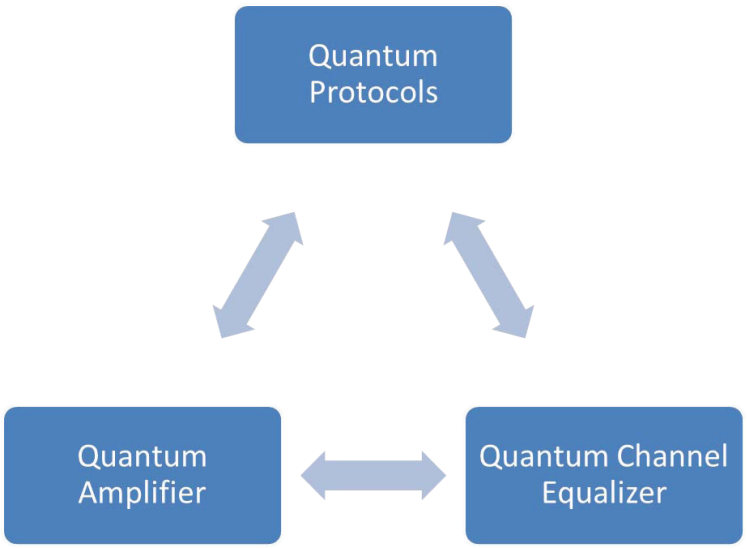


Figure 1.1. Like its classical counterpart, a good quantum repeater should be able to compensate channel attenuation with a quantum amplifier, and to combat channel distortion through a quantum equaliser. This quantum repeater should also operate by an efficient and robust protocol.

1.1.1 Introduction to quantum amplification

Signal amplification is a well researched topic in classical communication. Different equipment are designed to increase the amplitudes of optical signals [30–37], audio signals [38–41] and Radio Frequency (RF) signals [42–45]. Due to the no-cloning

theorem [46, 47], quantum states can not be amplified deterministically without adding noise [48–52]. The classical amplification methodologies therefore cannot be adopted in quantum regime directly. We can classify the proposed quantum amplification methodologies into deterministic linear amplification (DLA) [53–60] and probabilistic noiseless linear amplification (NLA) [29, 61–75]. Hybrid amplification combining DLA and NLA was also proposed and demonstrated [76].

With DLA, phase-insensitive amplification can be achieved deterministically for quantum states at the price of additional noise. Different DLA schemes are proposed based on solid state laser [56], parametric down-converters [57], and four wave mixing processes [58]. Amplification could also be controlled with a feedback loop to reduce the distortion and instabilities [77].

The NLA, on the other hand, is probabilistic and introduces no additional noise. It was firstly proposed by Ralph and Lund in the paper [61] and has been considered in a variety of contexts both theoretically [29] and experimentally [64–66]. There are also other NLA proposals based on conditional photon subtraction and addition [68, 69, 73, 74].

The first project of this PhD program focuses on the NLA schemes. Different NLA methodologies are reviewed in Section 2.2. Since the implementation of the amplification operation relies on the interference of the ancilla single photon with the input field at beam splitters, then the question of mode matching and pulse shapes is an important one that is not encompassed by the single mode treatment described above. This is also relevant if one considers the situation where information is encoded into multiple frequencies or, equivalently, into the temporal profile of the incoming field. In Chapter 3, we extend the analysis of the NLA to the continuous mode regime to explicitly take into account arbitrary pulse shapes for the input field and the ancilla photon and their effects on the amplification process. In particular we show that the amplification gain will be determined by the detection time, and that the shape of the ancilla photon is transferred to the amplified state.

1.1.2 Introduction to quantum communication protocols

Like all other kinds of communication, effective and robust communication protocols should be established before implementation of quantum communication. We can classify the quantum communication protocols into two fields: quantum networking protocols and QKD protocols.

1.1.2.1 Introduction to quantum networking protocols

Due to the attenuation and distortion of transmission channel, it is difficult to directly transmit a quantum state over long distances. An effective way to transmit a quantum state is by firstly generating entanglement between two remote nodes and then performing quantum teleportation with this entanglement pair [20–22].

Quantum networking protocols are proposed to realize entanglement between two or more distant nodes. Duan *et al.* designed a quantum repeater structure in the year 2001 [78]. With this kind of quantum repeater, entanglement can be achieved between two distant nodes. Several approaches have been proposed to improve the effectiveness and efficiency of the Duan–Lukin–Cirac–Zoller (DLCZ) protocol [79–85]. Some methodologies are also proposed to distribute entanglement between more than two distant nodes [86, 87]. These protocols are introduced and compared in this project. We extend this well-known protocol to a multi-node setting where W-states are generated between multiple nodes over long distances. The generation of multipartite W-states is the foundation of quantum networks, paving the way for quantum communication and distributed quantum computation.

1.1.2.2 Introduction to QKD protocols

In order to guarantee secure communication, the two communicating parties should produce a random shared key. This shared key is used to encrypt and decrypt messages and should be known to the two parties only. Because of the progress in quantum physics, distribution of cryptography keys with quantum states becomes possible.

In contrast to classical public key cryptography, which relies on the computational difficulty of certain mathematical functions and cannot provide any indication of eavesdropping at any point in the communication process, the security of QKD relies on the foundations of quantum mechanics. The advantage of QKD is the capability of the two communicating parties to detect the presence of any third party who also intends to gain knowledge of the key. This advantage comes from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general inevitably disturbs the system. The cryptography key is carried and produced by quantum states in QKD. A third party eavesdropper must in some way measure the quantum states and thus introduce detectable anomalies.

QKD is the most mature application field in quantum information. The Bennett–Brassard 1984 (BB84) scheme is proposed to distribute cryptography key between two distant nodes with the transmission of a quantum state sequence [26]. This BB84 scheme is theoretically proved to be absolutely reliable and experimentally demonstrated [27]. Other protocols, such as Decoy state QKD [88,89], Mu–Seberry–Zheng (MSZ) protocol [90] and Scarani–Acín–Ribordy–Gisin (SARG) 04 protocol [28] are also proposed and discussed. With optical fiber, experimentalists have achieved QKD beyond $150km$ [91]. QKD is also implemented over a distance of $1km$ with free space channel [92]. In June 2017, Chinese physicists led by Pan Jianwei measured entangled photons over a distance of 1203km between two ground stations, laying the groundwork for future intercontinental quantum key distribution experiments [93].

In order to secure classical communication in wireless sensor networks (WSN), protocols are needed to distribute cryptographic keys between more than two nodes. This project investigates and compares current QKD protocols and develops a multiparty quantum key distribution scheme. This multiparty QKD scheme can be used to guarantee absolute secure classical communication between multiple nodes in WSNs and Internet of Things (IOT).

1.1.3 Introduction of quantum channel equalisation

For many physical channels, such as telephone lines and optical fibers, not only are they bandlimited, but they also introduce distortions in their passbands. For example, if the transmission channel is frequency-selective, different frequency components of the transmitted signal would arrive at the receive end at different time. This causes the spreading of signal in time domain. If the pulse spreads beyond its allotted time interval, it would interfere with neighboring pulses and result in a kind of distortion called intersymbol interference (ISI).

One method to solve the ISI distortion is simply allocating a longer time frame to each symbol. However, these longer time frames would decrease the symbol rate and finally handicap the data rate. In order to tackle the ISI distortion while keeping high data rate, a module will be needed in the receiver end to recover signal from ISI distortion. This process is called equalisation and has been intensively researched in classical communication.

In quantum communication, quantum states are employed to carry information. Although scientists are still struggling to transmit a small number of quantum states once to distant destinations, equalisation of quantum channel would be indispensable to achieve a high quantum data rate once it comes to the time of distributed quantum computing and practical quantum communication. In addition, as the pulse shapes themselves of quantum states might be used for quantum information modulation, quantum channel equalization would be needed to recover the pulse shapes of transmitted quantum states.

During this PhD candidature, an equalisation methodology is developed to compensate the distortion from minimum phase quantum channel and non-minimum phase quantum channels. The proposed equalization structure is composed of simple optical components and therefore it is physically realisable and can be easily implemented.

1.2 Original Contributions

In order to solve the research problems mentioned in the Section 1.1, four separate research projects for quantum amplification, quantum networking protocols, QKD protocols and quantum channel equalisation are completed. Our research contributions in this thesis are summarized as follows:

- A dynamical model is developed to describe the operation of NLA in the regime of continuous modes. The dynamics conditioned on the detection of photons are analysed here, showing that the amplification gain depends on detection times and on the temporal profile of the input state and the auxiliary single photon state required by the NLA. It is also proved that the output amplified state inherits the pulse shape of the ancilla photon.

- By extending the well-known DLCZ protocol, a new scheme is introduced to generate distributed W-states over long distances based on atomic ensembles. The generation of multipartite W-states is the foundation of quantum networks, paving the way for quantum communication and distributed quantum computation.

- A methodology is developed to distribute cryptography keys between multiple nodes. This multiparty QKD scheme can be used to guarantee secure communication for wireless sensor networks and Internet of Things.

- A novel methodology is proposed to combat quantum channel distortion. This structure could be easily implemented with simple quantum components and may be applied with the newly developed waveguide chips.

1.3 Thesis Structure

The thesis is presented in seven chapters:

Chapter 1 provides a brief introduction to quantum communication. In this chapter, quantum amplification, quantum communication protocols and quantum channel equalisation are introduced separately. In addition, the original academic contributions are also defined.

Relevant literature is reviewed in Chapter 2. Section 2.2 introduces various NLA techniques. Comparison among different quantum networking protocols are presented in Section 2.3. Popular QKD protocols are then analysed and discussed in Section 2.4. Some popular channel equalisation techniques in classical communication are discussed in Section 2.5.

Chapter 3 introduces a dynamical model to describe the operation of the NLA in the regime of continuous modes inputs. Both the quantum scissor based NLA and the photon addition-subtraction based NLA are analysed. Simulation results are also presented to confirm theoretical analysis.

Chapter 4 describes the structure of distributed W-states generation over long distances. The implementation setup is introduced and success probability is analysed. It is also shown in this chapter that a small scale W-state could be used to generate a larger scale W-state through the process of entanglement swapping. In this chapter, it is proved that W-states could be used to implement quantum teleportation.

In Chapter 5, we firstly explain the importance and significance of multiparty QKD. Some scenarios requiring multiparty QKD are described for this explanation. A multiparty QKD scheme is presented in this chapter. Some technical challenges to practically implement this multiparty QKD scheme are mentioned in the end of this chapter.

Chapter 6 presents a physically realisable methodology to recover transmitted quantum states from quantum channel distortion. The minimum phase channel and non-minimum phase are discussed separately.

Chapter 7 reviews and concludes the thesis. In addition, some recommendations for future work are given. Finally, the original contributions to knowledge are re-summarized.

Chapter 2

Background

THIS chapter contains details of quantum communication techniques. Firstly, we introduce some preliminary knowledge about quantum mechanics and quantum information. After that, a number of quantum amplification methodologies are reviewed. Then the famous DLCZ protocol for quantum communication is discussed, followed by its extensions from different perspectives. Popular QKD protocols are then analysed and discussed. Some popular channel equalization techniques are finally presented.

2.1 Quantum mechanics and quantum information

In contrast to classical physics that explains matter and energy on a scale familiar to human experience, quantum mechanics explains the behaviour of matter and its interactions with energy on the scale of atoms and subatomic particles. Because quantum mechanics is usually used to describe behaviour quite different from that seen at larger length scales, many aspects of quantum mechanics are counterintuitive and can seem paradoxical. For example, the uncertainty principle of quantum mechanics means that the more closely one pins down one measurement (such as the position of a particle), the less accurate another measurement pertaining to the same particle (such as its momentum) must become.

Quantum mechanics benefits mankind in various ways. It has enormous success in the development of the laser, the transistor, the electron microscope, and magnetic resonance imaging. With its unique characteristics, it is realized that quantum mechanics can also be used to promote our information techniques in two aspects: quantum computing and quantum communication. Quantum computers are expected to be able to solve certain problems much faster than any classical computers [3–7] while quantum communication would provide more efficient and more reliable solutions for people to communicate.

A qubit is a unit of quantum informationthe quantum analogue of the classical binary bit. A qubit is a two-state quantum-mechanical system, such as the existence of a particle: here the two states are existence and nonexistence. In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a superposition of both states at the same time, a property that is fundamental to quantum computing.

The two states in which a qubit may be measured are known as basis states (or basis vectors) and are conventionally written as $|0\rangle$ and $|1\rangle$. A pure qubit state is a linear superposition of the basis states and can be represented as:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

where the complex numbers α and β are probability amplitudes and therefore they must be constrained by the equation:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.2}$$

An important distinguishing feature between a qubit and a classical bit is that multiple qubits can exhibit quantum entanglement. Entanglement is a nonlocal property that allows a set of qubits to express higher correlation than is possible in classical systems. Take, for example, two entangled qubits in the Bell state:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \tag{2.3}$$

Imagine that the two particles of $|\Psi_{00}\rangle$ are located far way from each other. When one qubit is measured, the measurement results would be either $|0\rangle$ or $|1\rangle$, each with a probability of $1/2$. The other qubit would collapse to the measured result at the same time.

2.2 Quantum amplification methodologies

This section begins with explaining that NLA can only be achieved non-deterministically. After that, two main NLA schemes based on quantum scissor and photon addition-subtraction are introduced separately.

2.2.1 Non-deterministic NLA

As discussed in Chapter 1, it was proved that a quantum state cannot be amplified deterministically without introducing additional noise [48–52]. Let us take coherent states for instance. Suppose we have a coherent state $|\alpha\rangle$. Assume this coherent

state can be amplified deterministically and without adding noise, then there is an unitary operator $\hat{T}$ that could produce the transformation:

$$\hat{T}|\alpha\rangle = |g\alpha\rangle \tag{2.4}$$

where g is a real number obeying $|g| > 1$. Now we can have:

$$\begin{aligned} \hat{T}\hat{a}\hat{T}^{\dagger}|g\alpha\rangle &= \hat{T}\hat{a}\hat{T}^{\dagger}\hat{T}|\alpha\rangle \\ &= \hat{T}\hat{a}|\alpha\rangle \\ &= \alpha\hat{T}|\alpha\rangle \\ &= \alpha|g\alpha\rangle \end{aligned} \tag{2.5}$$

Since $|g\alpha\rangle$ is a coherent state obeying $\hat{a}|g\alpha\rangle = g\alpha|g\alpha\rangle$, we can obtain $\hat{T}\hat{a}\hat{T}^{\dagger} = (1/g)\hat{a}$. Then the commutator of $\hat{T}\hat{a}\hat{T}^{\dagger}$ can be calculated as:

$$\begin{aligned} [\hat{T}\hat{a}\hat{T}^{\dagger}, \hat{T}\hat{a}^{\dagger}\hat{T}^{\dagger}] &= \frac{1}{g^2}[\hat{a}, \hat{a}^{\dagger}] \\ &= \frac{1}{g^2} \end{aligned} \tag{2.6}$$

which contradicts the following equation:

$$\begin{aligned} [\hat{T}\hat{a}\hat{T}^{\dagger}, \hat{T}\hat{a}^{\dagger}\hat{T}^{\dagger}] &= \hat{T}[\hat{a}, \hat{a}^{\dagger}]\hat{T}^{\dagger} \\ &= 1 \end{aligned} \tag{2.7}$$

Consequently, the assumption does not hold and the coherent state cannot be amplified deterministically without adding noise. In order to perform the amplification, one option is adding a noise operator to sustain the correct commutator described in the Equation 2.7. The other option is sacrificing the unitary characteristic of transformation and performing the amplification non-deterministically. There are two schemes proposed to amplify coherent states noiselessly. One is based on "quantum scissors" and the other is based on photon addition-subtraction.

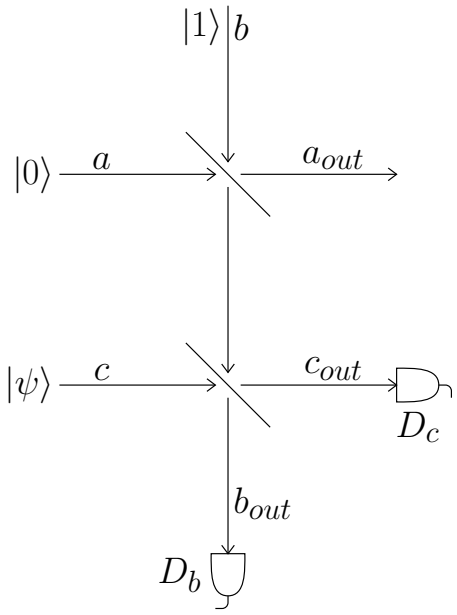


Figure 2.1. Quantum scissor: this module truncates a general state $|\psi\rangle = \sum_k^\infty c_k|k\rangle$ into $|\psi_{\text{trunc}}\rangle = \mathcal{N}(c_0|0\rangle + c_1|1\rangle)$, whenever a photon is detected in either one of the detectors D_b or D_c. Here $\mathcal{N}(\quad)$ denotes the normalization of the state.

2.2.2 Quantum scissor based NLA

The quantum scissor based NLA scheme works using the "quantum scissor" proposed by Pegg *et al* [94]. This "quantum scissor" is composed with two balanced beam splitters as shown in Figure 2.1. Using an auxiliary single photon $|1\rangle$ in one of the input ports, this module truncates a general state $|\psi\rangle = \sum_k^\infty c_k|k\rangle$ into $|\psi_{\text{trunc}}\rangle = \mathcal{N}(c_0|0\rangle + c_1|1\rangle)$, whenever a photon is detected in either one of the detectors D_b or D_c. Here $\mathcal{N}()$ denotes the normalization of the state.

As introduced in the paper [61], we have a coherent state $|\psi\rangle = |\alpha\rangle$ in the input channel c and an auxiliary single photon $|1\rangle$ in the input channel b. The input state then can be written as $|\Psi\rangle_{in} = |0\rangle_a|1\rangle_b|\alpha\rangle_c$. The second beam splitter of "quantum scissor" is replaced by a beam splitter with transmission rate η. Then we can obtain the transformation matrix S_{BS} from the input channels to output channels:

$$S_{\mathrm{BS}} = \begin{pmatrix} \sqrt{\eta} & i\sqrt{1-\eta} & 0 \\ \frac{i\sqrt{1-\eta}}{\sqrt{2}} & \frac{\sqrt{\eta}}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{-\sqrt{1-\eta}}{\sqrt{2}} & \frac{i\sqrt{\eta}}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}. \tag{2.8}$$

In the Heisenberg picture, the relationship between output channel operators and input channel operators can be described by Equation 2.9 as follows:

$$\begin{pmatrix} a_{out} \\ b_{out} \\ c_{out} \end{pmatrix} = S_{\mathrm{BS}} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \tag{2.9}$$

The output state of the system can also be described in the Schrödinger picture:

$$\begin{aligned} |\Psi\rangle_{out} &= U|\Psi\rangle_{in} \\ &= U|0\rangle_a|1\rangle_b|\alpha\rangle_c \\ &= Ub^\dagger U^\dagger U D_c(\alpha) U^\dagger U|0\rangle_{a,b,c} \\ &= Ub^\dagger U^\dagger U D_c(\alpha) U^\dagger|0\rangle_{a,b,c}, \end{aligned} \tag{2.10}$$

where in the last line we wrote the input state in terms of the creation and displacement operators and used the fact that the unitary operator U representing the evolution does not change the initial vacuum state. Note now that $Ub^\dagger U^\dagger$ and $UD_c(\alpha)U^\dagger$ correspond to the output operators in the Heisenberg picture. Inverting Equation (2.9), we can write:

$$|\Psi\rangle_{out} = \left(-i\sqrt{1-\eta}a^\dagger + \frac{\sqrt{\eta}}{\sqrt{2}}b^\dagger - \frac{i\sqrt{\eta}}{\sqrt{2}}c^\dagger\right) D_b\left(-i\frac{\alpha}{\sqrt{2}}\right) D_c\left(\frac{\alpha}{\sqrt{2}}\right)|0\rangle_{a,b,c}. \tag{2.11}$$

The probability of single photon detection in either c_{out} or b_{out} channel can be calculated as:

$$P = e^{-|\alpha|^2}(\eta + (1-\eta)|\alpha|^2). \tag{2.12}$$

If we have a detection event on the output channel corresponding to c_{out} and no clicks on the b_{out} channel. The output state $|\Psi\rangle_{out}$ would be projected with a projector $\Pi = |0\rangle_b|1\rangle_c\langle 1|_c\langle 0|_b = |0\rangle_b c^\dagger|0\rangle_c\langle 0|_c c\langle 0|_b$. Using Equation 2.11, we can write the unnormalized output state, $|\tilde{\Psi}\rangle_{out}^{cond}$, conditioned on this detection as

$$\begin{aligned}
|\tilde{\Psi}\rangle_{out}^{cond} &= \Pi \cdot |\Psi\rangle_{out} \\
&= |0\rangle_b|1\rangle_c\langle 0|_b\langle 0|_c c\left(-i\sqrt{1-\eta}a^\dagger + \frac{\sqrt{\eta}}{\sqrt{2}}b^\dagger - \frac{i\sqrt{\eta}}{\sqrt{2}}c^\dagger\right) \\
&\times D_b\left(-i\frac{\alpha}{\sqrt{2}}\right) D_c\left(\frac{\alpha}{\sqrt{2}}\right)|0\rangle_{a,b,c} \\
&= e^{\frac{-|\alpha|^2}{2}}\left(-i\sqrt{\frac{1-\eta}{2}}\alpha\, a^\dagger - \frac{i\sqrt{\eta}}{\sqrt{2}}\right)|0\rangle_a|0\rangle_b|1\rangle_c \\
&= -ie^{\frac{-|\alpha|^2}{2}}\sqrt{\frac{\eta}{2}}\left(1+\sqrt{\frac{1-\eta}{\eta}}a^\dagger\alpha\right)|0\rangle_a|0\rangle_b|1\rangle_c. \qquad (2.13)
\end{aligned}$$

Therefore, the normalized output state on channel a_{out} conditioned on this particular event is

$$|\Psi\rangle_{a,out}^{cond} = \frac{|0\rangle + g\alpha|1\rangle}{\sqrt{1+|g\alpha|^2}} \qquad (2.14)$$

where

$$g = \sqrt{\frac{1-\eta}{\eta}}$$

In the limit where $|g\alpha| \ll 1$, this state can be approximated as the coherent state $|g\alpha\rangle$ with a fidelity $F = e^{\frac{-|g\alpha|^2}{2}}/\sqrt{|g\alpha|^2+1}$. The amplitude of output signal will depend on the gain $g = \sqrt{\frac{1-\eta}{\eta}}$. Therefore, we can achieve different amplitudes for output state by changing the transmission rate of second beam splitter in Figure 2.1.

If the amplitude $|g\alpha|$ does not fulfill $|g\alpha| \ll 1$, then we can employ an N beam splitter to divide the input coherent state $|\alpha\rangle$ into N smaller coherent states $|\alpha'\rangle$, where $\alpha' = \frac{\alpha}{\sqrt{N}}$. As shown in Figure(2.2), the N smaller coherent states are amplified by N quantum scissors separately into $|g\alpha'\rangle$. The N amplified coherent states are then recombined by another N beam splitter into $|g\alpha\rangle$ in the output channel 1, conditional on no photon detection in the rest $N-1$ output channels.

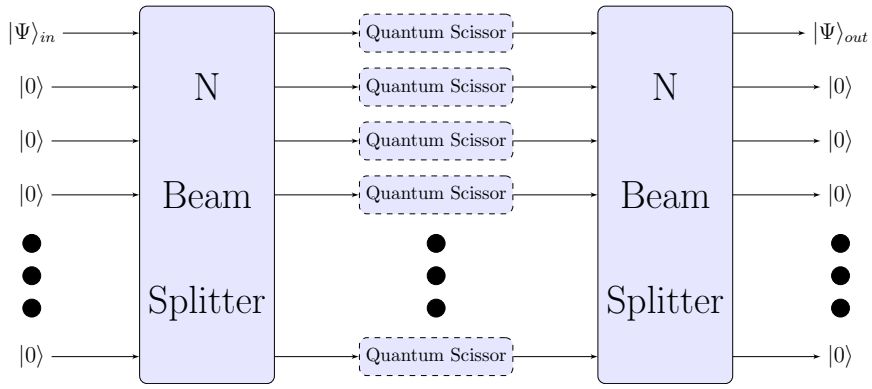


Figure 2.2. If the amplitude $|g\alpha|$ does not fulfill $|g\alpha| \ll 1$, then we can employ an N beam splitter to divide the input coherent state $|\alpha\rangle$ into N smaller coherent states $|\alpha'\rangle$, where $\alpha' = \frac{\alpha}{\sqrt{N}}$. As shown in this figure, the N smaller coherent states are amplified by N quantum scissors separately into $|g\alpha'\rangle$. The N amplified coherent states are then recombined by another N beam splitter into $|g\alpha\rangle$ in the output channel 1, conditional on no photon detection in the rest $N-1$ output channels.

The total success probability can be calculated as:

$$P = e^{-(1-g^2)|\alpha|^2}|\eta|^{\frac{N}{2}}. \tag{2.15}$$

which is state dependent and also decreases with increasing N. This indicates that a better approximation to the amplified state can be achieved at the price of reduced probability of success.

In order to send a photon further away, Gisin [29] proposed that the quantum scissor module could be used to amplify weak photonic state $\mathcal{N}(|0\rangle + \alpha|1\rangle)$ into $\mathcal{N}(|0\rangle + g\alpha|1\rangle)$. This NLA scheme was also demonstrated in a few experiments [64–67]. Haw et al. [76] performed a hybrid amplification, where both NLA and DLA are used. In all of these theoretical analyses and experimental demonstrations, the pulse shapes of quantum states are not considered. In the theoretical analysis [29, 61], both the input coherent state and auxiliary single photon are assumed to be in discrete mode. In the experimental setup [64–66], the input coherent state and auxiliary single photon are generated from the same source and thus they have the same

pulse shape. As we know, the pulse shape of a coherent state may change due to channel distortion in quantum communication. It may not be applicable to keep the pulse shape of input coherent state the same as that of auxiliary single photon in practical implementation. Therefore, an analysis of this quantum scissor based NLA scheme in continuous mode operation is necessary.

