Quantum-based Security in Optical Fibre Networks

Ross James Donaldson

Submitted for the degree of Doctor of Philosophy

Heriot-Watt University

School of Engineering and Physical Sciences

April 2016

ABSTRACT

Electronic communication is used everyday for a number of different applications. Some of the information transferred during these communications can be private requiring encryption and authentication protocols to keep this information secure. Although there are protocols today which provide some security, they are not necessarily unconditionally secure. Quantum based protocols on the other hand, can provide unconditionally secure protocols for encryption and authentication.

Prior to this Thesis, only one experimental realisation of quantum digital signatures had been demonstrated. This used a lossy photonic device along with a quantum memory allowing two parties to test whether they were sent the same signature by a single sender, and also store the quantum states for measurement later. This restricted the demonstration to distances of only a few metres, and was tested with a primitive approximation of a quantum memory rather than an actual one. This Thesis presents an experimental realisation of a quantum digital signature protocol which removes the reliance on quantum memory at the receivers, making a major step towards practicality. By removing the quantum memory, it was also possible to perform the swap and comparison mechanism in a more efficient manner resulting in an experimental realisation of quantum digital signatures over 2 kilometres of optical fibre.

Quantum communication protocols can be unconditionally secure, however the transmission distance is limited by loss in quantum channels. To overcome this loss in conventional channels an optical amplifier is used, however the added noise from these would swamp the quantum signal if directly used in quantum communications.

This Thesis looked into probabilistic quantum amplification, with an experimental realisation of the state comparison amplifier, based on linear optical components and single-photon detectors. The state comparison amplifier operated by using the well-established techniques of optical coherent state comparison and weak subtraction to post-select the output and provide non-deterministic amplification with increased fidelity at a high repetition rate. The success rates of this amplifier were found to be orders of magnitude greater than other state of the art quantum amplifiers, due to its lack of requirement for complex quantum resources, such as single or entangled photon sources, and photon number resolving detectors.

Acknowledgements

First of all I'd like to thank Professor Gerald S. Buller who was my mentor during my Undergraduate degree, and my supervisor during this PhD. His supervision and advice over the years has been invaluable and always guided me in the right direction.

I'd also like to thank Dr Robert Collins for his supervision and assistance during my PhD. Also for reading and fixing all the first drafts of papers, reports, and even this Thesis, that cannot have been easy.

I'd like to thank my collaborators over the years from Heriot-Watt University, Professor Erika Andersson, Dr Vedran Dunjko, Dr Petros Wallden, and Ryan Amiri. Especially Erika who proof-read Chapters of this Thesis, and also Ryan for helping me better understand some theoretical concepts behind quantum digital signatures.

From the University of Strathclyde, I'd like to thank Dr John Jeffers, Dr Electra Eleftheriadou, and Dr Luca Mazzarella. Especially John who has been a collaborator on all of the projects I have worked on, and also took the time to proof-read some Chapters of this Thesis.

From the University of Glasgow, I'd like to thank Stephen Barnett.

I'd like to thank everyone from the Single-Photon Group at Heriot-Watt University for their support over my PhD. I'd like to thank Loraine Markland for her assistance since the start of my PhD. Everyone involved in Friday football and Friday beers for keeping me fit and fat throughout the PhD.

I'd also like to thank Aurora Maccarone who has somehow managed put up with me in the office since the beginning of the PhD.

Finally I'd like to thank my family for support through my PhD, I'm sure they will be glad I'm no longer a tax dodging student.

ACADEMIC REGISTRY
Research Thesis Submission

Name*:*	Ross James Donaldson		
School/PGI:	Engineering and Physical Sciences		
Version: *(i.e. First, Resubmission, Final)*	Final	Degree Sought (Award **and** Subject area)	PhD Physics

Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1) the thesis embodies the results of my own work and has been composed by myself
2) where appropriate, I have made acknowledgement of the work of others and have made reference to work carried out in collaboration with other persons
3) the thesis is the correct version of the thesis for submission and is the same version as any electronic versions submitted*.
4) my thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5) I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.

* *Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.*

Signature of Candidate*:*		Date:	

Submission

Submitted By *(name in capitals):*	ROSS JAMES DONALDSON
Signature of Individual Submitting:	
Date Submitted:	

For Completion in the Student Service Centre (SSC)

Received in the SSC by *(name in capitals):*			
1.1 Method of Submission *(Handed in to SSC; posted through internal/external mail):*			
1.2 E-thesis Submitted (**mandatory for final theses)**			
Signature:		Date:	

Table of contents

List of Publications by the Candidate

Journal publications

R.J. Collins, **R.J. Donaldson**, V. Dunjko, P. Wallden, P.J. Clarke, E. Andersson, J. Jeffers, G.S. Buller, "Realization of quantum digital signatures without the requirement of quantum memory", Physical Review Letters, 113, 040502 (2014)

R.J. Donaldson, R.J. Collins, E. Eleftheriadou, S.M. Barnett, J. Jeffers, G.S. Buller, "Experimental Implementation of a quantum optical state comparison amplifier", Physical Review Letters, 114, 120505 (2015)

R.J. Donaldson, R.J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, G.S. Buller, "Experimental demonstration of kilometre-range quantum digital signatures", Physical Review A, 93, 012329 (2016)

Conference proceedings

R.J. Donaldson, R.J. Collins, V. Dunkjo, P.J. Clarke, E. Andersson, J. Jeffers, G.S. Buller, "An approach to experimental photonic quantum digital signatures in fiber", SPIE Dresden, Security and Defence, 8899, (2013)

R.J. Collins, **R.J. Donaldson**, V. Dunjko, P. Wallden, P.J. Clarke, E. Andersson, J. Jeffers, G.S. Buller, "An in fiber experimental approach to photonic quantum digital signatures that does not require quantum memory", SPIE Amsterdam, Security and Defence, 9254, (2014)

Chapter 1

Introduction

1.1 Introduction

The privacy and authenticity of electronic communications (e.g. e-commerce, online voting, stocks and share, emails) has become an extremely important topic given the current trend of moving to electronic communications for ease of use.

For instance, one party (Alice) may wish to send a private message to a receiver (Bob). Before sending the message they must share some encryption key, which allows them send the message over an insecure communication channel. Sharing of the key can be accomplished by several different methods, however an eavesdropper could intercept the key sharing and be able to almost effortlessly eavesdrop into the private messages.

One method to overcome the eavesdropper was to perform key sharing where partial information is given to a party to encrypt a private message. The remaining information kept by the other party allows them to decrypt the encrypted information, however this information isn't released meaning an eavesdropper would still require a large amount of effort to decrypting the message. This method is known as public-key cryptography, where in commonly used protocols Alice generates some parameters and sends some out into a public channel where Bob can receive them. Alice can decrypt the message encrypted by Bob based on the parameters she has kept.

Although the public key cryptography schemes allow efficient sharing of encryption keys, and can be used to provide authentication protocols as well, an eavesdropper can still intercept the encrypted message and try to break the encryption. These protocols are not unconditionally secure, meaning there is possibility they can be broken faster than a brute force attack which is simply guessing until they get the right answer.

The one-time pad is an encryption protocol which is unconditionally secure, however an eavesdropper could intercept the key during the sharing process. In order to provide unconditional secure encryption, the sending of the key must be made unconditionally secure. Quantum based protocols, where the security is based on the well-known laws of

quantum mechanics, can provide unconditionally secure encryption key, and digital signature sharing, which allows eavesdroppers to be revealed during the sharing. This solves two key issues with today's conventional protocols.

This Thesis focuses on two topics, quantum digital signatures (QDS) [1], and quantum amplification [2], more specifically experimentally realising those protocols. While quantum key distribution (QKD) [3], a more mature quantum technology, focuses on secure key distribution, QDS looks at the problem of message authentication and message transferability. Quantum amplification is also a less mature technology, focusing on amplifying quantum states, which could lead to applications in extending the transmission distance of QKD and QDS.

Chapter 2 will describe technology which was used to perform experiments carried out in this Thesis. It also includes overviews of other technologies which could be implemented and highlights the reasons why they are not chosen for the experimental realisations in this Thesis.

With the enabling technologies reviewed, Chapter 3 will focus on cryptography and digital signatures, with both conventional and quantum protocols described. Firstly, conventional protocols are introduced to give the reader an idea of how cryptography and digital signatures work. Hacking and breaking of conventional communications is a hot topic, so current and possible future methods are described [4]. With that covered the reasons why quantum methods of communications are being sought are highlighted.

Chapter 4 is the first experimental research Chapter, covering work on an experimental realisation of QDS which did not require any quantum memories [5]. Chapter 2 gives an overview of quantum memory technologies, after that it will be clear to see why quantum memory is not, at the moment, a good technology to rely on for quantum communication protocols [6]. This complete removal of quantum memory from the experimental implementation allowed a quantum digital signature protocol which was actually experimentally possible to build with today's technology.

Chapter 5 follows on from work carried out in Chapter 4, and describes an experimental realisation of a QDS protocol which could be carried out over kilometre ranges, also

without the requirement for quantum memory [7]. This experiment shows another major step forward for QDS becoming a commercially viable technology.

Chapter 6 moves onto the other topic of this Thesis, quantum amplification. Firstly, an overview of how amplification is carried out in conventional optical telecommunications is given. This is followed by methods for carrying out quantum optical amplification using non-deterministic post-processing.

Chapter 7 will describe the state comparison amplifier (SCAMP), a quantum optical amplifier based on photon addition and subtraction [8]. This amplifier does not require any complex quantum resources such as single-photon sources, or photon number resolving detectors, making its experimental implementation much simpler. As well as examining basic characteristics, the device is also tested for robustness against added optical noise from a wide, and a narrow band wavelength source.

Chapter 8 will describe some experiments which further investigated properties of state comparison amplifier. The first experiment was to increase the nominal gain to overcome experimental losses experienced in the Chapter 7 implementation. Noise robustness for this higher gain device was also investigated, but only with the narrow band wavelength source. Finally the device characteristics with an extra subtraction stage are described.

Chapter 9 will serve as a general conclusion to the Thesis. This will summarise each Chapter highlighting key results and discoveries. This chapter will also describe future work which could be undertaken, based on the conclusions.

1.2 Bibliography

[1] D. Gottesman and I. Chuang, "Quantum Digital Signatures," *arXiv.org*, no. 0105032v2, 2001.

[2] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Nov. 2005.

[3] W. Tittel, H. Zbinden, and N. Gisin, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[4] M. Campagna, L. Chen, Ö. Dagdelen, J. Ding, J. K. Fernick, N. Gisin, D. Hayford,

T. Jennewein, N. Lütkenhaus, M. Mosca, B. Neill, M. Pecen, R. Perlner, G. Ribordy, J. M. Schanck, D. Stebila, N. Walenta, W. Whyte, and Z. Zhang, *Quantum Safe Cryptography and Security*, no. 8. 2015.

[5] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[6] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nat. Photonics*, vol. 3, no. 12, pp. 706–714, Dec. 2009.

[7] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, "Experimental demonstration of kilometer-range quantum digital signatures," *Phys. Rev. A*, vol. 93, no. 1, p. 012329, Jan. 2016.

[8] 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, no. 12, p. 120505, 2015.

Chapter 2

Review of Enabling Technologies

2.1 Introduction

The topic of this Thesis falls under the area of quantum communications, a relatively new (and exciting) area in the subject of communications. As well as being new, the technologies and methods required for implementing quantum cryptographic protocols are vastly different to those used to carry out conventional protocols, which we use every day. This Chapter will deal with the technologies required to experimentally implement quantum communications protocols while the following Chapter will introduce some of those protocols with examples using the technologies highlighted here.

Understanding the technology which can be used for implementing quantum cryptographic protocols is vital, as this enables us to understand the practical limitations of quantum communications, and therefore make a better estimate of applications. For this reason, enabling technologies is covered before the communications Chapter, as some of the subtleties in quantum communications protocol workings may not appreciated without understanding the technology behind it.

The first section of this Chapter gives an overview of single-photon and attenuated laser sources, which provide the photons for quantum communications protocols which require the use of single or low photon number pulses of light. The second section describes photon detection technologies which are sensitive enough to detect the weak intensity light that is received in quantum communications protocols. The third section will give an overview of quantum memories, an important quantum technology for many quantum information experiments, and also quantum computers. The fourth section covers transmission media for quantum communications. Different transmission media have different characteristics, in terms of loss, and effect on photon properties, therefore the choice of transmission medium should be considered depending on the communications protocol.

2.2 Single-photon and attenuated laser sources

As will be discussed in greater detail in the following chapter, quantum key distribution (QKD) protocols require single-photon level pulses in order to provide protection from a range of eavesdropping attacks. In the original quantum key distribution proposal, [1], Alice sends a pulse train of single-photons, each with a corresponding information encoding. Later protocols have expanded this to coherent states [2] but perfect single-photon sources still offer significant advantages, such as improved transmission distance, bit rate [3], and therefore remain important. Additionally, single-photons have uses in optical quantum amplifiers [4], [5] and some applications of quantum computing [6].

Single-photon sources are desirable for QKD, other quantum communications and information experiments, such as quantum digital signatures (QDS) [7] may also find some benefit as well, as QDS can be performed using components similar to QKD. This section will deal with how these single-photon level pulses can be generated, and also give an overview of single-photon sources.

2.2.1 Weak coherent sources

Coherent sources, lasers, are well known for providing light which, when examined within the coherence time, is indistinguishable, i.e. the properties of the photons emitted during the coherence time are all identical. Coherent sources have emission which conforms to Poissonian photon statistics with random spacing of photons in the optical stream [8]. This means that they can be used to generate low mean photon number per pulse ($|\alpha|^2$) at the single-photon level, but are not true single-photon sources as there will be a statistical spread of photon numbers around the mean value.

The Poissonian statistics for the probability of finding a certain number of photons in a pulse is given in Figure 2.1 for low $|\alpha|^2$ of 0.1, 0.5, and 1. As $|\alpha|^2$ increases the probability of >1 photon being in a given pulse increases. However this increase in the probability of >1 photon per pulse for the pulses that generate the key has serious security implications for quantum key distribution as this can allow an eavesdropper to optimise certain attacks [9]. However, as will be seen in Chapter 3, the decoy-state QKD protocol implements different $|\alpha|^2$ to test the quantum channel for eavesdropper, allowing a greater $|\alpha|^2$ signal. However when $|\alpha|^2$ is reduced, the probability of a vacuum pulse, i.e. no photons being present increases, this will effectively reduce the maximum transmission distance and information transfer [9].

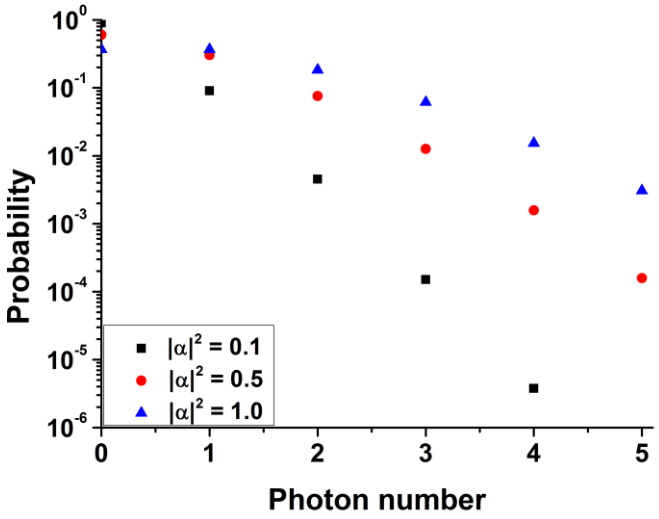


Figure 2.1 — Probability of a number of photons in a pulse, for a coherent source, given the mean photon number ($|\alpha|^2$).

Semiconductor laser technologies which emit in the visible and infrared regions (more specifically in the wavebands around 1310 and 1550 nm) are common devices used as attenuated coherent sources in quantum communications applications [10]–[14]. These wavelengths have been selected as they offer compatibility with the low loss windows in fused silica optical fibres of the type used for many telecommunications links [15] - this will be covered in more detail in section 2.5. These laser devices are inexpensive (primarily as they are now manufactured in bulk for the telecommunications industry), reliable, easy to operate, and generally operate either at or near room temperature.

The coherent laser source used to generate the low $|\alpha|^2$ photon streams in all experiments presented in this Thesis is the vertical-cavity surface-emitting laser (VCSEL) diode [16]. More specifically the Honeywell HFE4080-321, an indium-gallium-arsenide (InGaAs) quantum well active region with distributed Bragg gratings which emits at ≈850 nm [17]. The structure can be seen in Figure 2.2. This device is used with Peltier cooling and operates just below room temperature, and requires commonly available electrical injection electronics for operation making it a relatively simple device compared to single-photon sources.

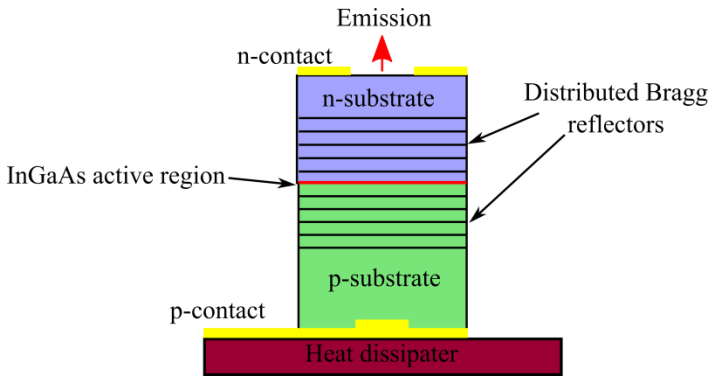


Figure 2.2 - Vertical-cavity surface-emitting laser (VCSEL) diode schematic. The device is constructed of an n and p substrate with an active region composed of multiple quantum wells. The device has distributed Bragg reflectors to create a resonance. Carriers are inserted through metal contacts placed either side of the substrates.

An applied current injects carriers into the semiconductor device, the carriers recombined in the active region emitting light, at a certain threshold current the device will produce. stimulated emission generated from the resonance will cause an exponential increase in light intensity. The device has the advantage of high bandwidth (several GHz), a "circular" output emission, and a narrow linewidth (<0.1nm), which makes it compatible with the proposed optical fibre based quantum communications systems used in this thesis.

Attenuated coherent laser sources are frequently used as the photon sources in quantum information experiments because of the relative ease of implementation. This ease of implementation has led to them being used as photon sources in current commercial QKD systems [18]–[20].

2.2.2 Coherent states

Attenuated coherent sources with low $|\alpha|^2$ give quantum states known as coherent states [8]. These are quantized electromagnetic field states based on the quantized harmonic oscillator. Quantum harmonic oscillators are known to have quantized energy levels of the form $E_n=\left(n+{}^{1}/_{2}\right)\hbar\omega$, with a position and momentum which satisfies the Heisenberg uncertainty principle [8]

Coherent states are denoted $|\alpha\rangle$ in Dirac notation, where $\alpha = X_1 + X_2$, $\alpha = |\alpha|e^{i\phi}$. X_1 and X_2 are quadratures in a phasor diagram shown in Figure 2.3. The phasor representation can be given with the phasor length $|\alpha|^2 = X_1^2 + X_2^2$ and an angle Φ.

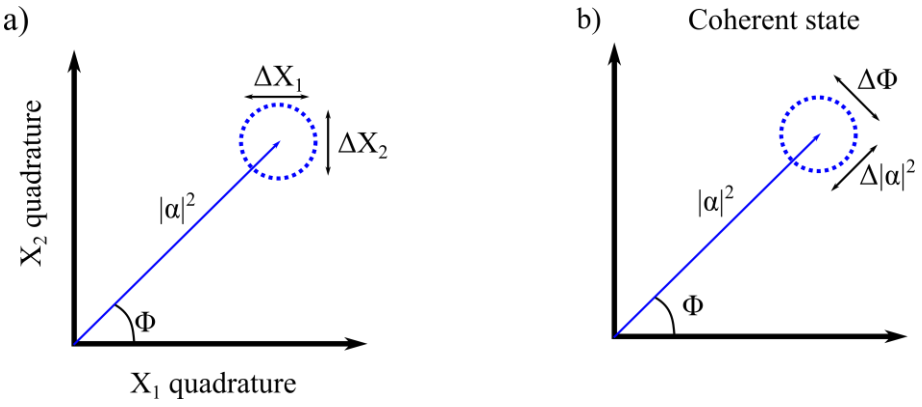


Figure 2.3- a) phasor diagram for a coherent state showing the quadrature uncertainties. b) coherent state quadrature uncertainties referring to the mean photon number $|\alpha|^2$ and the uncertainty in phase.

Coherent states are said to be a minimum uncertainty state, and so the uncertainties in each quadrature are equal, $\Delta X_1 = \Delta X_2 = \frac{1}{2}$. The length of $|\alpha|^2$ is related to the electric field amplitude, and for quantised light is made of discrete energy levels $E_{quantum} = (\bar{n}+1/2)\hbar\omega$. $\bar{n}$ is the average photon number hence why $|\alpha|^2$ is referred to as the mean photon number. The quadratures of uncertainty for the coherent state are taken as the uncertainty in the $|\alpha|^2$ length, and the uncertainty in the phase Φ. The photon number representation of a coherent state is given by Equation 2.1 where *n* is the photon number. Coherent states obey Poissonian photon number statistics.

$$|\alpha\rangle = \exp\left(-|\alpha|^2/2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \qquad \text{Equation 2.1}$$

2.2.2 Overview of single-photon sources

Although single-photon sources are not used in the experiments described in this Thesis, they are worth covering in an overview because they are important for QKD and other quantum information experiments. Single-photon sources can be classified into two categories, deterministic and probabilistic sources. The nature of a deterministic source is to emit a single-photon when it is excited, whereas a probabilistic source may or may not

emit a single-photon when it is excited (sometimes emitting more). A table of the key properties for type of single-photon source (including the attenuated coherent source) is given in Table 2.1.

As in the case of a coherent laser source, specific photon statistics can be used to characterise deterministic and probabilistic sources. Sub-Poissonian statistics, where the spread in photon number around the mean is smaller than the mean value, govern deterministic sources. Super-Poissonian emission, where the spread in photon number around the mean is greater than the mean value, governs the emissions for probabilistic sources e.g. entanglement sources.

Another important measure for single-photon sources is the spacing of each single-photon in the photon stream, which can be characterised by the second order correlation function ($g^2(0)$) measured by the Hanbury-Brown Twiss experiment [8], [21]. The emission of single-photons should have an approximately periodic separation (that is to say anti-bunched, i.e. photons are not emitted in clusters) if it is a perfect single photon source, i.e. emitting only one photon at a known time of excitation. A coherent laser source has a $g^2(0) = 1$ because its emission is randomly distributed, whereas a perfect single-photon source will have $g^2(0) \approx 0$, because only one photon or pair will be emitted at a time.

Deterministic single-photon sources, i.e. quantum dots [22]–[30], colour centres [31], [32], and single molecules [33], [34], are said to be true single-photon sources, as the internal photon emission processes only allow one photon to be emitted at a time. In many cases, the multiphoton events measured from these sources are due to simultaneous excitation and collection of multiple sites. Deterministic sources are an ideal technology for achieving the maximum range in quantum communication protocols. However, they are cumbersome to work with, some requiring cryogenics, but all requiring relatively high loss coupling optics which reduces the extraction efficiency of devices, leading to ”useful” count rates of <500 kHz at detectors, therefore can technically be seen as non-deterministic emitters are the actual emission is random. The anti-bunching $g^{(2)}(0)$ for these sources has been shown to be <<0.5 [35] (as low at 0.04 in colour centres [32]), showing that these sources exhibit strong single-photon qualities.

Source type	Probabilistic or deterministic emitter?	Electrically or Optically Driven?	Operating Temperature	General wavelength range	$g^{(2)}(0)$	Rate of emission
Coherent source [17]	Deterministic	Either	Can be cooled or heated	UV, Visible, IR	1	GHz
Quantum dot semiconductor [26]–[28], [36], [37]	Deterministic	Either	Cryogenic and room temp	UV, Visible, IR	<0.5	KHz
Quantum dot colour-centre N-V [32], [38], [39]	Deterministic	Primarily optical	Room temperature	600-800 nm	<0.1	KHz
Quantum dot colour-centre Si-V [32], [39]	Deterministic	Primarily optical	Room temperature	739 nm	<0.1	KHz
Single molecule of Terrylene [33], [36]	Deterministic	Optical	Room temperature	532 nm	No value found	KHz
Spontaneous parametric down-conversion [40]–[43]	Probabilistic	Optical	Heated down-conversion crystal (above room temperature)	Telecommunication	<0.1	MHz
Four-wave mixing [44]–[46]	Probabilistic	Optical	Room temperature	Telecommunication	<0.1	MHz

Table 2.1 - Single-photon source summary. [31], [33], [35], [43]

Spontaneous parametric down-conversion (SPDC) [8], [40], [41], [47], and four-wave mixing [31], [43], [44], [46], [48] are two examples of probabilistic sources. These do not emit single-photons, but instead emit pairs of correlated photons, the number of pairs emitted at a time is dependent on the excitation power [8]. The emission of more than one pair at a time could allow an eavesdropper to use photon number splitting attacks in a quantum communication protocol [49]. Therefore the excitation power needs to be reduced in order to lower the probability of >1 pair being emitted at one time. As a result the probability of emitting a single-photon pair has to be reduced substantially to <10% of the excitation rate [50]. To overcome this, SPDC systems have used high intensity excitation at GHz clock rates leading to MHz rate heralding with $g^{(2)}(0)$ <0.1 [51].

2.3 Single-photon detectors

This section will cover some single-photon detector (SPD) technologies [31], [51], [52] which have the sensitivity to measure single-photons. These detectors have applications such as light detection and ranging (LIDAR) [53], single-molecule spectroscopy [54], bioluminescence detection [55], as well as many others [31], [51], [52]. For this Thesis, more relevant applications of these detectors are found in the area of experimental quantum information/communications, such as QKD [31], quantum computation [56], quantum amplification [57], entanglement measurements [58], and also quantum digital signatures (QDS) [7], [59].

2.3.1 Single-photon detector properties

Properties of single-photon detectors can play a major role in the performance of quantum communications experiments, as will be seen in the next Chapter, improvements to detection technology has been one of the main reasons why QKD transmission distances have increased over the past 5 years [60], [61].

A perfect single-photon detector would generate the same measureable electrical output for each and every incident single-photon (known as unity detection efficiency) over the entire electromagnetic spectrum. If more than one single-photon is incident the electrical output scales linearly (or by a calibrated amount), allowing more than one incident single-photon to be distinguished. Once an incident photon has been registered, a perfect detector would immediately be primed and ready to detect any subsequent photons (i.e. it would have zero dead-time/rest-time). This would mean that it would be able to count photons at greater than GHz rates. Furthermore, an incident photon would only generate one output electrical pulse (zero afterpulsing probability) which was produced a consistent time after the photon was absorbed by the detector (zero timing jitter). In reality, single-photon detectors typically fall short of the ideal in at least one parameter and the choice of detector for a particular application is a process of compromise [51].

Timing jitter

As an example, photons are produced by a single-photon source with a precisely defined emission time. A histogram of the arrival times recorded using a perfect single-photon detector would give a single bin wide histogram peak, regardless of how small the duration of the histogram bins. However, when a non-perfect detector is used, a spread in the recorded arrival times is seen as a broadening of the peak in the histogram. The full-width-

at-half-maximum (FWHM) of this peak is one way of defining the timing-jitter (or time-resolution) of the detector, which is essentially the spread in times between an incident photon and the rising edge of the resulting electrical pulse [62]. This timing jitter can vary between detection technologies and even between different detectors in the same product range from the same manufacturer [63]. There are other ways to define the timing-jitter [64], however this Thesis will only consider the FWHM timing-jitter.

Dark counts

Dark counts are a phenomenon present in all real single-photon detectors to date, where the range of dark counts per second scales from the order of <1 to >1 × 10^6 depending on the device used [31]. They are essentially output electrical events from the detector which do not correspond to incident photons. Among other sources, these false detections can come from thermal excitation of carriers across the bandgap in the device, and this can counteract by cooling the detector to reduce thermal excitation. As will be seen later, cryogenically cooled detectors such as superconductors, have the lowest dark count rates because of the small probability of thermal excitation and optical isolation.

Afterpulsing

Afterpulsing is the detector phenomenon where one event triggers further events some time after the initial event. [65]. Afterpulsing is caused by the initial avalanche filling mid-gap trap states in the device which are later released, initiating further avalanches. This results in increased dark count rate for the device, as the count rate increases. The trap lifetime will increase significantly at lower temperatures, meaning that afterpulsing is more evident in cooled SPAD devices, such as InGaAs/InP SPADs. Often, such devices use a hold-off time where the device is not reset immediately after an avalanche, to allow the trapped states to empty without causing further avalanches. However, such an approach will reduce the maximum count rate possible. [66].

In order to minimise the afterpulse probability, the growth material must be very pure so that lattice defects (common trapping sites) are minimised [67]. Also a longer hold-off time before the complete reset is finished will allow greater time for the trapped charges to be released [68].

Maximum count rates & dead-time

When an incident photon is absorbed by a single-photon detector, it generates an electrical signal which is measured by some form of data recorder. After the detection has been made, generally the detector must reset in some way before it is ready to receive another photon. The time taken for the detector to reset and be able to receive another photon for measurement is known as detector dead-time because the detector cannot measure any incident photons while it is resetting. Each detector technology has a different method for resetting, for example superconductor based detectors typically use cooling [69] while semiconductors use an electrical bias [70] and these all have an intrinsic operational time. As described above, some SPADs are used with an intentionally long reset time, usually called a "hold-off time, to avoid the effects of afterpulsing. This dead-time, or hold-off time, will also limit the maximum number of events that can be recorded per second.

Single-photon detection efficiency

The terms single-photon detection efficiency (SPDE) and quantum efficiency are generally used interchangeably to describe single-photon detectors but they are two distinct parameters [52]. The quantum efficiency often refers to the efficiency with which an incident single-photon will release a carrier (or be absorbed by the material). The single-photon detection efficiency is the efficiency with which an incident photon will create a measurable event.

In practice, both quantum and detection efficiency are non-unity, meaning that there is not 100% probability of detecting an incident photon. Each technology has shown different efficiencies for both quantum and detection [43].

Photon number resolving capabilities

A detector which is photon number resolving (PNR) can distinguish how many photons were contained within an incident photon stream or pulse. Single-photon detectors can be placed into three categories, non-PNR, fully PNR and partially PNR [43], as a single-photon detector will be able to detect one photon, although many devices do not have inherent PNR properties. However if a PNR detector does not have unity quantum or single-photon detection efficiency, the recorded photon number is not the true value.

A non-PNR detector is a detector which has no inherent PNR capabilities, working as a binary single-photon counter, measuring whether there were no photons or ≥1 photons in the measurement [70]. Of course, non-unity quantum and detection efficiencies mean that it is not possible to say for certain that a lack of electrical output indicates no-incident photons. Similarly, dark counts and afterpulsing mean that it is not possible to say for certain that an electrical output does signify an incident photon. These devices are generally photomultiplier tubes or single-photon avalanche diodes, which typically have too much gain noise to distinguish between individual photons in an incident pulse.

Fully PNR detectors have inherent PNR properties and give an estimate of how many photons were contained in the incident photon pulse or stream. However for this to be a true representation of the number of photons present, a detection efficiency of unity is needed. Superconducting [71], quantum-dot [72] and visible-light photon counter [73] technologies have shown inherent PNR capabilities with less than unity efficiency. These devices have low inherent gain noise and can therefore distinguish photons by discrimination of voltages, however due to losses and inefficiencies this will not be a true value, only an estimate.

Finally, partially PNR detectors can be created from a non-PNR detector array, or by increasing the detector discriminator voltage of a superconductive nanowire. In the case of non-PNR arrays, each cell in the array is created from a non-PNR detector, therefore photons within an incident pulse must hit different cells in the array to provide an estimate the photon number, this has been shown for single-photon avalanche diodes [74], [75].

2.3.2 Avalanche photodiodes

A single-photon avalanche diode (SPADs) detector is a device which is biased above breakdown voltage and operated in Geiger mode to detect single-photons. They are a relatively well-established technology for quantum communication applications with several commercially available devices for the visible and telecommunications regions of the electromagnetic spectrum covering a range of different growth methods, device geometries and electrical addressing methods [31], [51], [52].