Another issue we need to take into account is the resolution time of photon detectors. Like pulse shapes of quantum states, the resolution time of photon detectors are assumed to be discrete as well in the literature mentioned above. This assumption may not be true in practical implementation. In Chapter 3, we will analyse the effects of photon detection resolution time.

2.2.3 Photon addition-subtraction based NLA

Another NLA scheme is based on photon addition-subtraction [68, 69, 71, 73, 74]. Like the quantum scissor based NLA, this scheme also begins with approximating a coherent state $|\alpha\rangle \approx |0\rangle + \alpha|1\rangle$ when $\alpha \ll 1$. As shown in Figure 2.3, this coherent state is firstly multiplied with a creation operator $\hat{a}^\dagger$. In experimental set up [73], this creation operator is implemented by conditional stimulated parametric down-conversion in a nonlinear crystal. Photon addition in the output signal mode is heralded by the detection of a single photon in the idler down-conversion channel [95, 96] (detector D_1 in the figure). If a single photon is detected in D_1, the state then can be written as:

$$\begin{aligned} \hat{a}^\dagger|\alpha\rangle &\approx \hat{a}^\dagger(|0\rangle + \alpha|1\rangle) \\ &= |1\rangle + \sqrt{2}\alpha|2\rangle \end{aligned} \tag{2.16}$$

After the photon addition, the single-photon subtraction is implemented by conditionally attenuating a state through the detection of (D_2 as shown in Figure 2.3) a single photon reflected from a high-transmissivity beamsplitter. If a single photon is detected in D_2, the state is attenuated and the resulted state is as follows:

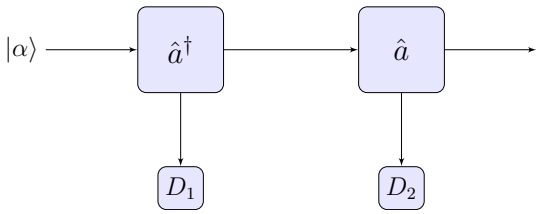


Figure 2.3. As shown in this figure, this coherent state is firstly multiplied with a creation operator $\hat{a}^\dagger$. In experimental set up [73], this creation operator is implemented by conditional stimulated parametric down-conversion in a nonlinear crystal. Photon addition in the output signal mode is heralded by the detection of a single photon in the idler down-conversion channel [95,96] (detector D_1 in the figure). After the photon addition, the single-photon subtraction is implemented by conditionally attenuating a state through the detection of (D_2) a single photon reflected from a high-transmissivity beamsplitter.

$$\begin{aligned}\hat{a}\hat{a}^\dagger|\alpha\rangle &\approx \hat{a}(|1\rangle + \sqrt{2}\alpha|2\rangle) \\ &= |0\rangle + 2\alpha|1\rangle \\ &\approx |2\alpha\rangle \end{aligned} \tag{2.17}$$

In this way, the weak coherent state $|\alpha\rangle$ is amplified into $|2\alpha\rangle$ with an amplification ratio 2. Because the parametric down-converter and the beamsplitter are placed in series along the path of a travelling coherent state, the application of $\hat{a}\hat{a}^\dagger$ operator can be heralded by looking for coincident detections from D_1 and D_2.

As proved in the paper [97–99], the multiphoton terms of input coherent states can be ensured to be negligible by the low parametric gain and beam splitter's low reflectivity in the photon addition and subtraction processes. This photon addition-subtraction based NLA outperform quantum scissor based NLA with higher effectiveness and higher fidelity of the final states to the ideal target coherent state $|g\alpha\rangle$.

In this photon addition-subtraction NLA scheme, the $\hat{a}\hat{a}^\dagger$ operator is applied conditionally on single photon detection in both the D_1 and D_2. Therefore, the temporal profile of $\hat{a}\hat{a}^\dagger$ operator is influenced by resolution time of the two photon detectors.

In Chapter 3, the effects of photon detector resolution time are discussed and the whole scheme is analysed in continuous mode operation.

2.3 Quantum networking protocols

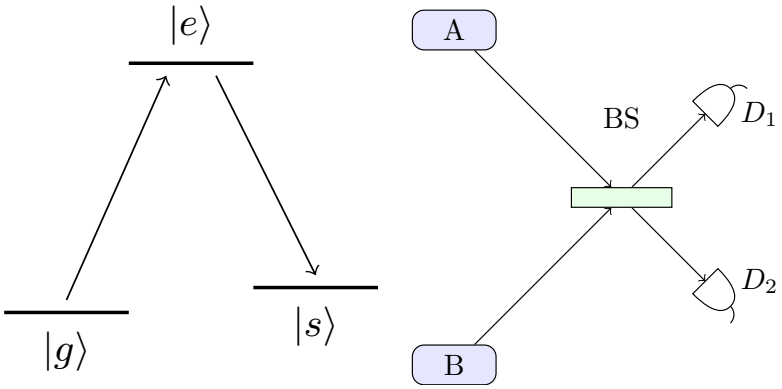
Entanglement should be generated over long distances in order to perform quantum teleportation between two distant nodes. A huge number of protocols have been proposed and demonstrated to implement remote entanglement, of which the most famous is the DLCZ protocol. In this section, we introduce the DLCZ protocol briefly and review some extensions of DLCZ protocols from various perspectives.

2.3.1 DLCZ protocol

The widely known DLCZ protocol can be used to generate entanglement between two distant atomic ensembles over long distances [78]. The atomic ensemble is prepared in the ground state $|g\rangle$. With a short, off-resonant laser pulse, we can generate entanglement between the atomic ensemble and the emitted single photon, as shown in the left subfigure of Figure 2.4. If we guide the emitted photons from the two atomic ensembles into a beam splitter and observe a single photon click in either D_1 or D_2, we achieve entanglement between the two distant atomic ensembles A and B, as shown in the right subfigure of Figure 2.4. With this approach, we can generate two entanglement pairs $A-B$ and $C-D$. The stored atomic excitations of B and C in Figure 2.5 can be converted into light and guided into another beam splitter to be measured further. If a single photon is detected, entanglement between A and D is achieved. Repeating this entanglement swapping process, we can achieve entanglement over significantly longer distances.

2.3.2 Extensions of DLCZ protocol

Duan *et al.* improved the efficiency of entanglement generation by detecting cavity decay through single-photon detectors [82]. Unlike the DLCZ protocol, in which the



(a) Three states of atomic ensemble

(b) Bell state measurement

Figure 2.4. The atomic ensemble is prepared in the ground state $|g\rangle$. With a short, off-resonant laser pulse, we can generate entanglement between the atomic ensemble and the emitted single photon, as shown in the left subfigure. If we guide the emitted photons from the two atomic ensembles A and B into a beam splitter and observe a single photon click in either D_1 or D_2, we achieve entanglement between the two distant atomic ensembles.

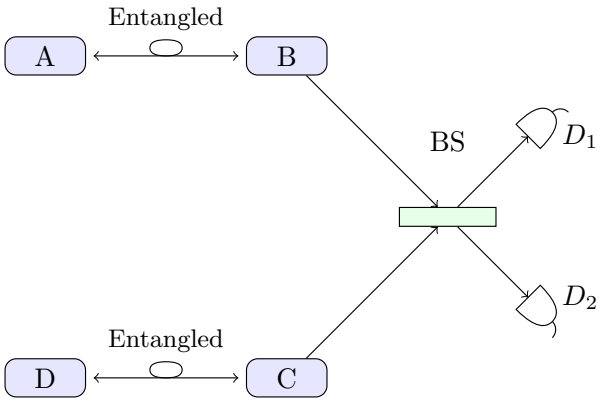


Figure 2.5. The stored atomic excitations of B and C can be converted into light and guided into another beam splitter to be measured. If a single photon is detected, entanglement between A and D is achieved. Repeating this entanglement swapping process, we can achieve entanglement over significantly longer distances.

emitted photons are collected directly, each of the two atoms is set in a standing-wave high-Q optical cavity. With proper driving pulses, the atoms are transferred with probability $p_c \approx 1$ from $|g\rangle$ to $|0\rangle$ or $|1\rangle$, inducing cavity decay pulses with polarization h or v. The decay pulses from the two cavities are interfering at a polarization beam splitter (PBS). If we detect one photon in each of the PBS outputs, we have achieved an entanglement between these atoms. This detecting method has proved to be more efficient than the DLCZ protocol in experiments [100, 101].

In the DLCZ protocol, entanglement is generated and swapped based on a Mach-Zehnder type interference. Since in the Mach-Zehnder type interference, effectiveness is sensitive to path length instabilities, Zhao *et al.* proposed a new quantum repeater architecture based on a two-photon Hong-Ou-Mandel type interference [81]. This architecture is proven to be 7 orders of magnitude more robust than the original DLCZ protocol.

Another challenge to implement the DLCZ protocol is the short atomic memory coherence times. As the entanglement generation and swapping are non-deterministic, it takes time to achieve entanglement over long distances. Quantum states needs to be stored in local memories during this period. Both quantum nodes are multiplexing [83] and multimode memories [84] can be used to speed up the entanglement swapping process and thereby lower the requirements for memory coherence times.

Like its classical counterpart, distributed quantum computing is required to utilize quantum computing resources at different locations [102]. To achieve distributed quantum computing, we must prepare entanglement between several distributed nodes. The distributed W-state entanglement can also be used to construct quantum networks, with which quantum communication between more than two nodes is possible [103]. However, no atomic-ensemble-based methodology that can generate entanglement between more than two distant nodes has been proposed yet. This project extends the DLCZ protocol to generate distributed W-states over long distances. These distributed W-states can be considered as entanglement among more

than two nodes, and may be used to implement quantum networks and distributed quantum computing in the future.

2.4 QKD protocols

In order to explain the following QKD protocols, it is convenient to introduce Alice and Bob, two parties who want to communicate secretly, as well as Eve, the unauthorized eavesdropper. In QKD, quantum states are employed to produce shared key between Alice and Bob. Both Alice and Bob have access to two channels: the quantum channel for exchanging quantum states and the classical public channel to detect eavesdropping. If Eve performs measurements on the transmitted quantum states, Alice and Bob will discover the eavesdropping in public communication.

2.4.1 BB84 protocol

BB84 Protocol is developed by Charles H. Bennett and Gilles Brassard and is the first QKD protocol [26]. Single photon states are used to produce shared cryptography key. Alice and Bob are connected by a quantum channel, usually an optical fiber. There is also a classical public channel, such as a phone cable or a wireless connection. Usually the same link is used for both channels.

In order to produce and distribute the cryptography key, Alice can choose between four non-orthogonal states. She has two bases with polarised photons:

The horizontal-vertical basis $\oplus$

- Horizontally polarised $|H\rangle$
- Vertically polarised $|V\rangle$

and the diagonal basis $\otimes$

- Left polarised $|L\rangle$

- Right polarised $|R\rangle$

The quantum states $|H\rangle$ and $|L\rangle$ are encoded as the classical bit 1 while $|V\rangle$ and $|R\rangle$ are 0. Alice prepares a sequence of single photon states by randomly choose their bases and polarization. Suppose n single photon states are prepared. The rest steps of BB84 scheme are as follows:

1. Alice sends the randomly chosen single photon states to Bob.

2. Randomly and independently, Bob chooses one of the two bases to measure the received quantum states. If he chooses the same basis as Alice for a quantum state, he will observe the same bit for this quantum state. Otherwise he will get an uncorrelated bit.

3. After measuring all of the received quantum states, Bob records a string of n bits. This bit string is called raw key.

4. Both Alice and Bob announce via public classical channel their chosen bases for every quantum state.

5. After comparing their chosen bases, the recorded bits from different chosen bases are discarded. m bits are left. This m bits are called sifted key. Because all the bases are chosen independently and randomly from two bases, m is expected to be about $0.5 * n$.

6. Bob chooses at random half of the remaining m bits to announce it publicly. Alice compares the announced $0.5m$ bits with her own bit string. If a significant inconsistency rate is found, the transmitted message might be eavesdropped and the sifted key should be discarded. The error rate that is estimated in this step can be used to bound the information Eve has about the sifted key

7. If the test passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys.

This privacy amplification could be achieved using a universal hash function. The amount by which this new key is shortened is calculated to reduce the probability of Eve having any knowledge of the new key to a very low value.

The following example is given to illustrate the process of BB84 protocol. Note that the bases are chosen by Alice and Bob independently and randomly. 10 quantum states are prepared by Alice. After receiving this quantum state sequence, Bob measures these 10 quantum states with randomly chosen bases and obtains the raw key. After that, both Alice and Bob announce their chosen bases and discard the bits where different bases are chosen. The remaining 5 bits become the sifted key and if their is no eavesdropping detected, this sifted key can be used as secret key for encryption and decryption.

Transmitted states	$\|H\rangle$	$\|H\rangle$	$\|L\rangle$	$\|R\rangle$	$\|V\rangle$	$\|V\rangle$	$\|H\rangle$	$\|V\rangle$	$\|R\rangle$	$\|L\rangle$
Alice's bit value	1	1	1	0	0	0	1	0	0	1
Bob's basis	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Bob's measure results	$\|R\rangle$	$\|H\rangle$	$\|H\rangle$	$\|R\rangle$	$\|V\rangle$	$\|V\rangle$	$\|L\rangle$	$\|V\rangle$	$\|H\rangle$	$\|L\rangle$
Raw key	0	1	1	0	0	0	1	0	1	1
Same basis?	N	Y	N	Y	N	Y	N	Y	N	Y
Sifted key	/	1	/	0	/	0	/	0	/	1

2.4.2 Photon number splitting attacks

As is introduced in Section 2.4.1, BB84 scheme provides an unconditional secure solution to implement QKD. Several long-distance QKD implementations have been developed with optical signals as information carriers and fibers as quantum channels. If single photon states are employed as information carriers, the security of QKD with BB84 scheme can be guaranteed. However, in most practical implementations, weak laser pulses are used to carry quantum information. Each pulse is a priori in a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ of weak intensity, typically $\mu \approx 0.1$ photons. This pulse can

be also written as a superposition of Fock states, $\sum_n p_n|n\rangle\langle n|$. The number n is distributed according to the Poissonian statistics of mean μ, $p_n = p_n(\mu) = e^{-\mu}\mu^n/n!$. If weak laser pulses are used to implement BB84 QKD protocol, some methodologies can be applied by Eve to obtain full information of transmitted quantum states [104, 105]. This is called a photon number splitting (PNS) attack.

If Eve is endowed with unlimited technological power within the laws of physics, the following PNS attack is in principle possible [104, 105]:

1. Eve counts the photon number of transmitted quantum states, using a photon number quantum nondemolition (QND) measurement.

2. If only one photon is observed, Eve blocks the state. If more than one photons are measured, she stores one photon in a quantum memory and transmit the remaining photons to Bob through a transparent quantum channel.

3. Eve waits until Alice and Bob publicly reveal the used bases and correspondingly measures the photon stored in her quantum memory. Because she knows the bases of every stored qubit, she can deterministically obtain the full information of quantum states.

In this eavesdropping process, Eve stored one photon for every transmitted quantum state. From Bob's perspective, the quantum states are attenuated substantially. If the transmission distance is short (typically less than $50km$) and the natural channel attenuation due to photon absorption of fiber material is lower than eavesdropping induced attenuation, this eavesdropping can be detected. If Eve does not want her eavesdropping to be detected, she need to store less photons and in this way she cannot obtain the full information of quantum states.

2.4.3 SARG 04 protocol

In order to tackle the problem of PNS attacks, the SARG 04 protocol was developed in the year 2004 [28]. Unlike the coding scheme in BB84 protocol, the basic idea of

SARG 04 protocol is that Alice encodes each bit into a pair of nonorthogonal states belonging to two or more suitable sets. This protocol is confirmed to be more robust than BB84 scheme against PNS attacks.

Applying PNS attack as introduced in Section 2.4.2, Eve needs to discriminate between two eigenstates of a known Hermitian operator after the sifting step. This is the extreme weakness of the BB84 protocol against PNS attack: when Eve can keep one photon, she obtains all the information. If we can can encode the classical bits in nonorthogonal states which cannot be discriminated deterministically by Eve, the robustness of QKD can be increased.

The SARG 04 protocol begins with Alice's preparation of two bit strings, a and b, each n bits long. She then encodes these two strings into a string of n qubits as follows:

$$|\Psi\rangle = \bigotimes_{i=1}^{n} |\Psi_{a_i b_i}\rangle \tag{2.18}$$

where a_i and b_i are the i^{th} bits of a and b, respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$\begin{aligned}
|\Psi_{00}\rangle &= |0\rangle \\
|\Psi_{10}\rangle &= |1\rangle \\
|\Psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\
|\Psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle
\end{aligned} \tag{2.19}$$

From the above four qubits, we can see that choice of basis is encoded in (either in the computational basis or the Hadamard basis) in the bit b_i. Without knowing bit b_i, it is impossible to distinguish all of these nonorthogonal quantum states with certainty. The rest steps of SARG 04 protocol are as follows:

1. Alice sends a sequence of n qubits $|\Psi\rangle$ over a public quantum channel to Bob. After Bob receives the qubit sequence, all three parties, namely Alice, Bob and Eve, have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits.

2. Bob proceeds to generate a string of random bits b' of the same length as b.

3. According to the bit value of b', Bob decide the basis (0 for computational basis and 1 for Hadamard basis) and measure the received n qubits independently.

4. Bob announces via public classical channel that he receives the sequence of n qubits.

5. For each sent qubit, Alice chooses one computational basis state and one Hadamard basis state such that the state of the transmitted qubit is one of these two states. Alice then announces those two states publicly. Alice will note whether the state is the computational basis state or the Hadamard basis state.

6. Bob now knows that the state of his qubit is one of the two states indicated by Alice. To determine the secret bit, Bob must distinguish between the two candidate states. For each qubit, Bob can check to see whether his measurement is consistent with either possible state. If it is consistent with either state, Bob announces that the bit is invalid, since he cannot distinguish which state was transmitted based on the measurement. If on the other hand, one of the two candidate states is inconsistent with the observed measurement (different states at the same basis), Bob announces that this qubit is valid. Now Alice and Bob form a key.

7. Alice randomly chooses half bits of the raw key and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see if more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy

amplification techniques to create some number of shared secret keys. The amount by which this new key is shortened is calculated based on how much information Eve could have gained about the old key.

For example if Alice transmits $|\psi_{00}\rangle$ and announces the two states $|\Psi_{00}\rangle$ and $|\Psi_{01}\rangle$. If Bob chooses the computational basis, his only possible measurement is $|\Psi_{00}\rangle$. This outcome is exactly the same as one of the announced states. In this case, this qubit will become invalid because it would also be a possible outcome if the transmitted state had been $|\Psi_{01}\rangle$. If Bob measures in the Hadamard basis, either $|\Psi_{01}\rangle$ or $|\Psi_{11}\rangle$ could be measured, each with probability 1/2. If the outcome is $|\Psi_{01}\rangle$ then again this state is consistent with one of the announced state and he can not decide the transmitted state. On the other hand, an outcome of $|\Psi_{11}\rangle$ cannot possibly be observed from a qubit in $|\Psi_{01}\rangle$. Thus in the case that Bob measures in the Hadamard basis and observes state $|\Psi_{11}\rangle$ (and only in that case), Bob can deduce which state was sent and therefore what the secret bit is. The probability of validity for a transmitted qubit is 1/4 and one valid qubit can generate 2 secret shared bits (a_i and b_i). So a qubit is expected to generate 1/2 bit on average, which is the same as in BB84 protocol.

If Eve applies the same PNS attack on this SARG 04 protocol, she stores one photon for every transmitted qubit. However, as Alice and Bob never announces their basis, it is impossible for Eve to deduce secret bits from the stored qubits.

The following example is given to illustrate the process of SARG 04 protocol. Note that the bases are chosen by Alice and Bob independently and randomly. 12 quantum states are prepared by Alice. After receiving this quantum state sequence, Bob measures these 12 quantum states with randomly chosen bases. After that, Alice chooses one computational basis state and one Hadamard basis state such that the state of the transmitted qubit is one of these two states. Three qubits are determined to be valid and 6 shared bits are produced.

Alice's bit string a	0	0	1	1	0	1	0	0	1	0	1	1
Alice's bit string b	0	1	1	1	0	1	0	1	0	0	1	0
Transmitted states	$\|\Psi_{00}\rangle$	$\|\Psi_{01}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{01}\rangle$	$\|\Psi_{10}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{10}\rangle$
Another announced states	$\|\Psi_{11}\rangle$	$\|\Psi_{10}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{01}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{01}\rangle$	$\|\Psi_{11}\rangle$
Bob's bit string b'	1	1	0	0	0	1	1	0	0	0	1	1
Bob's measure results	$\|\Psi_{01}\rangle$	$\|\Psi_{01}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{10}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{10}\rangle$	$\|\Psi_{00}\rangle$	$\|\Psi_{11}\rangle$	$\|\Psi_{01}\rangle$
Valid qubit?	Y	N	N	Y	N	N	N	N	N	N	N	Y
key	00	⁄	⁄	11	⁄	⁄	⁄	⁄	⁄	⁄	⁄	10

2.5 Channel equalisation techniques

In telecommunication, equalisation is the reversal of distortion incurred by a signal transmitted through a channel. Equalizers are used to render the frequency response of a communication channel flat from end-to-end. When a channel has been equalised the frequency domain attributes of the signal at the input are faithfully reproduced at the output. Telephones, DSL lines and television cables use equalizers to prepare data signals for transmission.

Equalizers are critical to the successful operation of electronic systems such as analog broadcast television. In this application the actual waveform of the transmitted signal must be preserved, not just its frequency content. Equalizing filters must cancel out any group delay and phase delay between different frequency components.

In classical communication, suppose a sequence of signals $\mathbf{S}$ is transmitted. $\mathbf{S}$ is a vector, of which the kth element S_k is the kth transmitted signal. If the channel response is a vector $\mathbf{H}$ and the additive noise is $\mathbf{N}$, the receiving signal sequence $\tilde{\mathbf{S}}$ would be:

$$\tilde{\mathbf{S}} = \mathbf{S} \otimes \mathbf{H} + \mathbf{N} \tag{2.20}$$

An equaliser with impulse response $\mathbf{E}$ would be needed to produce another signal sequence $\hat{\mathbf{I}} = \mathbf{E} \otimes \tilde{\mathbf{I}}$ that approximates the transmitted sequence $\mathbf{I}$ as much as possible. In this section, some equalisation techniques for LTI (linear time invariant) systems

are introduced. In classical communication, the channels are reasonably assumed to be LTI systems.

2.5.1 MMSE equaliser

One option to decide the equalisation sequence $\mathbf{E}$ is minimum mean square error (MMSE) equaliser. It is based on the mean square error (MSE) criterion.

Since we do not know the values of transmitted sequence $\mathbf{S}$ beforehand, each symbol S_k should be modelled as a random variable. The equalisation sequence $\mathbf{E}$ should be chosen to minimize the MSE between the original information symbols S_k and the output of the equaliser $\hat{S_k}$:

$$MSE = E[e_k^2] = E[(S_k - \hat{S_k})^2] \tag{2.21}$$

where $E[*]$ means the expectation operator. Assume the errors are generated by a stationary process. If the length of $\mathbf{E}$ is finite $(2L+1)$, the equaliser is a finite impulse response (FIR) filter and the MSE could be written as:

$$\begin{aligned} MSE &= E[(S_k - \sum_{j=-L}^{L} \tilde{S}_{k-j} E_j)^2] \\ &= E[(S_k - \tilde{\mathbf{S}}_k^T \mathbf{E})^2] \end{aligned} \tag{2.22}$$

where

$$\tilde{\mathbf{S}}_k = [\tilde{S}_{k-L}, \cdots\cdots, \tilde{S}_{k+L}]^T \tag{2.23}$$

$$\mathbf{E} = [E_{-L}, \cdots\cdots, E_L]^T \tag{2.24}$$

Since we want to minimize MSE by choosing suitable values for $\mathbf{E}$. By differentiating with respect to each element of $\mathbf{E}$ and setting the result to zero, we obtain:

$$E[\tilde{\mathbf{S}}_k(I_k - \tilde{\mathbf{S}}_k^T\mathbf{E})] = 0 \tag{2.25}$$

Rearranging, we obtain:

$$E[\tilde{\mathbf{S}}_k\tilde{\mathbf{S}}_k^T]\mathbf{E} = E[S_k\tilde{\mathbf{S}}_k] \tag{2.26}$$

Since the value of $E[\tilde{\mathbf{S}}_k\tilde{\mathbf{S}}_k^T]$ and $E[S_k\tilde{\mathbf{S}}_k]$ could be obtained by sending a training sequence. The MMSE equaliser sequence $\mathbf{E}$ could be found by solving Equation 2.26.

2.5.2 Decision feedback equaliser

We can write the kth signal of receiving sequence as follows:

$$\tilde{S}_k = S_kH_0 + \sum_{j\neq k} S_jH_{k-j} + \tilde{N}_k \tag{2.27}$$

where H_j is the jth element of the channel impulse response $\mathbf{H}$ and $\tilde{N}_k$ is the imposing noise. From Equation 2.27, we can see that if all the other symbols of the receiving sequence is known, we can eliminate ISI (Inter symbol interference) as follows:

$$\hat{S}_k = \tilde{S}_k - \sum_{j\neq k} S_jH_{k-j} \tag{2.28}$$

In practical implementation, we do not know all the symbols that are affecting the reception of the current symbol. However, we can use previously decided symbols provided that we have made correct decisions on them. This approach is known as decision feedback equaliser (DFE). A DFE is composed of a forward part $\mathbf{F}$ and a

feedback part **B**. Suppose **F** and **B** are vectors with length L_1+1 and L_2 respectively. Then we can obtain:

$$\hat{S}_k = \tilde{\mathbf{S}}_F^T \mathbf{F} + \mathbf{S}_B^T \mathbf{B} \tag{2.29}$$

where

$$\tilde{\mathbf{S}}_F = [\tilde{S}_{k+L_1}, \tilde{S}_{k+L_1-1}, \cdots\cdots, \tilde{S}_k]^T \tag{2.30}$$

$$\mathbf{S}_B = [S_{k-1}, S_{k-2}, \cdots\cdots, S_{k-L2}]^T \tag{2.31}$$

$$\mathbf{F} = [F_{-L_1}, F_{-L_1+1}, \cdots\cdots, F_0]^T \tag{2.32}$$

$$\mathbf{B} = [B_1, B_2, \cdots\cdots, B_{L_2}]^T \tag{2.33}$$

The MSE of this DFE is:

$$E[(S_k - \hat{S}_k)^2] = E[(S_k - \tilde{\mathbf{S}}_F^T \mathbf{E} - \mathbf{S}_B^T \mathbf{B})^2] \tag{2.34}$$

Since we need to minimize MSE, we need to differentiate with respect to **E** and **B** and make:

$$E[\tilde{\mathbf{S}}_F S_k - \tilde{\mathbf{S}}_F^T \mathbf{F} - \mathbf{S}_B^T \mathbf{B})] = 0 \tag{2.35}$$

$$E[\mathbf{S}_B S_k - \tilde{\mathbf{S}}_F^T \mathbf{F} - \mathbf{S}_B^T \mathbf{B})] = 0 \tag{2.36}$$

By solving the above equation, we can obtain the DFE **F** and **B** as follows:

$$\mathbf{F} = (E[\tilde{\mathbf{S}}_F \tilde{\mathbf{S}}_F^T] - E[\tilde{\mathbf{S}}_F \mathbf{S}_B^T] E[\mathbf{S}_B \tilde{\mathbf{S}}_F^T])^{-1} E[S_k \tilde{\mathbf{S}}_F] \tag{2.37}$$

$$\mathbf{B} = -E[\mathbf{S}_B \tilde{\mathbf{S}}_F^T] \mathbf{F} \tag{2.38}$$

2.6 Conclusion

Relevant literature in the field of quantum communication is reviewed. At first, a number of NLA schemes are introduced. After that, the DLCZ protocol is presented, followed by introduction of its extensions from various perspectives. Some popular QKD protocols are then discussed. Finally, we introduce the equalisation techniques in classical communication.

Chapter 3

Quantum Amplification

THIS chapter presents a dynamical model to describe the operation of the NLA in the regime of continuous modes inputs. Both the quantum scissor based NLA and the photon addition-subtraction based NLA are analysed. Simulation results are also presented to confirm theoretically analysis.

3.1 Introduction

One of the most thriving areas of quantum information is optical quantum communication, with a number of protocols taking advantage of quantum physics to achieve goals that wouldn't be possible classically [10, 18, 20]. Despite the numerous experiments demonstrating these protocols [19,21–23], the build up of realistic quantum networks that span large distances is still a major challenge due to attenuation and noise introduced by decoherence in the channels. In classical communication, the solution is to introduce repeater stations that amplify the signal making the transmission of information between distant nodes possible. In the quantum case, however, deterministic amplification inevitably introduces extra noise [48].

A possible way to achieve a noiseless amplification of an arbitrary quantum state is to let go of the deterministic aspect of the process and to consider a probabilistic protocol. This is the solution proposed by Ralph and Lund with the nondeterministic (but heralded) noiseless linear amplifier (NLA) introduced in Ref. [61]. The application of this scheme has been considered in a variety of contexts both theoretically [29] and experimentally [64–67] and is known as quantum scissor based NLA. Another NLA scheme is based on photon addition and subtraction [68, 69, 71, 73, 74].

In previous literature for both the two NLA schemes, the quantum states and operators are treated in discrete mode, which may not be true in practical implementation. A continuous-mode operation of NLA is therefore necessary. We also need to discuss the effects of photon detector resolution time, as the success of amplification in both the two NLA schemes is heralded by specific photon detection as introduced in Section 2.2.

This chapter is structured as follows: In Section 3.2, we describe the continuous-mode quantum scissor based NLA model and analyse the detailed dynamical behavior of a single, and also a couple of concatenated NLAs. In particular, we show that the shape of the ancilla single photon pulse gets mapped onto the amplified coherent state. We also simulate a range of different pulse shapes to investigate the effects of the temporal modes on the NLA operation. In Section 3.3, we apply the

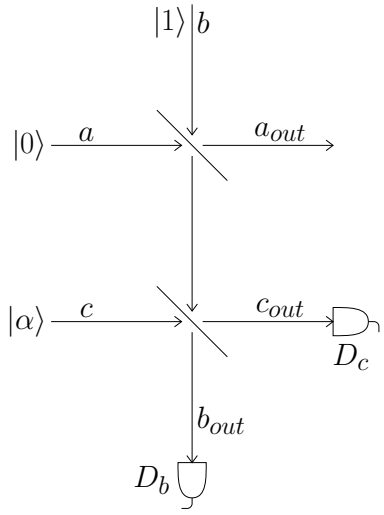


Figure 3.1. A single NLA module: a coherent state $|\alpha\rangle$ is amplified to $|g\alpha\rangle$ when one photon is detected in either one of the detectors. This amplification transformation is approximate, and only valid when $g\alpha$ is small. For larger coherent states, multiple amplifier modules need to be concatenated together.

same continuous mode analysis for the photon addition-subtraction based NLA. The research results are concluded and some open questions are discussed in Section 3.4.

3.2 Continuous-mode quantum scissor based NLA

The NLA protocol works using the "quantum scissor" [94] module shown in Figure 3.1. Using an auxiliary single photon $|1\rangle$ in one of the input ports, this module truncates a general state $|\psi\rangle = \sum_k^\infty c_k|k\rangle$ into $|\psi_{\text{trunc}}\rangle = \mathcal{N}(c_0|0\rangle + c_1|1\rangle)$, whenever a photon is detected in either one of the detectors D_b or D_c. Here $\mathcal{N}()$ denotes the normalization of the state. If the input state $|\psi\rangle$ is a coherent state $|\alpha\rangle$ and the top beam splitter has transmission η, then the output state after a detection event is $\mathcal{N}(|0\rangle + g\alpha|1\rangle)$, where $g = \sqrt{\frac{1-\eta}{\eta}}$. If $g\alpha$ is small enough, the state $\mathcal{N}(|0\rangle + g\alpha|1\rangle)$ is approximately $|g\alpha\rangle$ and thereby we have the coherent state $|\alpha\rangle$ amplified into $|g\alpha\rangle$ with an amplification ratio g. For larger coherent states, the truncated state is not a good approximation for the amplified state and the solution is to split the input into small coherent states that can then be amplified and recombined, as shown in [61].

Since the implementation of the amplification operation relies on the interference of the ancilla single photon with the input field at beam splitters, then the question of mode matching and pulse shapes is an important one that is not encompassed by the single mode treatment described above. This is also relevant if one considers the situation where information is encoded into multiple frequencies or, equivalently, into the temporal profile of the incoming field. In this section, we extend the analysis of the quantum scissor NLA to the continuous mode regime to explicitly take into account arbitrary pulse shapes for the input field and the ancilla photon and their effects on the amplification process. In particular we show that the amplification gain will be determined by the detection time, and that the shape of the ancilla photon is transferred to the amplified state.

3.2.1 Amplification with one NLA module

To analyse the continuous-mode operation of the NLA, we will consider the ancilla single photon and input coherent states of the form $|1_{\xi_1}\rangle$ and $|\alpha_{\xi_2}\rangle$, respectively, where ξ_1 and ξ_2 are the corresponding wavepacket shapes fulfilling the normalization condition $\int |\xi_1(t)|^2 dt = \int |\xi_2(t)|^2 dt = 1$. Note that we grouped all the time dependence of the coherent state in the $\xi_2(t)$ factor. We can then write

$$\langle n \rangle = |\alpha|^2, \tag{3.1}$$

where $\langle n \rangle$ is the mean number of photons in the coherent pulse [106].

This situation is depicted in Figure 3.2, where the total input state for all three channels a, b, and c is given by $|\Psi\rangle_{in} = |0\rangle_a |1_{\xi_1}\rangle_b |\alpha_{\xi_2}\rangle_c$. This state can also be written as the action of the creation operator for mode b and the displacement operator for mode c on the vacuum, *i.e.* $|\Psi\rangle_{in} = b^\dagger_{\xi_1} D_c(\alpha_{\xi_2}) |0\rangle_a |0\rangle_b |0\rangle_c$, where

$$b^\dagger_{\xi_1} = \int \xi_1(t) b^\dagger(t) dt, \tag{3.2}$$

with an equivalent definition for the other modes. $b(t)$ is the annihilation operator at the time point t.

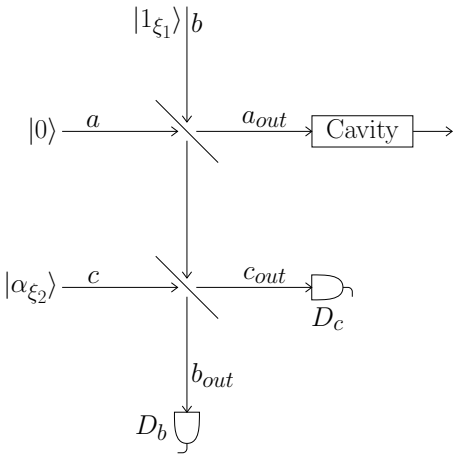


Figure 3.2. Compared with Figure 3.1, this dynamical amplification system have incoming signals written in the form $|1_{\xi_1}\rangle$ and $|\alpha_{\xi_2}\rangle$ because we take pulse shapes of signals into consideration. The cavity is used as probe to monitor the output signal in the simulation.

The transformation from the input channels to the output channels is given by the unitary matrix S_{BS} representing the action of the beam splitters on the system as follows:

$$\begin{pmatrix} a_{out} \\ b_{out} \\ c_{out} \end{pmatrix} = S_{\mathrm{BS}} \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \tag{3.3}$$

with

$$S_{\mathrm{BS}} = \begin{pmatrix} \sqrt{\eta} & i\sqrt{1-\eta} & 0 \\ \frac{i\sqrt{1-\eta}}{\sqrt{2}} & \frac{\sqrt{\eta}}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{-\sqrt{1-\eta}}{\sqrt{2}} & \frac{i\sqrt{\eta}}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}. \tag{3.4}$$

Here the top and bottom beam splitters of Figure 3.2 have transmissivities η and $1/\sqrt{2}$, respectively.

We can, alternatively, look at the output state of the system in the Schrödinger picture:

$$\begin{aligned}|\Psi\rangle_{out} &= U|\Psi\rangle_{in} \\ &= U|0\rangle_a|1_{\xi_1}\rangle_b|\alpha_{\xi_2}\rangle_c \\ &= Ub^\dagger{}_{\xi_1}U^\dagger U D_{(\alpha)_{c,\xi_2}}U^\dagger U|0\rangle_{a,b,c} \\ &= Ub^\dagger_{\xi_1}U^\dagger U D_c(\alpha_{\xi_2})U^\dagger|0\rangle_{a,b,c}, \end{aligned} \tag{3.5}$$

where in the last line we wrote the input state in terms of the creation and displacement operators and used the fact that the unitary operator U representing the evolution does not change the initial vacuum state. Note now that $Ub^\dagger_{\xi_1}U^\dagger$ and $UD_c(\alpha_{\xi_2})U^\dagger$ correspond to the output operators in the Heisenberg picture. Inverting Equation (3.3), we can write:

$$|\Psi\rangle_{out} = \left(-i\sqrt{1-\eta}a^\dagger_{\xi_1} + \frac{\sqrt{\eta}}{\sqrt{2}}b^\dagger_{\xi_1} - \frac{i\sqrt{\eta}}{\sqrt{2}}c^\dagger_{\xi_1}\right) D_b\left(-i\frac{\alpha_{\xi_2}}{\sqrt{2}}\right) D_c\left(\frac{\alpha_{\xi_2}}{\sqrt{2}}\right)|0\rangle_{a,b,c}. \tag{3.6}$$

3.2.1.1 Conditional Amplification: perfect detection case

We can now see the effect that the detection of a photon in any of one of the detectors has on the output state. In this sub-section, we discuss the situation where the time resolution of the photo-detectors is much shorter than the temporal width of the photon pulses, as in the case of experiments with solid-state quantum memories. Let's consider the case where, at a given time t_d, we have a detection event on the output channel corresponding to c_{out} and no clicks on the b_{out} channel. This happens with probability

$$P = e^{-|\alpha|^2}\left(\frac{\eta}{2}|\xi_1(t_d)|^2 + \frac{1-\eta}{2}|\alpha|^2|\xi_2(t_d)|^2\right) \tag{3.7}$$

and will project the state with the projector $\Pi = |0\rangle_b|1_{t_d}\rangle_c\langle 1_{t_d}|_c\langle 0|_b = |0\rangle_b c^\dagger(t_d)|0\rangle_c\langle 0|_c c(t_d)\langle 0|_b$. Using Eq.(3.6), we can write the unnormalized output state, $|\tilde{\Psi}\rangle^{cond}_{out}$, conditioned on this detection as

$$
\begin{aligned}
|\tilde{\Psi}\rangle_{out}^{cond} &= \Pi \cdot |\Psi\rangle_{out} \\
&= |0\rangle_b |1_{t_d}\rangle_c \langle 0|_b \langle 0|_c c(t_d) \left(-i\sqrt{1-\eta} a_{\xi_1}^\dagger + \frac{\sqrt{\eta}}{\sqrt{2}} b_{\xi_1}^\dagger - \frac{i\sqrt{\eta}}{\sqrt{2}} c_{\xi_1}^\dagger \right) \\
&\times D_b \left(-i\frac{\alpha_{\xi_2}}{\sqrt{2}} \right) D_c \left(\frac{\alpha_{\xi_2}}{\sqrt{2}} \right) |0\rangle_{a,b,c} \\
&= e^{\frac{-|\alpha|^2}{2}} \left(-i\sqrt{\frac{1-\eta}{2}} \xi_2(t_d) \alpha\, a_{\xi_1}^\dagger - \frac{i\sqrt{\eta}}{\sqrt{2}} \xi_1(t_d) \right) |0\rangle_a |0\rangle_b |1_{t_d}\rangle_c \\
&= -ie^{\frac{-|\alpha|^2}{2}} \sqrt{\frac{\eta}{2}} \xi_1(t_d) \left(1 + \frac{\xi_2(t_d)}{\xi_1(t_d)} \sqrt{\frac{1-\eta}{\eta}} a_{\xi_1}^\dagger \alpha \right) |0\rangle_a |0\rangle_b |1_{t_d}\rangle_c. \qquad (3.8)
\end{aligned}
$$

Therefore, the normalized output state on channel a_{out} conditioned on this particular event is

$$
|\Psi\rangle_{a,out}^{cond} = \frac{|0\rangle + g_0 g_1 \alpha |1_{\xi_1}\rangle}{\sqrt{1 + |g_0 g_1 \alpha|^2}} \qquad (3.9)
$$

where

$$
g_0 = \sqrt{\frac{1-\eta}{\eta}}
$$

and

$$
g_1 = \frac{\xi_2(t_d)}{\xi_1(t_d)}.
$$

If we detect single photon on the output channel corresponding to b_{out} and no clicks on the c_{out} channel. Then the normalized output state on channel a_{out} $|\Psi\rangle_{a,out}^{cond}$is $\frac{|0\rangle - g_0 g_1 \alpha |1_{\xi_1}\rangle}{\sqrt{1+|g_0 g_1 \alpha|^2}}$. A phase shifter can be utilized to transform this state to be the same as Equation 3.9.

In the limit where $|g_0 g_1 \alpha| \ll 1$, this state can be approximated as the coherent state $|g_0 g_1 \alpha_{\xi_1}\rangle$ with a fidelity $F = e^{\frac{-|g_0 g_1 \alpha|^2}{2}} / \sqrt{|g_0 g_1 \alpha|^2 + 1}$. The amplitude of output signal will depend on two gains, g_0 and g_1. The first is exactly the same as in the single mode calculations [61], while the second represents how well the temporal shape of the ancilla photon and the input coherent state match.

The behaviour of the gain g_1 for two unmatched pulses given by $|\xi_2(t)|^2 = e^{-t^2/(2\sigma^2)}/(\sigma\sqrt{2\pi})$ and $|\xi_1(t)|^2 = e^{-(t-t_1)^2/(2\sigma^2)}/(\sigma\sqrt{2\pi})$ is shown in the bottom panel

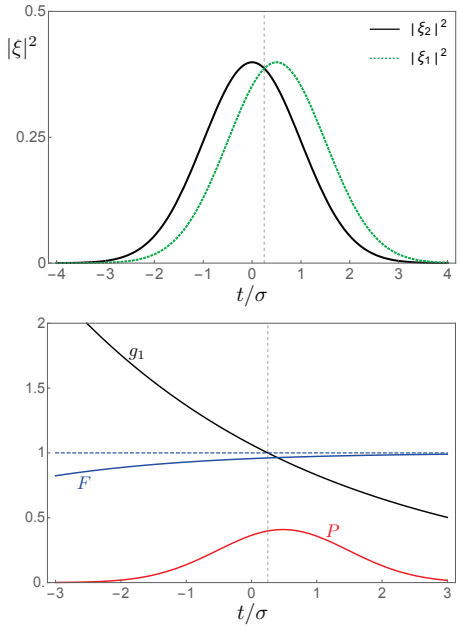


Figure 3.3. Top panel: input coherent state (solid, black) and ancilla single photon (green, dashed) pulse shapes. They were chosen to be Gaussian with the same standard deviation (σ) but shifted in time. Bottom panel: gain g_1, fidelity and probability of detection for the pulses shown on the top panel. The probability was multiplied by a factor of 10 to become more visible. The dotted vertical line in both plots show the point in time where the amplitude of the pulses coincide.

of Figure 3.3, together with the fidelity and the detection probability. Note that the detection time will determine whether the factor g_1 will represent gain ($\xi_2(t_d) > \xi_1(t_d)$) or attenuation ($\xi_2(t_d) < \xi_1(t_d)$) in the system. This asymmetry in the gain factor is just a consequence of the asymmetric NLA scheme where the output channel is only being fed by the ancilla photon, with no connection to the incoming coherent state.

The vertical dotted line in Figure 3.3 indicates the point in time where the amplitude of the pulses are the same and the total gain is simply g_0. To the left of this line, the gain increases at the expense of the fidelity: as $\xi_2(t_d)$ increases with respect to $\xi_1(t_d)$, the chance that the click on the detector came from the coherent field and that the single photon was reflected to the output channel increases. In the limit where $\xi_2(t_d) \gg \xi_1(t_d)$, it doesn't even make sense to talk about amplification as the

conditioned output state approaches the single photon state ($|\Psi\rangle^{cond}_{a,out} \approx |1_{\xi_1}\rangle$) and does not correspond to a scaled version of the input coherent state. To the right of the vertical line, the gain turns into attenuation and the amplification performance decreases as compared to the single mode case. Note that in the limit where $\xi_2(t_d) \ll \xi_1(t_d)$ the output state approaches the vacuum. In this case, the high fidelity is due to the large vacuum component of the small input coherent state.

3.2.1.2 Simulation and Analysis

To illustrate the effect of detection events in the amplifier, we performed simulations using a stochastic master equation (SME) describing the situation shown in Figure 3.2. The channel a_{out} is probed by a cavity for the seek of simulation. The channels b_{out} and c_{out} are monitored by photodetectors. In order to obtain the SME equation and simulate this dynamical system with the software Quantum Toolbox in Python(Qutip) [107], we need to model this whole dynamical system with $G = (S, L, H)$ [108] triplet.

In this project, a passive cavity is used to monitor the output signal of channel a. From the book [109, 110], we can describe the cavity with the following equations:

$$da = (-\frac{\kappa}{2})a \cdot dt - \sqrt{\kappa}du \tag{3.10}$$

where a is annihilation operator associated with the cavity mode. u stands for the incoming mode and κ is the coupling coefficient of the cavity. From the above equation, we can obtain the transfer function [111, 112] from the cavity mode to the incoming mode:

$$\frac{a(s)}{u(s)} = \frac{-\sqrt{\kappa}}{s + \frac{\kappa}{2}} \tag{3.11}$$

If the coupling coefficient κ is large enough (we set $\kappa = 100$ in the simulation), we can approximate the transfer function into a fixed ratio $-\frac{2}{\sqrt{\kappa}}$ and in this way we monitor the output signals with cavity modes.

In order to put this cavity into simulation, we need to represent this cavity in a $G = (S, L, H)$ form. Since κ is the coupling coefficient, we can use $G_{cavity} = (I, \sqrt{\kappa}a_{cavity}, 0)$ to represent the cavity as introduced in the paper [108] and a_{cavity} is the annihilation operator for cavity states. As there are three outputs in parallel, we can obtain the total output triple $G_{output} = (S, L, H)$:

$$G_{output} = (I, \begin{pmatrix} \sqrt{\kappa}a_{cavity} \\ 0 \\ 0 \end{pmatrix}, 0) \tag{3.12}$$

From the Figure 3.2, we can see there are three input signals in this dynamical system: $|0\rangle$, $|1_{\xi_1}\rangle$ and $|\alpha_{\xi_2}\rangle$. With the methodology introduced in the paper [113], we can represent the three incoming states in $G = (S, L, H)$ form as follows:

$$G_{input} = (I, \begin{pmatrix} 0 \\ \lambda(t)\sigma_- \\ \alpha\xi_2(t) \end{pmatrix}, 0) \tag{3.13}$$

Where σ_- is lower operator of a fictitious two-level system [113] and

$$\lambda(t) = \frac{1}{\sqrt{w(t)}}\xi_1(t)$$
$$w(t) = \int_t^\infty |\xi(s)|^2 ds$$

From the previous sections, we have calculated G triples for input signals, beam splitters and output signals respectively. Since the input part,beam splitters and output part are cascaded, we can calculate the total triple $G_{total} = (S_{total}, L_{total}, H_{total}) = G_{output} \lhd G_{beamsplitter} \lhd G_{input}$ based on the equation introduced in the paper [108]:

$$G_2 \lhd G_1 = (S_2S_1, L_2 + S_2L_1, H_1 + H_2 + Im(L_2^\dagger S_2 L_1)) \tag{3.14}$$

As we have three outputs in parallel, we can write down the total triple G_{total} in the form:

$$G_{total} = (S_{total}, \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix}, H_{total}) \tag{3.15}$$

Where the parameters L_1,L_2 and L_3 are coupling operators for the three channels of total dynamical system and they are:

$$\begin{aligned} L_1 &= i\sqrt{1-\eta}\lambda(t)\sigma_- + \sqrt{\kappa}a_{cavity} \\ L_2 &= \frac{\sqrt{\eta}}{\sqrt{2}}\lambda(t)\sigma_- + \frac{i}{\sqrt{2}}\alpha\xi_2(t) \\ L_3 &= \frac{i\sqrt{\eta}}{\sqrt{2}}\lambda(t)\sigma_- + \frac{1}{\sqrt{2}}\alpha\xi_2(t) \end{aligned}$$

In this dynamical system, we use photon detectors to measure the system. From the survey paper [114], we can obtain the stochastic master equation in photon-counting case as follows:

$$d\rho(t) = L_G^*\rho(t)dt + J_L\rho(t)dN(t) \tag{3.16}$$

where

$$L_G^*X = -i[H,\rho] + D_L^*\rho$$

$$J_L\rho(t) = \frac{L\rho L^\dagger}{tr\{\rho L^\dagger L\}} - \rho$$

and $dN(t) = dY - tr\{\rho L^\dagger L\}$ is a compensated Poisson process of intensity $tr\{\rho L^\dagger L\}$. Since we have two outputs L_2 and L_3 connected to photon detectors, we can write down the quantum filter for this dynamical system as:

$$\begin{aligned} d\rho(t) = \quad & -i[H,\rho] + D_{L_1}^*\rho + D_{L_2}^*\rho + D_{L_3}^*\rho \\ & + J_{L_2}\rho(t)dN_2(t) + J_{L_3}\rho(t)dN_3(t) \end{aligned} \tag{3.17}$$

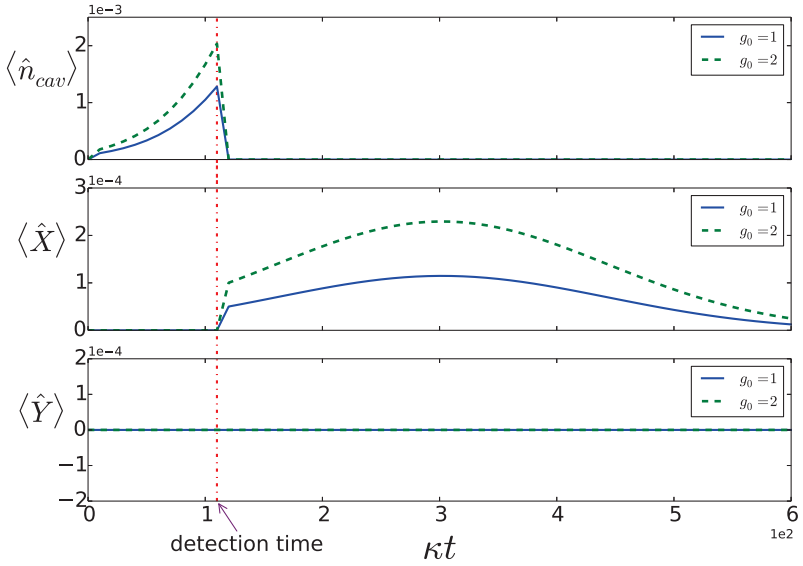


Figure 3.4. Stochastic simulation of a NLA showing the average number of photons in the cavity (top panel) and the X and Y quadratures of the cavity field (middle and bottom panels, respectively) for $\alpha = 0.001$ and the same shape for both the input coherent state and the ancilla single photon. Before a detection, the single photon populates the cavity but the detection projects the field into an approximated amplified version of the input coherent state. Solid blue line correspond to no amplification while dashed green is for $g_0 = 2$.

Figure 3.4 shows the results for two identical input Gaussian pulses $\xi_1(t) = \xi_2(t)$ and a gain $g_0 = 2$ (green-dashed curve). A curve with no gain ($g_0 = 1$) is shown for comparison with a detection event at the same time (solid-blue curve). The panels show, from top to bottom, the average number of photons in the cavity, and the X and Y quadratures of the cavity field.