As an example, a SPAD can be created from a positive-doped–negative-doped (p-n), or positive-doped–intrinsic–negative-doped (p-i-n) junction of semiconductor materials. The

process of doping introduces a controlled amount of impurities into a previously pure (intrinsic) semiconductor during the growth process such that the resulting material has a larger concentration of either holes (p-type) or electrons (n-type) [76]. When grown on top of one another the region around the interface between the materials forms a depletion region where no free carriers are present. A reverse bias current (which is greater than the breakdown level) is applied to the material, so that when an incident photon (of energy greater than the bandgap) is absorbed in the depletion region (releasing an electron-hole pair) the free carriers are accelerated. The acceleration gives kinetic energy to the free carriers, and when the energy is sufficient, they can undergo impact ionisation, releasing a carrier from the doped region. The newly created free carrier also undergoes acceleration, and can then undergo impact ionisation as well. At the very high electric fields above avalanche breakdown this results in a self-sustaining avalanche. Such a current can readily be measured with external circuitry. Once the avalanche current has been measured, the device must then be quenched, so that the avalanche process is stopped and the device can be reset for another photon measurement. This quenching process can be performed by passive, gated, or active quenching circuitry [31], [70].

Passive quenching involves a high impedance load connector in series with the SPAD device, when an avalanche is started the resistance of the SPAD reduces, resulting in an increase in the voltage over the load resistor. Consequently, the bias voltage across the SPAD reduces, bringing the device below breakdown, inhibiting the avalanche current. However, after this reset the SPAD must then be brought up to above breakdown voltage bias which can take up to five times the RC time constant of the circuit, leading to detector dead-times of >500 ns [70].

Active quenching [77], [78] involves external circuitry actively and rapidly quenching the avalanche process after it is detected. This can be significantly faster than passive quenching, allowing short recovery times (dead-times of the order of 10's of ns), therefore giving maximum count rates of >MHz [70], [77], [78].

Gated quenching is typically used in applications where the expected time of arrival of a photon can be known accurately such as QKD, and can reduce the effects of afterpulsing, which contributes to the overall dark count rate. The reverse bias voltage is only above the breakdown voltage for a given time, so an avalanche can be created during that time, if no avalanches are created the bias is lowered below the breakdown voltage [31], [70], [77].

Silicon single-photon avalanche diodes (Si-SPADs)

Silicon single-photon avalanche diodes (Si-SPADs) are a very well established technology for detection of visible and short wavelength infrared (IR) photons (400 – 1000 nm). The detection limit at the short wavelength is due to silicon's absorption in the UV, therefore the photons are generally all absorbed before they reach the depletion region, while the limit at the long wavelength is attributable to the bandgap of silicon, the lower energy longer wavelength photons cannot release carriers from the depletion region. The main commercially targeted applications for the Si-SPAD are in areas such as bio-imagining, where the levels of light emitted during the fluorescence of cells is small [79], but (for reasons that will be explained later) they have been selected as suitable detectors for the work presented in this Thesis, that is to say quantum information experiments performed in the short wavelength IR at around 850 nm.

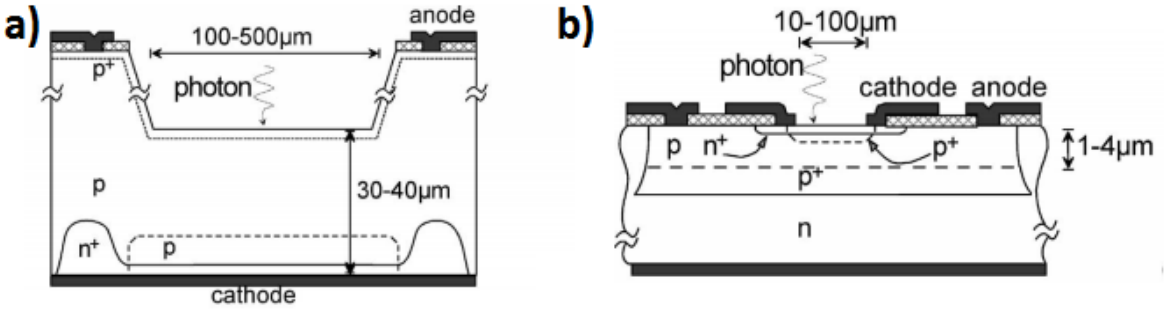


Figure 2.4 – a) thick and b) thin junction silicon single-photon avalanche diodes. The thickness refers to the size the depletion region. [80]

Different detector microstructures, Figure 2.4, can be used to enhance some properties of the detectors. For instance a thin-junction design (b) can give a lower timing jitter at the expense of detection efficiency [31]. A thick junction design (a) can give higher detection efficiency, at the expense of timing jitter [31]. A resonant cavity can be fabricated around a device to enhance the detection efficiency, at the expense of timing jitter as well [81].

An example of a thin junction device from ID Quantique can provide 5% typical detection efficiency, 40 ps timing resolution, 3% afterpulse probability, <100 dark count rate, and a dead-time of 45 ns [82]. While a thick junction Si-SPAD from Excelitas Technologies (previously PerkinElmer, before that, EG&G and initially RCA [83]), used in the experiments presented in the experimental Chapters of this Thesis, provides 40% detection

efficiency, 350 ps timing resolution, <400 dark count rate, 0.5% afterpulse probability, and dead-time of 20 ns [83]. Commercial resonant cavity detectors are not yet available, however examination of research-grade laboratory based detectors has shown detection efficiencies of 18%, 74 ps timing resolution, <50 dark count rate [62].

Indium-phosphide-based single-photon avalanche diodes (InP SPADs)

Another important wavelength region for single-photon detection is in the infrared (IR), around the so called telecommunications regions centred on wavelengths of 1310 nm and 1550 nm. These wavelength regions are extremely important because the transmission loss for standard silica optical fibre is low compared to other wavelengths (such as 850 nm). For this reason the telecommunications industry uses the IR wavelength region for communications. Many optical fibre QKD experiments are also implemented at IR wavelengths to ensure compatibility with the currently installed optical fibres.

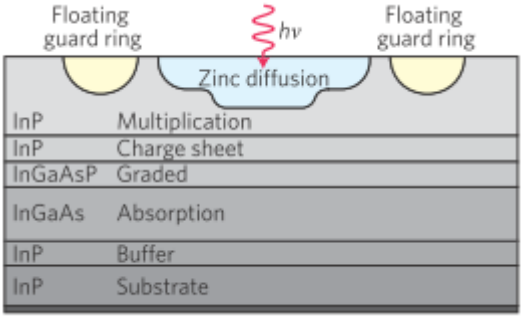


Figure 2.5 – InGaAs/InP single-photon avalanche diode structure. An InGaAs layer is used to absorb a photon generating carriers, while the InP is used as a multiplication region. [68]

Indium-Phosphide (InP) based APDs or SPADs are frequently used to detect single-photons at these wavelengths. InP multiplication devices use an Indium-Gallium-Arsenide (InGaAs) absorption layer (which has a high responsivity at 1550 nm), with a InP multiplication layer separated by an InGaAsP layer to smooth the valence band discontinuity (energy mismatch between the different valance band levels in InGaAs and InP) [31].

Commercial devices based on this later structure are available from (for example) ID Quantique [84]–[86], Laser Components [87], Micro-Photon-Devices [88], and Princeton-

Lightwave [89]. There are many common features of InP based devices, such as detection efficiency of up to 20%, timing resolution in the hundreds of picoseconds, kHz range dark count rate, and μs dead-times. Afterpulsing probability for such devices tends to be below 1%.

Similar to the case for the Si-SPADs, increasing the operating temperature increases the dark count rate but lowers the afterpulse probability [68], [90]. Increasing the excess bias voltage increases the detection efficiency [91] but also increases the dark count rate and afterpulse probability. The hold-off time of the device can be increased to counter-act any increase in afterpulsing, but doing so will, however, significantly reduce the maximum count rate of the detector [91].

InGaAs/InP SPADs have been shown to work at dark count rates as low as 1 count per second, at a quantum efficiency of 10% (at 1550 nm), at an operating temperature of 163 K [90]. These detectors were subsequently used to extend the range of QKD to 307 km over optical fibre using the coherent one-way protocol which will be explained in the next Chapter [61].

2.3.3 Superconducting single-photon detectors

Superconductivity is the physical phenomenon where a material no longer has electrical resistivity, and cannot be penetrated by magnetic fields. This can happen as long as the temperature, current, and magnetic field are below certain critical values characteristic of the material. This phenomenon can be used to create single-photon sensitive detectors with a variety of characteristics, particularly in terms of operation longer wavelengths.

Superconducting Nanowire Single-Photon Detectors

Superconducting nanowire single-photon detectors (SNSPDs) have received a lot of attention recently, because of the potentially advantageous detection characteristics in the infrared region [92]–[95]. In the region around the telecommunications wavelengths SNSPDs can provide high detection efficiency, low dark count rates, and significantly improved timing resolution which can be in the range of a few 10's pico-seconds. At present the most common material employed for nanowires is based on niobium nitrate (NbN), however research into other materials, such as niobium titanium nitrate (NbTiN) is ongoing [69]. Nanowires tend to operate at temperatures <7 K [52].

SNSPDs are fabricated from a very narrow (≈100 nm) stripe of superconducting metal, The wire is cryogenically cooled to below the superconducting threshold temperature, a current (I) is applied, which is just below the critical current threshold (I_c). When an incident photon is absorbed on the nanowire it creates a localised temperature increase (hot spot), which suppresses superconductivity in that immediate region and forces the current around the hot spot. The increase in current density around the edges of the hot spot means that the localised current density increases above the critical current density and causes the area of the detector to rapidly become a normal Ohmic conductor, producing a voltage spike that can be measured [31], [51], [52], [69]. A simplified diagram of the process is shown in Figure 2.6. The bias current on the detector is decreased while the hot spot cools, and increased once the nanowire is back to superconducting temperature, the time taken for it to do this gives the recovery time (essentially dead-time) of the detector which is typically in the nanosecond timescale.

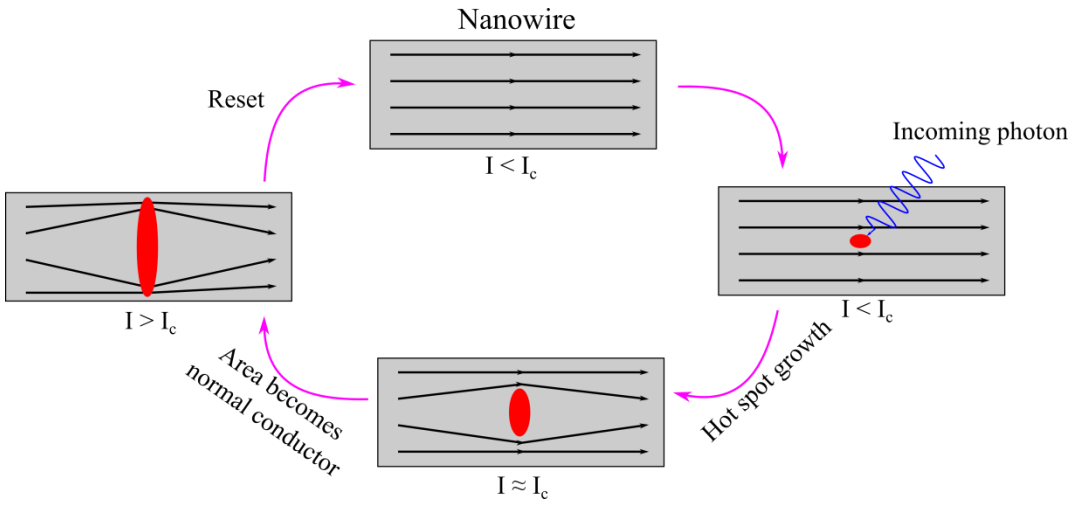


Figure 2.6 – Simplified diagram of photon measurement by a superconducting nanowire single-photon detector.

Single straight nanowires tend to have lower system detection efficiencies because photon detection is dependent on a photon striking the narrow cross section of the wire. As a result devices grown with the wire looping in a meander are commonly used to increase the fill-factor of the device and hence increase the overall system detection efficiency [52]. The detection efficiency and dark count rate are dependent on the bias current which is applied to the nanowire. A higher bias current (i.e. closer to the critical current) allows for higher detection efficiency, however this will increase the dark count rate [96].

Afterpulsing is not an issue for SNSPDs because of the hot spot dissipation process, however latching can occur, which is when a detector cannot reset, so the bias current needs to be reduced further to allow the detector to reset.

Nanowire detectors are starting to become more commercially available, with Single Quantum [96] and ID Quantique [93] in Europe, Scontel [97] in Russia, and Photon Spot [98] and QuantumOpus [99] in the United States already selling devices. At present, all of the commercial systems offer low timing jitter of <100 ps, low dark count rates <100 per second, and fast recovery times of <100 ns, and quantum efficiencies of >90% for 1550 nm, at a particular bias current. However precise overall system efficiencies can vary from device to device and are dependent on the bias current which also affects the dark count rate.

Transition edge sensor (TES)

Transition edge sensor (TES) single-photon detectors are high quantum efficiency devices that operate at milli-kelvin cryogenic temperatures, and also have photon number resolving (PNR) capabilities [31], [51], [52]. The TES is essentially a bolometer [100], measuring the absorption of electromagnetic radiation by observing a change in temperature, via the change in conductivity of a superconducting material. TESs have been successfully demonstrated using titanium [71], [101], [102], tungsten [103], and hafnium [104] as the absorber. A larger number of incident photons will result in a greater change in temperature and so TES devices with high sensitivity are inherently photon number resolving.

This highly sensitive device is created by depositing a thin layer of superconductive material on top of an insulator. In operation the thin layer is cooled to just below the critical temperature. When an incident photon is absorbed, the temperature of the superconductor will rise, increasing the resistance of the device, as shown for an example device in Figure 2.7 [105]. The amount of incident energy determines how much the conductivity will change and provides an estimation of the photon number.

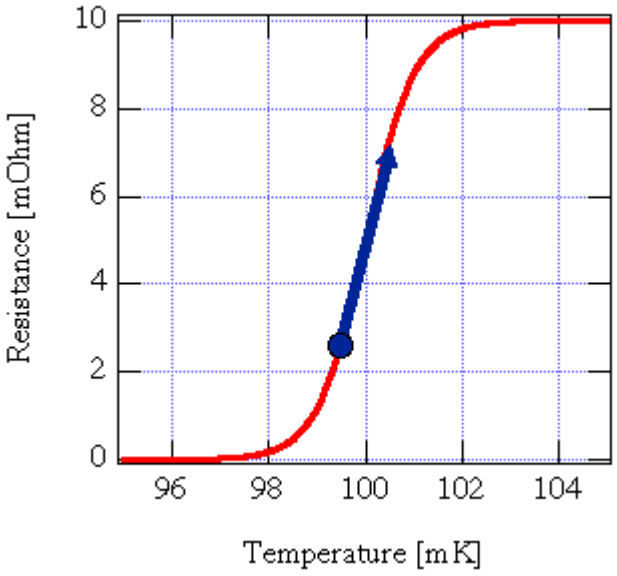


Figure 2.7 – Variation in electrical resistance of a transition edge sensor resistance in response to temperature. Taken from [105].

Although TESs have quantum efficiencies of > 90% for both 850 nm, and 1550 nm light [71], [103], along with PNR capabilities and extremely low dark count rates, the devices can be tricky to work with because of the milli-kelvin temperatures required to operate them. The devices also tend to have large recovery times (equivalent to dead-time), which are generally in the range of μs, limiting the clock frequency of an experiment that employs them. Research into improving the recovery time is ongoing and a TES with 190 ns recovery time was demonstrated in 2008 [101].

Photon numbers of up to a 100 [106], and up to 1000 [107] per pulse have been fully distinguished, which are substantially higher than the photon numbers per pulse typically used for quantum communications applications, however these could potentially be useful for wider quantum information experiments, quantum imaging or quantum metrology. Many TES detectors are only tested for PNR capabilities of up to 5 photons in a pulse [71], [102], [103].

2.3.4 Summary of representative detector technology characteristics

A range of single-photon detection technologies have been described in this Section. While the Si-SPAD is the only detector used in the experiments presented in this Thesis, other detector technologies were reviewed because these are technologies which are also

commonly used in quantum communications experimentation. When choosing a single-photon detection technology it is worth reviewing the application before purchase.

A detector deployed for use "in the field" or as a component is some form of commercial device would benefit from easy manoeuvrability, so detection technologies which do not require cryogenics and vacuum pumps may be beneficial for reasons of cost and convenience. Therefore semiconductor technologies which can be compact and cooled by thermo-electric cooling, like a SPAD, may be more desirable.

Superconducting detectors have low dark count rates, greatly reduced timing jitter, no afterpulsing, and high quantum efficiency over a large wavelength range, meaning that these are desirable in a lab environment. With improvements to cryogenic technology there is a possibility for systems to become smaller, making it more convenient for these to be used in fixed commercial applications but at present they remain impractical.

2.4 Quantum optical memories

Quantum optical memories, which shall hereafter just be referred to as quantum memories (and abbreviated to QM), allow a photonic quantum state to be stored, preserved with a high fidelity for a length of time, and finally recovered. Unlike classical memories, which only need to preserve the bit value of '1' or '0', quantum memories must preserve the quantum superposition which is susceptible to decoherence [108], where the state's interaction with the environment will cause the quantum properties to dissipate over time.

QM are a useful technology for the future of quantum information protocols [109]. They have a range of applications which they can be applied to, including quantum digital signatures (QDS) [110], quantum networks [111], [112], deterministic single-photon sources [109], and quantum repeaters [113]. However, due to the technical challenges associated with current quantum memories, the experiments described in the following Chapters do not implement quantum memories and in some cases were deliberately designed to remove any requirement for such technologies.

The ideal (QM) would have the following properties [109], [114]: Perfect fidelity, on-demand retrieval, unlimited storage time, lossless, scalable storage space, retrieval of photons can be made in any order, and are able to operate at GHz repetition rates.

	Overall storage efficiency (%)	Storage time	Fidelity (%)	Preserves
Single atom [115]	9.1	Up to 200 μs	93 (2 μs) 66 (86 μs)	6 polarisation states
Room temperature Atomic vapour [116]	5.5	20 μs	71.5	V/H polarisation states
Cold atomic vapour [117]	30 – 2	0.2 – 4 μs	-	-
Molecular gas [108]	18	1 ns	-	-
Bulk diamond/colour centre [118]	10	ps range	-	V/H polarisation states
Solid state [119]	69 – 45	1.3 – 2.6 μs	-	-

Table 2.2 – Review table of what was found to be, to the best of my knowledge, the most significant quantum optical memories for each category. A more profound table can be found in [109].

Implementations of QM have been shown in single atoms [115], atomic vapours [120], cold atoms [121], molecular gases [108], bulk/nitrogen vacancy diamond [118], [122], semiconductor vacancy centres [123], and in rare-earth doped crystals [119]. The focus of this Thesis is not QMs and in fact steps are made in each of the experimental Chapters to avoid using them, so the details of each method will not be discussed, however some examples of QM are given in Table 2.2.

Many QM technologies can only store information for nano-second timescales, and the associated experimental complexity means that it is sometimes worth considering an easier approach, such as high finesse optical cavities. High finesse optical cavities have been shown to reliably delay an optical path for μs time scales [124], [125], which simply implement an optical cavity where the optical path does a number of round trips until it is

able to escape the cavity. Also lengths of optical fibre can provide relatively lossless nano-second timescale delays, this method was actually used in the first implementation of quantum digital signatures which required QM between the swap and comparison mechanism, and the receiver measurement [7].

2.5 Transmission media

In quantum communications, wavelength choice and method of encoding the information is not only important for choosing detector and source technologies, but also the medium which photons are going to be transmitted through [126]. To date, quantum key distribution (QKD), the most developed quantum communications technology, has been demonstrated in free-space [127], and in silica optical fibre [128], [129].

Optical fibres can be used for built-up areas were line-of-sight communications are not possible. However, this installed telecommunications infrastructure typically also contains conventional optical amplifiers [130]–[132], routers and network nodes which quantum signals can affect the properties of the quantum signal[133], [134] (See Chapters 6, 7, and 8).

In order to get over this exponential loss from the silica optical fibre, many research groups are looking into free-space satellite QKD, where the satellite acts as a quantum node for a world-wide network, however there are many technical issues to overcome, such as signal disturbance from turbulence, and tracking of the satellite [135]–[137].

2.5.1 Free space

In free-space transmission for communications, the general idea is to send photons from one position to a receiver in a line-of-sight channel. Generally free-space communication in the past focused on ground-to-ground transmissions, but with the invention of the satellite communications, new applications of free-space communication were made available allowing the possibility of a worldwide network with satellite nodes. Figure 2.8 shows the transmittance of the atmosphere from ground to space over a range of wavelengths, and it can be seen there are a number of highly transmitting regions in the visible and infrared.

In 2007 ground-station–to–ground-station QKD was demonstrated at a distance of 144 km using a 1016 mm diameter aperture telescope in the Canary Islands as the receiver [138]. Since then research into free-space quantum communications has been more dedicated toward satellite communications [135], and also angular-momentum encoded photons [139], [140].

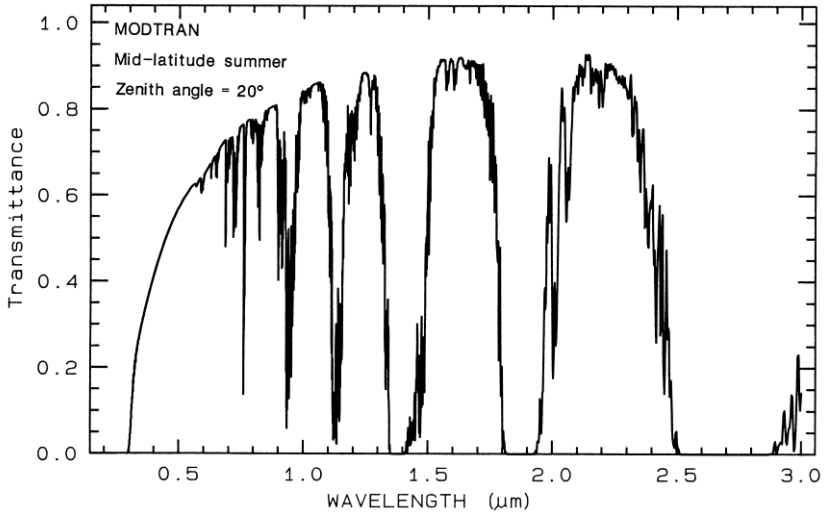


Figure 2.8 - Transmittance of light from space to the ground through the atmosphere versus wavelength. [141]

The experimental set-up for free-space communications involves a great deal of care during initial alignment, and ongoing operation requires continual monitoring of the alignment. At large transmission distances even small vibrations at the source can cause the alignment to shift by a significant amount at the receiver, and in turn reduce the overall bit rate of the communications [142]. Atmospheric conditions can also affect the communication channel, such as scintillation of the laser beam (i.e. the collimated beam pattern changes) [143], [144], and changes in transmission [145]. Also the background level of light could swamp a quantum signal. Quantum protocols generally use polarisation encoding in free-space protocols because the polarisation is largely un-affected by atmospheric propagation[146].

2.5.2 Optical fibre

Optical fibre is a popular medium for communication transfer and has largely replaced its predecessor the copper cable in the delivery of long-haul telecommunications signals.

Copper cables are comparatively bulky and costly while optical fibre was seen as a cheaper and higher data-rate alternative. Although fibre optics is now the dominant transmission medium in telecommunications, this was only made possible by improvements in technology such as optical amplifiers [130] (to increase the bandwidth), detectors and photon sources.

In optical fibre, losses can come from absorption, scattering, dispersion, bending, splicing/connections, mode-coupling, and bad alignment. Telecommunications generally use single-mode (at a wavelength of 1550 nm) 9 μm core diameter silica optical fibre to guide the light. Single-mode fibre helps prevent mode-dispersion for long transmission distances, allowing for high-bandwidth [15].

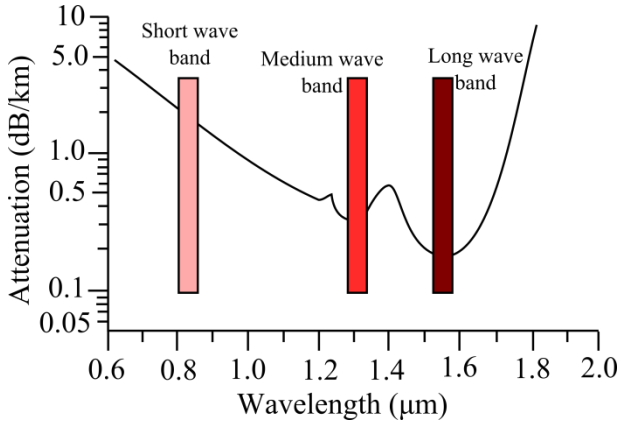


Figure 2.9 – Attenuation of a silica optical fibre showing the three bands of interest at 850, 1310, and 1550 nm. [147]

Three low-loss bands of interest, which also conveniently have semiconductor technology for sources and detection, can be seen in Figure 2.9. The medium and long wave bands, 1310 and 1550 nm respectively have low loss, with ≈0.31 and 0.25 dB/km. InP and InGaAs semiconductor technology offers a range of sources and detectors in these wavelengths. The final band, the short wave has higher loss, ≈2.2 dB/km, however at this wavelength silicon is an available detection technology, which was shown to have high quantum efficiencies (≈40% at 850 nm), low dark count rate (<400 s^{-1}), good timing jitter (100's ps), and does not need to be cryogenically cooled, allowing for a more compact device.

To overcome these losses in conventional telecommunications, optical amplifiers are periodically placed into the channel allowing intercontinental distances to be covered. These optical amplifiers allow the signal to be boosted in amplitude at the expense of added noise. This is generally not possible with quantum communication protocols as this goes against the no-cloning theorem, which are limits in transmission distance due to the inherent loss of silica optical fibres. Figure 2.10 shows the remaining percentage of original signal after propagating through silica optical fibre, from Corning Incorporated [148], without an optical amplifier. It is clear to see why many quantum communication protocols are implemented at 1550 nm, because this is the lowest loss wavelength in silica optical fibre.

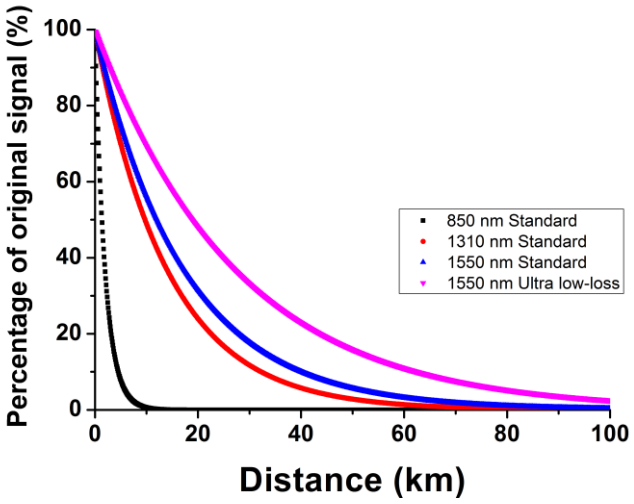


Figure 2.10 – Percentage of signal vs distance in silica single mode fibre for the three different wavelengths used in telecommunication and quantum communications.

Although silica standard single-mode fibre (at 1550 nm) is used by the telecommunications industry as standard, there have been developments in optical fibre manufacturing to create speciality low loss optical fibres, such as Corning SMF-28 ULL [149], which provides 0.16 dB/km loss around the 1550 nm window. Commercial quantum key distribution systems implemented in optical fibre are (or were) available from ID Quantique [150], MagiQ Technologies [20], SeQureNet [19], QuintessenceLabs [151].

2.6 Time-correlated-single-photon-counting

Time-correlated single-photon counting (TCSPC) is a technique of photon counting which allows the time of each photon to be recorded [152]. This is useful in a number of different research areas including LIDAR [53], imagining of single molecules [55]. More importantly for this Thesis, it can be used in quantum information and communication experiments to record timing information of the single qubits sent in order to perform post-processing.

While single-photon detectors allow photons to be counted, the information of arrival time is lost. TCSPC involves additional specialist equipment in order for timing information to be recorded. In TCSPC the output from the detector is fed into a discriminator which allows the device to record events which are above a certain threshold, i.e. reducing the overall noise. This discriminator gives a digital output which is then fed into a counter module which can record the event times accurately, the photon event time recordings are sometimes referred to as time-tags. [152]

In the experiments for this Thesis the TCSPC device is the Hydraharp 400 [153]. It is a time to digital converter with a 1 ps resolution, maximum data transfer rate of 4 Mb/s for the USB 2.0 version, and 12.5 Mb/s for the USB 3.0 version.

2.7 Bibliography

[1] C. H. Bennett and G. Brassard, "Quantum cryptography - public key distribution and coin tossing," in *International Conference on Computers, systems and signal processing*, 1984, p. 8.

[2] H.-K. Lo, *et al.*, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun. 2005.

[3] P. Sibson, *et al.*, "Chip-based quantum key distribution," pp. 1–5, 2015.

[4] N. Bruno, *et al.*, "Heralded amplification of photonic qubits," *Opt. Express*, vol. 24, no. 1, p. 125, Jan. 2016.

[5] S. Kocsis, *et al.*, "Heralded noiseless amplification of a photon polarization qubit," *Nat. Phys.*, no. 3, pp. 1–6, 2013.

[6] P. Walther, *et al.*, "Experimental one-way quantum computing.," *Nature*, vol. 434, no. 7030, pp. 169–176, 2005.

[7] P. J. Clarke, *et al.*, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.," *Nat. Commun.*, vol. 3, p. 1174, Jan. 2012.

[8] M. Fox, *Quantum Optics: An introduction*, 1st ed. Oxford: Oxford University Press, 2006.

[9] W. Tittel, *et al.*, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[10] S. Bhattacharya, *et al.*, "Decoy-state method for subcarrier-multiplexed frequency-coded quantum key distribution," *J. Opt. Soc. Am. B*, vol. 30, no. 4, p. 782, Mar. 2013.

[11] S. Krapick, *et al.*, "Bright integrated photon-pair source for practical passive decoy-state quantum key distribution," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 89, no. 1, pp. 1–5, 2014.

[12] H.-K. Lo, *et al.*, "Decoy state quantum key distribution.," *Phys. Rev. Lett.*, vol. 94, no. September 2004, p. 230504, 2005.

[13] Y. Zhao, *et al.*, "Experimental quantum key distribution with decoy states.," *Phys. Rev. Lett.*, vol. 96, no. 1, p. 070502, 2006.

[14] E. Meyer-Scott, *et al.*, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," *Phys. Rev. A*, vol. 84, no. 6, pp. 1–9, 2011.

[15] A. Ghatak and K. Thyagarajan, *An Introduction to Fiber Optics*. 1998.

[16] L. A. Coldren, *et al.*, "Vertical-Cavity Surface-Emitting Lasers," in *Optical Fiber Telecommunications IIIB*, Elsevier, 1997, pp. 200–266.

[17] J. Tatum and J. Guenter, "Modulating VCSELs," *Honeywell Int.*, pp. 1–19, 1998.

[18] ID Quantique, "Clavis 2." [Online]. Available: http://www.idquantique.com/photon-counting/clavis2-qkd-platform/. [Accessed: 14-Jan-2016].

[19] SeQurenet, "Cygnus Distribution Module," *SeQureNet SARL*, 2013. [Online]. Available: www.sequrenet.com.

[20] MagiQ Technologies, "MagiQ." [Online]. Available: http://www.magiqtech.com/. [Accessed: 13-Jan-2016].

[21] R. Hanbury-Brown and R. Q. Twiss, "Correlation between Photons in two Coherent Beams of Light," *Nature*, vol. 177, no. 4497, pp. 27–29, Jan. 1956.

[22] M. a M. Versteegh, *et al.*, "Observation of strongly entangled photon pairs from a nanowire quantum dot.," *Nat. Commun.*, vol. 5, p. 5298, Jan. 2014.

[23] M. J. Holmes, *et al.*, "Room-temperature triggered single photon emission from a III-nitride site-controlled nanowire quantum dot," *Nano Lett.*, vol. 14, no. 2, pp. 982–986, 2014.

[24] M. Zavvari and V. Ahmadi, "Quantum-Dot-Based Mid-IR Single-Photon Detector With Self-Quenching and Self-Recovering Operation," *IEEE Electron Device Lett.*, vol. 34, no. 6, pp. 783–785, 2013.

[25] K. Yamaguchi, *et al.*, "Stranski-Krastanov growth of InAs quantum dots with narrow size distribution," *Jpn. J. Appl. Phys.*, vol. 39, no. 12, pp. 1245–1248, 2000.

[26] J. Claudon, *et al.*, "A highly efficient single-photon source based on a quantum dot in a photonic nanowire," *Nat. Photonics*, vol. 4, no. 3, pp. 174–177, Jan. 2010.