Figure 3.5 shows Wigner function [110] for cavity state. The left figure shows Wigner function of cavity state immediately before a photon is detected while the right figure is the Wigner function of cavity states immediately after photon detection. The cavity is initially in the vacuum state and the field starts to build up before a detection event happens. This happens because, conditioned on the lack of detections, the single photon could only have been transmitted through the beam splitter

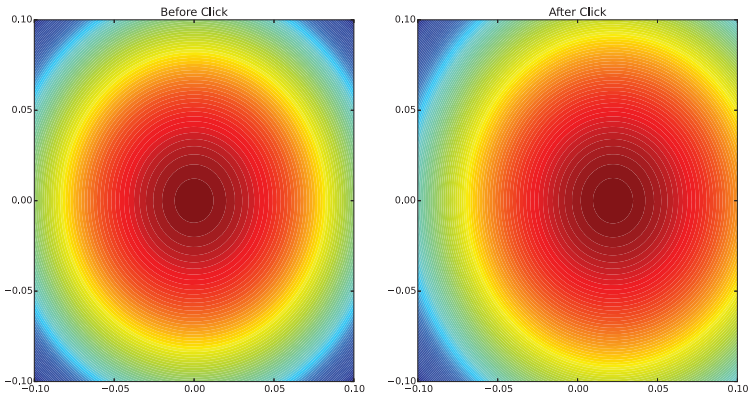


Figure 3.5. Wigner function for cavity state. The left figure shows Wigner function of cavity state immediately before a photon is detected while the right figure is the Wigner function of cavity states immediately after photon detection.

and fed into the cavity. When a photon is detected, then the field inside the cavity changes to the approximated amplified version of the coherent input, as seen in the sudden jump in the X quadrature of the field.

3.2.1.3 Conditional Amplification: detectors with finite time resolution

While in the previous section we discussed the situation where detections were instantaneous and one could resolve the photon temporal shape, in some experimental situations the photon pulses are in the femtoseconds range and therefore shorter than the time resolution of photodetectors. In this case, a detection does not single out a specific time for the event and we need to redefine the effect of measurement on the system. In this case we define a measurement superoperator $\Gamma(t_d)$ as

$$\Gamma(t_d)\rho = \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s)|1_s\rangle\langle 1_s|\rho|1_s\rangle\langle 1_s| \, ds, \tag{3.18}$$

where $[t_d - \frac{\tau}{2}, t_d + \frac{\tau}{2}]$ corresponds to the time resolution window of photodetectors, which is much longer than photon pulse width. $Q(t_d|s)$ is the probability of photon $|1_s\rangle$ measured at time t_d. ρ is the state before measurement and in this case, we have $\rho = |\Psi\rangle_{out}\langle\Psi|_{out}$ according to equation (3.6). So we can obtain the unnormalized conditional state:

$$\begin{aligned}\rho_{out}^{cond} &= \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s)P(s)\left(|0\rangle + g(s)\alpha|1_{\xi_1}\rangle\right)\left(\langle 0| + g(s)\alpha\langle 1_{\xi_1}|\right)\ ds \\ &\approx \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s)P(s)|g(s)\alpha_{\xi_1}\rangle\langle g(s)\alpha_{\xi_1}|\ ds, \end{aligned} \tag{3.19}$$

where $P(s) = e^{-|\alpha|^2}(\frac{\eta}{2}|\xi_1(s)|^2 + \frac{1-\eta}{2}|\alpha|^2|\xi_2(s)|^2)$ according to equation (3.7) and $g(s)$ is the gain ratio

$$\begin{aligned} g(s) &= g_0 \cdot g_{1s} \\ &= \sqrt{\tfrac{1-\eta}{\eta}} * \tfrac{\xi_2(s)}{\xi_1(s)} \end{aligned} \tag{3.20}$$

The result from Eq. (3.19) shows that the effect of finite detector resolution is to generate an output state which is a mix of amplified pure states with gains equivalent to those derived in the perfect time-resolution case. Note that, as in the perfect detection case, the output state is only approximately an amplified version of the input state.

3.2.2 Amplification with two NLA modules

As mentioned before, the output state of the NLA module is only a good approximation for an amplified coherent state when $|g_0 g_1 \alpha| \ll 1$. If the amplitude α of input state is large, one option is to split this state into two smaller coherent states with amplitudes $|\alpha'_{\xi_2}\rangle = |\frac{\alpha\xi_2}{\sqrt{2}}\rangle$, as shown in Figure 3.6. After that, these two smaller coherent states are put into two NLA modules separately. We assume that successful detections at NLA modules 1 and 2 occur at times t_1 and t_2, respectively. From Eq.(3.9), we can obtain the output states of the two NLA modules:

$$\begin{aligned} |\tilde{\Psi}_{NLA1}\rangle &= |0\rangle + g_0 g_{11}\tfrac{\alpha}{\sqrt{2}}|1_{\xi_1}\rangle, \\ |\tilde{\Psi}_{NLA2}\rangle &= |0\rangle + g_0 g_{12}\tfrac{\alpha}{\sqrt{2}}|1_{\xi_1}\rangle, \end{aligned} \tag{3.21}$$

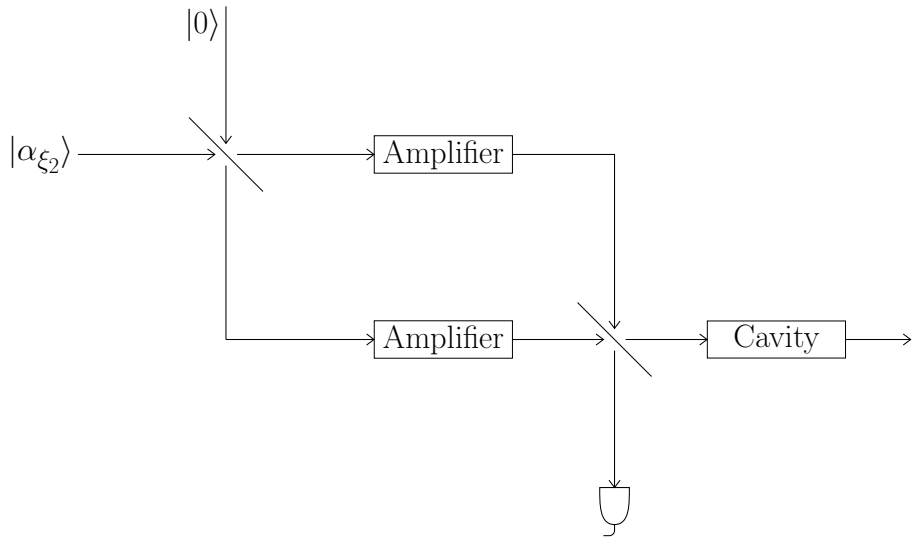


Figure 3.6. If the amplitude α of input state is large, one option is to split this state into two smaller coherent states with amplitudes $|\alpha'_{\xi_2}\rangle = |\frac{\alpha_{\xi_2}}{\sqrt{2}}\rangle$. After that, these two smaller coherent states are put into two NLA modules separately.

where $g_0 = \sqrt{\frac{1-\eta}{\eta}}$ is the single mode amplification gain, and $g_{11} = \frac{\xi_2(t_1)}{\xi_1(t_1)}$ and $g_{12} = \frac{\xi_2(t_2)}{\xi_1(t_2)}$ are the amplification ratios induced by differences in the pulse shapes. Note that we assumed that the two ancilla photons have the same shape $\xi_1(t)$ and we are considering the situation of perfect detector resolution. If we put these two amplified states into another balanced beamsplitter and observe no photon click in one output, then the recombined state from the other output will be

$$|\tilde{\Psi}\rangle_{out} = |0\rangle + g_0\frac{g_{11}+g_{12}}{2}\alpha|1\rangle_{\xi_1} + \frac{g_0^2 g_{11} g_{12}\alpha^2}{2\sqrt{2}}|2\rangle_{\xi_1}, \tag{3.22}$$

which, again, when properly normalized and in the limit of small gain and small input amplitude, can be approximated by a coherent state

$$|\tilde{\Psi}\rangle_{out} \approx |g_0\frac{g_{11}+g_{12}}{2}\alpha\rangle_{\xi_1}. \tag{3.23}$$

As in the case of a single NLA module, we see that the amplification ratio $g_0\frac{g_{11}+g_{12}}{2}$ is affected by the photon detection times. If the two photons are detected at the same time $t_1 = t_2 = t_d$, we obtain $g_{11} = g_{12} = g_1$ and the amplification ratio would be the same as that of that of a single module situation but with a higher fidelity $e^{\frac{-|g_0 g_1 \alpha|^2}{2}}\sqrt{\frac{|g_0 g_1 \alpha|^4}{4} + |g_0 g_1 \alpha|^2 + 1}$.

Figure 3.7 shows a stochastic simulation for the two modules case for $g_0 = 2$ (green-dashed) and the no gain case (solid-blue) for comparison. The two input pulses are Gaussian with the same width but shifted in time. In this case, the exact gains will depend on the detection times, as we have shown in our analytical calculations.

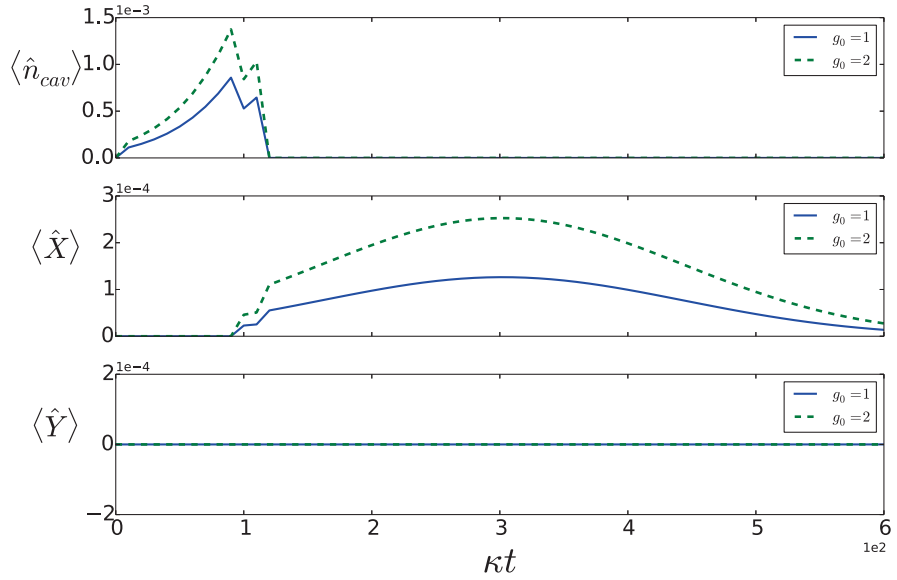


Figure 3.7. Amplification with two NLA modules: panels are the same as in Figure 3.4 but this time the input fields are mismatched. The gain g_1 will now depend on the exact detection times.

3.3 Continuous-mode photon addition-subtraction based NLA

In Section 2.2.3, a photon addition-subtraction based NLA scheme is introduced. The idea is to approximate a small coherent state $|\alpha\rangle$ as $|0\rangle + \alpha|1\rangle$ firstly and then apply a creation operator and an annihilation operator to this state so that the output state is $|\Psi_{out}\rangle = |0\rangle + 2\alpha|1\rangle \approx |2\alpha\rangle$. As shown in Figure 3.8, we can also analyse this photon addition-subtraction based NLA scheme dynamically. Instead of discrete modes in Figure 2.3, we have an input state $|\alpha_{\xi_1}\rangle$ with pulse shape ξ_1. ξ_2 represents the temporal profile of the added photon while ξ_3 is the temporal profile of

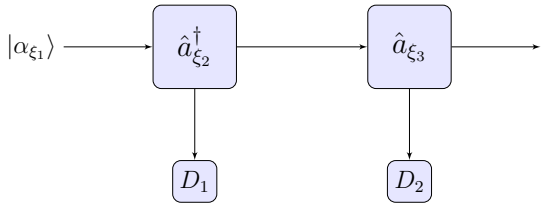


Figure 3.8. As shown in this figure, we can also analyse this photon addition-subtraction based NLA scheme dynamically. Instead of discrete modes in Figure 2.3, we have an input state $|\alpha_{\xi_1}\rangle$ with pulse shape ξ_1. The continuous mode creation operator $\hat{a}^\dagger_{\xi_2}$ and the annihilation operator $\hat{a}_{\xi_3}$ are applied to the input state.

photon absorbed by photon detectors. After the continuous mode creation operator $\hat{a}^\dagger_{\xi_2}$ and the annihilation operator $\hat{a}_{\xi_3}$ are applied, the output state can be written as:

$$
\begin{aligned}
|\Psi_{out}\rangle &= \hat{a}_{\xi_3}\hat{a}^\dagger_{\xi_2}|\alpha_{\xi_1}\rangle \\
&\approx \hat{a}_{\xi_3}\hat{a}^\dagger_{\xi_2}(|0\rangle + \alpha|1_{\xi_1}\rangle) \\
&= \hat{a}_{\xi_3}\hat{a}^\dagger_{\xi_2}(1+\alpha\hat{a}^\dagger_{\xi_1})|0\rangle \\
&= ([\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}] + \hat{a}^\dagger_{\xi_2}\hat{a}_{\xi_3})(1+\alpha\hat{a}^\dagger_{\xi_1})|0\rangle \\
&= ([\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}] + \alpha[\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + \alpha\hat{a}^\dagger_{\xi_2}\hat{a}_{\xi_3}\hat{a}^\dagger_{\xi_1})|0\rangle \\
&= ([\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}] + \alpha[\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + \alpha\hat{a}^\dagger_{\xi_2}([\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_1}] + \hat{a}^\dagger_{\xi_1}\hat{a}_{\xi_3}))|0\rangle \\
&= [\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}]|0\rangle + \alpha([\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + [\hat{a}_{\xi_3},\hat{a}^\dagger_{\xi_1}]\hat{a}^\dagger_{\xi_2})|0\rangle
\end{aligned}
\tag{3.24}
$$

where the commutation of an annihilation operator and a creation operator with different pulse shapes $[\hat{a}_{\xi_m},\hat{a}^\dagger_{\xi_n}]$ can be calculated as:

$$
\begin{aligned}
[\hat{a}_{\xi_m}, \hat{a}^\dagger_{\xi_n}] &= [\int \xi_m(t)\hat{a}_t dt, \int \xi_n(t)\hat{a}^\dagger_t dt] \\
&= \int \xi_m(t1)dt1 \cdot \int \xi_n(t2)dt2 \cdot [\hat{a}_{t1}, \hat{a}^\dagger_{t2}] \\
&= \int \xi_m(t1)dt1 \cdot \int \xi_n(t2)dt2 \cdot \delta(t1-t2) \\
&= \int \xi_m(t1)\xi_n(t1)dt1 \\
&= \int \xi_m(t) \cdot \xi_n(t)dt
\end{aligned} \tag{3.25}
$$

If we set $|\varphi_1\rangle = ([\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]\hat{a}^\dagger_{\xi_2})|0\rangle$, then the $\langle\varphi_1||\varphi_1\rangle$ can be obtained as follows:

$$
\begin{aligned}
\langle\varphi_1||\varphi_1\rangle &= \langle 0|([\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]\hat{a}_{\xi_1} + [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]\hat{a}_{\xi_2})([\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]\hat{a}^\dagger_{\xi_2})|0\rangle \\
&= \langle 0|[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]^2\hat{a}_{\xi_1}\hat{a}^\dagger_{\xi_1}|0\rangle + \langle 0|[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]^2\hat{a}_{\xi_2}\hat{a}^\dagger_{\xi_2}|0\rangle \\
&+ [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}][\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]\langle 0|(\hat{a}_{\xi_1}\hat{a}^\dagger_{\xi_2} + \hat{a}_{\xi_2}\hat{a}^\dagger_{\xi_1})|0\rangle \\
&= [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]^2 + [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]^2 + 2 * [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}][\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}][\hat{a}_{\xi_2}, \hat{a}^\dagger_{\xi_1}]
\end{aligned} \tag{3.26}
$$

Then the unnomalized output state in Equation 3.24 can be rewritten as follows:

$$
\begin{aligned}
|\Psi_{out}\rangle &= [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]|0\rangle + \alpha\sqrt{\langle\varphi_1|\varphi_1\rangle}(\frac{[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]}{\sqrt{\langle\varphi_1|\varphi_1\rangle}}\hat{a}^\dagger_{\xi_1} + \frac{[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]}{\sqrt{\langle\varphi_1|\varphi_1\rangle}}\hat{a}^\dagger_{\xi_2})|0\rangle \\
&= [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]|0\rangle + \alpha\sqrt{\langle\varphi_1|\varphi_1\rangle}|1_{\xi_4}\rangle \\
&= [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}](|0\rangle + \alpha\frac{\sqrt{\langle\varphi_1|\varphi_1\rangle}}{[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]}|1_{\xi_4}\rangle \\
&\approx [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]|\frac{\sqrt{\langle\varphi_1|\varphi_1\rangle}}{[\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]}\alpha_{\xi_4}\rangle
\end{aligned} \tag{3.27}
$$

where the single photon $|1_{\xi_4}\rangle$ is $\frac{|\varphi_1\rangle}{\sqrt{\langle\varphi_1|\varphi_1\rangle}} = \frac{([\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_2}]\hat{a}^\dagger_{\xi_1} + [\hat{a}_{\xi_3}, \hat{a}^\dagger_{\xi_1}]\hat{a}^\dagger_{\xi_2})|0\rangle}{\sqrt{\langle\varphi_1||\varphi_1\rangle}}$. So the input coherent state $|\alpha\rangle$ is amplified with an amplification gain G as follows:

$$
\begin{aligned}
G &= \frac{\sqrt{\langle\varphi_1|\varphi_1\rangle}}{[\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_2}]} \\
&= \frac{\sqrt{[\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_2}]^2 + [\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_1}]^2 + 2 * [\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_2}][\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_1}][\hat{a}_{\xi_2}, \hat{a}^{\dagger}_{\xi_1}]}}{[\hat{a}_{\xi_3}, \hat{a}^{\dagger}_{\xi_2}]}
\end{aligned} \tag{3.28}
$$

At the same time, the pulse shape of input state $|\alpha_{\xi_1}\rangle$ is changed into ξ_4 as described in Equation 3.27. If the special case comes when $\xi_1(t) = \xi_2(t) = \xi_3(t)$, then the amplification gain is $G = 2$, which is the same as the discrete analysis in the paper [73].

3.3.1 Conditional Amplification: perfect detection case

As introduced in the paper [73], the continuous mode creation operator $\hat{a}^{\dagger}_{\xi_2}$ and the annihilation operator $\hat{a}_{\xi_3}$ are induced by single photon click D_1 and D_2 respectively. In this sub-section, we discuss the situation where the time resolution of the photo-detectors is much shorter than the temporal width of the photon pulses, as in the case of experiments with solid-state quantum memories. Let's consider the case where at the time $t2$ and $t3$, two single photons are detected at D_1 and D_2 respectively. Then the output state can be obtained as:

$$
\begin{aligned}
|\Psi_{out}\rangle &\approx \hat{a}_{t3}\hat{a}^{\dagger}_{t2}|\alpha_{\xi_1}\rangle \\
&= [\hat{a}_{t3}, \hat{a}^{\dagger}_{t2}](|0\rangle + \alpha\frac{\sqrt{\langle\varphi_1|\varphi_1\rangle}}{[\hat{a}_{t3}, \hat{a}^{\dagger}_{t2}]}|1_{\xi_4}\rangle) \\
&\approx [\hat{a}_{t3}, \hat{a}^{\dagger}_{t2}]|\frac{\sqrt{\langle\varphi_1|\varphi_1\rangle}}{[\hat{a}_{t3}, \hat{a}^{\dagger}_{t2}]}\alpha_{\xi_4}\rangle
\end{aligned} \tag{3.29}
$$

If $t2 \neq t3$, the two single photon clicks happen at different time window, then we have $[\hat{a}_{t3}, \hat{a}^{\dagger}_{t2}] = 0$. Then the output state is not a coherent state but a single photon $|1_{t2}\rangle$. If this happen, it means the annihilation operator $\hat{a}_{\xi_3}$ destroy the single photon term of input coherent state $|\alpha_{\xi_1}\rangle$, leaving the single photon state $|1_{t2}\rangle$ which is created by $\hat{a}^{\dagger}_{\xi_2}$.

If $t2 = t3 = t_d$, the amplification gain is $G = \frac{\delta(0)+\xi_1(t_d)}{\delta(0)} \approx 1$ and the input is hardly amplified. The pulse shape also remains the same as that of input state because now we have $\xi_4 = \xi_1$. From another perspective, we can see that the more the input state $|\alpha_{\xi_1}\rangle$ gather at the time t, the more amplification gain we have.

3.3.2 Conditional Amplification: detectors with finite time resolution

While in the previous section we discussed the situation where detections were instantaneous and one could resolve the photon temporal shape, in some experimental situations the photon pulses are in the femtoseconds range and therefore shorter than the time resolution of photodetectors. In this case, a detection does not single out a specific time for the event and we need to redefine the effect of measurement on the system. Suppose the two photon detectors are the same and the detection time $t2 = t3 = t_d$, we define a measurement superoperator $\Gamma 1(t_d)$ as

$$\Gamma 1(t_d)\rho = \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s2)Q(t_d|s1)\hat{a}_{s2}\hat{a}_{s1}^{\dagger}\rho\hat{a}_{s1}\hat{a}_{s2}^{\dagger}\, ds1ds2, \tag{3.30}$$

where $[t_d - \frac{\tau}{2}, t_d + \frac{\tau}{2}]$ corresponds to the time resolution window of photodetectors, which is much longer than photon pulse width. $Q(t_d|s)$ is the probability of photon $|1_s\rangle$ measured at time t_d. ρ is the state before measurement and in this case, we have $\rho = |\alpha_{\xi_1}\rangle\langle\alpha_{\xi_1}|$. So we can obtain the unnormalized conditional state:

$$\begin{aligned}
\rho_{out}^{cond} &= \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s2)Q(t_d|s1)[\hat{a}_{s2}, \hat{a}_{s1}^{\dagger}]^2(|0\rangle + \alpha\frac{\sqrt{\langle\varphi_1||\varphi_1\rangle_{s1,s2}}}{[\hat{a}_{s2}, \hat{a}_{s1}^{\dagger}]}|1_{\xi 4}\rangle) \\
&\times (\langle 0| + \alpha\frac{\sqrt{\langle\varphi_1||\varphi_1\rangle_{s1,s2}}}{[\hat{a}_{s2}, \hat{a}_{s1}^{\dagger}]}\langle 1_{\xi 4}|)\; ds1ds2, \\
&\approx \int_{t_d-\frac{\tau}{2}}^{t_d+\frac{\tau}{2}} Q(t_d|s)^2|\alpha_{\xi_1}\rangle\langle\alpha_{\xi_1}|\; ds,
\end{aligned} \tag{3.31}$$

Unlike the quantum scissor based NLA, the effect of finite detector resolution here is to generate an output state which is approximately a pure state. Interestingly,

this generated output state is approximately the same as the perfection detection case.

3.4 Conclusions and Discussion

In this chapter, we firstly investigate the continuous mode performance of a quantum scissor based NLA scheme for coherent states, showing the effect of pulse shapes in the NLA gain. The pulse shape of the output signal is the same as the one from the auxiliary single photon, while its amplitude is influenced by both the input coherent state and the NLA parameters. Interestingly, gains higher than in the single mode case can be obtained for mismatched pulses, however, it comes at the expense of lower fidelities. The mismatch could also introduce an attenuation, depending on the detection times. This shows that in practical situations, one would have to have a good knowledge of the input pulse for the amplification to be successful.

We also discuss the continuous mode operation of photon addition-subtraction based NLA scheme. If we take the example of [73] and apply the continuous mode analysis we get the output state $|\Psi_{out}\rangle = \hat{a}_{\xi_3}\hat{a}^{\dagger}_{\xi_2}(1 + \alpha\hat{a}^{\dagger}_{\xi_1})|0\rangle$, where ξ_1 is the shape of the input state to be amplified and ξ_2 and ξ_3 the shapes of the field corresponding to the processes of addition and subtraction of photons. For $\xi_1(t) = \xi_2(t) = \xi_3(t)$ one recovers the single mode gain but mismatched shapes would have similar effects as quantum scissor based NLA scheme.

In order to compensate attenuation during communication channels, quantum amplifiers are needed to be incorporated in the building of quantum repeaters. Since the quantum states operate in continuous mode in practise, our analysis of NLA might be used in the design of quantum repeaters in the future.

Chapter 4

Generation of Distributed W-States over Long Distances

THIS chapter describes the structure of distributed W-states generation over long distances.

4.1 Introduction

Ultra-secure quantum communication between distant locations requires distributed entangled states between nodes. Various methodologies have been proposed to tackle this technological challenge, of which the so-called DLCZ protocol is the most promising and widely adopted scheme. This project aims to extend this well-known protocol to a multi-node setting where the entangled W-state is generated between nodes over long distances. The generation of multipartite W-states is the foundation of quantum networks, paving the way for quantum communication and distributed quantum computation.

The rest of this chapter is structured as follows: In Section 4.2, we introduce a methodology which can be used to generate distributed W-states. These generated distributed W-states can be used to generate other distributed W-states on larger scales as discussed in Section 4.3. After that, it is proved that W-states could be used to perform teleportation in Section 4.4. In Section 4.5 we conclude and discuss some open questions for future research.

4.2 Generation of distributed W-states

4.2.1 Atomic ensembles and photons

As introduced in [78], we can use an atomic ensemble to generate a quantum state $|\phi\rangle = (1 + \sqrt{p}S^\dagger a^\dagger)|0\rangle$ where $\sqrt{p}$ represents the low probability of atomic ensemble excitation, $S^\dagger$ denotes excitation operator for the atomic ensemble, and $a^\dagger$ is the single-photon creation operator. If we have $N + 1$ distant nodes, we can generate $N+1$ photons and the states can be written as $|\phi_i\rangle = (1+\sqrt{p}S_i^\dagger a_i^\dagger)|0\rangle \quad (0 \leq i \leq N)$. We call the first node which has the state $|\phi_0\rangle = (1 + \sqrt{p}S_0^\dagger a_0^\dagger)|0\rangle$ the main node, and the remaining N nodes, whose states are $|\phi_i\rangle = (1 + \sqrt{p}S_i^\dagger a_i^\dagger)|0\rangle \quad (1 \leq i \leq N)$, normal nodes.