[27] F. Hargart, *et al.*, "Electrically driven quantum dot single-photon source at 2 GHz excitation repetition rate with ultra-low emission time jitter," *Appl. Phys. Lett.*, vol. 102, no. 1, p. 011126, 2013.

[28] S. Buckley, *et al.*, "Engineered quantum dot single-photon sources.," *Rep. Prog. Phys.*, vol. 75, p. 126503, 2012.

[29] K. Watanabe, *et al.*, "Fabrication of GaAs Quantum Dots by Modified Droplet Epitaxy," *Jpn. J. Appl. Phys.*, vol. 39, no. Part 2, No. 2A, pp. L79–L81, Feb. 2000.

[30] K. Rivoire, *et al.*, "Fast quantum dot single photon source triggered at telecommunications wavelength," *Appl. Phys. Lett.*, vol. 98, no. 8, p. 083105, 2011.

[31] G. S. Buller and R. J. Collins, "Single-photon generation and detection," *Meas. Sci. Technol.*, vol. 21, no. 1, p. 012002, Jan. 2010.

[32] F. Jelezko and J. Wrachtrup, "Single defect centres in diamond: A review," *Phys. Status Solidi Appl. Mater. Sci.*, vol. 203, no. 13, pp. 3207–3225, 2006.

[33] W. E. Moerner, "Single-photon sources based on single molecules in solids," *New J. Phys.*, vol. 6, pp. 88–88, 2004.

[34] B. Lounis and W. E. Moerner, "Single photons on demand from a single molecule at room temperature," pp. 491–493, 2000.

[35] T. Heindel, *et al.*, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New J. Phys.*, vol. 14,

no. 8, p. 083001, 2012.

[36] X.-L. Chu, *et al.*, "Experimental realization of an optical antenna designed for collecting 99% of photons from a quantum emitter," *Optica*, vol. 1, no. 4, p. 203, 2014.

[37] T. Ishikawa, *et al.*, "Site-controlled InAs single quantum-dot structures on GaAs surfaces patterned by in situ electron-beam lithography," *Appl. Phys. Lett.*, vol. 76, no. 2, pp. 167–169, 2000.

[38] T. M. Babinec, *et al.*, "A diamond nanowire single-photon source.," *Nat. Nanotechnol.*, vol. 5, no. 3, pp. 195–9, Mar. 2010.

[39] M. Leifgen, *et al.*, "Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution," *New J. Phys.*, vol. 16, pp. 0–13, 2014.

[40] A. S. Solntsev, *et al.*, "Characterization of aperiodic domain structure in lithium niobate by spontaneous parametric down-conversion spectroscopy," *Laser Phys. Lett.*, vol. 12, no. 9, p. 095702, 2015.

[41] S.-Y. Baek and Y.-H. Kim, "Spectral properties of entangled photon pairs generated via frequency-degenerate type-I spontaneous parametric down-conversion," *Phys. Rev. A*, vol. 77, no. 4, p. 043807, Apr. 2008.

[42] ID Quantique, "ID350-PPLN periodically poled lithium niobate," 2014.

[43] M. D. Eisaman, *et al.*, "Invited Review Article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, 2011.

[44] O. Aso, M. Tadakuma, and S. Namiki, "Four-wave mixing in optical fibers and its applications," *dEp*, vol. 19, no. 19, pp. 63–68, 1999.

[45] J. Hansryd, *et al.*, "Fiber-based optical parametric amplifiers and their applications," *IEEE J. Sel. Top. Quantum Electron.*, vol. 8, no. 3, pp. 506–520, 2002.

[46] R. Wakabayashi, *et al.*, "Time-bin entangled photon pair generation from Si micro-ring resonator," *Opt. Express*, vol. 23, no. 2, p. 1103, 2015.

[47] H. Di Lorenzo Pires, *et al.*, "Type-I spontaneous parametric down-conversion with a strongly focused pump," *Phys. Rev. A*, vol. 83, no. 3, p. 033837, 2011.

[48] B. J. Smith, *et al.*, "Photon pair generation in birefringent optical fibers," *Opt. Express*, vol. 17, no. 26, p. 23589, 2009.

[49] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New J. Phys.*, vol. 4, pp. 44.1 – 44.9, Jul. 2002.

[50] N. Bruno, *et al.*, "Simple, pulsed, polarization entangled photon pair source," *Opt. Commun.*, vol. 327, pp. 3–6, 2014.

[51] M. D. Eisaman, *et al.*, "Invited review article: Single-photon sources and detectors.," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, Jul. 2011.

[52] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photonics*, vol. 3, no. 12, pp. 696–705, 2009.

[53] A. M. Wallace, *et al.*, "Design and evaluation of multispectral LiDAR for the recovery of arboreal parameters," *IEEE Trans. Geosci. Remote Sens.*, vol. 52, no. 8, pp. 4942–4954, 2014.

[54] Y. L. A. Rezus, *et al.*, "Single-Photon Spectroscopy of a Single Molecule," *Phys. Rev. Lett.*, vol. 108, no. 9, p. 093601, 2012.

[55] K. L. Walker, *et al.*, "Un-collimated single-photon imaging system for high-sensitivity small animal and plant imaging.," *Phys. Med. Biol.*, vol. 60, no. 1, pp. 403–420, 2015.

[56] T. D. Ladd, *et al.*, "Quantum computers.," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[57] R. J. Donaldson, *et al.*, "Experimental Implementation of a Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.*, vol. 114, no. 12, p. 120505, 2015.

[58] Z. Zhao, *et al.*, "Experimental realization of entanglement concentration and a quantum repeater.," *Phys. Rev. Lett.*, vol. 90, no. 20, p. 207901, 2003.

[59] R. J. Collins, *et al.*, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[60] S. Wang, *et al.*, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber.," *Opt. Lett.*, vol. 37, no. 6, pp. 1008–10, Mar. 2012.

[61] B. Korzh, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[62] P. J. Clarke, *et al.*, "Analysis of detector performance in a gigahertz clock rate

quantum key distribution system," *New J. Phys.*, vol. 13, p. 23, 2011.

[63] I. Rech, *et al.*, "Modified single photon counting modules for optimal timing performance," *Rev. Sci. Instrum.*, vol. 77, no. 3, pp. 33104–33105, 2006.

[64] N. J. Pilgrim, *et al.*, "Influence of absorber layer dopants on performance of Ge/Si single photon avalanche diodes," *J. Appl. Phys.*, vol. 113, no. 14, p. 144508, 2013.

[65] R. E. Warburton, *et al.*, "Ge-on-Si Single-Photon Avalanche Diode Detectors: Design, Modeling, Fabrication, and Characterization at Wavelengths 1310 and 1550 nm," *IEEE Trans. Electron Devices*, vol. 60, no. 11, pp. 3807–3813, 2013.

[66] S. T. Pantelides, "The electronic structure of impurities and other point defects in semiconductors," *Rev. Mod. Phys.*, vol. 50, no. 4, pp. 797–858, 1978.

[67] K. Iniewski, Ed., *Semiconductor Radiation Detection Systems*. Taylor & Francis, 2010.

[68] S. Pellegrini, *et al.*, "Design and performance of an InGaAs-InP single-photon avalanche diode detector," *IEEE J. Quantum Electron.*, vol. 42, no. 4, pp. 397–403, 2006.

[69] M. G. Tanner, *et al.*, "Optimised quantum hacking of superconducting nanowire single-photon detectors," pp. 1–8, 2013.

[70] A. Gallivanoni, *et al.*, "Progress in quenching circuits for single photon avalanche diodes," *IEEE Trans. Nucl. Sci.*, vol. 57, no. 6, 2010.

[71] D. Fukuda, *et al.*, "Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling.," *Opt. Express*, vol. 19, no. 2, pp. 870–875, 2011.

[72] B. E. Kardynał, *et al.*, "Photon number resolving detector based on a quantum dot field effect transistor," *Appl. Phys. Lett.*, vol. 90, no. 18, pp. 89–91, 2007.

[73] K. S. McKay, *et al.*, "Enhanced quantum efficiency of the visible light photon counter in the ultraviolet wavelengths.," *Opt. Express*, vol. 17, no. 9, pp. 7458–7464, 2009.

[74] X. Jiang, *et al.*, "InP-Based Single-Photon Detectors and Geiger-Mode APD Arrays for Quantum Communications Applications," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 1–12, May 2015.

[75] A. Rochas, *et al.*, "First fully integrated 2-D array of single-photon detectors in

standard CMOS technology," *Photonics Technol. Lett. IEEE*, vol. 15, no. 7, pp. 963–965, 2003.

[76] J. R. Woodyard, "Nonlinear circuit device utilizing germanium." Google Patents, 1950.

[77] S. Cova, *et al.*, "Active-quenching and gating circuits for single-photon avalanche diodes (SPADS)," *IEEE Trans. Nucl. Sci.*, vol. 29, no. 1, pp. 599–601, 1982.

[78] S. Cova, *et al.*, "Avalanche photodiodes and quenching circuits for single-photon detection," *Appl. Opt.*, vol. 35, no. 12, p. 1956, Apr. 1996.

[79] A. Kinkhabwala, *et al.*, "Large single-molecule fluorescence enhancements produced by a bowtie nanoantenna," *Nat. Photonics*, vol. 3, no. 11, pp. 654–657, Nov. 2009.

[80] F. Zappa, *et al.*, "Single-Photon Avalanche Diode Arrays for Fast Transients and Adaptive Optics," *IEEE Trans. Instrum. Meas.*, vol. 55, no. 1, pp. 365–374, 2006.

[81] M. Ghioni, *et al.*, "Resonant-cavity-enhanced single-photon avalanche diodes on reflecting silicon substrates," *IEEE Photonics Technol. Lett.*, vol. 20, no. 6, pp. 413–415, 2008.

[82] ID Quantique, "Visible single-photon detection module with high timing resolution and low dark count rate.," 2015.

[83] Excelitas Technology, "Single Photon Counting Modules," 2015.

[84] ID Quantique, "Infrared single-photon counter ID220: Cost-effective module for asynchronous," 2015.

[85] ID Quantique, "ID230 free-running InGaAs/InP photon counter with 50 Hz dark count rate at 10% quantum efficiency," 2015. [Online]. Available: http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf.

[86] ID Quantique, "Infrared single-photon counting system ID210 advanced system for single-photon detection with 100 MHz gated mode and free-running mode.," 2002.

[87] Laser Components, "Single Photon Counting Module COUNT Q Series."

[88] Micro Photon Devices, "InGaAs SPAD - gated," 2014.

[89] Princeton Lightwave, "High Speed Single Photon PGA-600HSU," no. 1, 2011.

[90] B. Korzh, *et al.*, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," *Appl. Phys. Lett.*, vol. 104, no. 8, p. 081108, Feb. 2014.

[91] A. Restelli, *et al.*, “Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz,” *Appl. Phys. Lett.*, vol. 102, no. 14, p. 141104, 2013.

[92] D. Rosenberg, *et al.*, “nanowire single photon detector array,” vol. 21, no. 2, pp. 1440–1447, 2013.

[93] ID Quantique, “ID280 - Superconducting nanowire single photon detector,” 2014.

[94] H. Shibata, *et al.*, “Superconducting nanowire single-photon detector with ultralow dark count rate using cold optical filters,” *arXiv Prepr. arXiv …*, pp. 1–5, 2013.

[95] C. Sijing, *et al.*, “Superconducting nanowire single-photon detection system and demonstration in quantum key distribution,” vol. 58, no. 10, pp. 1145–1149, 2013.

[96] single Quantum, “Single Quantum Eos X10 CS Closed-Cycle System.” [Online]. Available: http://www.singlequantum.com/cs/. [Accessed: 10-Nov-2015].

[97] Scontel, “Scontel superconducting nanotechnology.” [Online]. Available: http://www.scontel.ru/sspd/. [Accessed: 10-Nov-2015].

[98] Photon-spot, “Photon Spot.” [Online]. Available: http://www.photonspot.com/.

[99] A. J. Miller, “Quantum Opus.” [Online]. Available: http://www.quantumopus.com/. [Accessed: 10-Nov-2015].

[100] A. T. Lee, *et al.*, “A superconducting bolometer with strong electrothermal feedback,” *Appl. Phys. Lett.*, vol. 69, no. 12, pp. 1801–1803, 1996.

[101] D. Fukuda, *et al.*, “Photon number resolving detection with high speed and high quantum efficiency,” *Metrologia*, vol. 46, no. 4, pp. S288–S292, Aug. 2009.

[102] D. Rosenberg, *et al.*, “Noise-free high-efficiency photon-number-resolving detectors,” *Phys. Rev. A*, vol. 71, no. 6, p. 061803, 2005.

[103] A. E. Lita, *et al.*, “Counting near-infrared single-photons with 95% efficiency.,” *Opt. Express*, vol. 16, no. 5, pp. 3032–3040, 2008.

[104] A. E. Lita, *et al.*, “High-Efficiency Photon-Number-Resolving Detectors based on Hafnium Transition-Edge Sensors,” vol. 351, no. 2009, pp. 351–354, 2009.

[105] F. Group, “Transition edge sensors (TES),” 2014. [Online]. Available: http://web.mit.edu/figueroagroup/ucal/ucal_tes/. [Accessed: 09-Nov-2015].

[106] G. Brida, *et al.*, “Quantum characterization of superconducting photon counters,” *New J. Phys.*, vol. 14, no. 8, p. 085001, 2012.

[107] NIST, “Adding Up Photons with a TES,” 2010. [Online]. Available: http://www.nist.gov/pml/div686/tes.cfm. [Accessed: 09-Nov-2015].

[108] P. J. Bustard, *et al.*, “Toward quantum processing in molecules: A THz-bandwidth coherent memory for light,” *Phys. Rev. Lett.*, vol. 111, no. 8, pp. 1–5, 2013.

[109] C. Simon, *et al.*, “Quantum memories,” *Eur. Phys. J. D*, vol. 58, no. 1, pp. 1–22, Apr. 2010.

[110] D. Gottesman and I. Chuang, “Quantum Digital Signatures,” *arXiv.org*, no. 0105032v2, 2001.

[111] K. Nemoto, *et al.*, “Photonic Quantum Networks formed from NV- Centers,” pp. 1–11, Dec. 2014.

[112] B. Fröhlich, *et al.*, “Quantum Secured Gigabit Passive Optical Networks,” pp. 20–22, 2015.

[113] S. Bäuml, *et al.*, “Limitations on Quantum Key Repeaters,” no. May 2014, p. 41, 2014.

[114] A. I. Lvovsky, *et al.*, “Optical quantum memory,” *Nat. Photonics*, vol. 3, no. 12, pp. 706–714, Dec. 2009.

[115] H. P. Specht, *et al.*, “A single-atom quantum memory.,” *Nature*, vol. 473, no. 7346, pp. 190–3, May 2011.

[116] C. Kupchak, *et al.*, “Room-Temperature Single-photon level Memory for Polarization States.,” *Sci. Rep.*, vol. 5, p. 7658, Jan. 2015.

[117] K. F. Reim, *et al.*, “Single-Photon-Level Quantum Memory at Room Temperature,” *Phys. Rev. Lett.*, vol. 107, no. 5, p. 053603, Jul. 2011.

[118] D. G. England, *et al.*, “Storage and Retrieval of THz-Bandwidth Single Photons Using a Room-Temperature Diamond Quantum Memory,” vol. 053602, no. February, pp. 1–5, 2015.

[119] M. P. Hedges, *et al.*, “Efficient quantum memory for light.,” *Nature*, vol. 465, no. 7301, pp. 1052–1056, 2010.

[120] K. F. Reim, *et al.*, “Towards high-speed optical quantum memories,” *Nat. Photonics*, vol. 4, no. 4, pp. 218–221, 2010.

[121] K. S. Choi, *et al.*, “Mapping photonic entanglement into and out of a quantum memory.,” *Nature*, vol. 452, no. 7183, pp. 67–71, 2008.

[122] P. C. Maurer, *et al.*, “Room-Temperature Quantum Bit Memory Exceeding One Second,” *Science (80-.).*, vol. 336, no. 6086, pp. 1283–1286, 2012.

[123] M. Steger, *et al.*, “Quantum Information Storage for over 180 s Using Donor Spins in a 28Si ‘Semiconductor Vacuum,’” *Science (80-.).*, vol. 336, no. 6086, pp. 1280–1283, Jun. 2012.

[124] P. G. Kwiat, *et al.*, “Digital Delay Quantum Memory,” vol. 287, p. 61801, 2015.

[125] D. R. Herriott and H. J. Schulte, “Folded Optical Delay Lines,” *Appl. Opt.*, vol. 4, no. 8, p. 883, 1965.

[126] M. Campagna, *et al.*, *Quantum Safe Cryptography and Security*, no. 8. 2015.

[127] R. Ursin, *et al.*, “Free-Space distribution of entanglement and single photons over 144 km,” pp. 1–10.

[128] K. Gordon, *et al.*, “Quantum key distribution system clocked at 2 GHz.,” *Opt. Express*, vol. 13, no. 8, pp. 3015–20, Apr. 2005.

[129] R. J. Collins, *et al.*, “Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source,” *J. Appl. Phys.*, vol. 107, no. 7, p. 073102, 2010.

[130] B. Utreja and H. Singh, “A review paper on comparison of optical amplifiers in optical communication systems,” vol. 2, no. 11, 2011.

[131] M. J. Connelly, *Semiconductor Optical Amplifiers*, 1st ed. Kluwer Academic Publishers, 2002.

[132] M. N. Islam, “Raman amplifiers for telecommunications,” *IEEE J. Sel. Top. Quantum Electron.*, vol. 8, no. 3, pp. 548–559, 2002.

[133] V. Scarani, *et al.*, “Quantum cloning,” *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Nov. 2005.

[134] E. Eleftheriadou, *et al.*, “Quantum Optical State Comparison Amplifier,” *Phys. Rev. Lett.*, vol. 111, no. 21, p. 213601, Nov. 2013.

[135] J.-P. Bourgoin, *et al.*, “A comprehensive design and performance analysis of low Earth orbit satellite quantum communication,” *New J. Phys.*, vol. 15, no. 2, p. 023006, Feb. 2013.

[136] V. D’Ambrosio, *et al.*, “Complete experimental toolbox for alignment-free quantum communication.,” *Nat. Commun.*, vol. 3, p. 961, Jan. 2012.

[137] G. Vallone, *et al.*, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A*, vol. 91, no. 4, p. 042320, Apr. 2015.

[138] T. Schmitt-Manderbach, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 1–4, 2007.

[139] G. Vallone, *et al.*, "Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons," *Phys. Rev. Lett.*, vol. 113, no. 6, p. 060503, 2014.

[140] M. Mirhosseini, *et al.*, "High-dimensional quantum cryptography with twisted light," *New J. Phys.*, vol. 17, no. 3, p. 033033, 2015.

[141] A. Berk, L. *et al.*, "MODTRAN cloud and multiple scattering upgrades with application to AVIRIS," *Remote Sens. Environ.*, vol. 65, no. 3, pp. 367–375, 1998.

[142] S. Arnon, "Power versus stabilization for laser satellite communication.," *Appl. Opt.*, vol. 38, no. 15, pp. 3229–33, 1999.

[143] D. L. Fried, *et al.*, "Measurements of laser-beam scintillation in the atmosphere," *Josa*, vol. 57, no. 6, pp. 787–797, 1967.

[144] D. L. Fried and J. B. Seidman, "Laser-Beam Scintillation in the Atmosphere," *J. Opt. Soc. Am.*, vol. 57, no. 2, pp. 2–6, 1967.

[145] A. K. Majumdar and J. C. Ricklin, *Free-space laser communications: principles and advances*. 2008.

[146] G. R. Boyer, *et al.*, "Atmospheric birefringence under wind speed gradient shear," *J. Opt. Soc. Am.*, vol. 68, no. 4, p. 471, 1978.

[147] "Applications of optical properties of materials." [Online]. Available: http://what-when-how.com/electronic-properties-of-materials/applications-optical-properties-of-materials-part-4/.

[148] Corning, "Corning SMF-28e Optical Fiber Product Information," no. January. Corning Incorperated, Corning, NY, USA, 2005.

[149] Corning Incorporated, "Corning ® SMF- 28 ® ULL Optical Fiber," 2014.

[150] "ID Quantique." [Online]. Available: http://www.idquantique.com/. [Accessed: 13-Jan-2016].

[151] Quintessence labs, "Quintessence Labs," 2015. [Online]. Available:

http://www.quintessencelabs.com/. [Accessed: 17-Nov-2015].

[152] W. Becker, *Advanced Time-Correlated Single Photon Counting Techniques*, vol. 81. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[153] Picoquant, "HydraHarp 400 Single Photon Counting System User's Manual and Technical Data," vol. 1.2.

Chapter 3

Review of Cryptography and Digital Signatures

3.1 Introduction

This Chapter introduces the concept of conventional cryptography with the focus on key distribution, and digital signatures. Here, the term "conventional" is chosen to refer to the nature in which the cryptographic information is sent. For example a bright coherent laser source, something hand written, or by an electrical signal on a copper wire are all inherently classical in nature, because we are using large ensembles rather than single quantum particles. Conventional cryptography is sometimes referred to by those in the quantum fields as "classical cryptography". However, in the cryptography field that term is applied to protocols of antiquity and the term "conventional" is preferred. Although there are several other conventional cryptographic protocols the focus of this Thesis is on quantum key distribution and quantum digital signatures, so only the relevant conventional protocols are covered.

During the description of conventional cryptography, code-breaking and hacking is introduced and discussed to give the reader an idea as to why quantum communications is a vital area of research. It also highlights another are of research which aims at providing greater security for cryptography and digital signatures, conventional post-quantum cryptography.

The quantum communications section introduces quantum key distribution, the most well-established quantum communications technology, with brief descriptions of protocols that exists and the current limitations. Following this, another quantum communications protocol, quantum digital signatures, is introduced in advance of forming the primary topic of Chapters 4 and 5.

3.2 Conventional Cryptography

Conventional cryptography encompasses encryption methods used over thousands of years, such as hand written documents from the Egyptian or Roman era, to the electrical and optical signals sent today.

This section describes cryptographic schemes which can be used for encryption key distillation (sharing) and the digital signatures section. The two common methods of symmetric and asymmetric key cryptography are outlined to set the scene for later, more complex schemes. A major topic in the world of cryptography is the realisation of the quantum computer and its effect on how we will transmit secure information, so a discussion is given of the attacks that could be attempted with a quantum computer. Finally, a description is given of some conventional cryptographic schemes which are proven to be safe from known quantum computer attacks.

3.2.1 Symmetric Key Cryptography

In symmetric key cryptography both the sender and receiver have the same key. This key, which can be generated by either party, can be shared via a courier, a secure electronic connection, or any other secure means [1], [2]. The key is referred to as the cipher key, which can be applied to a plain text message creating an encrypted message also known as a cipher text. When the cipher key is re-applied to the cipher text, it will recreate the original plain text message as long as the cipher text was not altered in transit. An example for a plain text message is given in Figure 3.1, however if the 'Plain text message' was replaced with a signature it would become a signature scheme [3].

The scheme can also be used for generating a digital signature where the message is turned into a digital signature by applying the cipher key. After the key has been shared, the digital signature is then sent through the channel along with the message. The receiver can apply the cipher key to the message and if the retrieved digital signature is the same as the one sent with the message it can be said that the message is authenticated and not been tampered with during transit.

There are many different protocols which use symmetric key cryptography some basic examples are the Caesar shift [1], [2], and a modified version of the Caesar shift, which is known as the Vigenère shift[1], [2].

The one-time pad is another protocol for symmetric cryptography which, when perfectly implemented, can provide unconditional secure communications [4]. The one-time pad is a randomly generated one-time key, the length of the key is at least the same size as the message. An eavesdropper will have to perform a brute force attack to break the key, and

as the key length increases, the length of time taken to perform this attack will increase. However the symmetric key must be sent and stored by some secure means, as allowing an eavesdropper access to the entire key will enable them to read the encrypted information [1]. Therefore securely transporting the key in a conventional system is an issue that needs to be addressed.

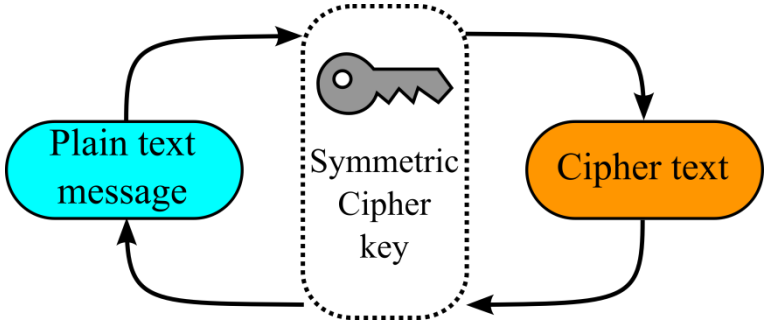


Figure 3.1 – A visual of how a symmetric key works.

3.2.2 Asymmetric key cryptography

Asymmetric key cryptography does not use the same single key to perform the initial transformation as is used for the subsequent decryption, unlike symmetric key cryptography. This is sometimes referred to as public-key cryptography because the key is made public, with many parties able to encrypt, or sign, a message for one receiver [5]. The security of asymmetric key cryptography lies in the present computational difficulty for an eavesdropper in figuring out all the parameters for the one-way function (the algorithm) from the publicly available information [6].

In asymmetric key cryptography, Alice (one party involved in the protocol) generates a public-key, to lock the information to be sent down a communication channel, and a private key, to read the information sent to her. These two keys are different but inter-related. The public key can be shared through an insecure channel (unlike in symmetric cryptography), so anyone with the public-key can encrypt a message (or sign a signature) and send it to Alice, but only Alice can decrypt them (or verify a signature) using the private key, as the public key does not allow anyone but Alice to decrypt (or verify the signature).

Public-key cryptography can be used for both key distribution and digital signature protocols, making them very useful in for electronic information interchange in today's world especially over the World Wide Web [7]. Diffie-Hellman key exchange [8], elliptic curve cryptography [9], digital signature algorithm [10], and the Rivest, Shamir and Adleman [11] (RSA) algorithm are all commonly used in internet communications for either encryption or digital signatures [7]. Other public key cryptography schemes based on other one-way functions can be used, although these are currently much slower [12].

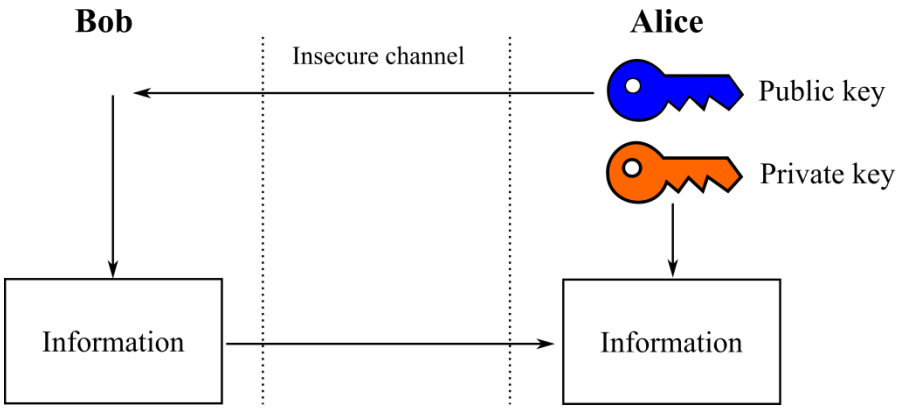


Figure 3.2 - Asymmetric key sharing. Alice and Bob swapping information through an insecure channel.

3.2.3 Breaking cryptography and a world with the quantum computer

For as long as cryptography has been around cryptanalysts have been around trying to figure out how to break encryption algorithms so that private information can be read or digital signatures could be forged [1]. One "basic" method an eavesdropper could use to find out the key is to simply guess until they get it right. The time taken to do this will depend on the bit size of the key, expressed as the length in bits N. The larger N, the more guesses a user will need to make in order to reach the right one, in the worse-case scenario this will be 2^N. This type of eavesdropping attack is known as a brute force attack, and is basically an exhaustive search which is very commonly used [13]. The time taken to perform the attack is primarily based on how many guesses can be performed per second, and is directly linked to the computational power available.

Problems such as integer factorisation and discrete logarithms, can be solved faster using quantum computers [14] running Shor's [15] or Grover's algorithm [16] when compared to conventional computers. Although Grover's algorithm does not offer as great a speed-up

as Shor's algorithm does. Shor's algorithm could render many of the cryptographic protocols used for encryption and digital signatures unusable. Public-key cryptography schemes widely used today such as Rivest, Shamir and Adleman [11], Diffie-Hellman [8], and the digital signature algorithm [10], are all reliant on the integer factorisation and discrete logarithms for their security. This means that a quantum computer will directly affect widely implemented cryptographic schemes used today. The threat of an attack being made by a quantum computer is something the cryptographic community needs to take into consideration when creating and testing the next generation of cryptographic protocols.

Although practical quantum computers capable of solving complex problems are not currently realisable, small-scale realisations using ion traps, neutral atoms, nuclear magnetic resonance, optical, and superconducting materials superconducting have been shown [17], [18]. The commercially available D-Wave One [19], [20] has generated considerable interest in the quantum computing community. However it is not able to run any of the known quantum search algorithms as it is a quantum annealing computer rather than a universal quantum computer. It appears quantum computers are on the horizon, and this could make many of today's cryptographic protocols based on public-key cryptography schemes highly vulnerable.

Quantum-safe protocols are required because of the social, political, and economic issues which could arise from the quantum speed-up in breaking some cryptosystems. So it is in the interest of governments and corporations to invest time and money into quantum-safe information technology [5], [12]. The term quantum-safe refers to cryptographic algorithms believed to be resistant to the reduction in time taken to hack that would be achievable with a quantum computer running a quantum search algorithm.

3.2.4 Conventional quantum-safe protocols

Although many of today's widely used cryptographic algorithms (based on public-key cryptography) will be made insecure with the creation of a large qubit quantum computer, there are still conventional cryptographic schemes which may still survive such as, hash-based [21], [22], code-based [23], lattice-based [24], and multivariate-quadratic-equations [25]. Although experts believe that Shor's algorithm [15] cannot be applied to these cryptosystems another quantum computer algorithm, Grover's algorithm [16], does have

some applications, but does not offer as great a speed-up as Shor's algorithm [5]. The research into the creation of quantum-safe algorithms is known as post-quantum cryptography.

Although conventional quantum-safe algorithms provide security for encryption and digital signatures against large classical computation and known quantum computer algorithms, currently known quantum-safe algorithms generally require larger key bit sizes compared to RSA. This is a disadvantage as algorithms such as RSA are typically used to secure things such as Google searches, which requires fast processing at a low cost in terms of both time and money [5]. While an RSA key could, for instance, be four thousand bits, a post-quantum key can be 100 times larger, with the corresponding increase in time and computational power required to create, store and process this larger key [5]. This is the reason why RSA and other cryptography schemes are so popular, because they are generally more efficient that other protocols.

One important thing for cryptography is to provide confidence in the security of the protocol or algorithm. This requires vigorous testing, by cryptanalysts, of different methods to break/hack the algorithm [5]. An algorithm that can withstand a number of different attacks is more trustworthy than one that cannot. Breaking cryptography can sometimes be about luck, and there may be some as yet unknown method to break an algorithm which no one has tried before or discovered. For instance, recently a new algorithm helped reduce the time it took to hack public-key cryptography [26]. If there is to be a quick change-over or upgrade to cryptography used today when the quantum computer arrives, with enough qubits to apply Shor's or Grover's algorithm, there is a need to investigate new approaches immediately.

Post-quantum cryptography's mathematical complex one-way functions promise to be robust against attacks from a quantum computer which would run Shor's algorithm [15], [27]–[29] although some algorithms are still vulnerable to Grover's algorithm [16], but it is not as swift. In order to push post-quantum cryptography forward, effort into development of algorithms and security testing is required to help build confidence and efficiency. Software and hardware, which is user friendly and low cost is also required if post-quantum cryptography is to take over from the public-key cryptography schemes.

3.3 Quantum cryptography

The previous sub-section described how conventional cryptography using complex one-way functions can help provide quantum-safe schemes, however there are other methods which can be used to provide quantum-safe schemes, with other advantages as well.

Quantum cryptography uses the well-known and tested laws of quantum mechanics to create secure cryptography schemes. Not only are the schemes quantum-safe, they also allow the detection of eavesdroppers before any private information has been shared, which is something conventional schemes cannot do [30].

The main focus of this section will be quantum key distribution and quantum digital signatures. Other quantum schemes exist for different tasks however these are beyond the scope of this thesis.

3.3.1 Quantum key distribution

Quantum key distribution (QKD) is often referred to as 'quantum cryptography', and fits into a wider topic of quantum communication along with protocols such as quantum-money [31], quantum digital signatures [32] (QDS), quantum bit commitment [33] (QBC), and quantum fingerprinting [34] (QF). QKD was first presented by Bennett and Brassard in 1984 [35], [36], hence the name of the original QKD protocol, BB84.

The development of QKD over the past 30 years has involved both theoreticians and experimentalists. Many QKD protocols have been proven to be unconditionally secure in terms of their theoretical protocol [37], [38]. The problem in QKD came with device and measurement security, where an eavesdropper could gain information from experimental imperfections [39] and a description of some common attacks is given in the subsequent security section. Many of the attacks described are also relevant to other quantum communications protocols such as QDS.

QKD provides a secure method of sharing a symmetric encryption key between two parties, Alice, and Bob. The benefit of QKD is its ability to detect an eavesdropper from the use of the single-photons to encode the information that will be used to form the key. In conventional cryptography, an optical fibre bending attack [40], [41] could be used to couple encoded light pulses from an optical fibre without being noticed by either party.

This attack essentially allows an eavesdropper to couple photons from a communications channel, allowing them to read the signal being sent. If one photon is being sent at a time, the eavesdropper will sometimes receive a photon, when they do they must make an optimum measurement on the photon and resend it (or a new photon encoded according to the measurement result) to the legitimate receiver. This optimum measurement is not perfect and will lead to mistakes, announcing the eavesdropper's presence to the legitimate parties if they sacrifice a small fraction of their measurement records in a classical post processing discussion.

QKD offers unconditionally secure one-time pad encryption key sharing, with eavesdropping exposing potential [42]. A basic diagram showing an outline of a QKD scheme is shown in Figure 3.3.

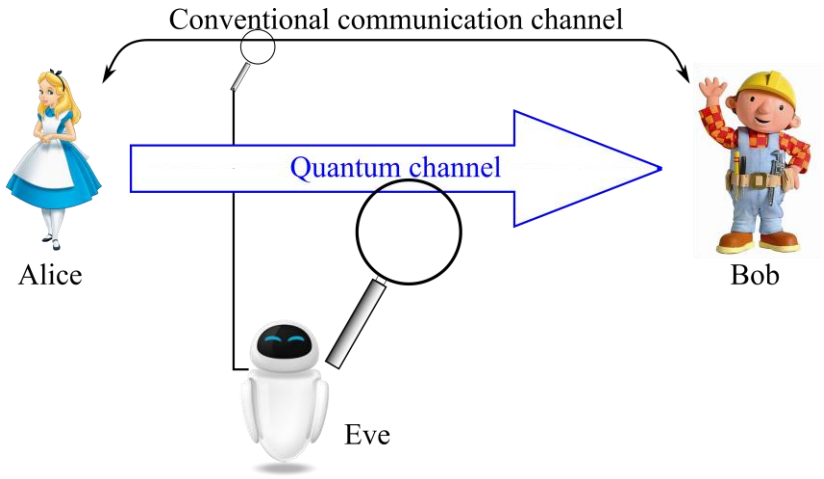


Figure 3.3 – A schematic of the basic layout for quantum key distribution.

Before going into protocol details it is useful to present some common features present in QKD protocols:

Raw count, sifted key, and secure key rates – The raw count rate is raw photon event count rate measured per second by a receiver on their photon detector(s). These raw photon events can then be filtered through classical communication to pick out photon events where the receiver made a measurement using the same basis as selected by the sender. The raw events counts that pass through this filtering process are the sifted key and give the sifted key rate of events per second (ignoring processing time). After the sifting the

sender and receiver generally share (and subsequently discard) some of the sifted key to check for errors, and sometimes perform some post processing on the sifted key as well. After this process is completed the sender and receiver are left with the secure key.

Quantum bit error rate (QBER) - The quantum bit error rate is, in its basic form, the number of incorrectly determined bits divided by the total number of bits [43]. The QBER value is affected by three mechanisms, the effect of the dark count rate on the detector, from the photon signal itself, and also from the eavesdropper. Dark counts are the number of inherent false events which a single-photon detector has and these were described in Chapter 2. The errors brought by the photon signal will depend on the effectiveness of the measurement which distinguishes the quantum states.

Error correction codes - Error correction codes are commonly used in QKD experiments and commercial systems, allowing the number of mismatches between Alice and Bob's shared secure key to be lowered [43], [44]. There are a number of different codes which can be used, which can be carried out over the public channel, and are relatively computationally intensive [42].

Privacy amplification - The aim of privacy amplification is to reduce the amount of information about the secret key that is held by an eavesdropper [44]. This is performed by taking the shared key from Alice and Bob, and producing a new shorter shared key using some mathematical function, for example a hash function [45]. Although this reduces the overall secure shared key rate, it does also mean that there is another security barrier in place to limit the effectiveness of eavesdropping.

3.3.2 Bennett-Brassard-84

BB84 was the first quantum key distribution protocol [35], [36], and is explained here to give a simple understanding of how QKD works - helping to assist when subsequently explaining less intuitive quantum communications protocols.

The original BB84 protocol is as follows [35]:

- Quantum distribution
    - Alice has two basis sets for encoding her single-photon, each has two orthogonal polarisations, one corresponding to binary digit (bit) value '1' and the other to bit value '0', as shown in Figure 3.4.
    - Alice randomly generates two equal length lists of bits via a random number generator. One list will be used to select the "basis set" and the other the "bit value" (polarisation)
    - For each individual single-photon Alice sets the polarisation of the photon according to the values in her two lists of binary digits.
    - Alice sends the polarisation encoded photon down the quantum channel to Bob.
    - Bob randomly chooses a basis set to measure in, and performs a measurement, storing the measured polarisation in some form of secure storage.
- Conventional sorting
    - Bob contacts Alice over the conventional communication channel and reveals which basis set he made each measurement in.
    - Alice confirms if Bob made the right or wrong choice of basis set for each measurement. If the right choice was made, the qubit information is kept and the same bit value for the polarisation is assigned independently by both parties without communicating this value. If the wrong choice of basis was made both parties throw away the qubit information.
    - Alice and Bob share a small part of their generated key to check for errors (QBER). If the number of errors is above a certain threshold (defined predominantly by natural experimental error and an assessment of the eavesdropper's capabilities), they abandon the shared encryption key, as they suspect an eavesdropper has been listening in or tampering.

Figure 3.5 shows how the BB84 protocols works without an eavesdropper. For comparison Figure 3.6 shows how the comparison of a subset of the key reveals an eavesdropper performing an intercept and resend attack [46].

	Basis set 1		Basis set 2	
Polarisation encoding	|V⟩	|H⟩	|-45⟩	|+45⟩
Classical bit value	0	1	0	1

Figure 3.4 – Quantum key distribution BB84 basis sets. There are two basis sets which allow for distinguishable measurements within a basis set.

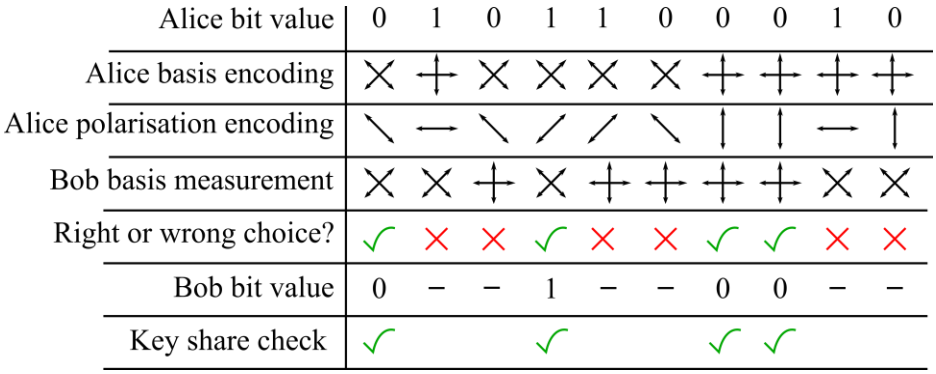


Figure 3.5 – Quantum key distribution using the BB84 polarisation protocol scheme for Alice and Bob with no eavesdropper in the quantum channel.

The effect of introducing an eavesdropper, Eve, who is performing an intercept and resend attack (see section 3.3.6 for more details) is shown in Figure 3.6. Like Bob, Eve only has a 50% chance of correctly choosing the right basis set to perform a distinguishable measurement. Eve will not know she has guessed the wrong basis set, but has to send on whatever she measured to ensure Alice and Bob count the photon she measured in their key. This is because if Bob does not measure a photon, Alice and Bob simply forget that qubit. The post processing discussion of the basis sets will only be made after Bob has received a photon, which must occur after Eve has made her measurement and transmitted the result. In the end this means that Eve will sometimes make a wrong measurement, which she then forwards onto Bob. This is only for the very basic of attacks. In the key share check, where Alice and Bob check for errors in a small number of key bits, Eve's

intercept and resend attack will be revealed by a QBER of 25% (for this simple attack) if she measures every photon pulse sent.

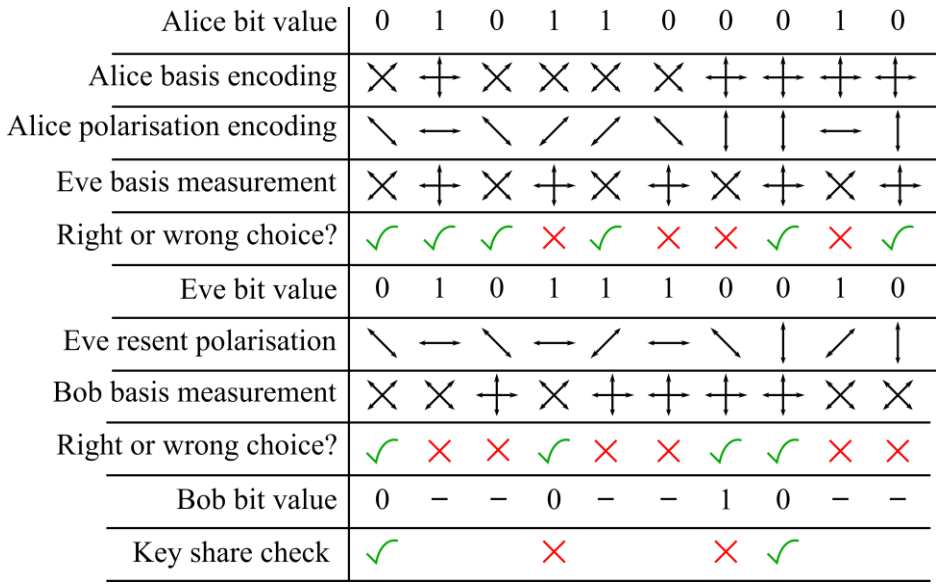


Figure 3.6 – Quantum key distribution BB84 polarisation protocol when an eavesdropper has been introduced performing an intercept and resend attack.

When practically realising QKD, some important assumptions need to be addressed. In the protocol outline Alice is encoding the key on her single-photon qubits, this prevents an eavesdropper from stealing information, for if there were two photons (or more), an eavesdropper could just measure one (or more) and leave the remainder for Bob. This is crucial to the security of QKD BB84 to prevent many attack strategies by Eve (see the subsequent 3.3.6 Security section).

In reality, single-photon sources which emit only a single photon when triggered were a far off prospect for use in QKD back in the early 1980's, and indeed much work still has to be done to create an on-demand, high repetition rate device. So in practice, many QKD protocols use an attenuated laser source. The laser light is attenuated so that it has a mean photon number per pulse ($|\alpha|^2$) which is less than 1, generally 0.1. Coherent laser light has Poissonian photon statistics and therefore there is a spread around $|\alpha|^2$ of photons observed per pulse (see Chapter 2), $|\alpha|^2$ must be less than 1 to reduce the probability of two photons being present in one pulse.

The first experimental demonstration was carried out over 32 cm of free-space using a wavelength of 552 nm, and $|\alpha|^2 = 0.12$. Photomultiplier tubes with 9% detection efficiency were used to detect the polarisation encoded weak coherent pulses. A secure key of 754 bits was transmitted in 10 minutes with a quantum bit error rate of 3.95 % [47]. Later realisations have been shown in optical fibre with entangled states at 1.45 km [48], and coherent state phase-encoding (with both optical fibre [49], [50] over >10 km, and waveguide embedded [51] interferometers). Also free-space applications using polarisation encoding of a coherent source at 205 m [52], and also entangled sources at 1.5 km [53].

Although BB84 was said to be unconditionally secure, the use of a coherent laser source in many applications meant that a maximum $|\alpha|^2$ of ≈0.l was allowed [54]. The limit in the allowable $|\alpha|^2$ means that the total transmission distance achievable is limited, see section 2.5 in Chapter 2.

3.3.3 Other protocols

Although the original BB84 protocol is now widely known, it is in fact not the most useful protocol because of the low $|\alpha|^2$ required during operation, which limits the maximum achievable transmission distance and overall secure bit rate. There are many other QKD protocols which several research groups use today instead of the original BB84, either to improve security, or to make use of technology which was not available at the time the BB84 protocol was proposed. Although these protocols are not implemented in this Thesis, it is worth noting that QKD protocols could also be adopted for quantum digital signature (QDS) protocols [55]. Therefore a summary of protocols is given in the following paragraphs. The decoy-state BB84 protocol is described in more depth because of the increased $|\alpha|^2$ value which is comparable to those used in QDS protocols in this Thesis.

The Ekert 91 protocol relies on entangled photon pair source(s), with Alice and Bob measuring correlations based on Bells inequalities [56]–[58]. While the use of entangled sources makes it secure against intercept and resend attacks, these sources are experimentally complex to implement successfully.

The Bennett-92 protocol is a simplified version of BB84, and directly encodes bit values using two non-orthogonal polarisations rather than using two basis sets. This reduces experimental complexity, however the net secure bit rate is reduced by 50% the BB84 rate due to the measurement. [59], [60]

The six-state protocol is an extension of the BB84 protocol, with an extra basis set in the implementation to reduce the effectiveness of an eavesdroppers attack. This extra basis set also reduces the net secure bit rate achievable in comparison to the BB84 by 1/3 [61]–[63], however asymmetric basis set choice can increase this.

The decoy-state BB84 is another protocol which expands on the original BB84 protocol, was introduced by Won-Young Hwang [64] in 2003 as a means of detecting a photon number splitting attack by an eavesdropper. The protocol uses three different intensity levels are generally called 'decoy 1', 'decoy 2', and the actual signal. The signal $|\alpha|^2$ is generally set close to 0.5, with the two decoy-states each being less than 0.25 [65]. The intensity of the attenuated coherent laser source is randomly modulated such that the probability for signal, 'decoy 1', and 'decoy 2' are *X*, *Y* and *Z*, where the decoy-states have lower probabilities than the signal-states to maximise the key generation [66]. The decoys are revealed after the quantum bits have been sent and allow Alice and Bob to gauge how much information an eavesdropper could have potentially gained.

The Scarani-Acín-Ribordy-Gisin-04 protocol implements the same experimental set-up as the BB84 protocol, with only changes made to classical post-processing to increase security against photon number splitting (PNS) attacks. Instead of a basis set being revealed, two encoding values are revealed; this means an eavesdropper performing a PNS attack will still not be able to make a perfectly distinguishing measurement. [67]–[72]

The coherent one-way protocol, which currently hold the greatest distance covered at 307 km, transfers the key information by intensity encoded time-bin pairs, allowing a simpler measurement set-up. This involves three time-bin pairs, one for each binary value, and also a decoy to check the coherence of the states received by Bob. This coherence check allows Alice to guess the maximum amount of information that an eavesdropper could have received. [73]–[77]

The differential-phase-shift protocol uses phase-shifted coherent pulses, where Bob interferes sequential pulses by an asymmetric Mach-Zehnder interferometer, with an optical path length of one pulse period, the phase difference between each pulse is used to transfer the key information [37], [78]–[81]. The round-robin-phase-shift protocol is an extension of the differential-phase-shift protocol where sequential pulse interference can be extended to more than one period [82].

Continuous-variable quantum key distribution encodes information over a continuous range of mean photon numbers and phase (i.e. two quadratures), and is implemented using ordinary photon detectors rather than specific single-photon detectors [83]. This protocol can use increased $|\alpha|^2$ values, at the cost of transmission distance, and could be a possible implementation for the quantum optical state comparison amplifier introduced in Chapter 7 and 8.

Measurement-device independent (MDI) QKD is aimed at reducing the assumptions of the measurement devices in Bob [84], [85]. It was shown that single-photon devices can be controlled by an eavesdropper leading to information being leaked [39].

Device-independent QKD is a protocol designed so that its security is not dependent on the QKD devices themselves, i.e. protected against malicious manufacturers [86].

3.3.4 Longest distance

As mentioned earlier the coherent one-way (COW) protocol holds the record for the longest distance QKD experiment in optical fibre, at 307 km [87]. The previous distance record was 260 km for a differential phase-shift (DPS) protocol [88] and several factors contributed to the increase in distance. Firstly, more efficient single-photon detectors were implemented in the COW protocol experiment, giving a factor of four increase in detection efficiency. The COW experiment also implemented ultra-low loss optical fibre [89] giving approximately 0.03 dB less loss per kilometre than the standard optical fibre [90] used in the DPS protocol.

The longest free-space demonstration of QKD was conducted in 2007 between two Canary Islands of La Palma and Tenerife [91]. This experiment was carried out over 144 km using the decoy-state BB84 protocol and achieved 12.8 bits/s at a wavelength of 850 nm. The

record has stood for some time and it is likely to remain for a few more years as the next stage for free-space QKD is satellite communications where there are many technological problems to overcome before an implementation can be carried out. However there are research groups around the world looking into satellite realisations [92]–[95]. Low-Earth orbit satellites can be as low as 200 km above sea level, where the attenuation would come from the Earth atmosphere [94].

3.3.5 Highest bit rates

When considering the highest secure bit rate, a transmission distance needs to be given in order to provide a valid comparison, otherwise the highest bit rate could be given for the optimum transmission distance for a particular system. Every system will have a different optimum transmission distance and the difference in performance outside that range may be significant. The distance of 50 km is something of a common data point between many QKD experiments and the highest secure bit rate over this distance was shown in [66], by Toshiba Research Europe Ltd in Cambridge UK. The secure bit rate was found to be 1.002 Mbits/s and was the system was shown to be able to be run continuously over 36 hours. This experiment used the T12 protocol.

At 100 km the COW experimental system which was used for the longest distance experiment also has the highest secure bit rate at ≈ 10 kbits/s [87].

3.3.6 Security

This section outlines some general attacks which are available for use by an eavesdropper. Some of these attacks, such as the photon number splitting attack, were mentioned in the previous section describing QKD protocols. These attacks are not limited to QKD and should also be considered for other quantum communication protocols, such as quantum digital signatures, which is reviewed after this section.

A general assumption in security proofs is that an eavesdropper has all physically probable technology available to them. For instance near unity detectors, long storage time high fidelity quantum memory, lossless measurements, and infinite computing power [42].

Beam-splitting attack

In a beam-splitting attack, Eve replaces the quantum channel with a lossless channel, and then uses a beamsplitter to split Alice's output with the appropriate fraction. This splitting fraction will correspond to the original loss of the quantum channel. In this way, for example, a 3dB loss quantum channel will allow Eve to split 50% of the pulses sent to Bob. This attack will not affect the photon count rate at Bob, because Eve is only taking what would be lost anyway. The aim of this attack is to split the multiphoton pulses, allowing Eve to measure information which will be shared between Alice and Bob. A multiphoton pulse will allow both Eve and Bob to measure the encoded information, which might be used in the secure key later. When Eve measures from a single-photon pulse, Bob will no longer receive a photon and therefore no information is transferred between him and Alice, meaning Eves measurement is voided. Although it can be seen that Eve will never gain much of the overall key, because using a coherent source will have a low probability of multi-photon pulses. This attack allows some mutual information to be shared between Alice, Bob and Eve. A schematic is shown in Figure 3.7

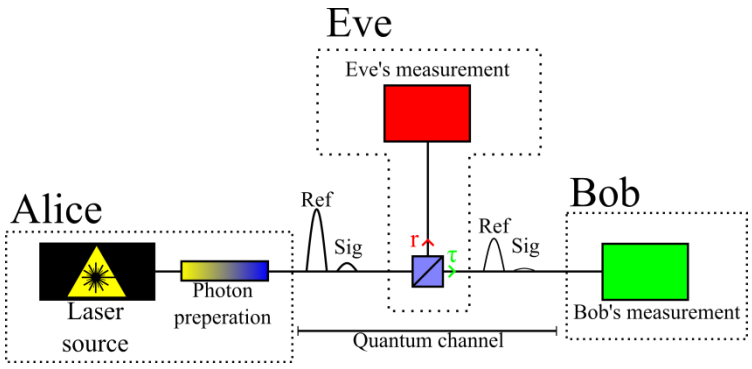


Figure 3.7 –Schematic diagram of a beam splitting attack by Eve on a quantum channel used by Alice and Bob.

Intercept-resend attack

Another common eavesdropping strategy that Eve can implement is the intercept-resend attack. As in the name, Eve intercepts the photons pulses being sent by Alice and measures them herself. She then resends fake copies of Alice's photon pulses to Bob [46], [96], [97]. A schematic of an attack is shown in Figure 3.8.

In Eve's measurement, she follows a three step process for optimising her measurements. First, she performs a non-demolition photon number measurement, which allows her to see how many photons she has received and can pick an optimum measurement for the pulses depending on how many photons are contained [98]. Secondly, she forwards on pulses with a low photon number to Bob, which cannot be distinguished as easily as multi-photon pulses. She discards a fraction which is proportional to the loss in the quantum channel. In the final third step, Eve measures the photons with a square-root measurement [99]–[101], which gives her the minimum value of error probability when distinguishing the photon states [46].

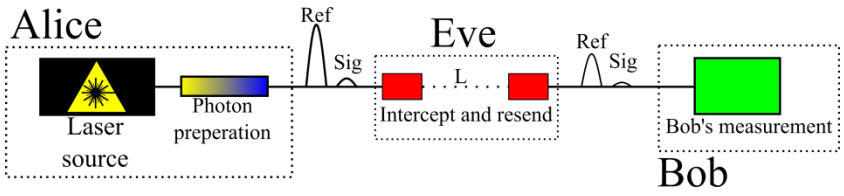


Figure 3.8 – Schematic set-up of an intercept and resend attack that could be performed by Eve on a BB84 phase mapped protocol.

In the basic intercept–resend attack on the BB84 protocol, Eve will simply guess between two basis sets and resend the answer she obtains. This will introduce an error of 25% in the secure key if she does this for every photon pulse sent [46]. By making more measurements, and eliminating more than one possible encoding of the possible four, Eve can reduce this error [42], but this requires multi-photon pulses.

Man-in-the-middle attack

In a man-in-the-middle attack, the eavesdropper, Eve, claims to be Bob [42]. Therefore the QKD protocol takes place between Alice and Eve, rather than Alice and Bob. After Eve receives the key which was meant for Bob, Eve will now be able to decrypt any documents which were only meant for Bob. A schematic of the attack is shown in Figure 3.9.

Clearly some form of authentication is needed in order for Alice to be able to tell whether Bob is really Bob [102]. Classically this is could be done by using some form of previously shared secret that only Alice and Bob will know, for instance a password set-up some time in advance of the communication [103].

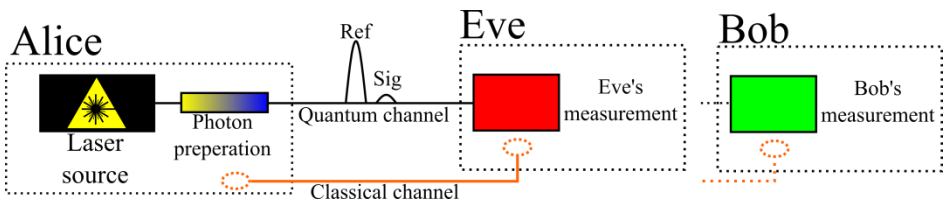


Figure 3.9 – Schematic of a man-in-the-middle attack performed by Eve.

An interesting idea using relativistic quantum bit commitment, which authenticates a user based on an arrival time of the photon, can allow for untrusted secure communication between parties [104].

Photon number splitting attack

A photon number splitting attack (PNS), [69], [105], is somewhat similar to the beam splitting attack mentioned previously. Eve breaks into the quantum channel connection from Alice to Bob and inserts a routing system. This routing system allows Eve to determine the photon number of each pulse using a non-demolition measurement [98]. If the pulse contains more than one photon, Eve sends one photon back into the quantum channel to be measured by Bob and keeps the excess photon(s) in a quantum memory for a later root-square measurement [99]–[101].

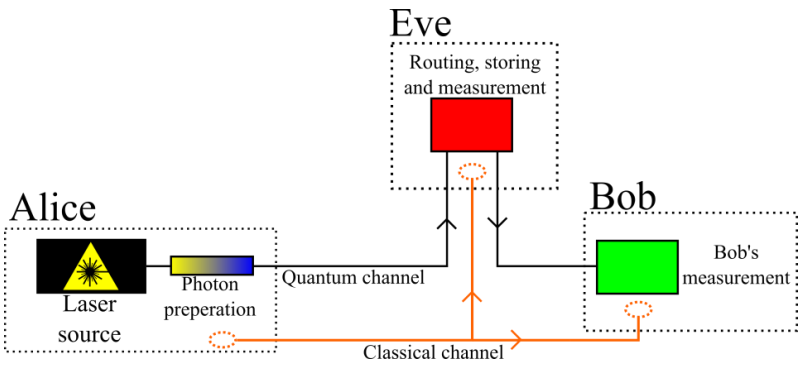


Figure 3.10 – A schematic of a photon number splitting attack that could be used by Eve.

In order for Eve to make the optimum measurement, she keeps her obtained photons stored in the quantum memory until Alice and Bob communicate over the classical channel for basis reconciliation. This way Bob will reveal when he made a measurement and which

basis set is the correct measurement. This is important for Eve because if Bob does not receive a photon count for a pulse Eve has photons stored for, she will have to discard them. A schematic is shown in Figure 3.10.

General side-channel attacks

Side-channel attacks take advantage of the imperfections which are present in a real QKD system. One example is the Trojan-horse attack where Eve probes Alice and Bob's equipment by sending bright pulses through the quantum channel and analysing back reflections from components which make up the system [103], [106], [107]. One main focus of side-channel attacks has been on the manipulation of detectors [39], [108]. A recent attack showed that the detection events on single-photon avalanche diodes could be controlled remotely by an eavesdropper [109]. The detectors were brought out of the regime in which they had single-photon sensitivity, and a remote eavesdropper could subsequently send their own information.

Physical layer quantum cryptography

Physical layer quantum cryptography is an recent development in QKD were a boundary has been placed in which attacks are currently actually physically possible [110]. For instance, in a free space QKD experiment which is used in line-of-sight applications, many Eavesdropper attacks would be noticed. If Eve is performing a PNS or beam-splitting attack, with current technology Alice and Bob will notice that Eve has placed some kind of routing/beamsplitter physically into the beam line. In the case of optical fibre communication, these attacks will still be relevant, as the optical fibre will generally be out of view and therefore the legitimate parties cannot physically see Eve.

In QKD these attacks were applied to both free-space and optical fibre communication, which in a sense is wrong to do, as it can limit the function of a technology for no other reason that a theoretical proof says it will be insecure at some point in the future [110]. Having physical layer quantum cryptography can help improve system performance based on a logical standpoint from how realistic an attack really is on system but as technology catches up with the theory it risks leaving us with weak or fatally flawed QKD systems [110].

3.4 Quantum Digital signatures

Digital signature schemes are as equally important as key sharing schemes in communication, as they can provide different forms of security such as message integrity (a message cannot be altered in transit), message authentication (a sender's message can be authenticated), and non-repudiation (a sender cannot deny creating the message). A scheme is unforgeable if a dishonest party cannot send a message pretending to be someone else. Non-repudiation in a scheme means that a signer cannot deny sending a message provided the scheme is unforgeable. Message transferability means that a message can be verified by an initial receiver, forwarded on and be verified by a secondary receiver, and so on [30].

Common conventional methods of creating digital signatures were mentioned earlier, such as Diffie-Hellman [8], elliptic curve cryptography [9], and Rivest-Shamir-Adleman [11]. These are based on one-way functions which were said to be insecure against attacks by a quantum computer using either Shor's [27] or Grover's [16] algorithm, which allow the quantum computer speed-up time in hacking attempts. This speed-up time is due to the quantum computer algorithms being more efficient in integer factorisation and discrete logarithms [18]. Grover's algorithm does also have some speed-up time for other one-way functions as was mentioned in Section 3.2.3.

Not all conventional digital signature schemes are based on factorisation or discrete logarithm problems, meaning that they are safe or more resistant to the speed-up time of known quantum algorithms [16], [27]. These digital signature schemes were hash-based, code-based, lattice-based, or multivariate-based schemes [5]. They are still complex one-way functions, however the speed-up time is not as significant for these problems as it is for factorisation and discrete algorithms [5]. Therefore they are said to be quantum-safe... at least for now.

One digital signature scheme which is similar to quantum digital signature schemes is the Lamport-Diffie one-time signature, a hash-based scheme [22]. In this scheme Alice wants to send a single signed bit, 0 or 1, some time in the future. Alice takes two randomly generated key inputs, k_0 (for binary message 0) and k_1 (for binary message 1), and puts then through a one-way hash function f. Alice then sends out the corresponding outputs of the hash function into the public channel. At a later time Alice send the single bit, 0 or 1,

and the corresponding randomly generated function input, k_0 or k_1. A receiver can apply the publically known hash-function to the input sent. If the function output sent earlier, and the one generated with the message are equal, then the message is authenticated. If they are not equal then the message cannot be authenticated. This signature can be used only once, and can be inefficient to generate. Later modifications were made to increase the efficiency of the scheme [21][30].

Although some one-way function schemes are quantum-safe, they can still be broken given enough time for a malicious party to use a brute force attack. For the ultimate security, schemes which are unconditionally secure are required. Unconditionally secure means that a protocol cannot be broken any faster than a brute-force attack [30].

Digital signature schemes can be made unconditionally secure if they do not rely on one-way functions [30]. In 1991 Chaum and Roijakkers proposed a scheme [111] in which the sender's signature elements were made up from elements transmitted by all the other participants who sent their elements anonymously, this prevents a sender trying to cheat as they cannot try to create a signature which will pass verification at one receiver and not another as they do not know which part to forge. Another conventional unconditionally secure scheme [112] allowed longer messages to be signed with more efficiency.

With unconditionally secure digital signature schemes available, why go to the quantum realm, introducing more experimental complexity? Quantum schemes allow assumptions about the communication channel to be reduced, or removed completely [30]. Quantum mechanics in QKD was shown to help reveal an eavesdropper in an insecure channel because of increased quantum bit error rate, this means that quantum digital signatures can also travel down insecure channels as long as sufficient checks are made. The conventional unconditionally secure digital signature schemes rely on broadcast channel, and anonymous secret sharing channels which can be difficult to implement and also expensive [30].

3.4.1 First introduction of quantum digital signatures

Quantum digital signature (QDS) protocols generally involve three parties, Alice, Bob, and Charlie. This is different from conventional digital signature scheme which involve between one and N depending on the protocol itself. QDS protocols have three main aims,

to provide authentication, prevent forgery signatures, and also message transferability. The third party in QDS protocols allows a swap and comparison to take place, allowing the receivers to check whether they were sent the same signature allowing them to authenticate and forward on messages sent. Alice is generally the sender, with Bob and Charlie the receivers. QDS protocols could be expanded to include more parties however this would change the security proofs of the protocols and make the experiments much more complex.

Quantum digital signature was first introduced by Gottesman and Chaung in 2001 [32]. The scheme involved quantum public-keys and conventional private keys. The quantum public-keys are constructed from quantum states, and the conventional private keys are classical strings [30]. The scheme is said to be a quantum analogue of the conventional Lamport-Diffie signature scheme described previously [22], [30].

For each possible future signed single bit, 0 or 1, Alice creates two random key classical strings (the private keys of length L), k_0 and k_1, and then creates quantum key strings using a classical to quantum one-way function which maps the classical signature into quantum states. This gives the public keys, two copies of which are sent out to each recipient.