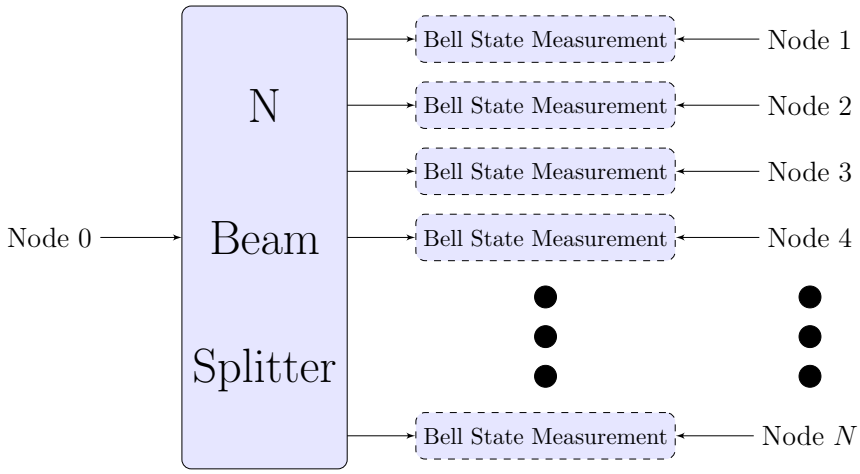


Figure 4.1. The main node state is first divided into N branches by multiple beam splitters or an N-channel beam splitter. Together with the N normal node states, the N main node state branches are guided to N Bell state measurement apparatuses. If we observe a single photon click in every Bell state measurement apparatus, we have achieved entanglement between these $N+1$ distant nodes.

4.2.2 Implementation

As shown in Figure 4.1, this main node state $|\phi_0\rangle = (1+\sqrt{p}S_0^\dagger a_0^\dagger)|0\rangle$ is first divided by multiple beam splitters or an N-channel beam splitter. The N output branches can be written as:

$$|\Psi_{main}\rangle = (1+\sqrt{p}\frac{1}{\sqrt{N}}S_0^\dagger \sum_{i=1}^{N} a_{0,b_i}^\dagger)|0\rangle, \tag{4.1}$$

where $a_{0,b_i}^\dagger$ are the creation operators for the different branches.

We then put the N normal nodes into different channels as shown on the right hand side of Figure 4.1. The resulting normal node states can be written as:

$$\begin{aligned} |\Psi_{normal}\rangle &= |\phi_1\rangle|\phi_2\rangle|\phi_3\rangle\cdot\cdot\cdot\cdot\cdot|\phi_N\rangle \\ &= \prod_{i=1}^{N}(1+\sqrt{p}S_i^\dagger a_{i,b_i}^\dagger)|0\rangle, \end{aligned} \tag{4.2}$$

where $a^{\dagger}_{i,b_i}$ are the creation operators of different nodes in different channels. $S^{\dagger}_i$ are the excitation operators of atomic ensembles in different nodes.

4.2.3 Bell State Measurement

The N branches of the main node state $|\Psi_{main}\rangle$ and the N normal node states $|\Psi_{normal}\rangle$ are guided into N Bell state measurement apparatuses as shown in Figure 4.1. We then do the same Bell state measurement as for the DLCZ method [78]. If we detect a single photon in either of the two-photon detectors in every Bell state measurement apparatus from 1 to N, the post-selected state on the atomic ensemble degrees of freedom can be written as:

$$|\Psi_{conditional}\rangle = \frac{1}{\sqrt{2}}(S_0 + \frac{1}{\sqrt{N}}\sum_{i=1}^{N}(S_i))\prod_{j=0}^{N}(S_j^{\dagger})|0\rangle \tag{4.3}$$

In this way we achieve entanglement between $N+1$ distant nodes. With this approach, we can generate two entanglement pairs states: $|\Psi_{conditional,A}\rangle$ and $|\Psi_{conditional,B}\rangle$. As shown in Figure 4.2, we can convert the stored atomic excitations of the two main nodes (Node 0_A and Node 0_B) into light and guide it into a beam splitter. If a single click is observed, we obtain entanglement between $2N$ nodes (N main nodes in group A and N in group B) as follows:

$$|\Psi_{final}\rangle = (\frac{1}{\sqrt{2N}}\sum_{i=1}^{N}(S_{i,A}) + \frac{1}{\sqrt{2N}}\sum_{i=1}^{N}(S_{i,B}))\prod_{i=1}^{N}(S_{i,A}^{\dagger})\prod_{i=1}^{N}(S_{i,B}^{\dagger})|0\rangle \tag{4.4}$$

The resulting state $|\Psi_{final}\rangle$ is a W-state between $2N$ distant nodes. In this manner, we generate entanglement between $2N$ distributed nodes. If $\mathbf{P}$ denotes the probability of successfully generating an entanglement between 2 nodes in the DLCZ protocol, the probability to generate entanglement between $2N$ nodes is $2(\frac{\mathbf{P}}{2})^{2N}$.

If $N = 2$, we generate an entanglement between 4 nodes and the resulting state can be written as:

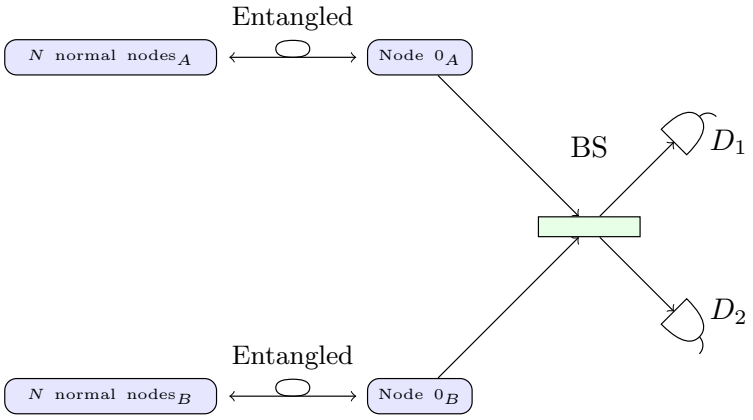


Figure 4.2. We can convert the stored atomic excitations of the two main nodes (Node 0_A and Node 0_B) into light and guide it into a beam splitter. If a single click is observed, we obtain entanglement between $2N$ nodes (N main nodes in group A and N in group B).

$$\begin{aligned} |\Psi_{final}\rangle &= \frac{1}{2}(S_0^\dagger S_1^\dagger S_2^\dagger + S_1^\dagger S_2^\dagger S_3^\dagger + S_0^\dagger S_2^\dagger S_3^\dagger + S_0^\dagger S_1^\dagger S_3^\dagger)|0\rangle \\ &= \frac{1}{2}(|0111\rangle + |1011\rangle + |1101\rangle + |1110\rangle) \end{aligned} \tag{4.5}$$

If $N = 1$, we generate entanglement between two nodes, similar to the DLCZ method. We can consider the DLCZ method as a special case ($N = 1$).

4.3 Entanglement Swapping

With the DLCZ implementation [78], we can generate entanglement between nodes A and D from two entanglement pairs $A - B$ and $C - D$ through a method called 'entanglement swapping'. In this way, we can form an entanglement pair over a longer distance using two entanglement pairs over shorter distances. By continuing to perform entanglement swapping, we can achieve entanglement between two nodes over significantly longer distances.

From the last section, we can obtain a W-state $|\Psi_{w1}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N}(S_i)\prod_{i=0}^{N}(S_i^\dagger)|0\rangle$ as shown on the left side of Figure 4.3. We prepare another entanglement pair $|\Psi_{pair}\rangle =$

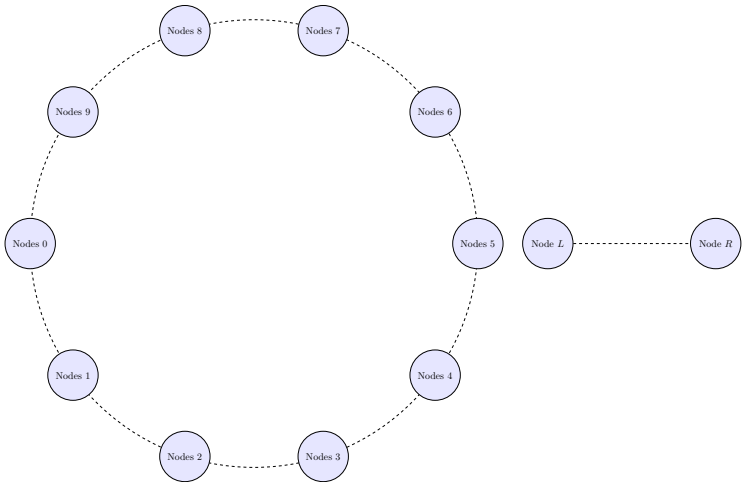


Figure 4.3. The entanglement swapping method can also be used for W-states. On the left side of this figure, we have entanglement between N nodes (here $N = 10$). We have entanglement between two nodes $Node\ L$ and $Node\ R$ as shown on the right side. Using the same entanglement swapping method as for the DLCZ protocol [78], we substitute $Node\ 5$ with $Node\ R$ and thereby generate a new W-state.

$\frac{1}{\sqrt{2}}(S_L^\dagger + S_R^\dagger)|0\rangle$ as shown on the right hand side. Using the same entanglement swapping as for the DLCZ protocol [78], we can obtain a state $|\Psi_{swap}\rangle$ as follows:

$$|\Psi_{swap}\rangle = \frac{1}{\sqrt{N}}(\sum_{i=0}^{4}(S_i) + S_R + \sum_{i=6}^{N}(S_i))\prod_{i=0}^{N}(S_i^\dagger)|0\rangle \tag{4.6}$$

From Equation 4.6, we can see that we substituted $Node\ 5$ with $Node\ R$ and thereby generated a new W-state. With this method, we can substitute every node of the previous W-state and form a new W-state with a bigger circle as shown in Figure 4.4. Continuing to perform this entanglement swapping, we can finally obtain a W-state on a larger scale.

4.4 Teleportation via W-states

Suppose we have a 3-qubit W-state which is shared between three distant nodes- Alice, Bob and Charlie:

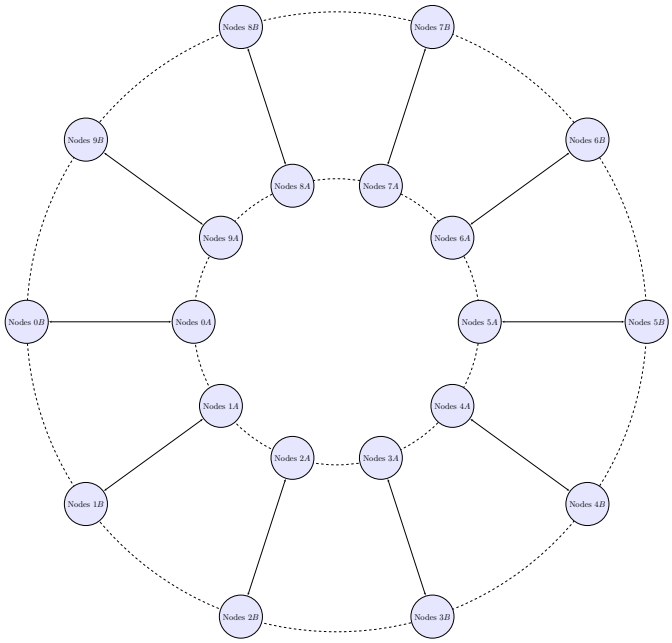


Figure 4.4. We can substitute every node of the previous W-state and form a new W-state on a larger scale.

$$|W\rangle = \frac{1}{\sqrt{3}}(|1\rangle_A|0\rangle_B|0\rangle_C + |0\rangle_A|1\rangle_B|0\rangle_C + |0\rangle_A|0\rangle_B|1\rangle_C) \tag{4.7}$$

Now Alice has another qubit $|\varphi\rangle_Q = \alpha|0\rangle_Q + \beta|1\rangle_Q$ and she wants to teleport this qubit to Charlie. The whole system $|\Phi_{whole}\rangle$ now is the tensor product of $|\varphi\rangle_Q$ and $|W\rangle$ as follows:

$$
\begin{aligned}
|\Phi_{whole}\rangle &= |\varphi\rangle_Q \otimes |W\rangle \\
&= \frac{1}{\sqrt{3}}(\alpha|0\rangle_Q + \beta|1\rangle_Q) \otimes (|1\rangle_A|0\rangle_B|0\rangle_C + |0\rangle_A|1\rangle_B|0\rangle_C + |0\rangle_A|0\rangle_B|1\rangle_C) \\
&= \frac{1}{\sqrt{6}}\alpha((|\Psi_{10}\rangle_{QA} + |\Psi_{11}\rangle_{QA})|0\rangle_B|0\rangle_C + (|\Psi_{00}\rangle_{QA} + |\Psi_{01}\rangle_{QA})(|1\rangle_B|0\rangle_C + |0\rangle_B|1\rangle_C)) \\
&\quad + \frac{1}{\sqrt{6}}\beta((|\Psi_{00}\rangle_{QA} - |\Psi_{01}\rangle_{QA})|0\rangle_B|0\rangle_C + (|\Psi_{10}\rangle_{QA} - |\Psi_{11}\rangle_{QA})(|1\rangle_B|0\rangle_C + |0\rangle_B|1\rangle_C)) \\
&= \frac{1}{\sqrt{6}}(|\Psi_{00}\rangle_{QA}(\alpha|10\rangle_{BC} + \alpha|01\rangle_{BC} + \beta|00\rangle_{BC}) \\
&\quad + |\Psi_{01}\rangle_{QA}(\alpha|10\rangle_{BC} + \alpha|01\rangle_{BC} - \beta|00\rangle_{BC}) \\
&\quad + |\Psi_{10}\rangle_{QA}(\alpha|00\rangle_{BC} + \beta|10\rangle_{BC} + \beta|01\rangle_{BC}) \\
&\quad + |\Psi_{11}\rangle_{QA}(\alpha|00\rangle_{BC} - \beta|10\rangle_{BC} - \beta|11\rangle_{BC})) \qquad (4.8)
\end{aligned}
$$

where $|\Psi_{00}\rangle$, $|\Psi_{01}\rangle$, $|\Psi_{10}\rangle$ and $|\Psi_{11}\rangle$ are four Bell states as follows:

$$
\begin{aligned}
|\Psi_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Psi_{01}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Psi_{10}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (4.9)
\end{aligned}
$$

After Alice performs Bell state measurement on the quantum pair $|\varphi\rangle_Q|\phi\rangle_A$, we obtain one of the four Bell states and the corresponding post selection state could be obtained from Equation 4.8. Then Bob measures his qubit. If Bob observes the state $|1\rangle_B$, then the quantum information can not be teleported to Charlie. If Bob observes the state $|0\rangle_B$, then Charlie can deduce the teleported state by manipulating his own qubit. The required manipulation operator is determined by the Bell state measurement result of Alice:

If $|\Psi_{00}\rangle$ is measured: The operator $\hat{\sigma}_x$ is needed to deduce the teleported state.

If $|\Psi_{01}\rangle$ is measured: The operator $\hat{\sigma}_x\hat{\sigma}_z$ is needed to deduce the teleported state.

If $|\Psi_{10}\rangle$ is measured: The operator I is needed to deduce the teleported state.

If $|\Psi_{11}\rangle$ is measured: The operator $\hat{\sigma}_z$ is needed to deduce the teleported state.

4.5 Summary

We have shown a method to generate an entanglement between multiple distant nodes by creating a W-state shared between them. Since W-states can be used to teleport quantum states, we may perform quantum teleportation with the distributed W-states generated using our methodology.

As the research field of quantum computing progresses, more complicated quantum algorithms are being proposed. In the future, when a single quantum computer is not capable of implementing such complicated algorithms, we may develop quantum algorithms to utilize quantum-computing resources in different locations with distributed W-states.

Like the DLCZ protocol, this methodology is based on a Mach-Zehnder type interference. As discussed in [81], the Hong-Ou-Mandel type interference is much less sensitive to path length instabilities. We may develop a method based on a Hong-Ou-Mandel type interference to generate distributed W-states over long distances.

As shown in Figure 4.1, the multiple nodes are classified as 1 main node and N normal nodes. In the future, we may implement the main node state in a satellite and the N normal nodes in N cities covered by the trajectory of the satellite. We can thus achieve an entanglement between multiple nodes in different cities.

Chapter 5

Multiparty QKD for Wireless Sensor Networks

IN this chapter, we explain the importance and significance of multiparty QKD. Some scenarios requiring multiparty QKD are described for this explanation. A multiparty QKD scheme is presented in this chapter. Some technical challenges to practically implement this multiparty QKD scheme are mentioned at the end of this chapter.

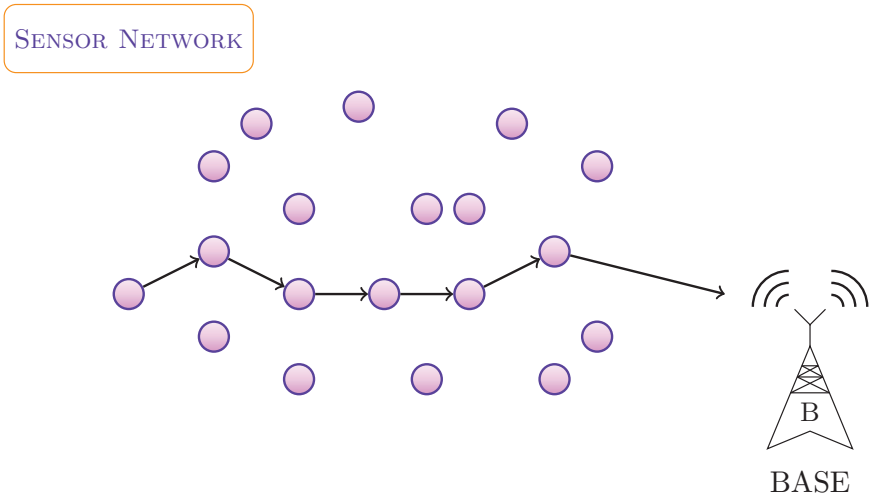


Figure 5.1. From this figure, we can see that there are a large number of nodes which are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure. The multiple sensor nodes can cooperatively pass their data through the network to a main location. The main location (sometimes called base) can also control sensor nodes through the network.

5.1 Introduction

Wireless sensor networks were initially motivated by military applications such as battlefield surveillance and control of unmanned aircraft vehicles (UAV). Nowadays WSNs are widely used in many industrial and consumer applications such as industrial process monitoring and control, bushfire monitoring, and so on. As we can see in Figure 5.1, there are a large number of nodes that are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure. Multiple sensor nodes can cooperatively pass their data through the network to main location. The main location (sometimes called base) can also control sensor nodes through the network.

5.2 Significance

Although WSN has been a rather mature research field, the security in WSNs is much less intensively studied than networks formation and routing algorithms. Since sensor nodes are often deployed in the malicious environment, methodologies should be applied to guarantee secure communication between multiple sensor nodes and the base. Let us assume that there are n sensor nodes in the WSN as shown in Figure 5.1. If an incident happens and m specific sensor nodes are needed to undertake a task, a task-specific cryptography key is needed to be produced and distributed between the base and the engaged m nodes. Consider the following two scenarios as examples:

- A fleet of n ships is dispatched from the base to patrol a big sea area. These n ships form a wireless sensor network and can communicate with each other. In the case that some intruders are observed in this sea area. The base may estimate that m ships in the vicinity of intruding incident are required to intercept the intruders while the rest of ships keep patrolling. In order to guarantee secure communication between these closest m ships, a shared job-specific (only for this intercepting job) cryptography key should be produced and distributed between the m ships and the base.

- The government of Nation Alpha sends n spies to n cities of Nation Beta. Before the dispatching, a cryptography key is produced and shared by the n spies and the headquarter. After a duration of time, some spies betray their duties due to counterespionage. It is confirmed that there are still m reliable active spies. To guarantee secure communication between these m reliable spies and the headquarter, a new cryptography key should be produced and distributed among the $m + 1$ nodes.

As it is proved that QKD can provide a reliable solution to produce secret shared cryptography key between two distant nodes, it should be applicable to extend the two node QKD schemes to a multipartite setup, by which cryptography keys can

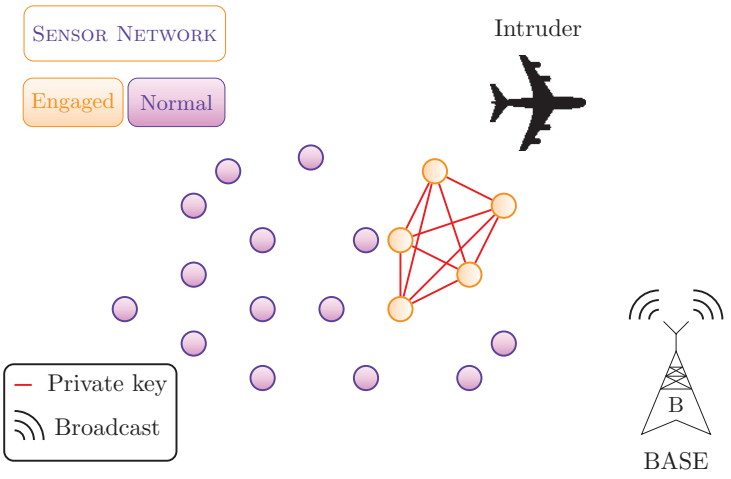


Figure 5.2. It is assumed that there are n sensor nodes in this WSN. If a incident happens and m specific sensor nodes are needed to undertake a task, a task-specific cryptography key is needed to be produced and distributed between the base and the engaged m nodes.

be produced and distributed between multiple distant nodes. For example, we can directly extend the BB84 protocol as follows:

1. Alice sends the randomly chosen single photon states to m receivers (Bob1, Bob2 $\cdots\cdots$ Bob$m$). Note that every Bob expects to receive the same qubit sequence of t qubits.

2. Randomly and independently, Every Bob chooses one of the two bases to measure the received quantum states. If he chooses the same basis as Alice for a quantum state, he will observe the same bit for this quantum state. Otherwise, he will only get uncorrelated bit.

3. After measuring all of the receiving quantum states, Bob$i$ records a bit string b_i of t bits. This bit string is called raw key.

4. Alice and all the Bobs announce via public classical channel their chosen bases for every quantum state.

5. After comparing their chosen bases, the recorded bits from different chosen bases are discarded. These $t1$ bits are left. This $t1$ bits are called sifted key. Because all the bases are chosen independently and randomly from two bases, $t1$ is expected to be about $t/2^m$.

If the cryptography key is needed to be distributed among a large number of sensor nodes (m is big), the success probability becomes extremely small ($1/2^m$). It means that in order to produce and distribute one bit of secret key, 2^m quantum states are expected to be sent to all the m Bobs according to this multiparty BB84 protocol. In most of WSN applications, this time-consuming scheme is not accepted.

We can also directly extend the SARG 04 protocol by preparing $m+1$-bit strings, a, $b1$, $b2$, $\cdots\cdots$, bm, each of t bits. This multiparty SARG 04 protocol is also confronted with the same efficiency problem as multiparty BB84 protocol. In this chapter, we propose a deterministic multiparty QKD scheme by which cryptography key can be produced and distributed between multiple sensor nodes deterministically and efficiently.

5.3 Preparation of Bell states

The Bell states are four specific maximally entangled quantum states of two qubits and we can write these four Bell states as follows:

$$\begin{aligned}
|\Psi_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Psi_{01}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Psi_{10}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Psi_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{5.1}$$

As shown in Figure 5.3, This multiparty QKD scheme begins with the preparation of m Bell states as follows:

$$\bigotimes_{k=1}^{m} \frac{1}{\sqrt{2}}(|0_{base\_k}0_{sensor\_k}\rangle + |1_{base\_k}1_{sensor\_k}\rangle) \tag{5.2}$$

where $base\_k$ denotes the kth prepared qubit in the base while $sensor\_k$ is the qubit prepared in the quantum memory of kth sensor node. With these m Bell states, we have m entanglement pairs between base and m sensor nodes respectively. Note that the m entanglement pairs can be prepared in advance, before the deployment of sensor nodes. Before the deployment of a sensor node, it is in the same location of the base and the two qubits of entanglement pair can be distributed locally. Taking the scenario of patrolling ships for example, the entanglement pairs can be distributed between a ship and the base locally during replenishment. If the wireless sensor network is composed with UAVs, entanglement pairs can be distributed between the base and a UAV during its recharging time. In this protocol, we assume that good quantum memories are available to keep stored qubits unchanged during work.

5.4 Preparation of GHZ states

A Greenberger–Horne–Zeilinger(GHZ) state is a certain type of entangled quantum state which involves at least three quantum subsystems or particles. If all the subsystems are two-dimensional, then it becomes a qubit GHZ state with the following format:

$$|GHZ\rangle = \frac{|0\rangle^{\otimes M} + |1\rangle^{\otimes M}}{\sqrt{2}} \tag{5.3}$$

where M is the number of particles in this GHZ state. We can call this GHZ state as an M qubit GHZ state. As shown in Figure 5.3, a $m+1$ qubit GHZ state needs to be prepared in the base or headquarters as follows:

$$\frac{1}{\sqrt{2}} \bigotimes_{t=0}^{m} |0_{GHZ\_t}\rangle + \frac{1}{\sqrt{2}} \bigotimes_{t=0}^{m} |1_{GHZ\_t}\rangle \tag{5.4}$$

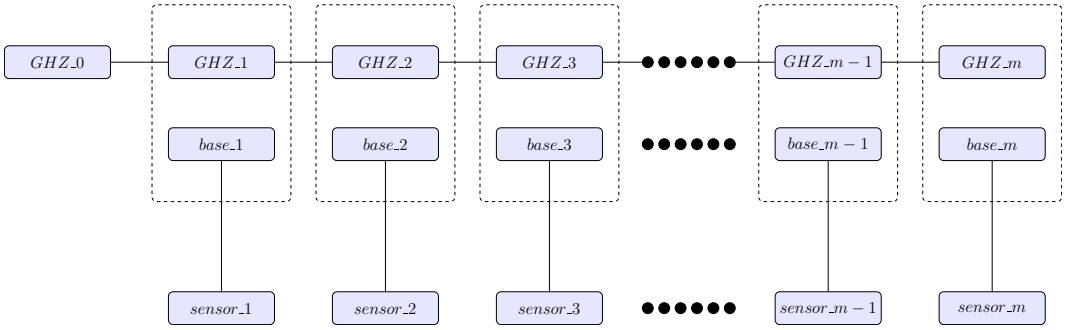


Figure 5.3. A multiparty QKD scheme for wireless sensor networks is presented in this figure. This scheme begins with the preparation of m distributed entanglement pairs. This can be prepared in advance before the deployment of sensor nodes. After that, a $m+1$ qubit GHZ state is generated in the base as shown on the top of this figure. m Bell state measurements then are performed on the m quantum pairs in the base (m dashed line box in the figure). After the announcement of measurement results, one classical bit can be produced and shared by these $m+1$ nodes. Repeating these steps and a secret random bit string can be shared by these $m+1$ nodes. This bit string can be utilized for encryption and decryption to guarantee secure classical communication.

where GHZ, t denotes the tth qubit of the prepared GHZ state. After preparation of m Bell states and a $m+1$ qubits GHZ state, the whole system can be written as:

$$|\Psi_{whole}\rangle = \bigotimes_{k=1}^{m} \frac{1}{\sqrt{2}}(|0_{base\_k}0_{sensor\_k}\rangle + |1_{base\_k}1_{sensor\_k}\rangle) \otimes (\frac{1}{\sqrt{2}}\bigotimes_{t=0}^{m}|0_{GHZ\_t}\rangle + \frac{1}{\sqrt{2}}\bigotimes_{t=0}^{m}|1_{GHZ\_t}\rangle) \tag{5.5}$$

5.5 Bell state measurement

m qubits of the GHZ states are assigned to the m base qubits, forming m new quantum pairs (corresponding to m dashed line boxes in Figure 5.3). If we implement a bell state measurement apparatus in the base and measure the mth quantum pair (qubit GHZ_m and $base\_m$), the measurement results would be one of the four

Bell states ($|\Psi_{00}^m\rangle$, $|\Psi_{01}^m\rangle$,$|\Psi_{10}^m\rangle$ and $|\Psi_{11}^m\rangle$). The four corresponding post-selection quantum states could be obtained from:

$$
\begin{aligned}
|\Psi_{whole}\rangle &= \bigotimes_{k=1}^{m} \frac{1}{\sqrt{2}}(|0_{base\_k}0_{sensor\_k}\rangle + |1_{base\_k}1_{sensor\_k}\rangle) \\
&\quad \otimes (\frac{1}{\sqrt{2}} \bigotimes_{t=0}^{m} |0_{GHZ\_t}\rangle + \frac{1}{\sqrt{2}} \bigotimes_{t=0}^{m} |1_{GHZ\_t}\rangle) \\
&= \frac{1}{2} \bigotimes_{k=1}^{m-1} (\frac{1}{\sqrt{2}}|0_{base\_k}0_{sensor\_k}\rangle + \frac{1}{\sqrt{2}}|1_{base\_k}1_{sensor\_k}\rangle) \\
&\quad \otimes (|0_{base\_m}\rangle|0_{GHZ\_m}\rangle|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle \\
&\quad + |0_{base\_m}\rangle|1_{GHZ\_m}\rangle|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle \\
&\quad + |1_{base\_m}\rangle|0_{GHZ\_m}\rangle|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle \\
&\quad + |1_{base\_m}\rangle|1_{GHZ\_m}\rangle|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle) \\
&= \frac{1}{2} \bigotimes_{k=1}^{m-1} (\frac{1}{\sqrt{2}}|0_{base\_k}0_{sensor\_k}\rangle + \frac{1}{\sqrt{2}}|1_{base\_k}1_{sensor\_k}\rangle) \\
&\quad \otimes (|\Psi_{00}^m\rangle(\frac{1}{\sqrt{2}}|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle + \frac{1}{\sqrt{2}}|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle) \\
&\quad + |\Psi_{01}^m\rangle(\frac{1}{\sqrt{2}}|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle - \frac{1}{\sqrt{2}}|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle) \\
&\quad + |\Psi_{10}^m\rangle(\frac{1}{\sqrt{2}}|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle + \frac{1}{\sqrt{2}}|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle) \\
&\quad + |\Psi_{11}^m\rangle(\frac{1}{\sqrt{2}}|0_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |1_{GHZ\_t}\rangle - \frac{1}{\sqrt{2}}|1_{sensor\_m}\rangle \bigotimes_{t=0}^{m-1} |0_{GHZ\_t}\rangle)))
\end{aligned} \tag{5.6}
$$

If we continue to perform Bell state measurements on all the m quantum pairs(m qubits in GHZ state and m qubit of the $base, k$ states). After the measurements, m new Bell states are observed as follows:

$$
\bigotimes_{k=1}^{m} |\Psi_{i_k,j_k}^k\rangle \tag{5.7}
$$

where i_k and j_k are measured results for the kth qubit pair. From the measured results, we can obtain the post-selection state with the remaining $m+1$ qubits as follows:

$$|\Psi_{postselection}\rangle = \frac{1}{\sqrt{2}}|0\rangle_{GHZ\_0}\bigotimes_{i=0}^{m}|i_k\rangle_{sensor\_k} + \frac{1}{\sqrt{2}}\prod_{j=1}^{k}(-1)^{j_k}|1\rangle_{GHZ\_0}\bigotimes_{i=1}^{m}|\bar{i_k}\rangle_{sensor\_k} \tag{5.8}$$

where $\bar{*}$ denotes the flip operation. From Equation 5.8, we can see that a new GHZ state is created after the m Bell state measurements. If these remaining $m+1$ qubits are measured by the base and the m sensor nodes separately, their measurement results would be correlated. For example, if we have two sensor nodes ($m=2$) and the measured results are $|\Psi_{01}^{1}\rangle$ and $|\Psi_{11}^{2}\rangle$. Then we have the measured results as follows:

$$\begin{aligned} i_1 &= 0 \\ j_1 &= 1 \\ i_2 &= 1 \\ j_2 &= 1 \end{aligned} \tag{5.9}$$

From the two Bell state measurement results, we can obtain the resulting entanglement as follows:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(|0\rangle_{GHZ,0}|i_1\rangle_{sensor\_1}|i_2\rangle_{sensor\_2} + (-1)^{j_1}(-1)^{j_2}|1\rangle_{GHZ\_0}|\bar{i_1}\rangle_{sensor\_1}|\bar{i_2}\rangle_{sensor\_2}) \\ =&\frac{1}{\sqrt{2}}(|0\rangle_{GHZ\_0}|0\rangle_{sensor\_1}|1\rangle_{sensor\_2} + (-1)^{1}(-1)^{1}|1\rangle_{GHZ\_0}|\bar{0}\rangle_{sensor\_1}|\bar{1}\rangle_{sensor\_2}) \\ =&\frac{1}{\sqrt{2}}(|0\rangle_{GHZ\_0}|0\rangle_{sensor\_1}|1\rangle_{sensor\_2} + |1\rangle_{GHZ\_0}|1\rangle_{sensor\_1}|0\rangle_{sensor\_2}) \end{aligned} \tag{5.10}$$

From Equation 5.8 and Equation 5.10, we can see that the qubit GHZ_0 would be measured as either 0 or 1, each with a probability of 1/2. For the qubit in the mth sensor node, the measurement result would be the same as GHZ_0 qubit if i_m is 0 and would be different if i_m is 1.

5.6 Multiparty QKD protocol

As introduced in previous sections, there are n sensor nodes in the WSN. Every sensor node is equipped with a quantum memory where each stored qubit is entangled with a qubit in the base in the format of $|\Psi_{00}\rangle$ Bell states. These distributed entanglement pairs are prepared in advance before the deployment of sensor nodes. If an incident is detected and the base estimates m sensor nodes in the vicinity of the incident are required to deal with this incident. In order to guarantee secure communication between these $m+1$ involving nodes (base and m engaged sensor nodes), a secret key should be produced and distributed to these $m+1$ nodes. The multiparty QKD protocol is proposed as follows:

1. m base qubits are identified in the base. Every one of these m qubits is entangled with a qubit stored in one of the m engaged sensor nodes. For example, the base qubit $|base\_k\rangle$ is identified to be entangled with $|sensor\_k\rangle$ in the kth engaged sensor node.

2. A $(m+1)$-qubit GHZ state is generated in the base.

3. m qubits of the GHZ states are assigned to the m base qubits, forming m new quantum pairs (corresponding to m dashed line boxes in Figure 5.3).

4. The base performs Bell states measurement to these m quantum pairs and obtains m results $|\Psi_{i_k j_k}\rangle$.

5. The Bell state measurement results are broadcasted out by the base.

6. The remaining qubit $|GHZ\_0\rangle$ and m sensor node qubits are all measured separately. Based on the measurement results, one classical bit is obtained in each sensor node (0 and 1 for $|0\rangle$ and $|1\rangle$ respectively).

7. For the sensor node where $i_k = 1$, its classical bit needs to be flipped.

In this way, one bit is produced randomly and distributed between these $m+1$ nodes. By repeating these seven steps again and again a bit string is produced and distributed. This shared bit string can be used for encryption and decryption.

5.7 Discussion

In the multiparty BB84 protocol, every qubit is measured with a basis randomly chosen from ($|0,1\rangle$ and $|+,-\rangle$). Measurement results are discarded unless Alice and all Bobs coincidentally choose the same basis. While in our scheme, no measurement result is discarded and the successful rate of measurement is theoretically 100%. In practical, however, this successful rate may be reduced due to channel noises, memory noises and measurement imperfections. The process of key generation and distribution is deterministic (not probabilistic) and so we call this scheme to be a deterministic protocol. Please note that this definition of 'deterministic' is different from that in some papers [115, 116] where the term 'deterministic' is predetermined before the task.

Since there is no qubit transmission during the QKD process, our scheme is safe against eavesdropping and impersonation in the same way as introduced in the paper [116]. The only communicating message in this multiparty QKD scheme is the broadcasting of measurement results from Alice to all Bobs. The eavesdropper cannot infer any information from these measurement results. If an impersonator blocks the Alice's message and sends fake measurement results to Bobs, different bit strings would be generated by different Bobs. So the impersonation could be detected by using some testing bits.

Like other QKD schemes, our protocol cannot prevent from physical attack (physically capturing a sensor node and accessing key). However, the sensor node can send an alarming message when being captured. After that, another key could be produced and shared by Alice and all Bobs except the captured one.

In this protocol, it is assumed that quantum memories are capable of storing qubits during the whole task. As scientists have achieved quantum storage duration in a few hours [117], this multiparty QKD protocol could be used for WSNs with short task time such as UAV networks and aircraft networks. Other WSNs might also embrace this QKD protocol with advanced quantum storage techniques in the future.

5.8 Conclusion

In this chapter, a multiparty QKD protocol for WSNs is proposed to guarantee secure communication between more than two distributed nodes. Like other QKD protocols, the security of this proposed multiparty QKD scheme relies on the foundations of quantum mechanics and thereby is unconditional reliable against eavesdropping. In addition, the secret key is produced and distributed deterministically, making this proposed QKD scheme much more efficient than multiparty BB84 protocol and multiparty SARG 04 protocol.

Although this QKD protocol is unconditionally reliable against eavesdropping, it can not be used to prevent another version of attack in WSNs-internal attacks. Internal attacks mean physically capturing an engaged node and accessing information from the hardware. For example, if one engaged sensor node is physically captured, the eavesdropper might obtain the shared key from the hardware. Consequently, the multiparty QKD should be implemented together with other security solutions to guarantee secure communication against all kinds of attacks.

This multiparty QKD scheme requires high order GHZ state which is fragile under the noises. In order to compensate the noises, some classical channel coding methods might be employed to add redundancy into the cryptography key.

In order to practically implement this multiparty QKD protocol, good quantum memory should be developed in advance. As discussed in Section 5.3, the quantum memory should be able to keep the stored quantum states with high fidelity during working. In Section 5.6, it is proved that one stored qubit can be used to deduce a

secret classical bit. The memory capacity of the quantum memory is also crucial as the shared bit string length is decided by the capacity of the quantum memory.

Chapter 6

Quantum Channel Equalisation

THIS chapter presents a physically realisable methodology to equalise quantum channel. The minimum phase channel and non-minimum phase all pass channel are discussed separately.

6.1 Introduction

Quantum optical states will be distorted when they are sent across components in experimental set up, or through channels in practical implementations. Suppose we have a single photon state $|1_{\xi_1}\rangle$ as follows:

$$\begin{aligned} |1_{\xi_1}\rangle &= \int \xi_1(t)\hat{a}^\dagger(t)dt|0\rangle \\ &= \int \xi_1(\omega)\hat{a}^\dagger(\omega)d\omega|0\rangle \end{aligned} \tag{6.1}$$

where the pulse shape ξ_1 fulfills the following equation:

$$\begin{aligned} \int |\xi_1(t)|^2 dt &= \int |\xi_1(\omega)|^2 d\omega \\ &= 1 \end{aligned} \tag{6.2}$$

As shown in Figure 6.1, the pulse shape ξ_1 of transmitted quantum state $|1_{\xi_1}\rangle$ would be changed to ξ_2 through the linear channel H as follows [118–120]:

$$\xi_2(t) = \xi_1(t) * h(t) \tag{6.3}$$

where $h(t)$ is the channel response and the symbol $*$ means convolution operator here. It is worthy noting that the communication channels in this chapter are assumed to be linear because in practise, a significant proportion of channel distortion could be reasonably modelled as linear systems. Equation 6.3 can also be used to describe the effect of a quantum channel on the pulse shape of a coherent state. The pulse shapes of optical quantum states play an important role in quantum communication and computation. Firstly, the pulse shapes may be used for quantum information modulation in quantum information systems [121, 122]. Secondly, some specific pulse shapes are required for quantum storage and retrieval [123, 124]. In

addition, the amplification gain of some quantum amplifiers depends on the optical pulse shapes [125]. So we need to design an equalization system E in the receiver end to recover this pulse shape into $\tilde{\xi_1}$, an approximation of ξ_1.

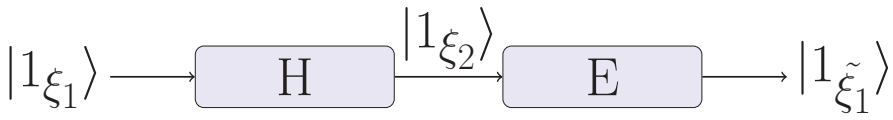


Figure 6.1. The pulse shape ξ_1 of transmitted quantum state $|1_{\xi_1}\rangle$ would be changed to ξ_2 through the channel H. The pulse shapes of single photon states play an important role in quantum communication and computation. So we need to design an equalisation system E in the receiver end to recover this pulse shape into $\tilde{\xi_1}$

A linear time-invariant channel is a minimum phase channel if the channel and its inverse are causal and stable. A causal and stable channel is a non-minimum phase channel if its inverse are causal and not stable. A non-minimum phase channel can be decomposed [126] into an attenuation channel H_a, a minimum phase channel H_{mp} and a non-minimum all pass filter (no energy is absorbed or reflected) H_{ap} as shown in Equation 6.4 as follows:

$$H = H_a * H_{mp} * H_{ap} \tag{6.4}$$

For example, suppose we have a quantum optical channel $H(s) = c\frac{s-a}{s+b}$. This non-minimum phase channel can be decomposed as:

$$\begin{aligned} H(s) &= c\frac{s-a}{s+b} \quad (a>0, b>0) \\ &= c * \frac{s+a}{s+b} * \frac{s-a}{s+a} \end{aligned} \tag{6.5}$$

To compensate the attenuation during channel, we have only one solution: sending more photons. An inverse of transmission channel's transfer function (input output relationship in frequency domain) $1/H_{mp}$ can be used to compensate the minimum

phase channel distortion H_{mp}. The main challenge of quantum channel equalization is the equalization of non-minimum all pass filter. For non-minimum phase channel, as there are non-negative zeros of its channel transfer function (s domain), a simple inverse would result in an unstable causal system. One option to solve this problem is using a quantum memory to store the signal and compensate the distortion in reversed time. The other approach is approximating the unstable inverse system with a stable causal system. As the design of quantum memory is still a big challenge [127], the approximating methodology is much more practical.

In the paper [128], a methodology to approximate unstable system with a stable system in continuous time is presented. Although the approximation is proven mathematically, it is hard to be implemented in quantum area. The approximation in classic digital system is discussed in the paper [129] and this method may provide some inspiration for the future quantum digital systems. B. D. Radlovic and R. A. Kennedy [130] introduced an adaptive methodology to equalise the distortion in acoustic communication.

Although the unique characteristics of quantum states bring us enormous benefits to improve our efficiency and reliability of communication and computation, these characteristics will also bring us huge challenge. For example, quantum sates can not be copied according to the non-cloning theory. From the paper [48], it is known that the quantum states can not be amplified deterministically without adding noise. Meanwhile, the measurement of quantum states is much more difficult than that of classical states according to the Heisenberg uncertainty principle. For these reasons, we can not directly apply classical equalization methodologies in quantum regime. This chapter illustrates a novel methodology which can be used to equalise quantum optical channels. This structure is composed only by photon detectors and simple quantum linear components like cavities and beam splitters. Therefore, it can be easily implemented and may be applied with the gradient echo memory(GEM) [131–133] or newly developed integrated photonic chips [134, 135].

The rest of this chapter is structured as follows: In Section 6.2, we analyse the effects of beam splitters and cavities on single photon states and coherent states. After that, we describe the structure that can be used to compensate minimum phase channel in Section 6.3. In Section 6.4, we prove that a cascading of optical cavities can be utilized to equalise non-minimum phase all pass channel. Finally we conclude and discuss some open questions for future research in Section. 6.5.

6.2 Effects of beam splitters and cavities on quantum optical states

Since we aim to design a physically realisable system to equalise quantum channel distortion, we need to analyse the functions of basic quantum components like cavities and beam splitters. In this section, we discuss the effects of beamsplitters and cavities on quantum optical states separately.

6.2.1 Effects of beam splitters on quantum optical states

A beam splitter is an optical device that splits a beam of light in two. The beam splitters play an essential role in quantum information. From the paper [108, 118], we can see the transfer function of a beam splitter is (2×2) matrix as follows:

$$H_{beamsplitter}(s) = \begin{pmatrix} \sqrt{\eta} & \pm\sqrt{1-\eta} \\ \mp\sqrt{1-\eta} & \sqrt{\eta} \end{pmatrix} \tag{6.6}$$

where η is transmissivity of the beam splitter. If a single photon $|\Psi_{in}\rangle = |1_{\xi_1}\rangle$ is split by a beam splitter with transfer function as Equation 6.6, we can obtain the output state as follows:

$$
\begin{aligned}
|\Psi_{out}\rangle &= U|\Psi_{in}\rangle \\
&= \int \xi_1(\omega) U \hat{b}^{\dagger}_{in}(\omega) U^{\dagger} d\omega |0\rangle \\
&= [\sqrt{\eta} \int \xi_1(\omega) \hat{b}^{\dagger}_{out1}(\omega) d\omega \pm \sqrt{1-\eta} \int \xi_1(\omega) \hat{b}^{\dagger}_{out2}(\omega) d\omega]|0\rangle \\
&= \sqrt{\eta}|1_{\xi_1}\rangle_{out1} \pm \sqrt{1-\eta}|1_{\xi_1}\rangle_{out2}
\end{aligned} \tag{6.7}
$$

Tracing out output 2, the state that comes out at output 1 is a mixed state as follows:

$$
\rho_{out1} = \eta|1_{\xi_1}\rangle\langle 1_{\xi_1}| + (1-\eta)|0\rangle\langle 0| \tag{6.8}
$$

If a coherent state $|\alpha_{\xi_1}\rangle$ is spilt by this beam splitter, the output state would be:

$$
\begin{aligned}
|\Psi_{out}\rangle &= U|\Psi_{in}\rangle \\
&= \int \xi_1(\omega) U Exp[\alpha \hat{b}^{\dagger}_{in}(\omega) - \alpha^* \hat{b}_{in}(\omega)] U^{\dagger} d\omega |0\rangle \\
&= \int \xi_1(\omega) Exp[\sqrt{\eta}\alpha \hat{b}^{\dagger}_{out1}(\omega) - \sqrt{\eta}\alpha^* \hat{b}_{out1}(\omega)] \\
&\times Exp[\pm\sqrt{1-\eta}\alpha \hat{b}^{\dagger}_{out1}(\omega) \mp \sqrt{1-\eta}\alpha^* \hat{b}_{out1}(\omega)] d\omega |0\rangle \\
&= |\sqrt{\eta}\alpha_{\xi_1}\rangle_{out1}| \pm \sqrt{1-\eta}\alpha_{\xi_1}\rangle_{out2}
\end{aligned} \tag{6.9}
$$

where $Exp[\quad]$ means the exponential operator. Unlike the single photon case where the two output states are entangled with each other, the two output states for coherent state cases are two pure coherent states with smaller amplitudes.

6.2.2 Effects of cavities on quantum optical states

A one-sided optical cavity can be modelled as a pair of mirrors [108]. One mirror is partially transmitting while the other one is completely reflective. The external

optical field interacts with light inside the cavity through the partially transmitting mirror and a Faraday isolator is used to separate the external optical field into input and output components. The transfer function of a cavity can be written as:

$$H_{cavity}(s) = \frac{s - \frac{\gamma}{2} \pm j\omega_0}{s + \frac{\gamma}{2} \pm j\omega_0} \tag{6.10}$$

where γ is coupling strength of the cavity and ω_0 is the detuning frequency. From this transfer function, we can see that an optical cavity can be modelled as an all pass filter for quantum optical states.

If a single photon $|\Psi_{in}\rangle = |1_{\xi_1}\rangle$ is sent across an optical cavity, the output state can be written as:

$$\begin{aligned} |\Psi_{out}\rangle &= U|\Psi_{in}\rangle \\ &= U \int \xi_1(\omega)\hat{b}^\dagger_{in}(\omega)d\omega|0\rangle \\ &= U \int \xi_1(\omega)\hat{b}^\dagger_{in}(\omega)d\omega U^\dagger|0\rangle \\ &= \int \xi_1(\omega)U\hat{b}^\dagger_{in}(\omega)U^\dagger d\omega|0\rangle \end{aligned} \tag{6.11}$$

From Equation 6.10, we can see the relation between the input state operator $b^\dagger_{in}$ and the output state operator $b^\dagger_{out}$ in Heisenberg picture as follows:

$$\begin{aligned} b_{out}(\omega) &= U^\dagger \hat{b}_{in}(\omega)U \\ &= H_{cavity}(j\omega)\hat{b}_{in}(\omega) \\ &= \hat{b}_{in}(\omega)e^{-2j*arctan(\frac{2(\omega\pm\omega_0)}{\gamma})} \end{aligned} \tag{6.12}$$

Then we can obtain the output state in Schrodinger picture as:

$$
\begin{aligned}
|\Psi_{out}\rangle &= \int \xi_1(\omega) U \hat{b}^{\dagger}_{in}(\omega) U^{\dagger} d\omega |0\rangle \\
&= \int \xi_1(\omega) e^{-2j*arctan(\frac{2(\omega \pm \omega_0)}{\gamma})} \hat{b}^{\dagger}_{out}(\omega) d\omega |0\rangle \\
&= \int \xi_2(\omega) \hat{b}^{\dagger}_{out}(\omega) d\omega |0\rangle \\
&= |1_{\xi_2}\rangle
\end{aligned} \tag{6.13}
$$

where the pulse shape of output single photon state is $\xi_2(\omega) = \xi_1(\omega) e^{-2j*arctan(\frac{2(\omega \pm \omega_0)}{\gamma})}$. With the same method, we can obtain the output state in Schrodinger picture if a coherent state $|\alpha_{\xi_1}\rangle$ sent across the cavity:

$$
\begin{aligned}
|\Psi_{out}\rangle &= \int \xi_1(\omega) U \hat{b}^{\dagger}_{in}(\omega) U^{\dagger} d\omega |0\rangle \\
&= \int \xi_1(\omega) U Exp[\alpha \hat{b}^{\dagger}_{in}(\omega) - \alpha^* \hat{b}_{in}(\omega)] U^{\dagger} d\omega |0\rangle \\
&= \int \xi_1(\omega) Exp[e^{-2j*arctan(\frac{2(\omega \pm \omega_0)}{\gamma})} \alpha \hat{b}^{\dagger}_{out}(\omega) - e^{2j*arctan(\frac{2(\omega \pm \omega_0)}{\gamma})} \alpha^* \hat{b}_{out}(\omega)] d\omega \\
&= |e^{-2j*arctan(\frac{2(\omega \pm \omega_0)}{\gamma})} \alpha_{\xi_1}\rangle
\end{aligned} \tag{6.14}
$$

From Equation 6.14, we can see that the effect of an optical cavity on coherent states are different from that on single photon states. For a single photon state, an optical cavity only change the phase of frequency distribution as ξ_1 is changed into ξ_2 in Equation 6.13. For a coherent state, the frequency distribution stays the same while the phase of the eigenvalue α changes.

6.3 Equalisation of minimum phase channels

In this section, we introduce a structure which can be used to equalise a minimum phase channel. Suppose we have a minimum phase channel whose transfer function can be written as follows:

$$H_{mp}(s) = \frac{s+a}{s+b} \quad (a > 0, b > 0) \tag{6.15}$$

After this minimum phase channel, the input quantum state $|1_{\xi_1}\rangle$ would result in an output state $|1_{\xi_2}\rangle$ where the pulse shape ξ_2 can be obtained from the following equation:

$$\xi_2(s) = \mathcal{N}[\frac{s+a}{s+b}\xi_1(s)] \tag{6.16}$$

Where $\mathcal{N}[\ \ ]$ denotes the normalization of the state. An inverse of this $H_{mp}(s)$ can be used to compensate this minimum phase channel. So we need to design an equalization system $E_{mp}(s)$ whose transfer function is as follows:

$$E_{mp}(s) = \frac{s+b}{s+a} \tag{6.17}$$

In order to achieve an equalization system $E_{mp}(s)$ with transfer function as Equation 6.17, let us begin with assuming there is a linear component with transfer function as Equation 6.17, then we have:

$$\begin{aligned} \hat{b}_{out}(\omega) &= U^{\dagger}\hat{b}_{in}(\omega)U \\ &= E_{mp}(j\omega)\hat{b}_{in} \end{aligned} \tag{6.18}$$

Then we can rewrite the operator for $\hat{b}_{in}(\omega)$ in Heisenberg picture as:

$$\begin{aligned} \hat{b}_{in}(\omega) &= UU^{\dagger}\hat{b}_{in}(\omega)UU^{\dagger} \\ &= {E_{mp}}^{\dagger}(j\omega)E_{mp}(j\omega)\hat{b}_{in}(\omega) \\ &= |E_{mp}(j\omega)|^2\hat{b}_{in}(\omega) \end{aligned} \tag{6.19}$$

From the above equation, we can see the magnitude of frequency response $|E_{mp}(j\omega)|^2 = 1$ for every frequency component ω. Then the channel must be an all pass channel.