Two recipients, Bob and Charlie, want to perform some swap and comparison mechanism to make sure they both have the same public-key sent from Alice. Bob (in this case) forwards on one of his copies of Alice's public-key to Charlie, who then takes his own copy of the "same" public-key and performs a measurement to test for mismatches between the two copies. If too many mismatches are found the protocol is aborted. If there are a small number of mismatches the protocol is continued, and Alice can send her binary message and the classical strings which make up the private keys to one of the recipients. If Bob receives the message and private keys, he performs a measurement to test for mismatches. If the mismatches are too numerous, Bob cannot authenticate the message and it is rejected. [32]

There were several issues with this scheme, one was the linear scaling of the key length L with size of message. Similar to the Lamport-Diffie one-time signature scheme the keys can only be used once, meaning that if more than one message is to be sent, the process of signing needs to be started from the beginning [22]. Finally, the swap and comparison mechanism, which allowed Bob and Charlie to confirm they were sent the "same" public-

key relied on quantum memory. The quantum memory was required in order for Bob and Charlie to store their states while waiting on the other party forwarding and also for Alice to forward the message. As was shown in the previous Chapter (section 2.4), quantum memories are currently not technologically advanced enough for this protocol [113].

3.4.2 First practically feasible quantum digital signature protocol

The first practically feasible QDS scheme came in 2006 in a paper by Andersson *et al.* [114]. This outlined a scheme using coherent states which no longer required quantum memory (QM) to perform the swap and comparison mechanism, which was a major step forward in practicality (however QM was still required for the state measurement). Instead of requiring Bob and Charlie to store quantum states and wait for copies to be forwarded by the other receiver, Andersson *et al.* proposed an optical multiport which performs state symmetrisation. This symmetrisation means that Alice cannot make the receivers disagree in the validation (message transferability). The multiport is shown in Figure 3.11.

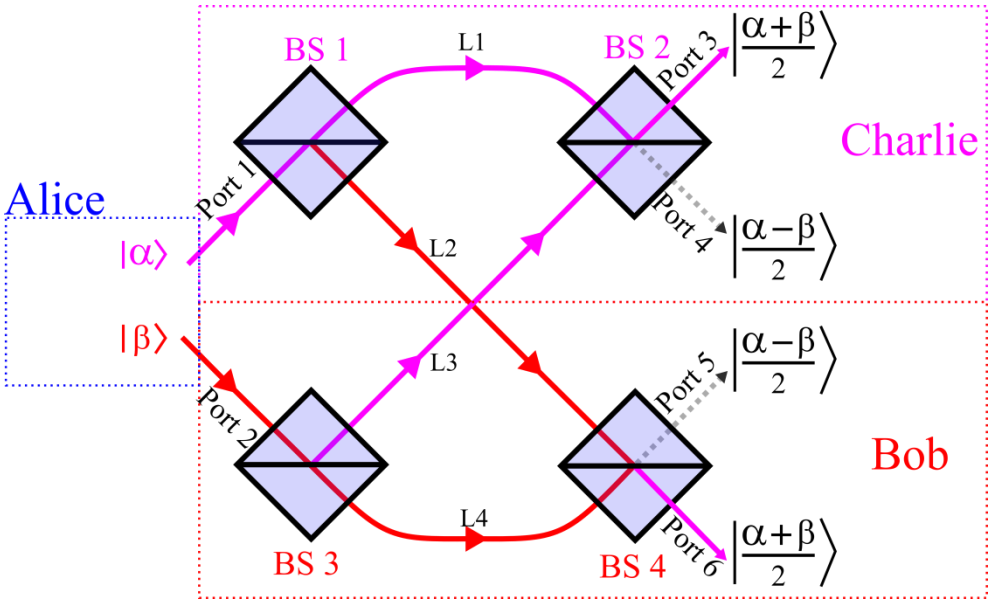


Figure 3.11 - A schematic of the all-optical fibre multiport, which is constructed of four 50:50 beamsplitters.

The optical multiport allowed Bob and Charlie to perform the swap and comparison mechanism in transit, meaning that they did not require a quantum memory as they did in the system proposed in the paper of Gottesman and Chuang [32]. The nature of the symmetrisation came from so called non-demolition measurements [115] at the second

beamsplitters which meant that Alice only needed to send one copy of the quantum signatures to Bob and Charlie, unlike in the Gottesman and Chuang scheme where two copies were sent to both recipients [30].

Overview of the security analysis

The security of QDS is a complex evolving field and the subject of ongoing research, therefore a full analysis is beyond the scope of this Thesis (the curious reader is directed to [116] for an introduction to the foundations of the field).This section aims to provide an accessible explanation of the basics of the security behind QDS so that the reader may appreciate what is expected to be seen in the experiments that follow without becoming entrenched in the fine detail. Figure 3.12 shows a basic diagram of how QDS was implemented in the systems reported in this Thesis, along with statements regarding the assumptions made about both the quantum and classical communication channels.

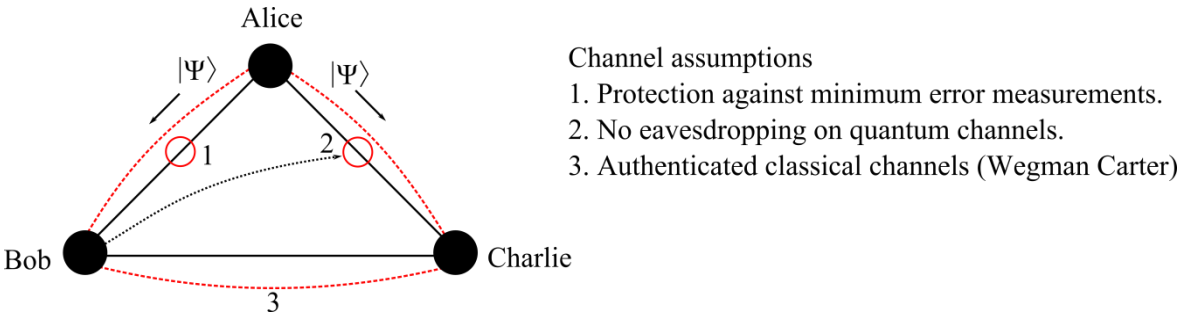


Figure 3.12- Schematic for general quantum digital signature experiment where Alice sends the same signature to Bob and Charlie.

Assumption 1 ("Protection against minimum error measurements") is based on Alice sending the same signature to both Bob and Charlie. In the protocol a certain measurement of the states is chosen which is to be implemented by both Bob and Charlie. However one of the receivers could apply a more optimised measurement (for example, a square root measurement [101]) closer to the sender (therefore at a reduced channel loss compared to the other receiver) allowing that receiver to know more accurate information about the quantum signature and thereby increase the probability that they can create a forged signature that will be accepted. This is taken into account during the security analysis by introducing a correction factor for the measurement that introduces the minimum possible error in the form of a parameter called $P_{\min}$.

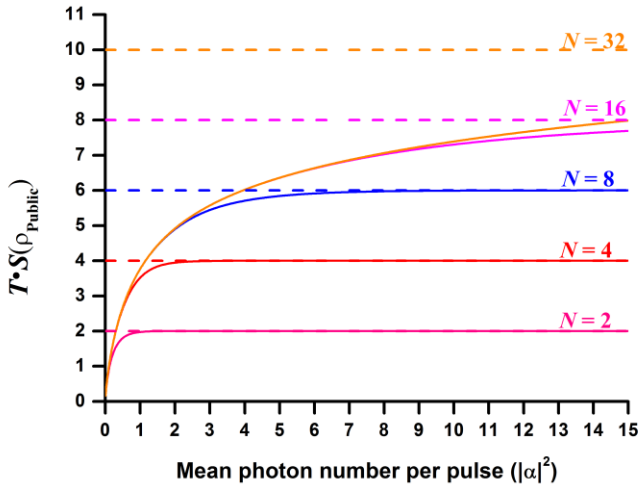


Figure 3.13- Von-Neumann entropy with mean photon number for different possible phase-encoding alphabets N.

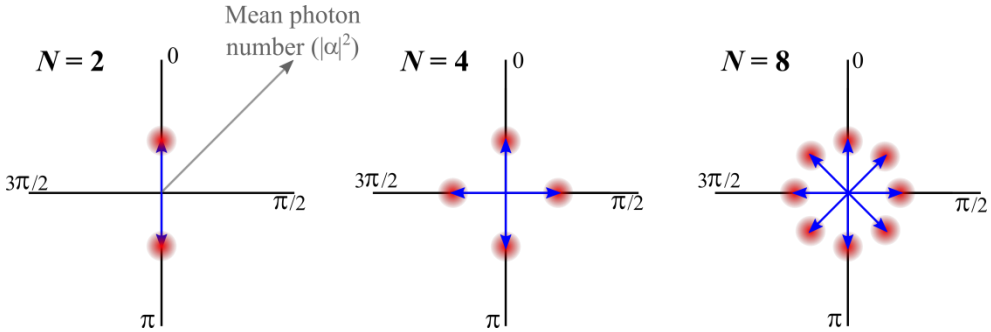


Figure 3.14 – Phase encoding overlap. Each red circle represents a phase-encoded coherent state with a given mean photon number ($|\alpha|^2$).

Although P_{min} is discussed later in relation to the experimental values, it is important to know at this stage that the amount on information a malicious party can gain from performing a minimum error measurement is related to the Von-Neumann entropy, the upper bound in accessible information available from a number of quantum states [117]. Figure 3.13 shows the Von-Neumann entropy (solid lines) along with the Shannon entropy (dashed lines) [118]. The Shannon entropy gives the classical limit for the amount of information that can be accessed, while the Von-Neumann gives the quantum equivalent. The Von-Neumann entropy means that at low $|\alpha|^2$ the upper bound on information available to malicious party is lower than the classical limit. By increasing the possible number of non-orthogonal states (Figure 3.14) in the protocol, *N*, the larger the Shannon

entropy limit, and therefore a larger $|\alpha|^2$ can be implemented. Therefore P_{min} is a correction factor based on the possible information a malicious party could gain determined by the $|\alpha|^2$ used in the experiment [101].

For assumption 2 ("No eavesdropping on quantum channels"), we assume that the quantum channels are inaccessible to eavesdropping from the other receiver. At first this may seem like a big assumption, however some of the eavesdropping attacks made by the other receiver would create mismatches in the signature measured by the intended receiver. A greater number of mismatches would mean that the intended receiver could reject a forged signature even though the other receiver knows a more information about the quantum signature sent by Alice. The problem comes when eavesdropping attacks such as beamsplitting, or photon number splitting attacks, which do not create any mismatches, are used.

Assumption 3 ("Authenticated classical channels") can be simplified to an assumption that the classical channels between all the parties are authenticated by the Wegman Carter universal hash function protocol [45] or a similar "quantum safe" conventional protocol. It seems strange to have a requirement that authenticated channels are used when one goal of QDS is to provide authentication, however QDS also provides message transferability, another property of digital signatures – and not one that can be provided by the Wegman Carter protocol.

QDS aims to provide security against three problems; accidently rejecting a correct signature, and accepting forgeries or repudiated signatures [118]. These probabilities that these situations will arise are denoted as P(hon rej), P(for), and P(rep), respectively. These can be understood in relation to the cost matrix, which is a matrix that can be assembled from the measurements made for QDS at a receiver. Equation 3.1 shows an example of a perfect cost matrix for a protocol using a 4 phase-encoding alphabet, namely $\{0, \pi/2, \pi, 3\pi/2\}$. The rows in the matrix correspond to the phase-encoding selected by Alice i.e. 0, $\pi/2$, π, or $3\pi/2$ (in that order, left to right) while the column corresponds to the possible outcome at the receiver for the interferometric unambiguous state elimination measurement, 'not 0', 'not $\pi/2$', 'not π', or 'not $3\pi/2$' (in that order, top to bottom).

$$\begin{pmatrix} 0 & 0.25 & 0.50 & 0.25 \\ 0.25 & 0 & 0.25 & 0.50 \\ 0.50 & 0.25 & 0 & 25 \\ 0.25 & 0.50 & 0.25 & 0 \end{pmatrix}$$

Equation 3.1

Equation 3.1 shows the perfect case where there is no channel loss, perfect interferometric visibility, and perfect detectors. However, in reality the diagonal elements will typically be non-zero and the off diagonal elements will not have the symmetry exhibited in the perfect case. These imperfections have implications in the security analysis. In order to protect against forgeries, honest rejections, and repudiated signatures, authentication and verification thresholds must be set. The parameters of interest from the cost matrix are the average value of the diagonal elements (P_h) and the guaranteed advantage (*guad*). P_h relates to how well a receiver's measurement is being performed, if the visibility of a measurement is not 100% then the diagonal elements will be larger than zero. The guaranteed advantage is the difference between the largest diagonal element, and smallest off-diagonal element, essentially the advantage a receiver has in rejecting a forged element. The conditions implied by assumption 1 mean that a correction factor needs to be applied to the guaranteed advantage in the case that one receiver is performing a minimum error measurement, this gives the modified advantage called the gap, *g*, which is calculated using the minimum error parameter P_{min} from earlier, P_h and *guad*.

The probability of a receiver honest rejection, *P*(hon rej), is based on the difference between the authentication threshold, s_a, and the average diagonal element value P_h. If the average diagonal elements approach the authentication threshold value, the probability that an honest rejection will occur will increase towards unity and the implementation of the protocol ceases to be viable. A greater number of mismatches will increase the probability that a message is accepted so it is important that the values of the diagonal elements of the cost matrix are low. This can be achieved by improving the visibility of the measurement apparatus, and using low dark count rate detectors can keep the probability of an honest rejection low.

The probability of a forged signature, *P*(for), being accepted is based on the difference between the advantage a malicious receiver has over the other receiver, C_{min}, and the verification threshold s_v. C_{min} takes into account the advantage that the receiver will have by performing the minimum error measurement (P_{min}) and their own measurement in

getting a forged element accepted by the receiver. From the cost matrix this is dependent on the average diagonal element value plus the *gap*, $P_h + g$. This is the probability that a message verifying receiver would reject an element based on their own measurement, and if the forwarding receiver performed a minimum error measurement, this value has to be higher than the verification threshold, so that the probability of accepting a forged element is low.

Repudiation is when Alice can deny sending a message, i.e. getting one receiver to accept the message, then getting the other receiver to reject the message. To protect against this the probability of repudiation, *P*(rep), is based on the difference between the verification threshold and authentication threshold, $s_a - s_v$. For the probability to be small, the verification threshold must be greater than the authentication threshold such that a message which passes the authentication must then be accepted by the other party with a large probability.

In the QDS protocols *P*(hon rej), *P*(for), and *P*(rep) are based on Hoeffding's inequalities and are computed as follows: $X_1,\ldots,X_L$ are independent random variables, each has a value 0, or 1. $\overline{X} = 1/L \sum X_i$ the empirical mean of the variables, and let $E(\overline{X})$ be the expectancy of the empirical mean. This gives Equations 3.2 and 3.3.

$$P\left(\overline{X} - E(\overline{X}) \geq t\right) \leq \exp(-2t^2 L) \qquad \text{Equation 3.2}$$

$$P\left(\left|\overline{X} - E(\overline{X})\right| \geq t\right) \leq 2\exp(-2t^2 L) \qquad \text{Equation 3.3}$$

For each QDS experiment the assumptions regarding the channel and measurement are slightly different therefore the formulations of probabilities based on Hoeffding's inequalities change slightly. Parameter *t* in the equations is the value which the probabilities are based on, and for each of the reasons given previously. In all QDS protocols presented in this Thesis the probabilities are made equal, as favouring one has no benefit over equally favouring. The authentication and verification thresholds are set to make these probabilities equal.

From these probabilities, the length of quantum signature can be calculated based on the probability of these attacks being successful. An arbitrary value of 0.01% was assigned for the first experimental implementation [118] and has remained consistent throughout subsequent experimental demonstrations to provide a comparable. However it should be noted that QKD experiments can offer threshold probabilities of 10^{-10} [119] which is a much smaller value. QDS could operate at the same threshold probabilities, at the expense of increasing the signature length. Because the Hoeffding's inequalities are exponential the increase in signature length is actually relatively small.

3.4.3 First experimental implementation.

Following the theoretical design of the multiport by Andersson *et al.* [114], in 2012 the first experimental implementation of QDS was shown by Clarke *et al.* [118]. The experiment system used for the experiment can be seen in Figure 3.15 [118]. Although this protocol managed to remove the requirement for QM in the swap and comparison mechanism, a long-term QM was required to store the coherent states at Bob and Charlie prior to the messaging stage. Bob and Charlie had to store the optical coherent states until Alice sent them the classical description which allowed them to perform a comparison between Alice's classical description and their stored states. However it did show a realisation of a QDS protocol, and also showed how the multiport can detect different signatures being sent to Bob and Charlie through symmetrising of the states sent by Alice.

In this protocol, Alice wishes to send a single bit binary message, *m*, which is either 0 or 1. She creates a separate quantum signature for both of these messages, which are comprised of a set of phase-encoded coherent states with *L* elements, and referred to as "signature half-bits". The length of the signature, *L*, is dependent on the experimental parameters, and the level of security required - this dependence will be considered in later Chapters.

The benefit of this experimental design was that it could be performed with a range of different non-orthogonal pairs of phase encodings, $N = 2, 4, 8, 16$, etc., because of the use of the phase modulators in all the encoding and decoding interferometers, Figure 3.15.

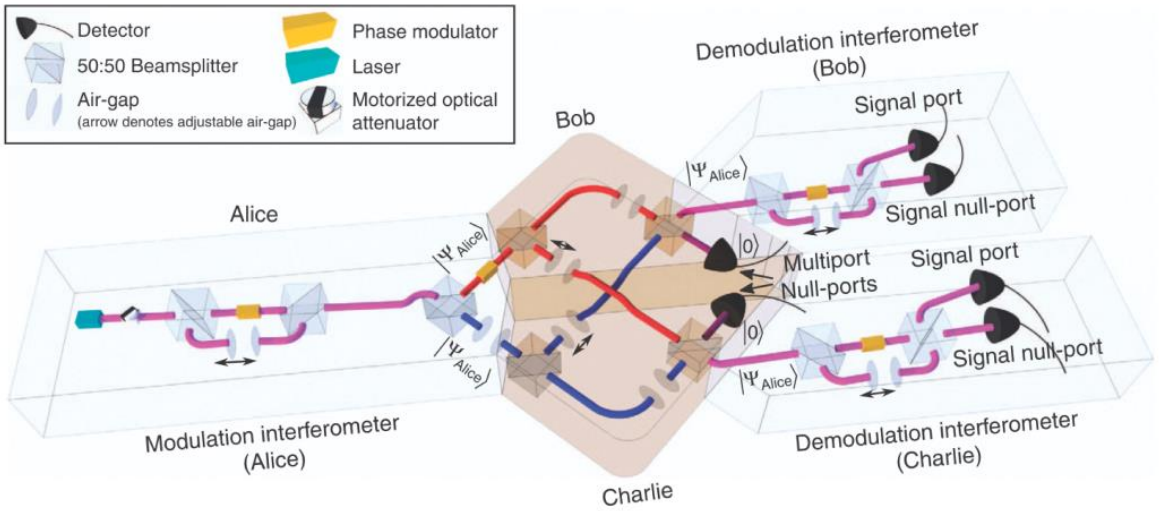


Figure 3.15 – First implementation of quantum digital signatures (QDS) [118].

This experiment also showed the effect of a cheating Alice, where she sends two different signatures through the multiport. This dishonest scenario was performed by sending a pattern of known states which were equal apart from 2 in every 16 states that was changed using a secondary phase modulator between Alice and one receiver. Figure 3.16 shows the raw and gated (temporally filtered) rates for an honest scenario for the multiport null-port detector and the detectors in the receivers interferometers [118]. The effect of the multiport swap and comparison mechanism showed a large increase in the count rate on the null-port detectors, as shown in Figure 3.17 [118]. This increase in the null-port detection would also lead to a decrease in the number of photons detected at the receiver. $|\alpha|^2$. In theory the null port detectors should have zero photon events when the signatures are equal, however due to dark counts and imperfect visibility this is not the case, however, when the signatures are different, the number of photon events increases due to distinguishable states.

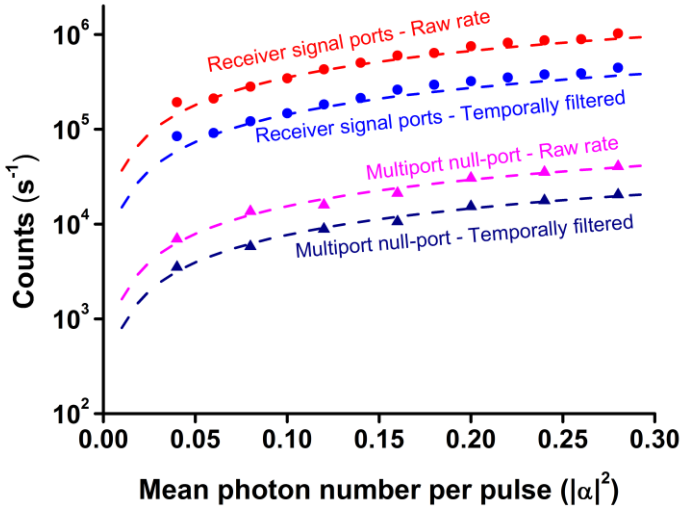


Figure 3.16 - Raw and gated (temporally filtered) count rates for the receiver detectors and the detector on the multiport null-port [118].

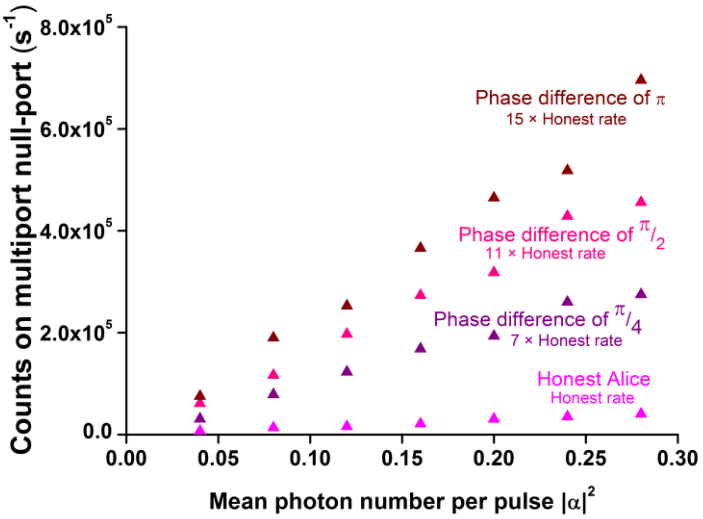


Figure 3.17 - Photon count rate on the multiport null-port for a phase shift on 2 in 16 pulses. [118]

The next stages in QDS are to completely remove the requirement for quantum memory throughout the protocol [120], [121], and also to increase the transmission distance to greater than 5 metres [122] and experimental realisations of these are the topics of subsequent chapters in this thesis.

3.5 Cryptography overview

Cryptography is split into three main areas, cryptographer, cryptanalyst, and algorithm designer/implementer [5]. The cryptographers come up with schemes to encrypt, decrypt, sign, verify, etc. One job of cryptanalysts is to come up with methods to break the cryptographers work and if they pass the tests, algorithm designers and implementers create software and hardware for wider use. One of the main concerns with the widespread conventional cryptography methods used in electronic communication (the internet, emails, bank transactions), is the possibility of a quantum computer which could use Shor's [27] or Grover's [16] algorithm to quickly break cryptographic protocols.

Two fields of research are currently involved in developing cryptographic protocols which are resistant to attacks by a quantum computer.

The first field described in this Chapter was quantum-safe, so called post-quantum communications, which is favoured by the conventional cryptography community. This uses complex mathematical one-way functions which are robust to the speed-up introduced by known quantum computer attacks. Developments into more efficient protocols and testing security through vigorous attacks are currently being performed to try and create mechanisms to keep conventional communications safe with similar or better performance than we have currently. These protocols are said to be quantum-safe for now, however they can still be broken by such things as the brute-force attack, or if an efficient algorithm is found for the problem in the future.

Quantum communications is one favoured by many physicists, which uses the well-known and tested properties of quantum mechanics to provide unconditionally secure cryptography. So far quantum key distribution, which provides secure encryption key transfer, is the most developed with commercially available systems already available. Quantum digital signatures are slowly gaining attention because they can be used to provide authentication, and message transferability, which are seen as very important communication applications.

It is thought that post-quantum cryptography could be carried out on commonly available conventional CPU devices, and could generate giga-keybits per second. Quantum

communications would generate kilo-keybits per second and requires costly speciality hardware. [5]

So this begs the question, why go with quantum communications when it is expensive and requires speciality hardware? The answer lies with quantum mechanics potential to detect eavesdroppers/malevolent parties during the secure transfer of key/signature. Even if a cryptosystem is breakable with a large computer or quantum computer attack, the time taken to do this may still be long enough for the information to be made irrelevant. If an eavesdropper listens into the transfer of the key/signature transferred by conventional methods, this means they have the key straight away, and there is no need for the crypto-attack. A conventional system can be attacked in such a way, for instance fibre bending [40], [41], but quantum communications protocols are designed so that if someone is listening in, they can be detected [42]. Hence, governments and organisations spend time and money on developing quantum communications [12].

Perhaps we shall leave the last word on post-quantum cryptography to Daniel J. Bernstein of the University of Illinois at Chicago.

> "*Maybe this preparation is unnecessary. Maybe we will not actually need post-quantum* [or quantum] *cryptography. Maybe nobody will ever announce the successful construction of a large quantum computer. However, if we do not do anything, and if it suddenly turns out years from now that users do need post-quantum* [or quantum] *cryptography, years of critical research time will have been lost*." – adapted from "Post-Quantum Cryptography" by Daniel J. Bernstein (2009) [5]

3.6 Bibliography

[1] S. Singh, *The Code Book*, 1st ed. London: First Anchor Books Edition, 1999.

[2] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, 2nd ed. Simon & Schuster, 1997.

[3] D. R. Stinson, *Cryptography: theory and practice*, Third., no. ISBN 1–58488–508–4. Chapman & Hall/CRC, 2006.

[4] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, no. July 1928, pp. 379–423, 1948.

[5] D. J. Bernstein, *Introduction to post-quantum cryptography*. Springer Berlin Heidelberg, 1998.

[6] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed., vol. 3. Boca Raton: Chapman & Hall/CRC, 2006.

[7] J. Galbraith and R. Thayer, "The Secure Shell (SSH) Public Key File Format," *IETF Trust etwork Work. Gr. Req. Comments*, vol. 4716, 2006.

[8] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] M. S. Anoop, "Elliptic Curve Cryptography," *Infosecwriters*, 2015. [Online]. Available: http://www.infosecwriters.com. [Accessed: 01-Dec-2015].

[10] S.-M. Yen and C.-S. Laih, "Digital signature algorithm," *IEEE Trans. Comput.*, vol. 44, no. 1, pp. 729–730, 1995.

[11] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] M. Campagna, *et al.*, *Quantum Safe Cryptography and Security*, no. 8. 2015.

[13] K. Apostol, *Brute-force Attack*. SaluPress, 2012.

[14] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," *Proc. R. Soc. A Math. Phys. Eng. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985.

[15] P. W. Shor, "Algorithms for quantum computation: discrete logarithms andfactoring," *Proc. 35th Annu. Symp. Found. Comput. Sci.*, pp. 124–134, 1994.

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," p. 8, 1996.

[17] M. Chapman and T. Heinrichs, "Approaches to quantum information processing and quantum computing," *A Quantum Inf. Sci. Technol. ...*, vol. 2, 2004.

[18] T. D. Ladd, *et al.*, "Quantum computers.," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[19] D-Wave, "D-Wave." [Online]. Available: http://www.dwavesys.com/. [Accessed: 08-Dec-2015].

[20] N. Jones, "The Quantum Company," *Nature*, vol. 498, no. 7454, pp. 286–288, 2013.

[21] R. C. Merkle, “One Way Hash Functions and {DES},” *Adv. Cryptology---CRYPTO~’89*, pp. 428–446, 1989.

[22] L. Lamport, “Constructing digital signatures from a one-way function,” *SRI Int. Comput. Sci. Lab.*, vol. 94025, no. October, pp. 1–8, 1979.

[23] R. J. Mceliece, “A public-key cryptosystem based on algebraic coding theory.” 1978.

[24] J. Hoffstein, *et al.*, “NTRU: A ring-based public key cryptosystem,” *Algorithmic number theory; Lect. Notes Comput. Sci.*, vol. 1423, pp. 267–288, 1998.

[25] J. Patarin, “Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms,” *Adv. Cryptology-EUROCRYPT*, pp. 1–40, 1996.

[26] T. Kleinjung, *et al.*, “Factorization of a 768-bit RSA modulus,” *Adv. Cryptol.*, pp. 1–22, 2010.

[27] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” vol. 26, no. 5, p. 28, 1995.

[28] A. Ekert and R. Jozsa, “Quantum computation and Shor’s factoring algorithm,” *Rev. Mod. Phys.*, vol. 68, no. 3, pp. 733–753, 1996.

[29] E. Martín-López, *et al.*, “Experimental realization of Shor’s quantum factoring algorithm using qubit recycling,” *Nat. …*, vol. 6, no. October, pp. 773–776, 2012.

[30] R. Amiri and E. Andersson, “Unconditionally Secure Quantum Signatures,” *Entropy*, pp. 5635–5659, 2015.

[31] S. Wiesner, “Conjugate coding,” *ACM SIGACT News*. 1983.

[32] D. Gottesman, *et al.*, “Quantum Digital Signatures,” *arXiv.org*, no. 0105032v2, 2001.

[33] J. Silman, *et al.*, “Fully distrustful quantum bit commitment and coin flipping,” *Phys. Rev. Lett.*, vol. 106, no. 22, pp. 2–5, 2011.

[34] R. T. Horn, *et al.*, “Single-Qubit Optical Quantum Fingerprinting,” *Phys. Rev. Lett.*, vol. 95, no. 15, p. 150502, 2005.

[35] C. H. Bennett and G. Brassard, “Quantum cryptography - public key distribution and coin tossing,” in *International Conference on Computers, systems and signal processing*, 1984, p. 8.

[36] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[37] K. Wen, *et al.*, “Unconditional security of single-photon differential phase shift quantum key distribution,” *Phys. Rev. Lett.*, vol. 103, no. 17, pp. 1–4, 2009.

[38] K. Tamaki and H. K. Lo, “Unconditionally secure key distillation from multiphotons,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 73, no. 1, pp. 1–4, 2006.

[39] M. G. Tanner, *et al.*, “Optimised quantum hacking of superconducting nanowire single-photon detectors,” pp. 1–8, 2013.

[40] M. Zafar Iqbal, *et al.*, “Optical fiber tapping: Methods and precautions,” *8th Int. Conf. High-Capacity Opt. Networks Emerg. Technol. HONET 2011*, no. figure 2, pp. 164–168, 2011.

[41] K. Shaneman and S. Gray, “Optical network security: technical analysis of fiber tapping mechanisms and methods for detection and prevention,” *IEEE MILCOM 2004. Mil. Commun. Conf. 2004.*, vol. 2, pp. 711–716, 2004.

[42] N. Gisin, *et al.*, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[43] H. Zbinden, *et al.*, “Quantum cryptography,” *Appl. Phys. B Lasers Opt.*, vol. 67, no. 6, pp. 743–748, 1998.

[44] W. Tittel, *et al.*, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[45] J. L. Carter, *et al.*, “Universal Classes of Hash Functions,” in *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing*, 1977, pp. 106–112.

[46] M. Curty and N. Lütkenhaus, “Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key- distribution protocol with weak coherent pulses,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 71, no. 6, pp. 1–10, 2005.

[47] C. Bennett, *et al.*, “Experimental quantum cryptography,” *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992.

[48] A. Fedrizzi, *et al.*, “Practical quantum key distribution with polarization entangled photons,” *2005 Eur. Quantum Electron. Conf. EQEC ’05*, vol. 2005, no. 16, p. 303, 2005.

[49] C. Gobby, *et al.*, “Quantum key distribution over 122 km of standard telecom fiber,”

Appl. Phys. Lett., vol. 84, no. 19, pp. 3762–3764, 2004.

[50] C. Marand, *et al.*, "Quantum key distribution over distances as long as 30 km.," *Opt. Lett.*, vol. 20, no. 16, p. 1695, Aug. 1995.

[51] Y. Nambu, *et al.*, "BB84 quantum key distribution system based on silica-based planar lightwave circuits," *Japanese J. Appl. Physics, Part 2 Lett.*, vol. 43, no. 8 B, pp. 1109–1110, 2004.

[52] W. T. Buttler, *et al.*, "Free-space quantum key distribution," *Phys. Rev. A*, vol. 57, no. 4, p. 5, 1998.

[53] I. Marcikic, *et al.*, "Free-space quantum key distribution with entangled photons," *Appl. Phys. Lett.*, vol. 89, no. 10, pp. 2004–2007, 2006.

[54] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," *Phys. Rev. Lett.*, vol. 93, no. September, pp. 1–4, 2004.

[55] V. Dunjko, *et al.*, "Quantum digital signatures with quantum key distribution components," *arXiv Prepr. arXiv1403.5551*, pp. 1–13, 2014.

[56] S. Cobourne, "Quantum Key Distribution Protocols and Applications," *Surrey TW20 0EX, Engl.*, no. March, 2011.

[57] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[58] A. K. Ekert, *et al.*, "Practical Quantum Cryptography Based on Two-Photon Interferometry," *Phys. Rev. Lett.*, vol. 69, no. 9, pp. 1293–1295, 1992.

[59] K. Tamaki, *et al.*, "Security of the Bennett 1992 quantum-key distribution against individual attack over a realistic channel," *Phys. Rev. A*, p. 16, 2002.

[60] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, 1992.

[61] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, no. 6, pp. 4238–4248, 1999.

[62] H. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," vol. 10001, pp. 1–9, 2008.

[63] D. G. Enzer, *et al.*, "Entangled-photon six-state quantum cryptography," vol. 4, pp.

1–8, 2002.

[64] W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication.,” *Phys. Rev. Lett.*, vol. 91, no. August, p. 057901, 2003.

[65] L. O. Mailloux, *et al.*, “Quantum key distribution: examination of the decoy state protocol,” *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 24–31, Oct. 2015.

[66] A. R. Dixon, *et al.*, “Continuous operation of high bit rate quantum key distribution,” *Appl. Phys. Lett.*, vol. 96, no. 2010, pp. 2008–2011, 2010.

[67] V. Makarov and J. Skaar, “Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols,” no. 7491, p. 9, 2007.

[68] Y.-C. Jeong, *et al.*, “An experimental comparison of BB84 and SARG04 quantum key distribution protocols,” *Laser Phys. Lett.*, vol. 11, no. 9, p. 095201, Sep. 2014.

[69] D. a. Kronberg and S. N. Molotkov, “Robustness of quantum cryptography: SARG04 key-distribution protocol,” *Laser Phys.*, vol. 19, no. 4, pp. 884–893, 2009.

[70] S. Ali, S. Mohammed, *et al.*, “Practical SARG04 quantum key distribution,” *Opt. Quantum Electron.*, vol. 44, no. 10–11, pp. 471–482, 2012.

[71] B. Xu, *et al.*, “The Security of SARG04 Protocol in Plug and Play Quantum Key Distribution system with an Untrusted Source,” *Source*, vol. 1, no. 2, pp. 1–9, 2011.

[72] S. Ali and M. R. B. Wahiddin, “Fiber and free-space practical decoy state QKD for both BB84 and SARG04 protocols,” *Eur. Phys. J. D*, vol. 60, no. 2, pp. 405–410, 2010.

[73] D. Stucki, *et al.*, “Coherent one-way quantum key distribution,” *Proc. SPIE*, vol. 6583, p. 65830L–65830L–4, 2007.

[74] C. Branciard, *et al.*, “Zero-Error Attacks and Detection Statistics in the Coherent One-Way Protocol for Quantum Cryptography,” no. Appendix C, 2006.

[75] M. Dušek, *et al.*, “Generalized beam-splitting attack in quantum cryptography with dim coherent states,” *Opt. Commun.*, vol. 169, no. 1–6, pp. 103–108, 1999.

[76] D. Stucki, *et al.*, “Fast and simple one-way quantum key distribution,” *Appl. Phys. Lett.*, vol. 87, no. 19, pp. 1–3, 2005.

[77] P. Sibson, *et al.*, “Chip-based quantum key distribution,” pp. 1–5, 2015.

[78] K. Inoue, *et al.*, “Differential phase shift quantum key distribution.,” *Phys. Rev.*

Lett., vol. 89, no. 3, p. 037902, 2002.

[79] K. Wen, *et al.*, "Unconditionally Security of Single Photon Differential Phase Shift Quantum Key Distribution," *Time*, vol. 17, no. 11, pp. 1–5, 2008.

[80] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 71, no. 4, pp. 3–6, 2005.

[81] K. Inoue, *et al.*, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, pp. 1–4, 2003.

[82] J.-Y. Guan, *et al.*, "Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 114, no. 18, pp. 1–5, 2015.

[83] P. Jouguet, *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, Apr. 2013.

[84] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, no. 6, p. 062319, 2012.

[85] Y. Liu, *et al.*, "Experimental Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 111, no. 13, p. 130502, Sep. 2013.

[86] N. Gisin, *et al.*, "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier," *Phys. Rev. Lett.*, vol. 105, no. 7, p. 070501, Aug. 2010.

[87] B. Korzh, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[88] S. Wang, *et al.*, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber.," *Opt. Lett.*, vol. 37, no. 6, pp. 1008–10, Mar. 2012.

[89] Corning Incorporated, "Corning ® SMF- 28 ® ULL Optical Fiber," 2014.

[90] Corning Incorporated, "Corning ® SMF- 28 e +® LL Optical Fiber," 2011.

[91] T. Schmitt-Manderbach, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 1–4, 2007.

[92] G. Vallone, *et al.*, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels," *Phys. Rev. A*, vol. 91, no. 4, p. 042320, Apr. 2015.

[93] V. D'Ambrosio, *et al.*, "Complete experimental toolbox for alignment-free quantum communication.," *Nat. Commun.*, vol. 3, p. 961, Jan. 2012.

[94] J.-P. Bourgoin, *et al.*, "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, no. 2, p. 023006, Feb. 2013.

[95] D. E. Bruschi, *et al.*, "Spacetime effects on satellite-based quantum communications," *Phys. Rev. D*, vol. 90, no. 4, p. 045041, Aug. 2014.

[96] J. Lin, *et al.*, "Intercept-Resend Attacks on Semi-quantum Secret Sharing and the Improvements," *Int. J. Theor. Phys.*, vol. 52, no. 1, pp. 156–162, 2013.

[97] M. Dehmani, *et al.*, "Quantum key distribution with several intercepts and resend attacks with partially non-orthogonal basis states," *Opt. - Int. J. Light Electron Opt.*, vol. 125, no. 2, pp. 624–627, 2014.

[98] B. R. Johnson, *et al.*, "Quantum Non-demolition Detection of Single Microwave Photons in a Circuit," *Nat. Phys.*, p. 5, 2010.

[99] N. Dalla Pozza, *et al.*, "Optimality of square-root measurements in quantum state discrimination," *Phys. Rev. A*, vol. 91, no. 4, pp. 1–10, 2015.

[100] S. Huang, "Square-root measurement for pure states," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 72, no. 2, pp. 1–6, 2005.

[101] P. Wallden, *et al.*, "Minimum-cost quantum measurements for quantum information," pp. 1–19, Dec. 2013.

[102] D. Ljunggren, *et al.*, "Authority-based user authentication in quantum key distribution," *Phys. Rev. A*, vol. 62, no. 2, pp. 1–7, 2000.

[103] F. G. Deng, *et al.*, "Improving the security of multiparty quantum secret sharing against Trojan horse attack," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 72, no. 4, pp. 1–4, 2005.

[104] Y. Liu, *et al.*, "Experimental unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 112, no. 1, pp. 1–5, 2014.

[105] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New J. Phys.*, vol. 4, pp. 44.1 – 44.9, Jul. 2002.

[106] N. Gisin, *et al.*, "Trojan-horse attacks on quantum-key-distribution systems," *Phys.*

Rev. A, pp. 1–7, 2006.

[107] N. Jain, *et al.*, "Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," *New J. Phys.*, vol. 16, 2014.

[108] A. Vakhitov, *et al.*, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *J. Mod. Opt.*, vol. 48, no. 13, pp. 2023–2038, 2001.

[109] L. Lydersen, *et al.*, "Thermal blinding of gated detectors in quantum cryptography," *Opt. Express*, vol. 18, no. 26, p. 27938, Dec. 2010.

[110] M. Sasaki, *et al.*, "Quantum Photonic Network : Concept , Basic Tools , and Future Issues," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 49–61, 2015.

[111] D. Chaum and S. Roijakkers, "Unconditionally Secure Digital Signatures," *Proc. 10th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, pp. 206–214, 1991.

[112] G. Hanaoka, *et al.*," in *Advances in Cryptology — ASIACRYPT 2000*, 2000, pp. 130–142.

[113] K. F. Reim, *et al.*, "Towards high-speed optical quantum memories," *Nat. Photonics*, vol. 4, no. 4, pp. 218–221, 2010.

[114] E. Andersson, *et al.*, "Experimentally realizable quantum comparison of coherent states and its applications," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 74, no. 2, pp. 1–11, 2006.

[115] P. Grangier, *et al.*, "Quantum non-demolition measurements in optics," *Nature*, vol. 396, pp. 537–542, 1998.

[116] V. Dunjko, "Ideal quantum protocols in the non-ideal physical world," Heriot-Watt University, 2012.

[117] J. von Neumann, "Die quantenmechanische Statistik," in *Mathematische Grundlagen der Quantenmechanik SE - 4*, Springer Berlin Heidelberg, 1996, pp. 101–157.

[118] P. J. Clarke, *et al.*, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.," *Nat. Commun.*, vol. 3, p. 1174, Jan. 2012.

[119] K. Patel, *et al.*, "High bit rate quantum key distribution with 100 dB security," *Cleo 2013*, p. QTu2C.3, 2013.

[120] R. J. Collins, *et al.*, "Realization of Quantum Digital Signatures without the

Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[121] V. Dunjko, *et al.*, "Quantum Digital Signatures without Quantum Memory," *Phys. Rev. Lett.*, vol. 112, no. 4, p. 040502, Jan. 2014.

[122] V. Dunjko, *et al.*, "Quantum digital signatures with quantum key distribution components," *Phys. Rev. A*, vol. 89, no. 4, p. 022336, 2014.

Chapter 4

Experimental Realisation of a Quantum Digital Signature Scheme Which Does Not Require Quantum Memory

4.1 Introduction

Conventional digital signature schemes are used every day in e-commerce to help provide protection against forging, and they also grant message transferability. However, many of the widely used signature schemes are not unconditionally secure. This means that the security relies on assumptions about the mathematical complexity of the protocol. Quantum digital signature (QDS) schemes on the other hand can be unconditionally secure, making use of the probabilistic nature of quantum mechanics. The only previous experimental realisation of a QDS protocol relied on long term, on-demand quantum memory (QM), which is not technologically feasible at this time, as described in Chapter 2 [1], [2]. The experimental realisation of QDS presented in this Chapter uses an improved protocol allowing for QDS to be performed without the need for any QMs, which is a major step towards practical applications.

4.1.1 Introduction to protocol for multiport implementation

Protocols for QDS have two stages, a distribution stage and a messaging stage. For our experimental implementation we are encoding in four possible states, $|a\rangle$, $|ae^{i\pi/2}\rangle$, $|ae^{i\pi}\rangle$, and $|ae^{i3\pi/2}\rangle$, although this is only limited by the experimental set-up, as each non-orthogonal pair requires one extra asymmetric Mach-Zehnder interferometer at the receiver to perform the measurement. In theory any number of non-orthogonal states could be used this requires modifications to the measurement system and theoretical model.

In the case of the multiport based QDS protocol the two stages are as follows:

Distribution stage

1. For each possible future one-bit message $k = 0,1$, Alice generates two copies of her quantum signatures, QuantSig_k. The quantum signature has a length L (which is determined by experimental properties, and calculated during the analysis section

of this Chapter), with each qubit element (which is a coherent state of amplitude $|\alpha|^2$) randomly chosen from her four available phase states $\{\alpha, \alpha e^{i\pi/2}, \alpha e^{i\pi}, \alpha e^{i3\pi/2}\}$. The information which makes up the signature is stored classically by Alice and is known as PrivKey$_k$.

2. Alice sends one copy of Quantsig$_k$ to each recipient, in this case Bob and Charlie.
3. Bob and Charlie then pass their phase-encoded coherent state elements of Quantsig$_k$ through the multiport to perform the swap and comparison mechanism. For each signature element they note whether they detect a photon at their multiport null-port photon detector. After the multiport each signature element is passed to the state discrimination measurement stage. This measurement could be unambiguous state discrimination or elimination, but the difference is only post-selection analysis. The measurement outcomes are stored in secure classical storage.

After the distribution stage Alice will have PrivKey$_k$, the complete classically stored information about QuantSig$_k$. Bob and Charlie will have confirmed they were sent the same signature by monitoring detection events on the multiport null-ports. They will also have their state discrimination or elimination measurements of separate signature elements stored classically. They are now ready to perform the messaging stage, a process that may take place a significant time after the distribution stage has occurred.

Messaging stage

1. To send a signed one-bit message, k, Alice sends the private key (PrivKey$_k$) and the message (k) to the desired recipient which we will assume as being Bob for now (although Charlie would perform the same processes).
2. Bob checks for mismatches between the private key sent by Alice (PrivKey$_k$) and his quantum signature. An authentication threshold, s_a, is applied to the matching to prevent forging. If fewer than $L \cdot s_a$ mismatches occur for Alice eliminated signature, then the message is accepted. If otherwise, the message is rejected.
3. To forward the message to Charlie, Bob forwards the message and the private key (k PrivKey$_k$) sent to him by Alice.
4. Charlie also checks for matches, similarly to that carried out by Bob, but instead applies verification threshold, s_v. If fewer than $L \cdot s_v$ occur, the message is accepted. Otherwise it is rejected. The verification threshold is chosen $0 \leq s_a \leq s_v < 1$, so the verification threshold is always larger than the authentication threshold, as there

will always be some extra experimental error in the swap and comparison mechanism leading to mismatches between the signatures measured by Bob and Charlie.

4.2 Unambiguous state discrimination/elimination quantum digital signatures

To overcome the need for QM in the swap and comparison mechanism, the first experimental QDS protocol [3] used an all-optical fibre multiport, which made use of non-demolition measurements to perform the swap and comparison mechanism [4]. Although the protocol did not require QMs in the multiport, it did however require them for Bob (Charlie) to perform their state discrimination measurement. The protocol proposed in [5] by Dunjko *et al.*, allows QDS to be carried out without relying on QM for the state discrimination measurement. This is due to an improved method of state discrimination which allows a state to be distinguished without prior information other than knowledge of the set of possible phase encodings of the coherent states. Without this reliance on QM, QDS becomes considerably more practical, and can be realised with existing optical components.

4.2.1 State discrimination measurement

In quantum communication, as in all communication, it is important for a receiver to be able to correctly interpret the information being sent. Generally when dealing with secure quantum communication protocols the mean photon number is low. Therefore it is important that the receiver has an optimised quantum measurement.

In this experiment two similar measurements were carried out using the same set-up, which were unambiguous state discrimination (USD), and unambiguous state elimination (USE). USD is optimised to only accept the right answer, and therefore fully identifies the phase encoding of the state sent. USE on the other hand, aims to eliminate states which were not sent. Keeping in mind that QDS is a communication protocol, USE allows for a far greater success rate in measurement than USD. This is because USD, in our 4-phase encoding case, relies on 3 photon correlated events, while USE only relies on 1 photon event. This allows USD to rule out three of the four states, identifying one, and USE to only rule out one. The mean photon number ($|\alpha|^2$) reaching the detectors is generally <1, therefore the probability of 3 photons, which have been routed correctly, triggering detection events is extremely small when compared to the probability of one detected photon event. Figure 2.1 shows the probability of a observing a certain number of photons in a particular pulse

for a given $|\alpha|^2$ per pulse. It can be seen that even at a $|\alpha|^2 = 1$, the probability of 3 photons being measured is less than 10%, at Alice, before any communications channel or detector loss.

Unambiguous state discrimination

Unambiguous state discrimination allows the phase encoding of a state to be fully discriminated based on correlated detections and non-detections. In order to perform the measurement a receiver only needs to know what possible non-orthogonal states are available for Alice's phase-encoding. An experimental representation of how USD works with linear optics for four possible phase-encodings is shown in Figure 4.1. The input state, labelled $|\beta\rangle$, comes from Alice is split into two paths. One path is interfered with a reference on BS2 which is setup to possibly rules out one or both of the 0 or π non-orthogonal pair, while the other path is interfered with a phase reference difference of $^{\pi}/_{2}$ on BS3 which possibly rules out one or both the $^{\pi}/_{2}$ or $^{3\pi}/_{2}$ pair.

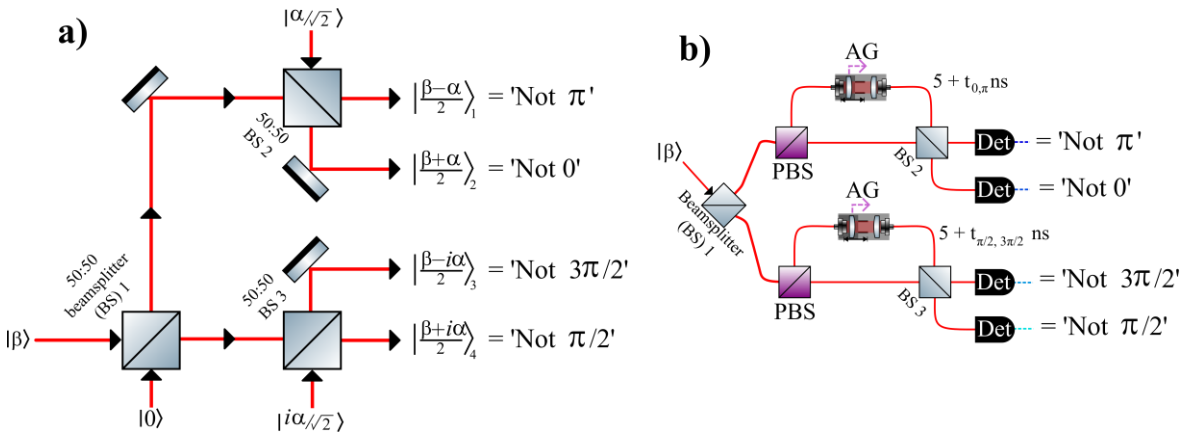


Figure 4.1 – a) unambiguous state discrimination and unambiguous state elimination schematic [6]. *b) Unambiguous state discrimination and unambiguous state elimination measurement used in the quantum digital signatures experimental implementation BS – beamsplitter, PBS – polarisation beamsplitter, AG – air-gap, Det – photon detector. AGs allow the reference photons to be set with a known delay to fully distinguish in either non-orthogonal pair set in the experiment.*

In an experimental system it is difficult to create reference beams locally at a receiver from a local oscillator that maintain phase locking with the sender's source and therefore allow for high visibility and stability over extended durations. Therefore the use of unbalanced

asymmetric interferometers which are polarisation routed allows a reference beam to be split from the signal paths and recombined on BS2 and 3 once their phases have been adjusted. For comparison with Figure 4.1 a), the interferometers used in the experiment are shown in Figure 4.1 b). Each BS, as well as the outputs, is labelled using the same notation for reference.

From the raw detection events of each detector, the time-tags are gated to only include events from times when photon pulses are expected. This gating procedure is undertaken to reduce the effects of dark counts and spurious photons from coupled background light. From the gated events, the number and precise detector groupings of three photon time-correlations are discriminated. Table 4.1 shows the three photon time-correlations expected for when Alice sends a certain state. For example, when Alice sends 'π', Bob expects to measure a photon on his 'Not 0', 'Not $^{\pi}/_{2}$', and 'Not $^{3\pi}/_{2}$' detectors. This is because each interferometer is locked off to fully distinguish two of the four possible phase-encodings. Therefore in one interferometer only one detector should trigger events, while in the other both detectors should trigger events for the same input phase.

		Alice sends			
		0	$\pi/2$	π	$3\pi/2$
Bob measures	'Not 0'	✗	✓	✓	✓
	'Not $\pi/2$'	✓	✗	✓	✓
	'Not π'	✓	✓	✗	✓
	'Not $3\pi/2$'	✓	✓	✓	✗

Table 4.1- Unambiguous state discrimination (USD) measurement based on four phase encodings. In a system containing interferometers with perfect visibility and detectors with no dark counts, Bob will never eliminate the state sent by Alice, therefore the diagonal elements in the table are denoted with crosses to indicate they should not trigger events.

Although unambiguous state discrimination allows a receiver to determine a state fully, the overall success rate of a measurement is low, due to the requirement for three time-correlated photon events. Quantum communication experiments generally use $|\alpha|^2 < 1$, so the probability of having three photons in a pulse is at the very most 10%, and this is at the

output of Alice. After transmission losses and insertion losses and non-unity detection efficiency, the likelihood of detecting 3 photons will typically be extremely low.

Unambiguous state elimination

USE in this experiment is a very similar measurement to USD, with the collection of data being the same, Figure 4.1 a) and b), but the post-selection analysis different. USE relies on eliminating states from a known set of phase encodings rather than trying to distinguish one. This means it can rely on one photon event in order to at least eliminate one possible state. If more than one photon event is time-correlated, this allows more than one state to be eliminated at a time.

USE works well with QDS because we are only looking for mismatches in the signature elements, if Alice sends a phase-encoding of 'π', and only eliminates '$\pi/2$', this does not count as a mismatch because the 'π' phase-encoding has not been eliminated. Table 4.2 shows what events the four detectors at Bob (one of the receivers) would be expecting based on the four states that Alice sends.

		Alice sends			
		0	π/2	π	3π/2
Bob measures	'Not 0'	~~?~~	?	?	?
	'Not π/2'	?	~~?~~	?	?
	'Not π'	?	?	~~?~~	?
	'Not 3π/2'	?	?	?	~~?~~

Table 4.2- Unambiguous state elimination (USE) detector clicks. The '?' denotes that a detector may or may not fire in the measurement process. The 'X' marks across the box denotes that a detector firing will count as a mismatch in the comparison stage, in other words it shouldn't fire in a perfect system.

Because USE yields a result with single detection events, unlike USD which requires three simultaneous detected events, the overall success rate of USE is a significantly higher than USD, leading to improved rates in signature transmission.

4.2.2 Definitions of security

The security of QDS was described in the previous Chapter, this section serves as security definitions for this protocol giving the equations for the probabilities an honest rejection, accepting a forgery, and repudiation, P(hon rej), P(for), and P(rep) respectively.

The definitions of security for this scheme are [6]:

- A QDS protocol is secure against forging if the probability of a recipient successfully producing a private key for a message m, which will pass verification by the other recipients, decays exponentially as a function of the quantum signature length L increasing.
- A QDS protocol is secure against repudiation if, for any malicious activity by Alice, the probability of a message failing the verification stage with a recipient once it has already passed the authentication stage with another recipient decays exponentially as a function of the quantum signature length L increasing.

The security analysis is based on the Hoeffding's inequalities, which gives an upper bound on random variable probabilistic scenarios [7]. The full analysis can be found in the supplementary material of [6], which gives a more in-depth theoretical analysis of how these are created. These were also discussed in the previous Chapter. The probabilities for an honest rejection, accepting a forgery, and repudiation are given in Equation 4.1, 2 and 3 respectively.

$$P(\text{hon rej}) \leq \exp\left(-2\left(s_a - P_h\right)^2 L\right) \qquad \text{Equation (4.1)}$$

$$P(\text{for}) \leq \exp\left(-2\left(C_{\min} - s_v\right)^2 L\right) \qquad \text{Equation (4.2)}$$

$$P(\text{rep}) \leq \exp\left(-\frac{\left(s_v - s_a\right)^2}{2} \mathrm{L}\right) \qquad \text{Equation (4.3)}$$

It is assumed that a legitimate user is equally interested in robustness against forging and repudiation. The authentication threshold and verification threshold were chosen to be $s_a = P_h + {}^{g}/_{4}$ and $s_v = P_h + 3\,{}^{g}/_{4}$ respectively, so that the bound on probability could be made equal. This leads to:

$$P(\text{for})=P(\text{rep})=P(\text{hon rej})\leq \exp\left(-\frac{g^2}{8}L\right) \qquad \text{Equation (4.4)}$$

The parameters for the equations can be found in Chapter 3 section 3.4.2.

4.2.3 Experimental setup and methods

The experimental set-up for the newly proposed protocol was superficially similar to that used for the previous experimentally realised protocol presented [3]. There were two main optical differences in the new set-up, one was the use of polarisation beamsplitters (PBS) as beam combiners and splitters, shown in Figure 4.2 a).

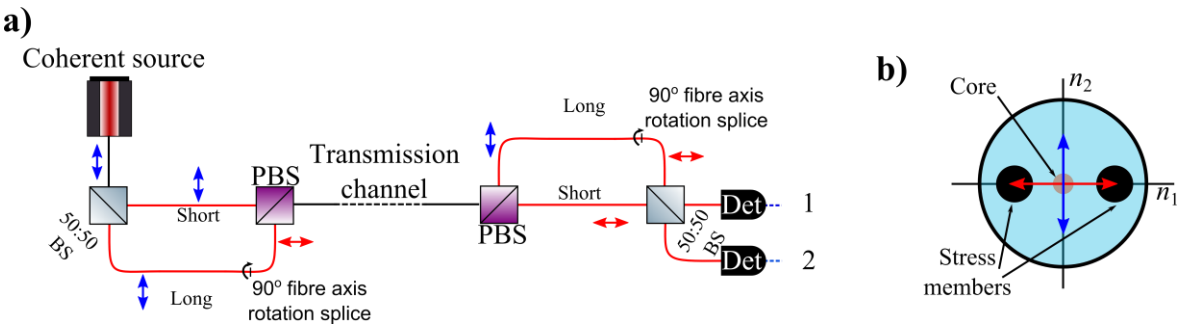


Figure 4.2 – a) Polarisation routing in two unbalanced Mach-Zehnder interferometers. The blue and red double headed arrows indicate the linear polarisations of the photons propagating in the fibre at that point. Photon events are measured on photon detectors (Det). b) shows a cross section of the polarisation-maintaining optical fibre and the supported propagating polarisation with fixed refractive indices n_1 and n_2.

Figure 4.2 b) shows a cross section of the polarisation maintaining optical fibre highlighting the two polarisations which are supported by the structure. Stress-members (generally modified glass) either side of the optical-fibre core, represented by black dots, set up two fixed refractive indices, n_1, and n_2. This allows the fibre to support two fixed polarisations propagations, represented by the blue and red arrows. In the previous experiment the unbalanced asymmetric Mach-Zehnder interferometers were constructed using solely 50:50 BSs, this lead to peaks on a histogram caused by light taking non-interfering paths, later gated out, which meant that half the light intensity was routed to "useless" paths and did not contribute to the usable count rate essentially reducing the $|\alpha|^2$ of the gated count rate. Polarisation routing [8] was introduced in order to increase the gated rate and therefore increase the raw-to-gated count rate ratio. Figure 4.3 shows a

representation of the interfering and non-interfering peaks, in a histogram, with and without polarisation routing. The interferometers were constructed of polarisation-maintaining optical fibre, which allowed two polarisations to propagate down the optical fibre unaltered. By rotating the axis of a fibre 90° relative to another during the fusions splices made during construction the relative polarization of the photons were rotated when passing from one optical fibre to another.

The second difference was the use of two interferometers to perform the USD/USE measurement, where before, only one per user was required. In the new protocol, the measurement interferometers do not require phase modulators, unlike the previous experiment, so each interferometer was locked off to distinguish between phase-encoded coherent states within one of the two pairs of non-orthogonal states. For every non-orthogonal pair used, one more interferometer is required to fully distinguish those states.

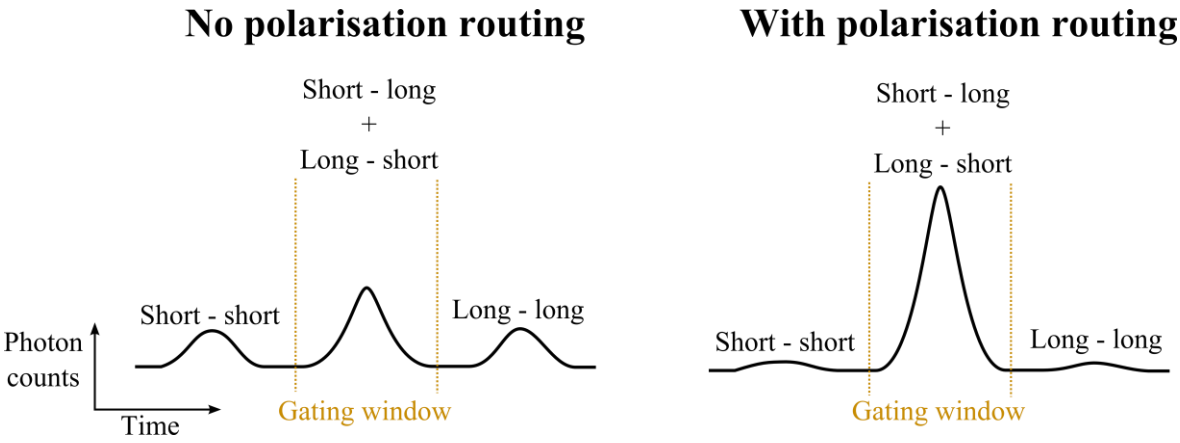


Figure 4.3 – A drawing of a histogram when Alice and Bob are using (right) and not using (left) polarisation routing. Routing using the polarisation routing approach reduces the non-interfering peaks and increases the number of photons present in the interfering peak.

There are several benefits to a receiver that does not require phase modulators (which are active components). Firstly, a receiver no longer requires expensive RF electronics to drive them. Secondly, temperature stabilisation was easier since phase modulators can dissipate electrical energy in the form of heat. Finally the potential for a receiver to be integrated on chip is more viable, as loss-less phase modulation at higher frequencies remains difficult on chip. However some groups have recently made steps to improve transmitter and receiver integrated devices [9]. Silicon Oxynitride was their chosen

material for the receiver as it has chip-to-fibre coupling (≈ 2 dB) and waveguide propagation loss (≈ 0.2 dB/cm) than indium-phostphide (InP), the material the transmitter was fabricated on. The detection of single-photons for the receiver in [10] was off chip leading to a higher loss, but there is research interest into integrated single-photon detection [11].

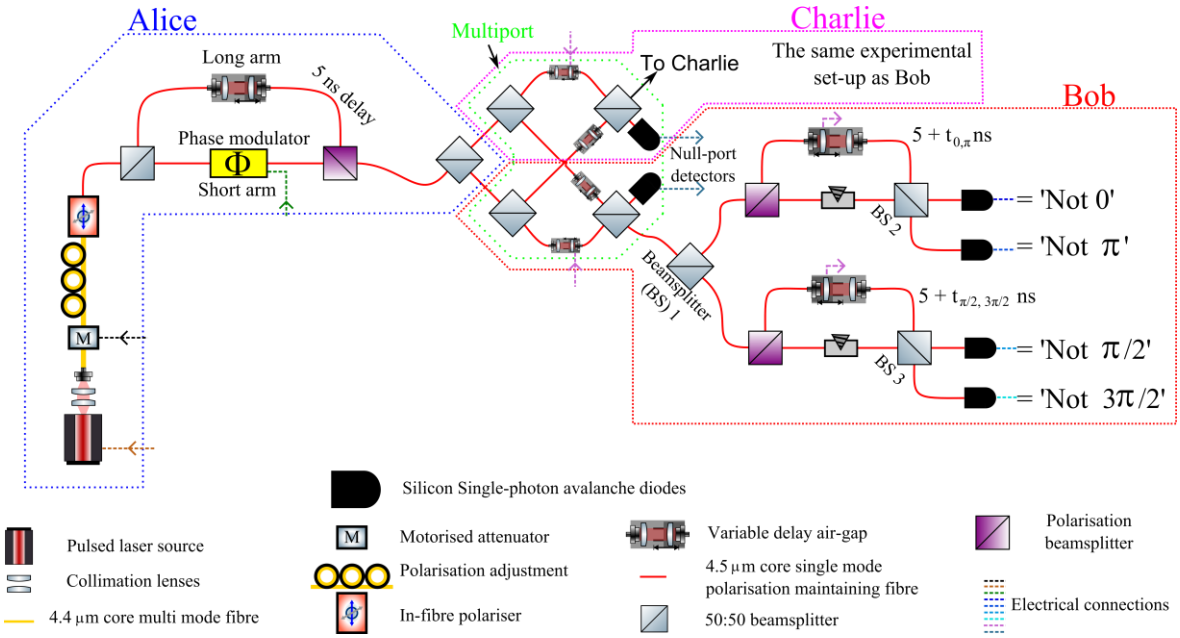


Figure 4.4 – Schematic of the optical setup for the experimental realisation of quantum digital signatures which does not require quantum memory.