If the channel is not all pass, we cannot achieve the equalisation with single-input single-output linear quantum components. So we can only design a multiple-input multiple-output system to equalise the minimum phase channel as shown in Figure 6.2.

This equalisation structure is composed with two beam splitters and one cavity. From Equation 6.10, we can see the transfer function of a cavity is all pass function. If we configure the coupling strength of a cavity to be $\gamma = 2 \times a$ and the detuning frequency to be $\omega_0 = 0$, the transfer function $H_c(s)$ of this cavity is as follows:

$$H_c(s) = \frac{s-a}{s+a} \tag{6.20}$$

Suppose the transmissivity of two beam splitters in Figure 6.2 are $\sqrt{\alpha}$ and $\sqrt{\beta}$ respectively. From Equation 6.6 and Equation 6.10, the whole system can be represented as:

$$\begin{pmatrix} \hat{b}_{out,1} \\ \hat{b}_{out,2} \end{pmatrix} = E_{mp1}(s) \times \begin{pmatrix} \hat{b}_{in,1} \\ \hat{b}_{in,2} \end{pmatrix} \tag{6.21}$$

where the whole transfer matrix $E_{mp1}(s)$ is:

$$\begin{aligned} E_{mp1}(s) &= \begin{pmatrix} \sqrt{\alpha} & \sqrt{1-\alpha} \\ -\sqrt{1-\alpha} & \sqrt{\alpha} \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & H_c(s) \end{pmatrix} \times \begin{pmatrix} \sqrt{\beta} & \pm\sqrt{1-\beta} \\ \mp\sqrt{1-\beta} & \sqrt{\beta} \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{\alpha\beta} \mp H_c(s)\sqrt{1-\alpha}\sqrt{1-\beta} & \pm\sqrt{\alpha}\sqrt{1-\beta} + H_c(s)\sqrt{1-\alpha}\sqrt{\beta} \\ -\sqrt{1-\alpha}\sqrt{\beta} \mp H_c(s)\sqrt{\alpha}\sqrt{1-\beta} & \mp\sqrt{1-\alpha}\sqrt{1-\beta} + H_c(s)\sqrt{\alpha\beta} \end{pmatrix} \\ &= \begin{pmatrix} M & N \\ Q & P \end{pmatrix} \end{aligned} \tag{6.22}$$

Then we can have:

$$\begin{aligned} \hat{b}_{out,1} &= M \times \hat{b}_{in,1} + N \times \hat{b}_{in,2} \\ \hat{b}_{out,2} &= Q \times \hat{b}_{in,1} + P \times \hat{b}_{in,2} \end{aligned} \tag{6.23}$$

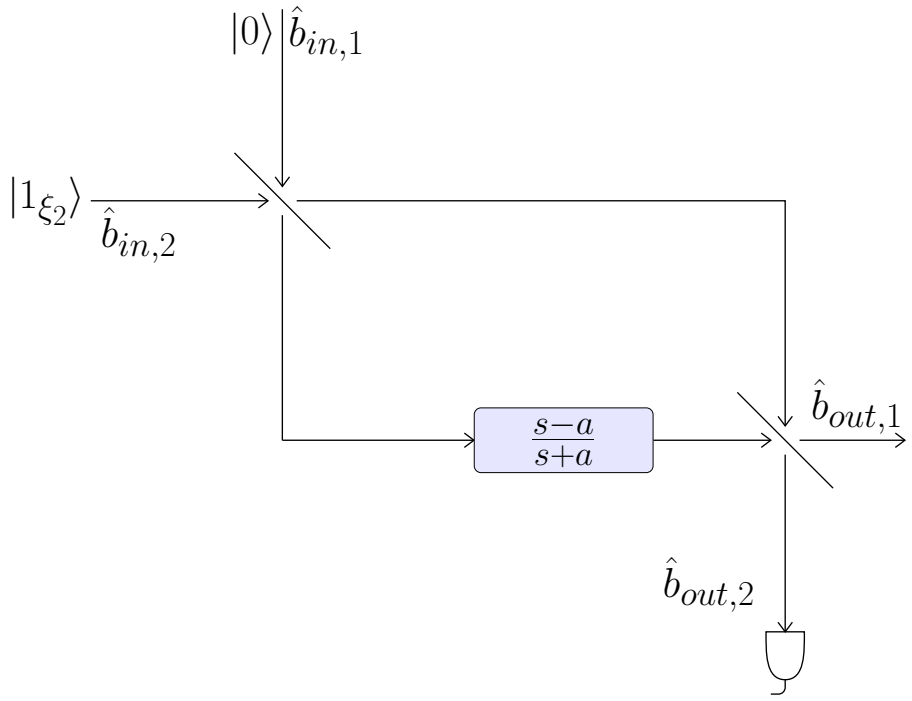


Figure 6.2. This figure shows a structure which can be used to equalise minimum phase channel. This structure is composed with two beam splitters and one optical cavity. The transfer function $H_c(s)$ of this cavity is $\frac{s-a}{s+a}$. The transmissivity of the two beam splitters are $\sqrt{\alpha}$ and $\sqrt{\beta}$ respectively.

where the coefficient M,N,Q and P are:

$$\begin{aligned}
M &= \frac{(\sqrt{\alpha\beta} \mp \sqrt{1-\alpha}\sqrt{1-\beta})s + (\sqrt{\alpha\beta} \pm \sqrt{1-\alpha}\sqrt{1-\beta})a}{s+a} \\
N &= \frac{(\pm\sqrt{\alpha}\sqrt{1-\beta} + \sqrt{1-\alpha}\sqrt{\beta})s + (\pm\sqrt{\alpha}\sqrt{1-\beta} - \sqrt{1-\alpha}\sqrt{\beta})a}{s+a} \\
Q &= \frac{(-\sqrt{1-\alpha}\sqrt{\beta} \mp \sqrt{\alpha}\sqrt{1-\beta})s + (-\sqrt{1-\alpha}\sqrt{\beta} \pm \sqrt{\alpha}\sqrt{1-\beta})a}{s+a} \\
P &= \frac{(\mp\sqrt{1-\alpha}\sqrt{1-\beta} + \sqrt{\alpha\beta})s + (\mp\sqrt{1-\alpha}\sqrt{1-\beta} - \sqrt{\alpha\beta})a}{s+a}
\end{aligned} \tag{6.24}$$

If the transmitted signal is a single photon state $|1_{\xi_1}\rangle$ and the receiving signal is $|1_{\xi_2}\rangle$. With the same methodology as shown in Section. 6.2, the output sate of this equalisation structure can be calculated as:

$$
\begin{aligned}
|\Psi_{out}\rangle &= U|\Psi_{in}\rangle \\
&= \int \xi_2(\omega) U \hat{b}^{\dagger}_{in,2}(\omega) U^{\dagger} d\omega |0\rangle \\
&= (\sqrt{\alpha}\sqrt{\beta} \mp \sqrt{1-\alpha}\sqrt{1-\beta}) \\
&\times \int \xi_2(\omega) \frac{j\omega + \frac{\sqrt{\alpha}\sqrt{\beta} \pm \sqrt{1-\alpha}\sqrt{1-\beta}}{\sqrt{\alpha}\sqrt{\beta} \mp \sqrt{1-\alpha}\sqrt{1-\beta}} a}{j\omega + a} \hat{b}^{\dagger}_{out,1} d\omega \\
&+ (\sqrt{1-\alpha}\sqrt{\beta} \pm \sqrt{\alpha}\sqrt{1-\beta}) \\
&\times \int \xi_2(\omega) \frac{j\omega + \frac{\sqrt{1-\alpha}\sqrt{\beta} \mp \sqrt{\alpha}\sqrt{1-\beta}}{\sqrt{1-\alpha}\sqrt{\beta} \pm \sqrt{\alpha}\sqrt{1-\beta}} a}{j\omega + a} \hat{b}^{\dagger}_{out,2} d\omega
\end{aligned}
\tag{6.25}
$$

where $\hat{b}_{out,1}$ and $\hat{b}_{out,2}$ are operators for the two output channels respectively. The state comes out from output 1 is a mix state. If we put a photon detector in the output 2 and have no photon measured, all the energy of input signal photon goes to output 1 and the pulse shape of conditional output state $|1_{\tilde{\xi}_1}\rangle$ would be:

$$
\tilde{\xi}_1(s) = \mathcal{N}[\frac{s + \frac{\sqrt{\alpha}\sqrt{\beta} \pm \sqrt{1-\alpha}\sqrt{1-\beta}}{\sqrt{\alpha}\sqrt{\beta} \mp \sqrt{1-\alpha}\sqrt{1-\beta}} a}{s+a} \xi_2(s)] \tag{6.26}
$$

If we can configure the transmissivity of the two beam splitters $\sqrt{\alpha}$ and $\sqrt{\beta}$ to make the coefficient $b = \frac{\sqrt{\alpha}\sqrt{\beta} \pm \sqrt{1-\alpha}\sqrt{1-\beta}}{\sqrt{\alpha}\sqrt{\beta} \mp \sqrt{1-\alpha}\sqrt{1-\beta}} a$, the equalisation of minimum phase channel for single photon state is achieved.

If a coherent state $|\alpha_{\xi_1}\rangle$ is transmitted, we can also use the same structure to equalise minimum phase channel distortion by configuring the parameters of beam splitters and optical cavities. Unlike the single photon state case where a photon detector can be used to recover the signal back to $|1_{\xi_1}\rangle$ probabilistically, the two output of this structure would be two pure coherent states $|c_1\alpha_{\xi_1}\rangle$ and $|c_2\alpha_{\xi_1}\rangle$. c_1 and c_2 are two attenuation coefficients determined by the configuring parameters.

6.4 Equalization of non-minimum phase all pass channel

Suppose we have an all pass filter, with a transfer function as follows:

$$H_{ap}(s) = \frac{s-a}{s+a} \quad (a > 0) \tag{6.27}$$

A simple inverse of $H_{ap}(s)$ would lead to unstable systems as discussed in Section 6.1. In order to equalise this non-minimum phase all pass channel, we choose to design a stable structure with transfer function $\tilde{E}_{ap}(s)$. $\tilde{E}_{ap}(s)$ is an approximation of $E_{ap}(s)$, the unstable inverse of $H_{ap}(s)$:

$$\tilde{E}_{ap}(s) \approx E_{ap}(s) = \frac{s+a}{s-a} \tag{6.28}$$

6.4.1 Approximation of non-causal but stable inverse

We can introduce another component to cancel the unstable pole of $E_{ap}(s)$ as Equation 6.29:

$$\tilde{E}_{ap}(s) = \sqrt{\frac{(e^{-\tau s} - e^{-\tau a})}{(e^{\tau s} - e^{-\tau a})}} \frac{(s+a)}{(s-a)} \tag{6.29}$$

Note that $\tilde{E}_{ap}(s)$ is stable since the positive pole of $E_{ap}(s)$ has been cancelled by the new term. If we increase the parameter τ to make τa is big enough, the term $e^{-\tau a}$ can be neglected and $\tilde{E}_{ap}(s)$ can be approximated as:

$$\begin{aligned} \tilde{E}_{ap}(s) &\approx \sqrt{\frac{e^{-\tau s}}{e^{\tau s}}} \frac{(s+a)}{(s-a)} \\ &= \sqrt{e^{-2\tau s}} \frac{(s+a)}{(s-a)} \\ &= e^{-\tau s} E_{ap}(s) \end{aligned} \tag{6.30}$$

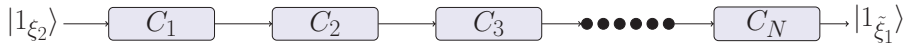


Figure 6.3. This figure shows that a series of cavities can be used to equalise non-minimum phase all pass channel. If we set the coupling strength of every cavity to be $\gamma = 2a$ and detuning frequency of the number n cavity $((n \in (-\infty, \infty))\&\&(n \neq 0))$ to be $\frac{2n\pi}{\tau}$, we can implement an equalisation system with transfer function in Equation 6.32.

From the above equation, we can see that the stable system $\tilde{E}_{ap}(s)$ can be used to approximate an unstable system $E_{ap}(s)$ with a time delay of τ. This $\tilde{E}_{ap}(s)$ can also be written as:

$$\begin{aligned}\tilde{E}_{ap}(s) &= \sqrt{\frac{e^{-\tau a}(e^{-(s-a)\tau}-1)}{e^{-\tau a}(e^{(s+a)\tau}-1)}}\frac{(s+a)}{(s-a)} \\ &= \sqrt{\frac{(e^{-(s-a)\tau}-1)}{(e^{(s+a)\tau}-1)}}\frac{(s+a)}{(s-a)}\end{aligned} \tag{6.31}$$

If we factorize the first term of Equation 6.31, we can obtain:

$$\begin{aligned}\tilde{E}_{ap}(s) &= \frac{(s-a)\prod_{n=1}^{\infty}(s-a\pm\frac{2n\pi j}{\tau})}{(s+a)\prod_{n=1}^{\infty}(s+a\pm\frac{2n\pi j}{\tau})}\frac{(s+a)}{(s-a)} \\ &= \frac{(s-a)}{(s+a)}\prod_{n=1}^{\infty}(\frac{s-a\pm\frac{2n\pi j}{\tau}}{s+a\pm\frac{2n\pi j}{\tau}})\frac{(s+a)}{(s-a)} \\ &= \prod_{n=1}^{\infty}(\frac{s-a\pm\frac{2n\pi j}{\tau}}{s+a\pm\frac{2n\pi j}{\tau}})\end{aligned} \tag{6.32}$$

From the transfer function of cavities in Equation 6.10, we can achieve the $\tilde{E}_{ap}(s)$ with a series of cavities as shown in Figure 6.3.

Note that there are N cavities as shown in Figure 6.3 as we cannot provide infinite cavities practically. In practical implementation, we need to cascade as many cavities as possible to achieve a good approximation.

6.4.2 Phase change analysis

The transfer function of the cavity series can also be written as:

$$\tilde{E}_{ap}(s) = \prod_{n=-\infty}^{\infty} \left(\frac{s - a + \frac{2n\pi j}{\tau}}{s + a + \frac{2n\pi j}{\tau}}\right)\frac{(s+a)}{(s-a)} \tag{6.33}$$

Since Equation 6.33 is composed with all pass filters and the magnitude keep unchanged all the time. we can analyze the phase change only with the following equation:

$$\tilde{E}_{ap}(j\omega) = \prod_{n=-\infty}^{\infty} \left(\frac{j\omega - a + \frac{2n\pi j}{\tau}}{j\omega + a + \frac{2n\pi j}{\tau}}\right)\frac{(j\omega+a)}{(j\omega-a)} \tag{6.34}$$

Then the phase change of the whole system can be calculated as:

$$\begin{aligned}\angle(\tilde{E}_{ap}(j\omega)) = &\sum_{n=-\infty}^{\infty} \left(\angle(j\omega - a + \frac{2n\pi j}{\tau}) - \angle(j\omega + a + \frac{2n\pi j}{\tau})\right) \\ &+ \angle(j\omega + a) - \angle(j\omega - a) \\ &= -2 \times \sum_{n=-\infty}^{\infty} \left(\arctan(\frac{\omega}{a} + \frac{2\pi n}{\tau a})\right. \\ &\left. + 2 \times \arctan(\frac{\omega}{a})\right.\end{aligned} \tag{6.35}$$

As introduced in the Section 6.4.1, we increase the parameter τ to make τa big enough. Then we can transform the summation Equation 6.35 into integration as follows:

$$\begin{aligned}\angle(\tilde{E}_{ap}(j\omega)) \approx &-\frac{\tau a}{\pi} \times \int_{-\infty}^{\infty} \arctan(\frac{\omega}{a} + \varepsilon)d\varepsilon \\ &+ 2 \times \arctan(\frac{\omega}{a}) \\ &= -\tau\omega + 2\arctan(\frac{\omega}{a})\end{aligned} \tag{6.36}$$

which is exactly the phase change of $e^{-\tau s}E_{ap}(s)$.

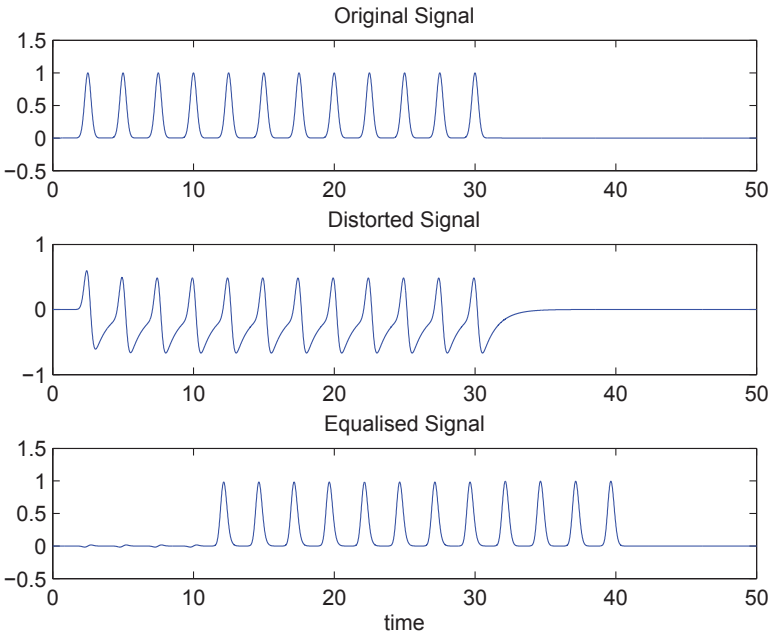


Figure 6.4. This figure shows a simulation of non-minimum phase channel equalization. The top subplot depicts the original sequence of single photon states. The middle subplot describe the distorted signal after a all pass non-minimum phase channel. The bottom one is for the equalised signal with the proposed equalization structure of this paper. From this figure, we can see the transmitted signal is recovered well with a time delay of $10s$.

6.4.3 Simulation results

Figure 6.4 shows a simulation of non-minimum phase channel equalization. The top subplot depicts the original sequence of single photon states. The middle subplot describes the distorted signal after an all pass non-minimum phase channel. The bottom one is for the equalised signal with the proposed equalization structure of this paper. From this figure, we can see the transmitted signal is recovered well with a time delay of $10s$.

It is shown in Figure 6.3 that the coupling strength of every cavity should be set into $\gamma = 2a$ and the detuning frequency of the number n cavity $((n \in [-N, N])\&\&(n \neq 0))$ should be set into $\frac{2n\pi}{\tau}$.

6.5 Conclusion

In this chapter, an equalisation methodology is proposed to compensate quantum optical communication channel. Equalisation for both single photon states and for coherent states are analysed. Since quantum optical communication channel can be decomposed into a minimum phase channel and a non-minimum phase all pass channel, we design equalisation structure for these two kinds of channels separately.

Since this equalization system is based on simple quantum components like cavities and beam splitters, it is rather realisable and could be implemented easily with GEM and programmable waveguide chip. The channel analysed in this paper may not only refer to practical optical communication channel, but also be applicable for quantum signal processing locally including quantum storage, manipulation and transforming. One promising application of this equalisation methodology is combatting channel distortion in quantum repeaters in the future.

As we discussed in Section 6.1, the other option to equalise a quantum non-minimum phase channel is using a quantum memory to store the distorted state and processing it in the reversed time. As the technology of quantum memory progresses, this option may become possible in the years to come. This non-causal quantum equalization system needs to be investigated in the future.

With the proposed equaliser, the transfer function of the quantum channel is assumed to be known to us. However, this assumption may not be true in the practical communication. Therefore, systems are needed to be designed in the future to obtain the transfer function of the communication channel. In addition, we assume that the channel responses keep unchanged during the whole communication process. Further quantum adaptive equalisation methodology may be proposed in the future to equalise the quantum channel adaptively. We might also adapt some blind and adaptive equalization algorithm in classical communication into quantum area.

In this project, we do not consider the effects of noise. The proposed quantum channel equaliser is similar to zero-forcing equalisers in classical communication. As

noise ia always present in quantum communication, we may extend this proposed quantum equaliser by maximizing the signal noise ratio in the future.

Chapter 7

Conclusions and Future Work

THIS chapter concludes the thesis by reviewing the work done, re-summarizing the original contributions, and recommending future work that could be undertaken by others.

7.1 Review of and conclusions from the work in this thesis

Quantum repeaters are indispensable for quantum communication. In order to implement quantum communication, three aspects of quantum repeaters need to be addressed: quantum state amplification, quantum channel equalisation and quantum communication protocols. This thesis presents four research projects in the field of quantum communication. The first project is an analysis of continuous mode operation of non-deterministic NLA. During this project, a dynamical NLA is designed and analysed. The second and third projects contribute to the two fields of quantum protocol-quantum networking and QKD. The second project is engaged to develop a protocol for generating W-states over long distances. A multiparty QKD scheme is proposed during the third project. Quantum equalisers are designed to compensate for channel distortion in the fourth project.

Most of quantum amplification schemes are proposed based on discrete mode analysis. However, continuous mode quantum states are much more common in real application. During the first project, we investigate the continuous mode operation of two popular kinds of NLA-quantum scissor based NLA and photon addition-subtraction based NLA. For the quantum scissor based NLA, we find that the pulse shape of the output signal is the same as the one from the auxiliary single photon, while its amplitude is influenced by both the input coherent state and the NLA parameters. For photon addition-subtraction based NLA, it is proved that the amplification gain is as expected only when the pulse shape of input state equals that of the creation operator and annihilation operator. Simulations are performed to confirm the theoretical results.

In the second project, a protocol is proposed to generate entanglement between multiple distant nodes by creating a W-state shared between them. Since W-states can be used to teleport quantum states, we may perform quantum teleportation with the distributed W-states generated using our methodology. As the research

field of quantum computing progresses, more complicated quantum algorithms are being proposed. In the future, when a single quantum computer is not capable of implementing such complicated algorithms, we may develop quantum algorithms to utilize quantum computing resources at different locations with distributed W-states.

In the third project, a multiparty QKD scheme for WSNs is proposed to guarantee secure communication between more than two distributed nodes. Like other QKD protocols,the security of this proposed multiparty QKD scheme relies on the foundations of quantum mechanics and is thereby unconditional secure against eavesdropping. In addition,the secret key is produced and distributed deterministically, making this proposed QKD scheme much more efficient than multiparty BB84 protocol and multiparty SARG 04 protocol.

The last project is engaged for quantum channel equalisation. A quantum channel can be decomposed into minimum phase channel and a non-minimum phase all pass channel. The equalisation of these two kinds of channels are discussed separately. Both single photon states and coherent states are considered in this project.

7.2 Recommendations on future Work

Compared to classical communication, quantum communication is a much newer research field. Therefore, there are a huge number of research gaps in this field. Due to the limitation of time and equipment, some research problems have not been solved in this PhD candidature. All these research problems could be taken as the research gap of other research projects in the future.

7.2.1 Investigation of modulation schemes with photonic pulse shapes

Pulse shape manipulation plays an very important role in completion of both the NLA project and the equalisation project. With the dynamic NLA structure, we

find that the output coherent state inherits the pulse shape of driving single photon state. In the channel equalisation project, the proposed equalisation structures can be used to manipulate pulse shapes of single photon states and coherent states. With these pulse shape manipulation methodologies, it might be possible in the future that quantum information is modulated into the photonic pulse shapes.

7.2.2 Quantum cryptography for wireless sensor networks

In the project of multiparty QKD, we develop a scheme of producing and distributing cryptography keys over long distances. This multiparty QKD scheme can guarantee secure communication between multiple sensor nodes against eavesdropping. However, it can not be used to prevent internal attacks. If an engaged sensor node is physically captured, the secret information might be accessed by attackers through hardware. The QKD scheme might be synthesised with other cryptography techniques in order to guarantee security against all kinds of attacks.

7.2.3 Quantum equalisation implementation with waveguide chips and GEMs

In the channel equalisation project, the proposed equalisation structures are composed of simple optical components like beam splitters and optical cavities. Therefore, these structures are physically realisable and can be implemented easily. It might be possible in the future to apply the proposed equalisation methodologies with waveguide chips and GEMs.

7.2.4 Further investigation of quantum channel equalisation techniques

As discussed in Chapter 6, another option to equalise a non-minimum phase all pass channel is using quantum memory to store the distorted states and performing the equalisation in the reversed time. This may be further investigated in the future.

With the proposed equaliser, the transfer function of the quantum channel is assumed to be known to us. However, this assumption may not be true in the practical communication. Therefore, systems are needed to be designed in the future to obtain the transfer function of the communication channel. In addition, we assume that the channel responses stay unchanged during the whole communication process. Further quantum adaptive equalisation methodologies may be proposed in the future to equalise the quantum channel adaptively. We might also adapt some blind and adaptive equalization algorithms from classical communication into the quantum area.

7.3 Conclusion

This chapter summarizes the research carried out in the duration of the PhD candidature. The research done in this thesis contributes to knowledge of quantum amplification, quantum communication protocols and quantum channel equalisation. The thesis provides a general method for (a) the continuous mode operation of non-deterministic NLA, (b) generation of distributed W-states over long distances, (c) multiparty QKD for wireless sensor networks and (d) equalisation of quantum communication channels. The contributions in this thesis could be used by other researchers in their own studies and applications. The work in this thesis and the recommendations on future work in Section 7.2 will create more research possibilities in the field of quantum communication.

Bibliography

[1] M. Shell. How to Use the IEEEtran LaTeXClass. [Online]. Available: http://www.ngi2009.eu/IEEEtran_HOWTO.pdf [29 July 2010].

[2] Bureau International des Poids et Mesures. The international system of units (SI). [Online]. Available: http://www.bipm.org/utils/common/pdf/si_brochure_8_en.pdf [29 July 2010].

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov 1994, pp. 124–134.

[4] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, "Efficient networks for quantum factoring," *Phys. Rev. A*, vol. 54, pp. 1034–1063, Aug 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.54.1034

[5] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 439, no. 1907, pp. 553–558, 1992. [Online]. Available: http://rspa.royalsocietypublishing.org/content/439/1907/553

[6] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Quantum algorithms revisited," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 339–354, 1998. [Online]. Available: http://rspa.royalsocietypublishing.org/content/454/1969/339

[7] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 400, no. 1818, pp. 97–117, 1985. [Online]. Available: http://rspa.royalsocietypublishing.org/content/400/1818/97

[8] J.-y. Wang, B. Yang, S.-k. Liao, L. Zhang, Q. Shen, X.-f. Hu, J.-c. Wu, S.-j. Yang, H. Jiang, Y.-l. Tang, B. Zhong, H. Liang, W.-y. Liu, Y.-h. Hu, Y.-m. Huang, B. Qi, J.-g. Ren, G.-s. Pan, J. Yin, J.-j. Jia, Y.-a. Chen, K. Chen, C.-z. Peng, and J.-w. Pan, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, p. 387, 2013.

[9] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, p. 040502, Jul 2015. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.115.040502

[10] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999. [Online]. Available: http://www.sciencemag.org/content/283/5410/2050.abstract

[11] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.67.661

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, Part 1, pp. 7 – 11, 2014, theoretical Aspects of Quantum Cryptography celebrating 30 years of {BB84}. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0304397514004241

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992. [Online]. Available: http://dx.doi.org/10.1007/BF00191318

[14] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," *Opt. Express*, vol. 16, no. 23, pp. 18 790–18 797, Nov 2008. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-16-23-18790

[15] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, "Long-distance quantum key distribution in optical fibre," *New Journal of Physics*, vol. 8, no. 9, p. 193, 2006. [Online]. Available: http://stacks.iop.org/1367-2630/8/i=9/a=193

[16] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, Jul 2005. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.72.012326

[17] S. H. Shams Mousavi and P. Gallion, "Decoy-state quantum key distribution using homodyne detection," *Phys. Rev. A*, vol. 80, p. 012327, Jul 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.80.012327

[18] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.85.441

[19] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key

distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.111.130502

[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.70.1895

[21] D. Bouwmeester, J.-W. Pan, K. Mattle, and M. Elbi, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, p. 575, 1997.

[22] A. Furusawa, J. L. Srensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998. [Online]. Available: http://www.sciencemag.org/content/282/5389/706.abstract

[23] W. Hnsel, H. Hffner, C. F. Roos, J. Benhelm, R. Blatt, M. Riebe, C. Becher, D. F. V. James, G. P. T. Lancaster, F. Schmidt-Kaler, and T. W. Krber, "Deterministic quantum teleportation with atoms," *Nature*, vol. 429, no. 6993, pp. 734–737, 2004.

[24] T. Schaetz, J. Britton, C. Langer, M. D. Barrett, R. Ozeri, J. D. Jost, D. J. Wineland, W. M. Itano, E. Knill, J. Chiaverini, and D. Leibfried, "Deterministic quantum teleportation of atomic qubits," *Nature*, vol. 429, no. 6993, pp. 737–739, 2004.

[25] H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, H. Shen, T. Fernholz, and E. S. Polzik, "Deterministic quantum teleportation between distant atomic objects," *Nature Physics*, vol. 9, no. 7, p. 400, 2013.

[26] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7 – 11, 2014, theoretical Aspects of Quantum Cryptography celebrating 30 years of BB84. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0304397514004241

[27] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992. [Online]. Available: http://dx.doi.org/10.1007/BF00191318

[28] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, Feb 2004. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.92.057901

[29] N. Gisin, "How far can we send a photon?" in *12th International Conference on Quantum Communication, Measurement and Computing (QCMC)*, ser. Quantum Communication, Measurement and Computing (QCMC), Hefei,China, 2014.

[30] J. R. Taylor, "Tutorial on fiber-based sources for biophotonic applications," *Journal of Biomedical Optics*, vol. 21, no. 6, p. 061010, 2016. [Online]. Available: http://dx.doi.org/10.1117/1.JBO.21.6.061010

[31] W. H. Renninger, A. Chong, and F. W. Wise, "Giant-chirp oscillators for short-pulse fiber amplifiers," *Opt. Lett.*, vol. 33, no. 24, pp. 3025–3027, Dec 2008. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-33-24-3025

[32] L. Zhang, H. Jiang, S. Cui, and Y. Feng, "Integrated ytterbium-raman fiber amplifier," *Opt. Lett.*, vol. 39, no. 7, pp. 1933–1936, Apr 2014. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-39-7-1933

[33] K. S. Abedin, J. M. Fini, T. F. Thierry, V. R. Supradeepa, B. Zhu, M. F. Yan, L. Bansal, E. M. Monberg, and D. J. DiGiovanni, "Multicore erbium doped fiber amplifiers for space division multiplexing systems," *Journal of Lightwave Technology*, vol. 32, no. 16, pp. 2800–2808, Aug 2014.

[34] K. S. Abedin, M. F. Yan, J. M. Fini, T. F. Thierry, L. K. Bansal, B. Zhu, E. M. Monberg, and D. J. DiGiovanni, "Space division multiplexed multicore erbium-doped fiber amplifiers," *Journal of Optics*, vol. 45, no. 3, pp. 231–239, 2016. [Online]. Available: http://dx.doi.org/10.1007/s12596-015-0285-2

[35] C. Gaida, M. Kienel, M. Müller, A. Klenke, M. Gebhardt, F. Stutzki, C. Jauregui, J. Limpert, and A. Tünnermann, "Coherent combination of two tm-doped fiber amplifiers," *Opt. Lett.*, vol. 40, no. 10, pp. 2301–2304, May 2015. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-40-10-2301

[36] B. G. Ward, "Maximizing power output from continuous-wave single-frequency fiber amplifiers," *Opt. Lett.*, vol. 40, no. 4, pp. 542–545, Feb 2015. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-40-4-542

[37] L. Rapp, "Feedforward control techniques for erbium–doped fiber amplifiers — challenges and solutions," *Journal of Optics*, vol. 45, no. 3, pp. 209–230, 2016. [Online]. Available: http://dx.doi.org/10.1007/s12596-015-0289-y

[38] M. Otala, "Transient distortion in transistorized audio power amplifiers," *IEEE Transactions on Audio and Electroacoustics*, vol. 18, no. 3, pp. 234–239, Sep 1970.

[39] M. Otala, "Circuit design modifications for minimizing transient intermodulation distortion in audio amplifiers," *J. Audio Eng. Soc*, vol. 20, no. 5, pp. 396–399, 1972. [Online]. Available: http://www.aes.org/e-lib/browse.cfm?elib=2065

[40] J. Lammasniemi and K. Nieminen, "Distribution of the phonograph signal rate of change," *J. Audio Eng. Soc*, vol. 28, no. 5, pp. 316–319, 1980. [Online]. Available: http://www.aes.org/e-lib/browse.cfm?elib=3986

[41] M. Petri-Larmi, M. Otala, and J. Lammasniemi, "Psychoacoustic detection threshold of transient intermodulation distortion," *J. Audio Eng. Soc*, vol. 28, no. 3, pp. 98–105, 1980. [Online]. Available: http://www.aes.org/e-lib/browse.cfm?elib=4002

[42] P. Colantonio, F. Giannini, and E. Limiti, *High Efficiency RF and Microwave Solid State Power Amplifiers*, 1st ed. US: John Wiley & Sons Inc, 2009.

[43] N. Kumar and A. Grebennikov, "Distributed power amplifiers for rf and microwave communications," 2015.

[44] J. Pang, S. He, Z. Dai, C. Huang, J. Peng, and F. You, "Design of continuous-mode gan power amplifier with compact fundamental impedance solutions on package plane," *IET Microwaves, Antennas Propagation*, vol. 10, no. 10, pp. 1056–1064, 2016.

[45] E. McCune, "Fundamentals of switching rf power amplifiers," *IEEE Microwave and Wireless Components Letters*, vol. 25, no. 12, pp. 838–840, Dec 2015.

[46] W. H. Zurek and W. K. Wootters, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[47] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271 – 272, 1982. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0375960182900846

[48] C. M. Caves, "Quantum-mechanical noise in an interferometer," *Phys. Rev. D*, vol. 23, pp. 1693–1708, Apr 1981. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevD.23.1693

[49] J. A. Vaccaro and D. T. Pegg, "Phase properties of optical linear amplifiers," *Phys. Rev. A*, vol. 49, pp. 4985–4995, Jun 1994. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.49.4985

[50] B. R. Mollow and R. J. Glauber, "Quantum theory of parametric amplification. i," *Phys. Rev.*, vol. 160, pp. 1076–1096, Aug 1967. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRev.160.1076

[51] B. R. Mollow and R. J. Glauber, "Quantum theory of parametric amplification. ii," *Phys. Rev.*, vol. 160, pp. 1097–1108, Aug 1967. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRev.160.1097

[52] R. Loudon, O. Jedrkiewicz, S. M. Barnett, and J. Jeffers, "Quantum limits on noise in dual input-output linear optical amplifiers and attenuators," *Phys. Rev. A*, vol. 67, p. 033803, Mar 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.67.033803

[53] V. Josse, M. Sabuncu, N. J. Cerf, G. Leuchs, and U. L. Andersen, "Universal optical amplification without nonlinearity," *Phys. Rev. Lett.*, vol. 96, p. 163602, Apr 2006. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.96.163602

[54] M. H. Devoret, F. Schackert, R. Vijay, S. M. Girvin, M. Metcalfe, D. E. Prober, N. Bergeal, R. J. Schoelkopf, V. E. Manucharyan, and L. Frunzio, "Phase-preserving amplification near the quantum limit with a josephson ring modulator," *Nature*, vol. 465, no. 7294, pp. 64–68, 2010.

[55] H. Nha, G. J. Milburn, and H. J. Carmichael, "Linear amplification and quantum cloning for non-gaussian continuous variables," *New Journal of Physics*, vol. 12, no. 10, p. 103010, 2010. [Online]. Available: http://stacks.iop.org/1367-2630/12/i=10/a=103010

[56] "Fluctuations in amplification of quanta with application to maser amplifiers," *Journal of the Physical Society of Japan*, vol. 12, no. 6, pp. 686–700, 1957. [Online]. Available: http://dx.doi.org/10.1143/JPSJ.12.686

[57] A. Yariv and W. Louisell, "5a2 - theory of the optical parametric oscillator," *IEEE Journal of Quantum Electronics*, vol. 2, no. 9, pp. 418–424, September 1966.

[58] H. P. Yuen and J. H. Shapiro, "Generation and detection of two-photon coherent states in degenerate four-wave mixing," *Opt. Lett.*, vol. 4, no. 10, pp. 334–336, Oct 1979. [Online]. Available: http://ol.osa.org/abstract.cfm?URI=ol-4-10-334

[59] Z. Y. Ou, S. F. Pereira, and H. J. Kimble, "Quantum noise reduction in optical amplification," *Phys. Rev. Lett.*, vol. 70, pp. 3239–3242, May 1993. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.70.3239

[60] J. A. Levenson, K. Bencheikh, D. J. Lovering, P. Vidakovic, and C. Simonneau, "Quantum noise in optical parametric amplification: a means to achieve noiseless optical functions," *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B*, vol. 9, no. 2, p. 221, 1997. [Online]. Available: http://stacks.iop.org/1355-5111/9/i=2/a=009

[61] T. C. Ralph and A. P. Lund, "Nondeterministic noiseless linear amplification of quantum systems," in *Ninth International Conference on Quantum Communication, Measurement and Computing (QCMC)*, A. Lvovsky, Ed.

[62] J. S. Neergaard-nielsen, Y. Eto, C.-w. Lee, H. Jeong, and M. Sasaki, "Quantum tele-amplification with a continuous-variable superposition state," *Nature Photonics*, vol. 7, no. 6, p. 439, 2013. [Online]. Available: http://dx.doi.org/10.1038/nphoton.2013.101

[63] F. Ferreyrol, M. Barbieri, R. Blandino, R. Tualle-Brouri, and P. Grangier, "Implementation of a non-deterministic optical noiseless amplifier," in *Quantum Electronics Conference Lasers and Electro-Optics (CLEO/IQEC/PACIFIC RIM), 2011*, Aug 2011, pp. 965–967.

[64] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, "Heralded noiseless amplification of a photon polarization qubit," *Nature Physics*, vol. 9, no. 1, p. 23, 2013.

[65] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, "Measurement-based noiseless linear amplification for quantum communication," *Nature Photonics*, vol. 8, no. 4, p. 333, 2014.

[66] T. C. Ralph, G. Y. Xiang, A. P. Lund, G. J. Pryde, and N. Walk, "Heralded noiseless linear amplification and distillation of entanglement," *Nature Photonics*, vol. 4, no. 5, pp. 316–319, 2010.

[67] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, "Implementation of a nondeterministic optical noiseless amplifier," *Phys. Rev. Lett.*, vol. 104, p. 123603, Mar 2010. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.104.123603

[68] P. Marek and R. Filip, "Coherent-state phase concentration by quantum probabilistic amplification," *Phys. Rev. A*, vol. 81, p. 022302, Feb 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.81.022302

[69] J. Fiurášek, "Engineering quantum operations on traveling light beams by multiple photon addition and subtraction," *Phys. Rev. A*, vol. 80, p. 053822, Nov 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.80.053822

[70] J. Jeffers, "Nondeterministic amplifier for two-photon superpositions," *Phys. Rev. A*, vol. 82, p. 063828, Dec 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.82.063828

[71] H.-J. Kim, S.-Y. Lee, S.-W. Ji, and H. Nha, "Quantum linear amplifier enhanced by photon subtraction and addition," *Phys. Rev. A*, vol. 85, p. 013839, Jan 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.85.013839

[72] E. Eleftheriadou, S. M. Barnett, and J. Jeffers, "Quantum optical state comparison amplifier," *Phys. Rev. Lett.*, vol. 111, p. 213601, Nov 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.111.213601

[73] A. Zavatta, J. Fiurek, and M. Bellini, "A high-fidelity noiseless amplifier for quantum light states," *Nat. Photonics*, vol. 5, pp. 52–60, 2011.

[74] M. A. Usuga, C. R. Mller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, "Noise-powered probabilistic concentration of phase information," *Nat. Physics*, vol. 6, pp. 767–771, 2010.

[75] R. J. Donaldson, R. J. Collins, E. Eleftheriadou, S. M. Barnett, J. Jeffers, and G. S. Buller, "Experimental implementation of a quantum optical state comparison amplifier," *Phys. Rev. Lett.*, vol. 114, p. 120505, Mar 2015. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.114.120505

[76] J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam, "Surpassing the no-cloning limit with a heralded hybrid linear amplifier for coherent states," *Nature Communications*, vol. 7, p. 13222, 2016.

[77] N. Yamamoto, "Quantum feedback amplification," *Phys. Rev. Applied*, vol. 5, p. 044012, Apr 2016. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevApplied.5.044012

[78] L. Duan, P. Zoller, M. D. Lukin, and J. I. Cirac, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, 2001. [Online]. Available: http://dx.doi.org/10.1038/35106500

[79] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar 2011. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.83.33

[80] K. Kim, M.-S. Chang, R. Islam, S. Korenblit, L.-M. Duan, and C. Monroe, "Entanglement and tunable spin-spin couplings between trapped ions using multiple transverse modes," *Phys. Rev. Lett.*, vol. 103, p. 120502, Sep 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.103.120502

[81] B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, "Robust creation of entanglement between remote memory qubits," *Phys. Rev. Lett.*, vol. 98, p. 240502, Jun 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.240502

[82] L.-M. Duan and H. J. Kimble, "Efficient engineering of multiatom entanglement through single-photon detections," *Phys. Rev. Lett.*, vol. 90, p. 253601, Jun 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.90.253601

[83] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, "Multiplexed memory-insensitive quantum repeaters," *Phys. Rev. Lett.*, vol. 98, p. 060502, Feb 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.060502

[84] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories,"

Phys. Rev. Lett., vol. 98, p. 190503, May 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.190503

[85] N. Sangouard, C. Simon, J. c. v. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," *Phys. Rev. A*, vol. 76, p. 050301, Nov 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.76.050301

[86] X.-Y. Chang, D.-L. Deng, X.-X. Yuan, P.-Y. Hou, Y.-Y. Huang, and L.-M. Duan, "Experimental realization of an entanglement access network and secure multi-party computation," *Scientific reports*, vol. 6, p. 29453, 2016.

[87] S. J. Devitt, A. D. Greentree, A. M. Stephens, and R. Van Meter, "High-speed quantum networking by ship," *Scientific reports*, vol. 6, p. 36163, 2016. [Online]. Available: https://link.aps.org/doi/10.1038/srep36163

[88] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012326, Jul 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.72.012326

[89] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, p. 070502, Feb 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.96.070502

[90] Y. Mu, J. Seberry, and Y. Zheng, "Shared cryptographic bits via quantized quadrature phase amplitudes of light," *Optics Communications*, vol. 123, no. 1, pp. 344 – 352, 1996. [Online]. Available: http://www.sciencedirect.com/science/article/pii/0030401895006885

[91] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography," *Japanese Journal of Applied Physics*, vol. 43, no. 9A, p. L1217, 2004. [Online]. Available: http://stacks.iop.org/1347-4065/43/i=9A/a=L1217

[92] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, pp. 3283–3286, Oct 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.81.3283

[93] J. Yin, Y. Cao, Y. H. Li, S. K. Liao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, B. Li, and H. Dai, "Satellite-based entanglement distribution over 1200 kilometers." *Science*, vol. 356, no. 6343, p. 1140, 2017.

[94] D. T. Pegg, L. S. Phillips, and S. M. Barnett, "Optical state truncation by projection synthesis," *Phys. Rev. Lett.*, vol. 81, pp. 1604–1606, Aug 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.81.1604

[95] A. Zavatta, S. Viciani, and M. Bellini, "Quantum-to-classical transition with single-photon-added coherent states of light," *Science*, vol. 306, no. 5696, pp. 660–662, 2004. [Online]. Available: http://science.sciencemag.org/content/306/5696/660

[96] A. Zavatta, S. Viciani, and M. Bellini, "Single-photon excitation of a coherent state: Catching the elementary step of stimulated light emission," *Phys. Rev. A*, vol. 72, p. 023820, Aug 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.72.023820

[97] V. Parigi, A. Zavatta, M. Kim, and M. Bellini, "Probing quantum commutation rules by addition and subtraction of single photons to/from a light field," *Science*, vol. 317, no. 5846, pp. 1890–1893, 2007. [Online]. Available: http://science.sciencemag.org/content/317/5846/1890

[98] A. Zavatta, V. Parigi, M. S. Kim, H. Jeong, and M. Bellini, "Experimental demonstration of the bosonic commutation relation via superpositions of quantum operations on thermal light fields," *Phys. Rev. Lett.*, vol. 103, p. 140406, Oct 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.103.140406

[99] M. S. Kim, H. Jeong, A. Zavatta, V. Parigi, and M. Bellini, "Scheme for proving the bosonic commutation relation using single-photon interference," *Phys. Rev. Lett.*, vol. 101, p. 260401, Dec 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.101.260401

[100] J. McKeever, J. R. Buck, A. D. Boozer, A. Kuzmich, H.-C. Nägerl, D. M. Stamper-Kurn, and H. J. Kimble, "State-insensitive cooling and trapping of single atoms in an optical cavity," *Phys. Rev. Lett.*, vol. 90, p. 133602, Apr 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.90.133602

[101] A. Kuhn, M. Hennrich, and G. Rempe, "Deterministic single-photon source for distributed quantum networking," *Phys. Rev. Lett.*, vol. 89, p. 067901, Jul 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.89.067901

[102] V. S. Denchev and G. Pandurangan, "Distributed quantum computing: A new frontier in distributed systems or science fiction?" *SIGACT News*, vol. 39, no. 3, pp. 77–95, Sept. 2008. [Online]. Available: http://doi.acm.org/10.1145/1412700.1412718

[103] J. Joo, Y.-J. Park, S. Oh, and J. Kim, "Quantum teleportation via a w state," *New Journal of Physics*, vol. 5, no. 1, p. 136, 2003. [Online]. Available: http://stacks.iop.org/1367-2630/5/i=1/a=136

[104] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.1330

[105] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052304, Apr 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.052304

[106] R. Loudon, *The quantum theory of light*, 3rd ed. Oxford;New York: Oxford University Press, 2000.

[107] J. Johansson, P. Nation, and F. Nori, "Qutip 2: A python framework for the dynamics of open quantum systems," *Computer Physics Communications*, vol. 184, no. 4, pp. 1234 – 1240, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0010465512003955

[108] J. Gough and M. James, "The series product and its application to quantum feedforward and feedback networks," *Automatic Control, IEEE Transactions on*, vol. 54, no. 11, pp. 2530–2544, Nov 2009.

[109] H. . Bachor and T. C. Ralph, *A guide to experiments in quantum optics*, 2nd ed. Weinheim: Wiley-VCH, 2004.

[110] C. W. Gardiner and P. Zoller, *Quantum noise: a handbook of Markovian and non-Markovian quantum stochastic methods with applications to quantum optics*, 3rd ed. New York; Berlin: Springer, 2004.

[111] M. Yanagisawa and H. Kimura, "Transfer function approach to quantum control-part i: Dynamics of quantum feedback systems," *Automatic Control, IEEE Transactions on*, vol. 48, no. 12, pp. 2107–2120, Dec 2003.

[112] M. Yanagisawa and H. Kimura, "Transfer function approach to quantum control-part ii: Control concepts and applications," *Automatic Control, IEEE Transactions on*, vol. 48, no. 12, pp. 2121–2132, Dec 2003.

[113] B. D. O. Anderson, *Optimal filtering*. Englewood Cliffs, N.J: Prentice-Hall, 1979.

[114] L. Bouten, R. V. Handel, and M. R. James, "An introduction to quantum filtering," *SIAM Journal on Control and Optimization*, vol. 46, no. 6, pp. 2199–2241, 2007. [Online]. Available: http://dx.doi.org/10.1137/060651239

[115] N.-R. Zhou, L.-J. Wang, J. Ding, L.-H. Gong, and X.-W. Zuo, "Novel quantum deterministic key distribution protocols with entangled states," *International Journal of Theoretical Physics*, vol. 49, no. 9, pp. 2035–2044, Sep 2010. [Online]. Available: https://doi.org/10.1007/s10773-010-0387-1

[116] X. Li and D. Zhang, "Multiparty quantum determined key distribution protocol using ghz states," in *2010 International Conference on Networking and Digital Society*, vol. 1, May 2010, pp. 203–206.

[117] M. Zhong, M. P. Hedges, R. L. Ahlefeldt, J. G. Bartholomew, S. E. Beavan, S. M. Wittig, J. J. Longdell, and M. J. Sellars, "Optically addressable nuclear spins in a solid with a six-hour coherence time," *Nature*, vol. 517, no. 7533, pp. 177–180, 2015. [Online]. Available: http://dx.doi.org/10.1038/nature14025

[118] G. Zhang and M. R. James, "On the response of quantum linear systems to single photon input fields," *IEEE Transactions on Automatic Control*, vol. 58, no. 5, pp. 1221–1235, May 2013.

[119] T. M. Stace and H. M. Wiseman, "Approximate method for treating dispersion in one-way quantum channels," *Phys. Rev. A*, vol. 73, p. 012317, Jan 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.73.012317

[120] T. M. Stace, C. H. W. Barnes, and G. J. Milburn, "Mesoscopic one-way channels for quantum state transfer via the quantum hall effect," *Phys. Rev. Lett.*, vol. 93, p. 126804, Sep 2004. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.93.126804

[121] N. A. Gershenfeld and I. L. Chuang, "Bulk spin-resonance quantum computation," *Science*, vol. 275, no. 5298, pp. 350–356, 1997.

[122] D. Goswami, "Laser phase modulation approaches towards ensemble quantum computing," *Phys. Rev. Lett.*, vol. 88, p. 177901, Apr 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.88.177901

[123] J. Ahn, T. C. Weinacht, and P. H. Bucksbaum, "Information storage and retrieval through quantum phase," *Science*, vol. 287, no. 5452, pp. 463–465, 2000.

[124] N. Yamamoto and M. R. James, "Zero-dynamics principle for perfect quantum memory in linear networks," *New Journal of Physics*, vol. 16, no. 7, p. 073032, 2014. [Online]. Available: http://stacks.iop.org/1367-2630/16/i=7/a=073032

[125] Y. Li, A. R. R. Carvalho, and M. R. James, "Continuous-mode operation of a noiseless linear amplifier," *Phys. Rev. A*, vol. 93, p. 052312, May 2016. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.93.052312

[126] J. G. Proakis and D. G. Manolakis, *Digital signal processing: principles, algorithms, and applications*, 3rd ed. Englewood Cliffs, NJ: Prentice Hall International, 1996.

[127] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, "Quantum channels and memory effects," *Rev. Mod. Phys.*, vol. 86, pp. 1203–1259, Dec 2014. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.86.1203

[128] L. Balogh and R. Pintelon, "Stable approximation of unstable transfer function models," *IEEE Transactions on Instrumentation and Measurement*, vol. 57, no. 12, pp. 2720–2726, Dec 2008.

[129] T. J. Moir, "Inverting non-minimum phase fir transfer functions with application to reverberant speech," *International Journal of Speech Technology*, vol. 17, no. 3, pp. 245–252, 2014. [Online]. Available: http://dx.doi.org/10.1007/s10772-014-9227-7

[130] B. D. Radlovic and R. A. Kennedy, "Nonminimum-phase equalization and its subjective importance in room acoustics," *IEEE Transactions on Speech and Audio Processing*, vol. 8, no. 6, pp. 728–737, Nov 2000.

[131] A. L. Alexander, J. J. Longdell, M. J. Sellars, and N. B. Manson, "Photon echoes produced by switching electric fields," *Phys. Rev. Lett.*, vol. 96, p. 043602, Feb 2006. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.96.043602

[132] G. Hétet, J. J. Longdell, A. L. Alexander, P. K. Lam, and M. J. Sellars, "Electro-optic quantum memory for light using two-level atoms," *Phys. Rev. Lett.*, vol. 100, p. 023601, Jan 2008. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.100.023601

[133] M. R. Hush, A. R. R. Carvalho, M. Hedges, and M. R. James, "Analysis of the operation of gradient echo memories using a quantum inputoutput model," *New Journal of Physics*, vol. 15, no. 8, p. 085020, 2013. [Online]. Available: http://stacks.iop.org/1367-2630/15/i=8/a=085020

[134] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," *Science*, vol. 320, no. 5876, pp. 646–649, 2008. [Online]. Available: http://science.sciencemag.org/content/320/5876/646

[135] N. Rotenberg, P. Türschmann, H. R. Haakh, D. Martin-Cano, S. Götzinger, and V. Sandoghdar, "Small slot waveguide rings for on-chip quantum optical circuits," *Opt. Express*, vol. 25, no. 5, pp. 5397–5414, Mar 2017. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-25-5-5397