The optical system is shown in Figure 4.4 (which contains dashed lines which link to the electronic configuration of the experiment given in Figure 4.6). The source of photons for this experiment was a vertical-cavity surface-emitting laser (VCSEL) diode (Honeywell GaAs HFE4093-342 [12]), which was gain-switched by an Agilent 81134A pulse pattern generator (PPG) [13], through a Maxim drive board (EV 3996 [14]) at 100 MHz. The VCSEL emission had a central wavelength of 849.817 nm with a spectral full-width at half-maximum (FWHM) of 0.045 nm Figure 4.5 a). The temporal response of the VCSEL emission, Figure 4.5 b), shows a FWHM of 0.537 ns, however this is the measured response from the thick-junction Si-SPAD [15] and is detector-limited. The VCSEL was in a free-space package and was highly divergent, and therefore it had to be collimated and coupled into a single-mode fibre. The use of polarisation maintaining (PM) fibre in the construction of this experiment meant the polarisation of light in the single-mode fibre had to be aligned with one of the two axes of propagation of the PM fibre. This was carried out by polarisation adjustments from a "bat ear" type paddle based static polarisation controller

[16]. The optical power generated was attenuated down to a low mean photon level via a computer controlled optical attenuator (OZ-optics [17]), which allowed the $|\alpha|^2$ to be set for an experimental run.

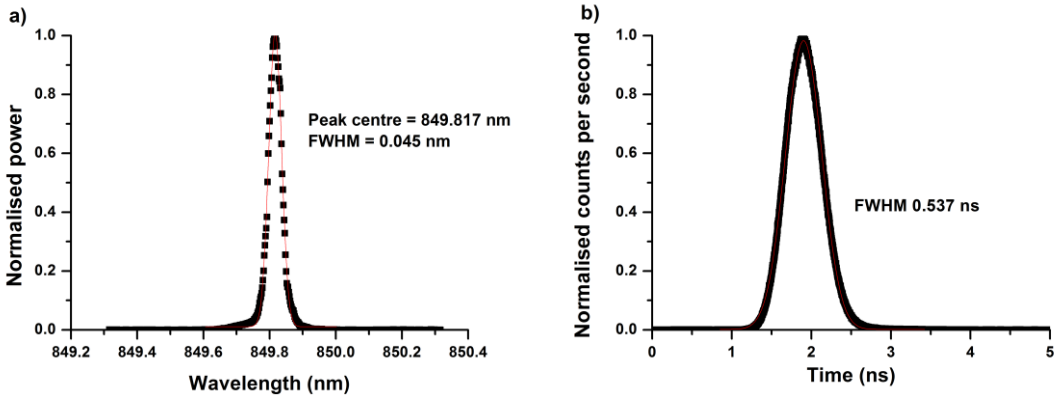


Figure 4.5 – Vertical-cavity-surface-emitting-laser (VCSEL) diode spectrum (a) and temporal response at 100 MHz clocking frequency (b).

Alice split the pulses into two paths at the entrance to her unbalanced asymmetric Mach-Zehnder (UAMZ) interferometer. The short path featured a phase modulator [18], driven at a clock frequency of 100 MHz by a non-return-to-zero (NRZ) signal from an Agilent 81110A PPG [19], which was used to phase-encode the attenuated photon pulses (coherent states) in one of the four phases, 0, $\pi/2$, π, or $3\pi/2$. The long path, which had a 5 ns approximate delay with respect to the short path, was used as a reference, and therefore was left unaltered. The long arm featured a collimated air-gap (Oz Optics [20]), which also allowed optical attenuation, and small adjustments to the timing of the delay. These features allowed the user sufficient control to perform loss balancing and timing calibration during construction, and then remain fixed at a particular optimum value during operation of the system. The two paths were recombined on a PBS which was used as a "lossless" beam combiner. This "lossless" recombination was performed by rotating one of the paths PM fibre axis by 90° during construction, allowing both the signal and reference to exit through one output port with crossed polarisations.

After the recombination of the paths by Alice, she sent her pulse train, composed of pairs of orthogonally polarised pulses separated by 5 ns (a signal pulse at the 100 MHz clock frequency followed by the reference pulse which is delayed by ≈5 ns) to a 50:50 BS which equally split the intensity of Alice's coherent states into two. This is an optical way of

Alice generating her two copies of quantum signatures which can be sent to Bob and Charlie. We define the $|\alpha|^2$ at the outputs of the 50:50 BS and use inline optical attenuation (again based on knife edges) to ensure that the $|\alpha|^2$ was identical in both arms.

Bob and Charlie took their copies of the coherent states from Alice and perform the swap and comparison mechanism using the multiport which was described previously. The multiport was constructed of PM fibre, and features collimated adjustable air-gaps (with adjustable optical attenuation) in each arm allowing a user to easily loss balance for high visibility (approximately 99.7%). The monitoring of the null-ports was carried out using commercially available thick junction PerkinElmer (initially RCA, then EG&G and now Excelitas) SPCM-AQ-12 Geiger-mode Si-SPADs [15], with a mean detection efficiency of 40.5 % (at a wavelength of 850 nm), dark count rate of 320 counts per second, and a FWHM timing jitter of 380 ps [21].

One issue was encountered in the multiport from the implementation of polarisation routing: the two polarisations were sometimes not arriving at the final beamsplitters at the same time, meaning reduced visibility at the multiport and further measurements. One polarisation gave a 99.7% visibility while the other was found to vary. PM fibre has two axes of propagation set up by induced birefringence from stress members. This sets up a fast and slow axis of propagation which have very slightly different refractive indices. Slightly different refractive indices would not be a problem for short distances, but over 5 m this slight difference in propagation speed allowed for a phase shift between the reference and signal polarisations whilst in transit. In practice, external stresses caused by temperature changes and air-conditioning recirculation slightly changed this phase difference.

After Bob confirmed, using the multiport, that he was sent the same quantum signature elements, he performed his state discrimination measurement. Bob had two UAMZ interferometers of their own, one which is locked off to fully distinguish in the 0 or π non-orthogonal pair, and the other for the $\pi/2$ or $3\pi/2$ pair. The USE measurements were recorded using thick junction PerkinElmer SPCM-AQ-12 Geiger-mode Si-SPADs at the output of each interferometer. Triggered events are then recorded by time-tagging hardware (PicoQuant HydraHarp 400 [22]) for USE and USD analysis later.

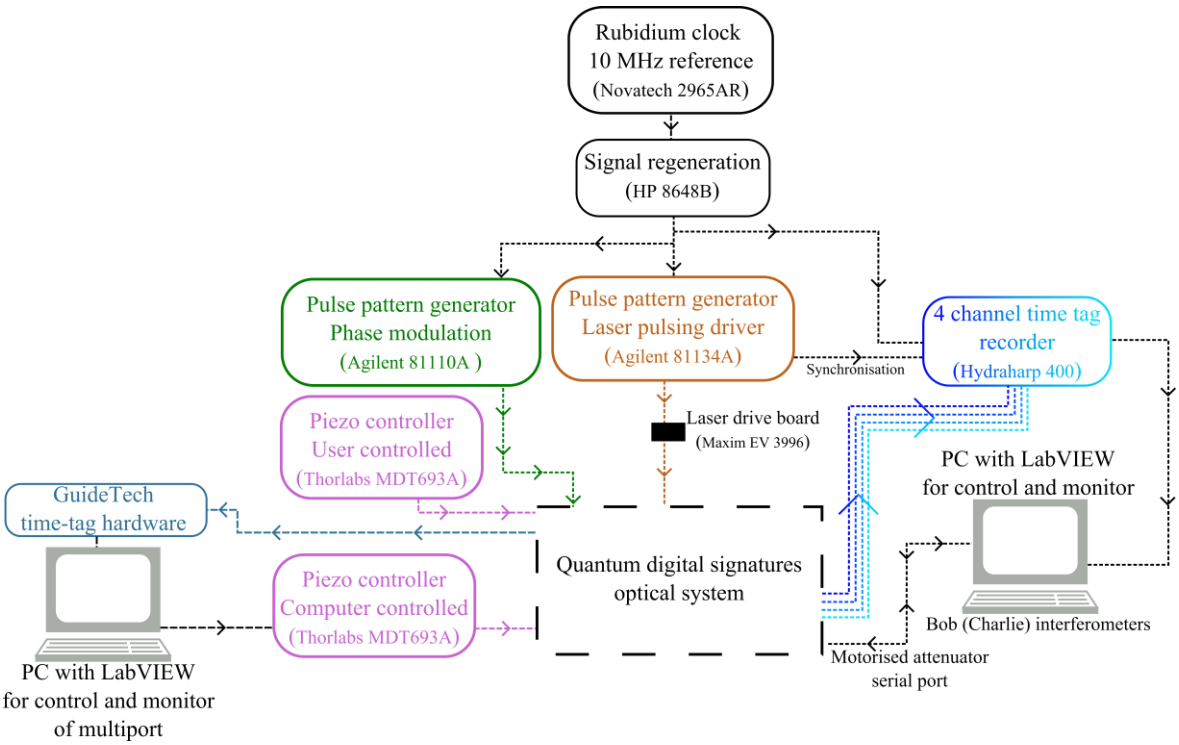


Figure 4.6 – The electrical system that drives the optical system and collects the data.

Figure 4.6 shows the electronic system for the experiment. A 10 MHz rubidium clock (NovaTech [23]) set a common reference synchronisation signal for all the electrical controllers. The output from the rubidium clock signal had too low a voltage to trigger all of the equipment in the system and required amplification from a frequency synthesiser (Hewlett Packard 8648B [24]) which had lower timing jitter than if an amplifier was used. The $LiNbO_3$ phase modulator [18] in Alice's short arm is electrically modulated by the Agilent 81110A PPG [19]. Modulating at a clock rate of 100 MHz, the PPG sent a repeated 4-level NRZ pattern consisting of the four possible phase encodings in the experiment, Figure 4.7. A repeated pattern was used to help the user generate histograms to monitor the visibility of the interferometers. In a real system a pseudo-random generator would be used to select the phase encodings randomly from the N possible phases available in the alphabet. The piezo-bricks in the air-gaps were controlled by voltage sources (ThorLabs MDT630B) with a range of 0 to 100 V.

On Bob's side, the null-port detector was monitored by a program written using National Instruments LabVIEW [25], which recorded time-tag events when the USD/USE measurements were being made. When it was not collecting data, the program maximises the visibility of the multiport output by minimising the count rate measured on the null-

port detectors. It controls the count rate by adjusting the relative optical path length via the voltage applied over a piezo-brick. A separate LabVIEW program also recorded time-tag events on the time-tagging hardware based on instructions from the user.

4.2.4 Methods

This sub-section will describe operation of the system and collection of time tagged photon arrival data. Initial set-up involved adjusting the electrical delay of the phase modulator signal to maximise the visibility of the two interferometers for measurement. The four-level repeater pattern used for the experiment was created using two square pulse trains from the Agilent 81110A PPG are shown in Figure 4.7. The flat top of the square wave (corresponding to the voltage required for a particular phase encoding) was ideally 10 ns wide, when running at 100 MHz, but in practice the "flat" top was only 8 ns due to switching signal rise and fall time. The "flat" top was also not perfectly level, as it exhibited some ringing and overshoot corresponding to ±0.2 % of the flat top value, meaning a 1 or 2 degree possible variation in our set phase-encodings. The 4-level values were also co-dependent on each other as even the '0' voltage was a combination of two '0' voltage signals. The voltage levels between each of the four states was not perfectly equal (therefore the non-orthogonal states were not 100% non-orthogonal), optically, the visibility for one non-orthogonal pair will be better than the other. The delay of the phase modulator driving signal relative to the laser was adjusted so that the optical pulses arrived at the phase modulator at times that gave optimum visibility. The standard set-up procedure involved optimising the visibility for both interferometers.

The LabVIEW program which monitored the multiport via the null-port detector was set-up first, as USE measurements could not happen before the multiport was optimised. As mentioned in section 4.2.4 the multiport had some long-term visibility stability issues because of the fibre length in the interferometer arms and additional path length differences caused by the polarisation routing effects. Initially the path length changes due to temperature and induced stresses were operating on timescales too short to allow for sufficient control for reliable operation, so patience was required until the system reached a level of mechanical and thermal equilibrium where the LabVIEW program was able to compensate for any further drift.

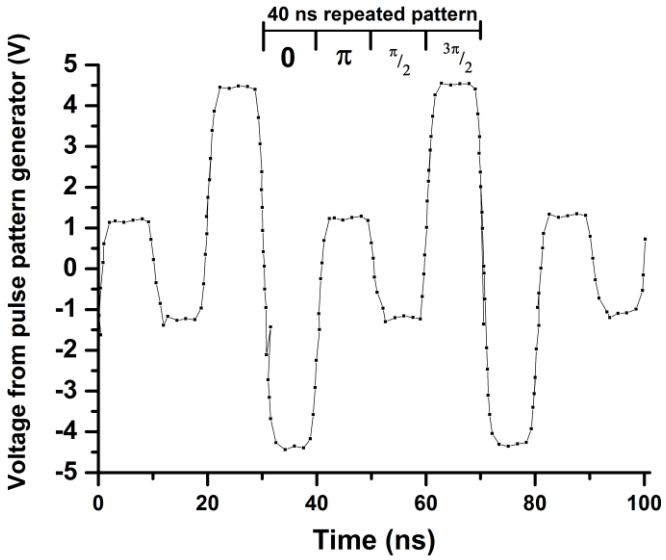


Figure 4.7 – Oscilloscope output measured from the Agilent 81110A pulse pattern generator [19] *which is driving the phase modulator.*

Another LabVIEW program monitored Bob's interferometers and recorded data when the complete system was stable. It generated four histograms, one for each detector which gave the user visual feedback on the interference. The user used this information to adjust the voltage of the piezo-bricks in each interferometer, adjusting for small changes in path length to improve the visibility. When the visibility reached a suitable level, time-tags were recorded and a new measurement was set up.

For processing the data, a program written in MATLAB [26] took the raw recorded time-tags, and placed a 4 ns duration gate was centred on each of the four histogram peaks (a peak for each phase-encoding). Analysis of the raw, gated, and coincidence counting was performed using the process presented in the proceeding section.

4.2.5 Experimental results and analysis

The presentation of the experimental results here will follow the logical method of processing from the raw time-tagged photons, to manipulation of data to generate state discrimination matrices, and finally the analysis of those matrices into meaningful values such as the signature half-bit length L that allows the digital signature protocol to be secure.

The experiment was carried out over a range of $|\alpha|^2$ per pulse between 1 and 11.5. This range was originally chosen to increase the overall USD success rate, the USE analysis was performed much later on the same results.

As mentioned previously in the description of the experimental set-up, polarisation routing was used in Alice and Bob's (Charlie's) interferometers to increase the percentage of signal gated count rates. It was found that the percentage of gated counts recorded per second was on average 88% of the raw count rate for the signal count rate, i.e. the photons counted at the receiver interferometers, because of the use of polarisation routing. This is significant improvement over the previous experiment where the gated count rate percentage was <40%, because of the non-interfering peaks and background noise [3]. Figure 4.8 shows the total raw and gated count rates for the experiment in black and red respectively for Bob.

The other data shown in Figure 4.8 is the null-port raw and gated count rates, in blue and pink respectively. The general trend for the total count rate (raw and gated) was to increase with $|\alpha|^2$, as would be expected. The total gated count rate for the multiport null-port detector is 73.6% of the total raw count rate on average, showing that most of the triggered events are coming from the gated region. In theory, if Alice is sending Bob and Charlie the same quantum signature elements, and there is perfect loss balancing in the multiport, there should be no photons reaching the null-port detector, apart from background light and dark counts. This should lead to a gated percentage of around 20%, composed of 4 × 2 ns gates (= 8 ns) of the entire timing histogram of 40ns duration, because the events are spread randomly throughout the histogram. Because the gated count rate percentage is found to be higher than 20% this suggests a non-unity visibility. This makes sense, because of the polarisation routing issue in the multiport where the two orthogonal polarisations propagating down the polarisation-maintaining fibre were found to have varying visibilities.

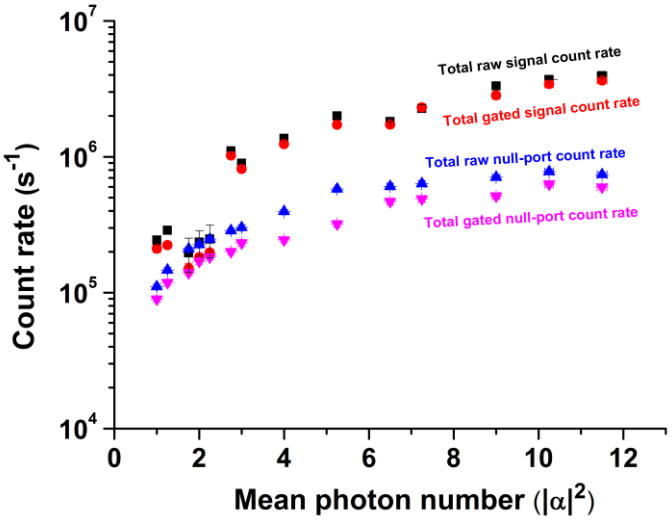


Figure 4.8 – Total raw and gated count rates for the signal-ports and null port. The signal-ports refer to the summed measured events from Bob's four detectors in his USD/USE measurement, and the null-port refers to the one detector that is attached to the multiport non-demolition measurement.

This system used USE/USD to remove the requirement for a QM at each receiver. We can generate the USE/USD success rates, for correct and incorrect cases from the gated count records. For USE, success is described as the case when Bob (Charlie) has eliminated 1 or more possible phase-encodings, but has not erroneously eliminated the phase-encoding actually sent by Alice. An incorrect success would be when Bob (Charlie) has incorrectly eliminated the phase-encoding actually sent by Alice. For USD, success is when Bob (Charlie) manages to fully distinguish the phase-encoding actually sent by Alice from the three photon time-correlations (and one correlated non-event). A failure would be when Bob (Charlie) fully distinguishes a phase-encoding which was not that sent by Alice.

Figure 4.9 shows the USE a) and USD (b) total rates (black), along with correct (red) and incorrect (blue) rates. One major difference between USE and USD is the total rate (correct + incorrect). It can be seen that even at the top of the $|\alpha|^2$ range used, the total USD success rate does not even reach the lowest USE success rate.

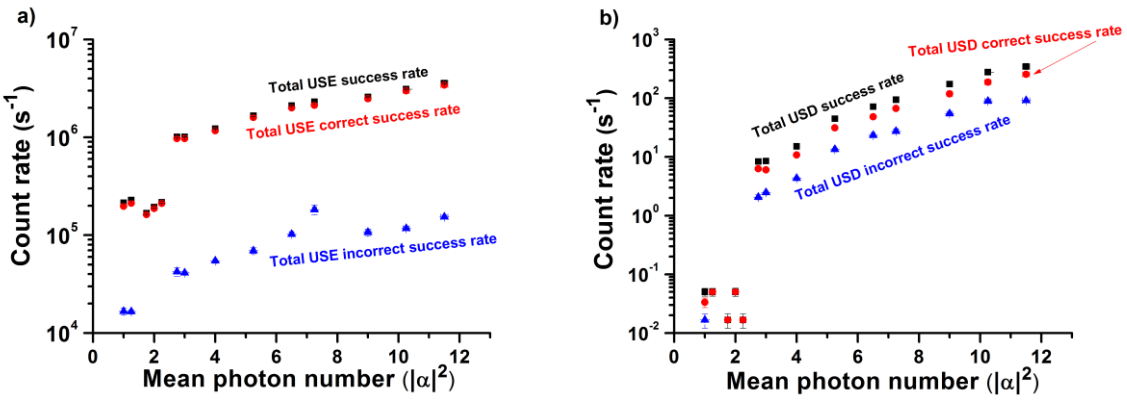


Figure 4.9 – Total success rates for unambiguous state elimination (USE) a) and discrimination (USD) measurements b).

From Figure 4.9 a) it can be seen that the correct rate of USE far outweighs the incorrect rate, with the average correct USE rate being 95.3%. Given that the total USE rate is the gated count rate (because every detected photon can eliminate a state), and the signal gated rate is 88% of the raw rate, the overall average correct USE rate was 83.8% of the total raw signal count rate. The incorrectly eliminated rate is substantially lower, meaning incorrect eliminations are less frequent. The number could be reduced further if the purity of the transmitted phase-encodings and the visibility of the interferometers were improved.

Figure 4.9 b) shows the total USD success rate, along with the total correct and incorrect rates. There were two big differences between the data seen in Figure 4.9 a) and b). First is the scale of the *y*-axis, both figures were plotted using the same raw data, but there was a massive difference in success count rate for USE and USD. The probability that three photons are in a pulse that made it to the detectors was low due to the high loss of the multiport (>8.5 dB) and the interferometers (>4 dB), and being correctly routed, then detected (with each detector having 40.5 % detection efficiency). The second difference was the percentage of USD success rate which was found to be, on average, 78.73%. This average was slightly skewed higher, because for the $|\alpha|^2$ 1.25, 1.75, 2, and 2.25, there were only ever correct states distinguished. This meant that the portion of incorrectly distinguished states was actually around a quarter of what is recorded. The total USD success rate was found to range from 2.14×10^{-5} to 3.57×10^{-3} % of the raw signal count rate as the $|\alpha|^2$ increased, substantially lower than the USE rate.

USD was originally considered as a method to perform the state discrimination by Bob/Charlie, because it can fully distinguish which phase-encoding has been sent by Alice and was thought to have a low probability of eliminating the state actually sent by Alice. Initial tests which were performed using a $|\alpha|^2 = 1$ showed that the USD success rate was insufficient to be practically useful, and therefore to improve this rate higher $|\alpha|^2$ was required. In QDS we only need to test for mismatches between signature elements and therefore USE would have been enough to eliminate phase-encodings and perform a mismatch test.

Knowing the USE success rate is useful for gauging how well a system is performing in terms of count rate. This information is a fundamental element of QDS, but this information alone cannot tell us the important system properties, such as the signature half-bit length *L*. The rest of the section follows the analysis process taken from the supplementary material of [15].

$$\begin{pmatrix} 2105 & 15627 & 21495 & 6022 \\ 9859 & 1405 & 8849 & 22571 \\ 33588 & 6364 & 1344 & 11948 \\ 14616 & 20824 & 15590 & 1149 \end{pmatrix}$$

Equation 4.5

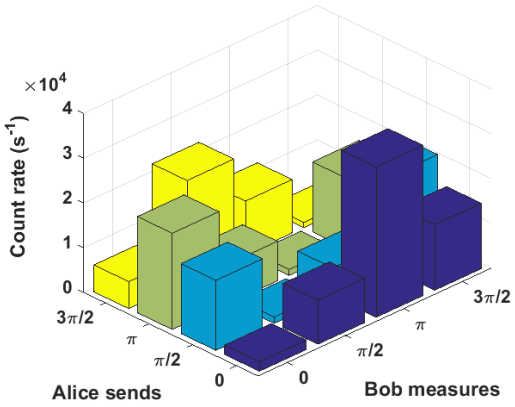


Figure 4.10 - Count matrix visual representation based on the matrix in Equation 4.5.

The USE measurements can be placed into a photon count matrix, as shown numerically in Equation 4.5 and graphically in Figure 4.10, where the columns correspond to what Alice sent (0, $\pi/2$, π, and $3\pi/2$), and the rows, Bob's (Charlie's) measurement detector (not 0, not $\pi/2$, not π, and not $3\pi/2$). Each element represents a number of detector events at that particular detector for the specified transmitted phase. The following example for this

analysis used a $|\alpha|^2$ of 2, as represents the count matrix with minimum error due to Poisson statistics.

The count matrix has some features which are worthy of note. Firstly, there is a minimum down the diagonal, where Bob eliminates the state actually sent by Alice; any values recorded here are the incorrect USE successes. Maxima occur in each column where Bob (Charlie) are eliminating the state which is π out of phase with the one sent by Alice. The other two values in each column are referred to as "50%" peaks, where Bob (Charlie) are eliminating states orthogonal to the one sent by Alice. This means that they are equally likely to reach either detector and will give equal peaks on each histogram that contain 50% of the counts in the maximum. If Bob's (Charlie's) interferometer has 100% visibility and the states being sent by Alice are perfect (exactly the desired phase) and pure (non-variant within a particular phase), then these 50% peaks will be equal. In all experimental cases, these peaks are not equal, this is because the 50% peaks where not taken into account when looking at the overall system visibility of the interferometers, only the maximum and minimum were considered. This coupled with the fact that there were slight differences in the set phases due to the uncertainty in the electrical modulation led to discrepancies in the phase-encodings actually set.

The count matrix Equation 4.5 was divided by the clock-rate (100 MHz in this case) of the experiment to give Bob's (Charlie's) probability of detecting an event based what Alice sends, shown in Equation 4.6. This is called the Cost matrix [3], [5], [6]

$$C = \begin{pmatrix} 2.105 & 15.627 & 21.495 & 6.022 \\ 9.859 & 1.405 & 8.849 & 22.571 \\ 33.588 & 6.364 & 1.344 & 11.948 \\ 14.616 & 20.824 & 15.590 & 1.149 \end{pmatrix} \times 10^{-5} \qquad \text{Equation 4.6}$$

Equation 4.7 is the Cost matrix for an honest scenario (C^{h}), the probability that Bob eliminate the phase-encoding that was actually sent by Alice. Even if Bob is being honest, there will still be a mismatch due to experimental error. The probability of an honest mismatch was denoted by P_{h}, and is the average of the diagonal elements in Equation 4.7, giving 1.50×10^{-5}.

$$C^h = \begin{pmatrix} 2.105 & 1.405 & 1.344 & 1.149 \\ 2.105 & 1.405 & 1.344 & 1.149 \\ 2.105 & 1.405 & 1.344 & 1.149 \\ 2.105 & 1.405 & 1.344 & 1.149 \end{pmatrix} \times 10^{-5} \qquad \text{Equation 4.7}$$

Equation 4.8, *C*', is a variation of the original Cost matrix (Equation 4.6), and is the difference offset by the honest Cost matrix in Equation 4.7, essentially $C' = C - C^{h}$. This generates a matrix which shows the difference in off-diagonal values and the diagonal values for each column, these values represent the advantage that Bob had over a forger in identifying a forged signature element. If all the values were '0' a forger could guess any value and be likely to get it accepted. The guaranteed advantage (*guad*), is the minimum advantage Bob had over a forger, i.e. the smallest non-zero element in Equation 4.8, in this case the value was 4.87×10^{-5}. Since the lowest element was the worst-case scenario, we applied this value to all non-diagonal elements, shown as Equation 4.9.

$$C' = \begin{pmatrix} 0 & 14.2 & 20.2 & 4.87 \\ 7.75 & 0 & 7.5 & 21.4 \\ 31.5 & 4.96 & 0 & 10.8 \\ 12.5 & 19.4 & 14.2 & 0 \end{pmatrix} \times 10^{-5} \qquad \text{Equation (4.8)}$$

$$C^{l} = \begin{pmatrix} 0 & 4.87 & 4.87 & 4.87 \\ 4.87 & 0 & 4.87 & 4.87 \\ 4.87 & 4.87 & 0 & 4.87 \\ 4.87 & 4.87 & 4.87 & 0 \end{pmatrix} \times 10^{-5} \qquad \text{Equation (4.9)}$$

$$g = P_{\min} \times guad \qquad \text{Equation (4.10)}$$

The *guad* tells us Bob's minimum advantage over a forger, in measuring a state but the forger themselves can have some advantage if the $|\alpha|^2$ was high enough for them to split off photons and performed their own measurement, essentially improving their chance of sending the correct forged state. If a malevolent party was able to eliminate one of the four possible phase-encodings they would have improved their chances of getting a forged signature element accepted. The minimum error measurement that a malevolent party can perform is known as $P_{\min}$ taken from [27] is plotted for our range of $|\alpha|^2$ in Figure 4.11 a) from Equation 4.11. $P_{\min}$ was a correction factor for our guaranteed advantage, the returned value is known as the *gap g* (Equation 4.10) which is used to calculate the signature half-bit length *L*.

$$\lambda_1 = 2\exp(-|\alpha|^2)\left(\cos(|\alpha|^2)+\cosh((|\alpha|^2)\right)$$

$$\lambda_2 = 2\exp(-|\alpha|^2)\left(\sin(|\alpha|^2)+\sinh((|\alpha|^2)\right)$$

$$\lambda_3 = 2\exp(-|\alpha|^2)\left(\cosh(|\alpha|^2)-\cos((|\alpha|^2)\right)$$

$$\lambda_4 = 2\exp(-|\alpha|^2)\left(\sinh(|\alpha|^2)-\sin((|\alpha|^2)\right)$$

$$P_{min}=1-\frac{1}{16}\left|\sum_i \sqrt{\lambda_i}\right|^2 \qquad \text{Equation (4.11)}$$

Figure 4.11 b), c) and d) show the guaranteed advantage (*guad*), the *gap* and P_h, respectively for the range of $|\alpha|^2$ in the experiment. Each plot can be seen to follow a general trend, with some experimental outliers. In plots b) and c) $|\alpha|^2$s 6.25 and 7.25 have been omitted because of their unphysical value, during analysis it was found out that one of the minimum diagonal elements in each was greater than an off-diagonal element, resulting in a negative values. This can be seen manifesting in d), where the 7.25 value is very out of the data trend.

Figure 4.11 b) shows that the general trend of the *guad* was to increase with $|\alpha|^2$, because this is a probability relating the USE detection rate, as the $|\alpha|^2$ increases so does the count rate, and therefore the probability increases. Uncertainties in the guaranteed advantage depend on the variation in the overall visibility, so larger uncertainties correspond to unstable measurement runs, for instance points 9.5 and 10.25. As mentioned previously, $|\alpha|^2$ of 6.25 and 7.25 have been omitted as they gave unphysical (negative) values, meaning that the at least one diagonal element has a larger value than an off-diagonal element.

Figure 4.11 c) shows a general decrease in *gap* with increasing $|\alpha|^2$, this is due to the correction factor from P_{min} which decreases exponentially with $|\alpha|^2$. The errors in the y-axis are propagated forward in Equation (4.10). Following on from the *guad*, $|\alpha|^2$ 6.25 and 7.25 were omitted due to unphysical (negative) values, implying that the diagonal elements were actually larger than off-diagonal elements, i.e. the visibility had drifted so much between step-up and measurement that the interferometer was no longer optimised for distinguishing the correct values.

In Figure 4.11 d), P_h, the probability of an honest rejection, shows a general increase with $|\alpha|^2$ because it a probability related to the USE success rate (really incorrect rate), as the $|\alpha|^2$ increases so does the count rate. An outlier in P_h is the $|\alpha|^2$ 7.25 value and as mentioned previously this is because it was found that a diagonal element was larger than an off-diagonal element, this would results in a bad overall visibility for the QDS system. Uncertainties in the y-axis were found to be because of variation in the visibility, as P_h is the smallest value in the Cost matrix, changes in visibility will create large variations in the values seen.

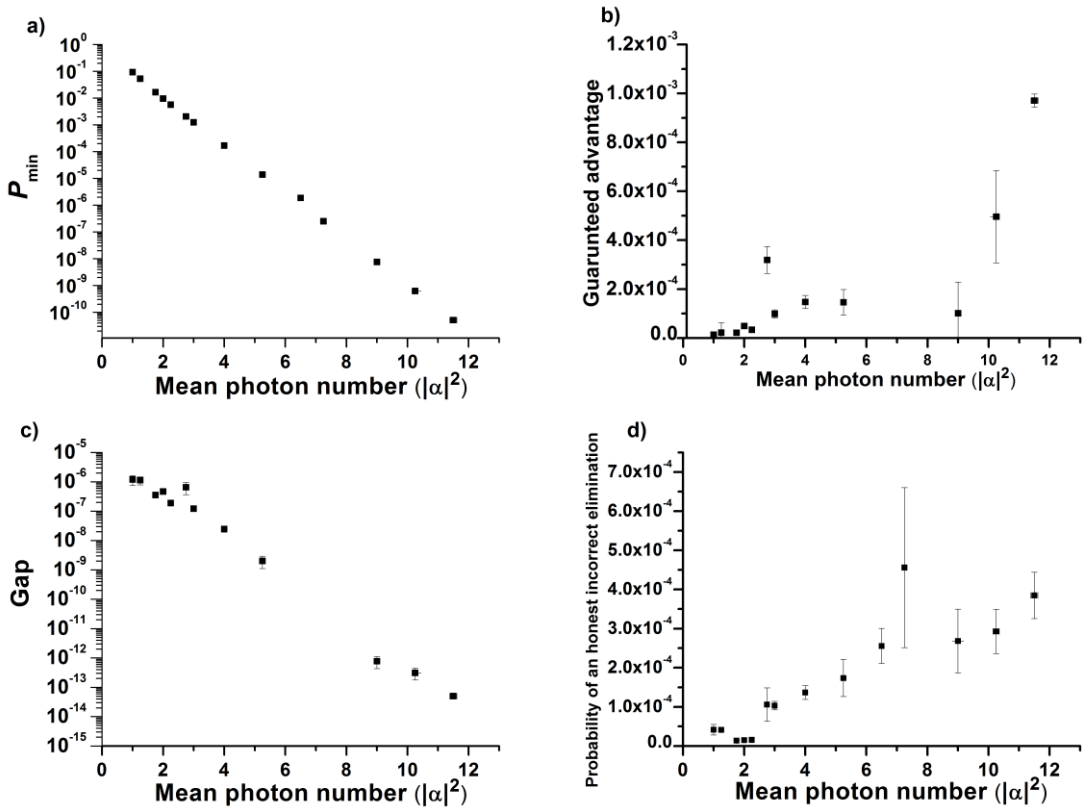


*Figure 4.11 – a) the minimum error correction factor (P_{min}) calculated using Equation 4.11, b) the guaranteed advantage a receiver has over an malevolent party (*guad*), c) the corrected* gap *between the highest diagonal element and lowest off-diagonal element (*gap*), and d) the probability that a receiver will honestly reject the correct phase-encoding (P_h).*

At this point all the parameters needed to calculate the signature half-bit length, *L*, have been calculated and we can proceed to determine a value for that parameter. In the security analysis it was said that the probability for forging, repudiation and an honest rejection should be made equal, as expressed in Equation (4.12). In the supplementary material of Collins *et al.* [15], the probability that a malevolent party is able to forge a half-bit was given to be 0.01%. Since this is a somewhat arbitrary value, this thesis presents values of 0.01%, 0.1%, 1% and 10% as well to show changes in *L* with different levels of security.

$$P(\text{for})=P(\text{rep})=P(\text{hon rej})\leq \exp\left(-\frac{g^2}{8}L\right) \qquad \text{Equation (4.12)}$$

Figure 4.12 shows the resulting plot of half-bit length for each $|\alpha|^2$ at the different percentage of forging values. It can be seen that the lengths are staggeringly large and

only increase with $|\alpha|^2$, due to the *gap* decreasing (Figure 4.11 c)). The length expression depends on $1/g^2$ and the *gap* is a decreasing number with increasing $|\alpha|^2$ as was seen from Figure 4.11 c). Although the half-bit length does decrease when the probability of forging is increased, it does not make a significant difference on the whole, as for every step shown in Figure 4.12 (0.01→0.1→…), the half-bit length only decreases by around 50%.

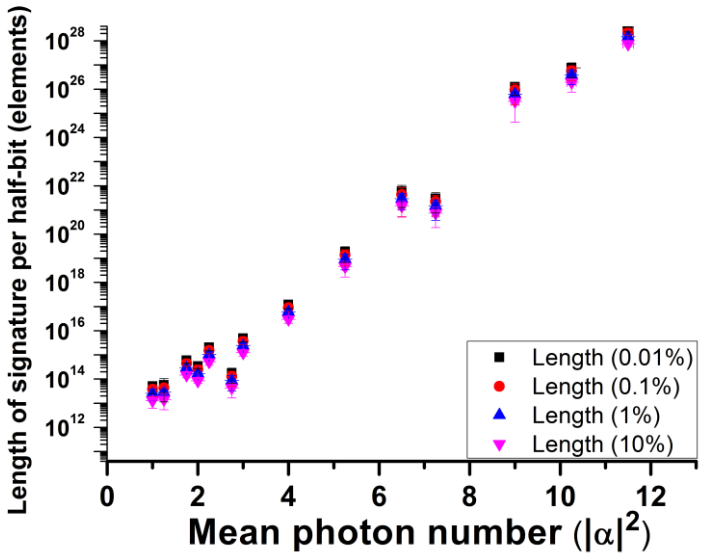


Figure 4.12 – Signature half-bit length L for different security levels.

Although the length is an important parameter, arguably a more important one is how long is it takes someone to send the signature half-bit. Note that the smallest length was calculated for a $|\alpha|^2$ of 1, found to be 5.13×10^{13} for a probability of forging of 0.01%.

The time taken for Alice to send one signature half-bit length (for each of the different security levels) is shown in Figure 4.13. The values for the time taken are calculated by dividing the signature half-bit length by the clock frequency used in the experiment, in this case 100×10^6 Hz. This method is used because in an experiment, Alice, Bob and Charlie omit signature elements when they did not receive any photons. If Bob and Charlie were required to receive the whole signature in order it would take a much longer time. The time given is in seconds, and the time taken increases with the greater $|\alpha|^2$, which is counter-intuitive, because a higher success rate should mean less time. However due to the security analysis, the more photons available, the more advantage a malevolent party has, therefore the signature length must be longer. To put the values in perspective for the shortest half-bit length, 5.13×10^{13}, for a $|\alpha|^2$ of 1 at a 0.01% probability of forging, the

time taken is 5.13×10^5 seconds, which is approximately 6 days. Quite a long time considering Alice needs to send two sequences of this length (one for her future bit 0 message, and one for her future bit 1 message).

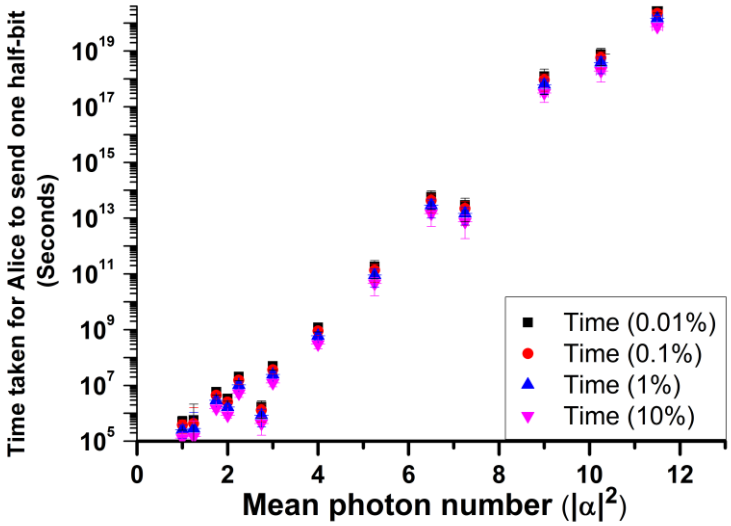


Figure 4.13 – Time taken in seconds for Alice to send one signature half-bit length to Bob (Charlie).

4.3 Discussion and conclusion

Now that the data from this QDS experiment has been fully analysed following [6], it would be a good idea to compare our best measurement with that of the previous QDS experiment. One point to note, that calculation of probability of forging, repudiation and honest rejection was different in each paper, therefore the length calculation was different. Equation (4.12) shows the expression for this experiment while Equation (4.13) shows the expression used for the previous experiment. The difference in the equations is dependent on the security assumptions of the channel.

$$P(\text{for})=P(\text{rep})=P(\text{hon rej})\leq 2\exp\left(-\frac{2}{9}g^2L\right) \qquad \text{Equation (4.13) [28]}$$

In the main paper and the supplementary material of the previous QDS experimental realisation [3] the *gap* used as their example was 8.03×10^{-4}, giving a signature half-bit length of 6.91×10^7. The previous experimental system also ran at 100 MHz clock-rate and therefore Alice took 0.691 seconds to send one signature half-bit. While in this

experiment it was shown that the shortest length would be 5.13×10^{13}, which took 5.13×10^{5} seconds for Alice to send.

Although these are significantly different, there are several points which should be noted. Firstly, this new experiment uses a detection method realised without QM technology, while the previous implemented a detection method which simulated a QM using optical fibre, therefore although this new experiment may seem to take longer, the previous experiment could not be realised in a practical manner with current QM technology [1].

Secondly, the $|\alpha|^2$ ranges for each experiment was different. In the previous experiment it was 0.04 to 0.27, the experiment presented in this Chapter ranged from 1 to 11.5. Intuitively, it may appear that the newly presented system should perform better, as a higher mean photon number suggests a higher probability of detecting photons, but this neglects the security analysis. One of the key elements in calculating the signature half-bit length L is the *gap*, which is calculated using Equation 4.10, and incorporates the correction factor $P_{\min}$. At a $|\alpha|^2$ of 1, $P_{\min}$=0.0924 and drops approximately by a power of 10 every integer of 1 in the $|\alpha|^2$, Figure 4.11 a). This means that any benefit of increasing the USE count rate is lost immediately, and actually reducing the $|\alpha|^2$ to less than one is more beneficial. In the $|\alpha|^2$ range used in the previous experiment, $P_{\min}$ goes from 0.6357-0.4035, much higher than the range used in the new Chapter presented here. Although the results presented in this Chapter are calculated using the USE success rates, the experimental originally used USD hence the values of $|\alpha|^2$ are higher in this Chapter to increase the success rate of three photon correlations. USE analysis can simply be performed using the same data for USD. USE was adopted so much later that the multiport and other components had already been decommissioned, therefore lower $|\alpha|^2$ could not be measured.

In conclusion, this Chapter has shown an experimental realisation of a QDS protocol presented in [14]. The protocol was conceived in order to improve the realisable applications of QDS by performing a state distinguishing measurement which stores the measured phase-encoding information classically, rather than requiring a QM in order to store the optical coherent state. As mentioned earlier and in the literature review, QM technology today is currently not in a state where it could be used in this application and therefore ways to avoid QM are sought. Without the requirement for QM, QDS become a more realisable quantum technology. Another basic improvement was the use of

polarisation routing, which increased the percentage of gated counts from <40% to 88% of the total counts.

Using the security analysis from the supplementary material in [6], parameters were generated from the data cost matrices to calculate the signature half-bit length. For a 0.01% probability of forging, the shortest signature half-bit length was found to be 5.13×10^{13} for a $|\alpha|^2$ of 1. This gave a time for Alice to send of 5.13×10^5 seconds, which is approximately 5.94 days. The signature half-bit length, and time taken for Alice to send only increases with $|\alpha|^2$. This is due to the decrease in error a malevolent party will have in creating a forgery.

4.4 Improvements and future work

As mentioned in discussion and conclusion the performance of this new experiment when compared to the previous one was actually longer in terms of signature half-bit length, and hence the time required for Alice to send one half-bit. One method to improve this would be using lower $|\alpha|^2$ range in the experimental testing. As mentioned the $P_{\min}$ correction factor used to calculate the *gap* is a decreasing function with increasing $|\alpha|^2$. Therefore to improve the *gap*, a lower $|\alpha|^2$ would be of more benefit than trying to increase the *gap* with count rates. This will be discussed further in the following Chapter also on experimental QDS.

A second way to improve upon the QDS experiment would be to find a more efficient way to perform a swap and comparison test. The multiport was the first step in realising the original QDS protocol by Gottesman and Chuang in [29], by removing the need for QM technology. But the multiport introduces complexity and instability because it is two intertwined interferometers. The polarisation routing used in this experiment was also affected by the multiport because of its construction with PM-fibre. The two birefringent axes have different refractive indices, which can also change slightly depending on stresses on the fibre. This meant that temperature changes in the room cause the two polarisations to travel at different velocities. Over the 5 m distance this mean that phase shifts could be induced creating a lower visibility multiport. If the distance between the multiport BSs would be increased, the effect would be made worse, therefore the multiport limits the range at which QDS can be carried out. A new swap and comparison mechanism which is performed classically may be a way to increase the distance of QDS and increase the half-bit rate.

A third way to improve the system may be to use a narrow spectral linewidth laser. Since coherence length is inversely related to spectral linewidth [30], a narrower linewidth would mean the coherence length would increase. Distributed feedback (DFB) and distributed Bragg reflector (DBR) laser diodes are known to have narrow linewidths of kHz region at wavelengths around 1550 nm [31] while the VCSEL diode used in this experiment had a linewidth of 18.7 GHz at 850 nm.

Changing to a longer wavelength (say at the low loss telecommunications window around 1550 nm) would also increase stability as changes in path length correspond to relatively smaller changes in visibility due to the longer wavelength. A $\pi/2$ change in path length at 850 nm wavelength corresponds to approximately 212.5 nm, while for 1550 nm this corresponds to 387.5 nm, almost double the value. Therefore it can be seen that a system would be relatively more stable at 1550 nm. This could be combined with the transition to narrower linewidth lasers outlined above to further enhance the stability.

Finally, increasing the clock-rate of the system could help shorten the time taken for Alice to send a signature half-bit. This system now is clocked at 100 MHz, where as many new QKD systems operate in the GHz regime, if the maximum clock rate for the labs pulse pattern generator was to be used 3.3 GHz, an approximation of a power of 10 could be taken off the time taken.

4.5 Acknowledgements

Dr Vedran Dunjko, Dr Petros Wallden, and Professor Erika Andersson established the protocol which was previously published in [5]. The multiport used in the experiment was previously constructed by Dr Robert J. Collins and Dr Patrick J. Clarke working under the supervision of Prof Gerald Buller, although the author conducted optimisation of the operating parameters in this application.

4.6 Bibliography

[1] K. F. Reim, *et al.*, "Towards high-speed optical quantum memories," *Nat. Photonics*, vol. 4, no. 4, pp. 218–221, 2010.

[2] A. I. Lvovsky, *et al.*, "Optical quantum memory," *Nat. Photonics*, vol. 3, no. 12, pp. 706–714, Dec. 2009.

[3] P. J. Clarke, *et al.*, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.," *Nat. Commun.*, vol. 3, p. 1174, Jan. 2012.

[4] E. Andersson, *et al.*, "Experimentally realizable quantum comparison of coherent states and its applications," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 74, no. 2, pp. 1–11, 2006.

[5] V. Dunjko, *et al.*, "Quantum Digital Signatures without Quantum Memory," *Phys. Rev. Lett.*, vol. 112, no. 4, p. 040502, Jan. 2014.

[6] R. J. Collins, *et al.*, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[7] V. Bentkus, "On Hoeffding's inequalities," *Ann. Probab.*, vol. 32, no. 2, pp. 1650–1673, 2004.

[8] C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km.," *Opt. Lett.*, vol. 20, no. 16, p. 1695, Aug. 1995.

[9] A. Liu, *et al.*, "A high-speed silicon optical modulator based on a metal – oxide – semiconductor capacitor," *Nature*, vol. 427, no. February, pp. 615–619, 2004.

[10] P. Sibson, *et al.*, "Chip-based quantum key distribution," pp. 1–5, 2015.

[11] B. Calkins, *et al.*, "High quantum-efficiency photon-number-resolving detector for photonic on-chip information processing.," *Opt. Express*, vol. 21, no. 19, pp. 22657–70, Sep. 2013.

[12] J. Tatum and J. Guenter, "Modulating VCSELs," *Honeywell Int.*, pp. 1–19, 1998.

[13] Keysight Technologies, "81133A and 81134A 3.35 GHz Pulse Pattern Generators," pp. 1–10, 2015.

[14] Maxim Integrated Products, "Maxim: MAX3996 Evaluation Kit," pp. 1–7, 2002.

[15] Perkin-Elmer Optoelectronics, "SPCM-AQRH Single Photon Counting Module," *Perkin-Elmer Optoelectron. Datasheet*, pp. 1–10, 2002.

[16] Thorlabs, "Manual Fiber Polarization Controllers User Guide," *Rev E*, 2014.

[17] Oz Optics ltd, "DD-100 Motor driven attenuators," pp. 1–23, 2000.

[18] Photline, "NIR-MPX800 series phase modulator," 2010.

[19] Agilent Technologies, “Agilent 81110A 165/330 MHz Agilent 81104A 80 MHz Pulse/Pattern Generators,” 2000.

[20] Oz Optics ltd, “Optical delay lines,” pp. 1–7, 2009.

[21] P. J. Clarke, *et al.*, “Analysis of detector performance in a gigahertz clock rate quantum key distribution system,” *New J. Phys.*, vol. 13, p. 23, 2011.

[22] M. Wahl, *Modern TCSPC Electronics: Principles and Acquisition Modes*. Berlin: Springer International Publishing Switzerland, 2014.

[23] Novatech Instruments Inc, “Models 2960AR and 2965AR Disciplined Rubidium Frequency Standards,” pp. 1–8, 2004.

[24] Agilent Technologies, “Agilent 8648A / B / C / D Signal Generators Spectral purity Internal reference oscillator,” no. March 2007, 2012.

[25] National Instruments, “LabVIEW 8.5.”

[26] Mathworks, “MATLAB 2014b (8.4.0.118713).” The MathWorks Inc., Natick, Massachusetts, 2014.

[27] P. Wallden, *et al.*, “Minimum-cost quantum measurements for quantum information,” pp. 1–19, Dec. 2013.

[28] P. J. Clarke, *et al.*, “Supplementary material: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light,” *Nat. Commun.*, vol. 3, p. 1174, Nov. 2012.

[29] D. Gottesman and I. Chuang, “Quantum Digital Signatures,” *arXiv.org*, no. 0105032v2, 2001.

[30] R. Paschotta, “RP Photonics Consulting GmbH.” [Online]. Available: https://www.rp-photonics.com/encyclopedia.html.

[31] Thorlabs, “Single Frequency Laser SFL1550S,” 2011.

Chapter 5

Experimental Demonstration of Kilometre Range Quantum Digital Signatures Using Quantum Key Distribution Hardware

5.1 Introduction

The previous Chapter of this thesis showed the final steps in protocol improvements which allowed QDS to be carried out without the requirement of quantum memory (QM) for the swap and comparison mechanism or the state discrimination measurement. At present, QM has not reached the technical maturity to be a practical option for this application [1]–[3], as discussed in Chapters 2.

When comparing the experimental performances of the two experimentally realised systems, it turned out that the revised system (presented in Chapter 3) which did not require QM, [4], was still out-performed by the original which did require QM [5]. Given that QM technology at the moment cannot provide on-demand, unity fidelity, long storage time, and large capacity, an implementation which requires QM will not be practical at this time [2], [3], [6].

A measure of performance in QDS is the length L of a signature half-bit, and how long it would take a user to send one half-bit. In the first experimental implementation, which required QM, the optimised coherent state sequence length L was found to be 6.91×10^7 elements, meaning that it takes a total of 0.691 seconds to send one signature half-bit at the 100 MHz clock frequency employed. The second experimental implementation, which does not require any QM, required an optimised half-bit length of 5.13×10^{13}, taking a total of 5.13×10^5 seconds to send at a clock frequency of 100 MHz.

There are several factors which caused the modified system without QM to have a longer signature half-bit length than the first experimental realisation. One was the use of relatively high mean photon numbers of >1, leading to a very small minimum error measurement value. The passive phase modulators used to perform the measurement were more susceptible to rejection events if the phase encoded by Alice was not 100% correct.

Fluctuating visibility in the multiport due to external stresses on the optical fibre meant an overall lower visibility.

In this Chapter, a new protocol is used in order to overcome some of these issues and allow demonstrations of QDS over kilometre ranges in optical fibre. The new protocol no longer required the optical multiport, allowing greater transmission distances to be covered. Lower mean photon numbers are investigated to keep the minimum error measurement value at a more optimum level.

5.1.1 Range of mean photon number per pulse

As explained in the previous Chapter the overall performance of a QDS system is not just dependent on the photon count rate measured by a receiver. The coherent state sequence length of the signature half-bits are calculated from a parameter known as the gap, *g*, which is generated from the cost matrix and the minimum error measurement of a malicious party. From the cost matrix we also calculate the guaranteed advantage (Guad), the advantage a receiver has in rejecting a forged signature element. From the minimum error measurement, a correction factor for this advantage, dependent on the mean photon number per pulse ($|\alpha|^2$) is calculated, and called P_{min} [7], plotted in Figure 5.1 a).

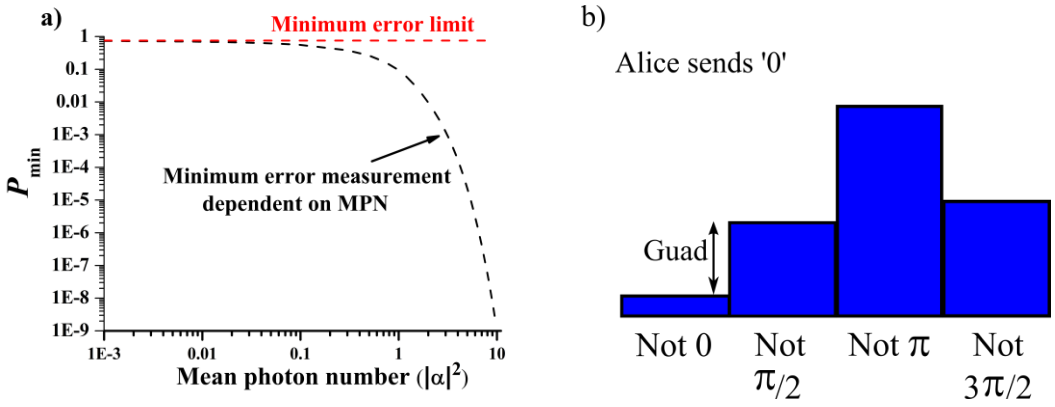


Figure 5.1 – a) minimum error measurement correction factor dependence on the mean photon number. b) An extracted column from the cost matrix showing the minimum, maximum and "50% peaks" which are used in analysis.

The general trend of P_{min} is to decrease with increasing $|\alpha|^2$. Although the probability of photon detection increases for a legitimate receiver as more photons are propagating through the system, so it also increases for a malicious receiver. An interesting note is that as $|\alpha|^2 \rightarrow 0$, $P_{min} \rightarrow 0.75$. This limit in the correction factor is reached because when guessing a forged state a malicious party, will still have a 1:4 chance of actually guessing the correct case. Therefore the advantage is reduced to ¾, because guessing incorrectly has a probability of being rejected by the receiver. For reference the trend of P_{min} is shown in Figure 5.1 a), and is calculated using Equation 4.11 from the previous Chapter.

In simple terms the guaranteed advantage is the difference between the smallest off-diagonal element and largest diagonal element in the cost matrix, as shown in Figure 5.1 b). Figure 5.1 b) presents a schematic of an example case of the Guad where these two values arise from the same column in the cost matrix. This is not necessarily always the case and in practice these two values could come from different columns in the cost matrix. If the cost matrix retains the same overall distribution with increasing $|\alpha|^2$ then the Guad will increase because the probabilities will increase, this was shown in the previous Chapter.

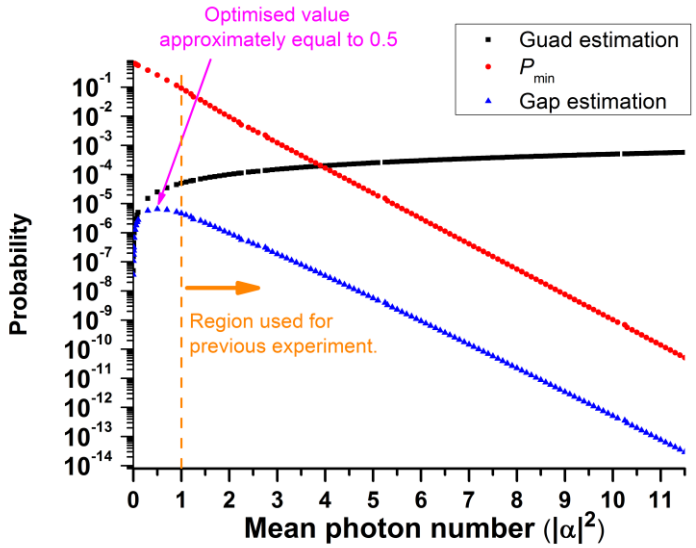


Figure 5.2 – Estimating the optimum mean photon number $|\alpha|^2$ based on a linear fit of the Chapter 4's guaranteed advantage (Guad) and the P_{min} value for each $|\alpha|^2$. It can be seen that the gap estimation has a peak value of around $|\alpha|^2 = 0.5$.

The gap, g, is calculated as $g = P_{min} \times$ Guad. Given that the values of P_{min} decrease with increasing $|\alpha|^2$ while the value of the Guad increases with increasing $|\alpha|^2$, there will be an optimum $|\alpha|^2$ where the gap will have the largest value. From the previous Chapter results, a function can be fitted to the guaranteed advantage data. Along with P_{min} values an optimum gap value for the previous experiment is found to be at $|\alpha|^2 \approx 0.5$, Figure 5.2. Therefore the range of $|\alpha|^2$ values used in this experiment should comprise a range of values that includes 0.5 (preferably somewhere near the centre) so that this effect can be seen.

5.1.2 Multiport – swap and comparison mechanism

Previous experimental implementations of QDS relied on a multiport [4], [5], [8], [9], which allowed quantum signature elements (phase-encoded coherent states), sent from Alice, to be swapped and compared in transit to two receivers (Bob and Charlie). This multiport swap and comparison mechanism can be seen in Figure 3.12. As was more fully described in Chapter 2 and 3, the multiport symmetrises the states which are sent into it, meaning that if Bob and Charlie are given the same signature, the output at ports 3 and 6 is equal to the input, however if the inputs are different, the output of the multiport is symmetrised and photons will appear at the multiport "null-ports" (ports 4 and 5 in Figure 3.12).

While the multiport is capable of carrying out an all-optical, non-demolition swap and comparison operation, it has some serious implications and limitations which prevent QDS implementations based on it becoming a viable commercial technology.

The multiport in the previous experimental implementations was constructed from panda-eye polarisation maintaining (PM) optical fibre [10], [11] coupled linear optical components. To connect all these components together optical fibre splicing is used, but in doing so, some optical loss is introduced (≈0.3 dB per splice [12]). As well as splicing losses, component and bending losses are also present in the multiport, resulting in a loss from Alice's input to Bob's (Charlie's) output of ≈8.5 dB or approximately 14 % of the input optical power exiting at Bob's (Charlie's) output ports. Since the optical fibre transmission medium has a loss it is possible to equate -8.5 dB to approximately 38 km and 3.8 km direct links of telecommunications optical fibre at 1550 nm and 850 nm

respectively. Clearly, the high loss of the multiport severely reduces the long-range transmission potential of QDS protocols based around it.

The multiport is a physically "large" construction because of the components involved, but the optical path lengths are only ≈ 5 m. It is essentially two intertwined Mach-Zehnder interferometers, therefore as the optical path lengths increase, it becomes progressively more difficult to keep the relative optical path length differences stable [13]. This limits the usable length of fibre in the multiport (and therefore the separation between Bob and Charlie) to very short distances (i.e. << 1km) and makes operation in deployed fibre (where environmental fluctuations are impossible to avoid) prohibitively challenging. Additionally, the fibre length of the two crossing paths in the centre of the multiport fibre is the maximum range of the QDS protocol, as Bob and Charlie must be in local control of each of their halves of the multiport. Given that the range of these fibres is likely to be of the order of metres, and at best a few 10s of metres, this would severely limit the potential range of end applications for QDS.

As mentioned in the previous Chapter, polarisation routing in the sender and receiver interferometers was introduced in order to increase the number of photons routed through the correct, interfering optical paths, i.e. useful photon events [14]. The two polarisations could travel at different velocities in the multiport depending on the mechanically and thermally induced stresses on the fibre [10], [15]. This led to a non-optimal visibility in the multiport which varied throughout the day, as shown in Figure 5.3. Although the effect of the polarisation routing could have been avoided with non-PM components, this would require polarisation controllers to compensate for polarisation drift and these introduce additional losses and complexities to this system. This can be considered as yet another argument against the use of the multiport in a practical QDS system.

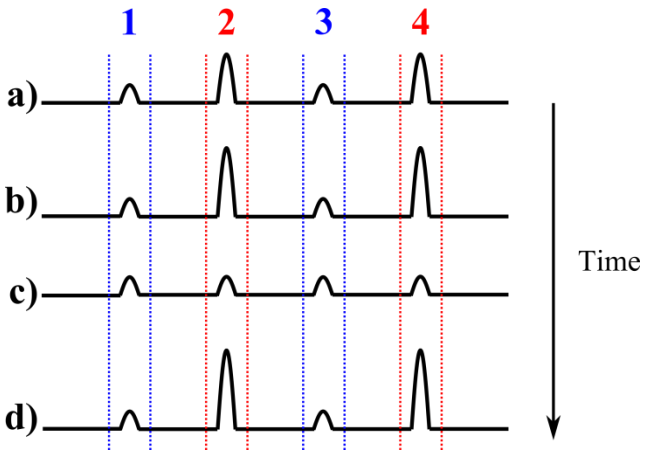


Figure 5.3 –A schematic of the histograms seen from multiport null-port detector in the previous quantum digital signature protocol which required the multiport, but no quantum memory. The figure shows four peaks on four different histogram traces taken separately in time. Pulses 1, and 3 are 10 ns apart, corresponding to the signal sent by Alice, while 2 and 4 and 10 ns apart and correspond to the reference sent by Alice.

Many issues with the multiport have been discussed, including its high optical loss, restricted distance (realistically of the order of 10s of metres) and the challenging issues with the use of a polarisation routing implementation. These issues suggest that an alternative is most likely required for practical applications of QDS. In practice, it is possible to carry out a swap and comparison mechanism conventionally, using post-selected conventional information. Since the multiport is the only major optical component that previously distinguished a QDS system from a phase basis set QKD system – once it is removed [16] optical and electrical components which are similar to a QKD system can be used to transmit QDS. It has been shown already that quantum key distribution (QKD) technology is capable of transmitting over distances of up to 307 km in optical fibre [17], so this simplification of the physical hardware offers the prospect of significantly enhanced QDS transmission distances.

In the following scenario Bob and Charlie each had a channel between themselves and Alice. There is also a secure channel between Bob and Charlie for post-selection communication. Alice sends Bob and Charlie copies of a quantum signature, the receivers then measure and store the information received by conventional means. For the receivers to be assured that they were sent the same signature, they must perform some form of swap

and comparison mechanism. For each signature element Bob (Charlie) flips a coin and decides whether to keep the element or send it onto Charlie (Bob) and then forgetting the value just sent. The element is sent through the secure channel shared between them. This can be created by another QKD link. At the end of the swap mechanism, Bob (Charlie) is ideally left with 50% of his own signature elements, and 50% of Charlie's (Bob's). Note, sometimes Bob (Charlie) may keep an element and also receive the same element from Charlie (Bob). The comparison part of the mechanism comes when Alice decides to send a message and the conventional signature. Bob (Charlie) checks for mismatches separately against signature elements sent by Alice, and Charlie (Bob). Hence, this approach means that a swap and comparison operation can be performed without a multiport and without quantum resources in the link between Bob and Charlie.

Based on the approximation of the $|\alpha|^2$ which allows for an optimised gap *g*, and that a swap and comparison mechanism can be carried out classically rather than quantum mechanically, a QDS protocol can be devised to show an improved distance over previous systems. This chapter will present a revised protocol [16] and then demonstrate how it can be adapted and experimentally implemented in optical fibre.

5.2 Kilometre range quantum digital signatures

5.2.1 Introduction to protocol

This revised QDS protocol suggested by Dunjko *et al.* [16] performs the swap and comparison mechanism by swapping classical information of the USE measurement outcomes over secured channels. This means there are no high optical loss components between a sender and receiver, apart from the optical fibre connections and any losses associated with them. Two protocols were presented in [16], P1, and P2, both can be implemented without the multiport. The protocol implemented in this experimental realisation is a variation of P1, where Bob and Charlie are sent the same signature.

While this protocol uses four non-orthogonal states $|a\rangle$, $|ae^{i\pi/2}\rangle$, $|ae^{i\pi}\rangle$, and $|ae^{i3\pi/2}\rangle$, more or less non-orthogonal states could be used. Four was thought to be the optimum number of non-orthogonal states for balancing the security requirements, and experimental complexities. As the number of non-orthogonal states increases, the upper bound of $P_{\min}$ increases because a malevolent party will have less probability of guessing correctly.

Therefore it would be more beneficial for security to have a greater number of non-orthogonal phase-states. However as was mentioned previously, for every non-orthogonal pair added another measurement interferometer needs to be added to the experimental set-up, which can become practically difficult to operate and manage.

QDS protocols typically have two stages, one for distribution of the signature, and one for the messaging stage. The two stages of the protocol are outlined below:

***Distribution* stage**

1. For each future possible one-bit message, $k = 0, 1$, Alice generates two (since there are two parties in this protocol) copies of the quantum signature $QuantSig_k = \bigotimes_{l=1}^{L} p_l^k$ where p_l^k is randomly chosen from her four available BB84 [18] phase-encodings $b_l^k \in \{\alpha, \alpha e^{\frac{i\pi}{2}}, \alpha e^{i\pi}, \alpha e^{\frac{3i\pi}{2}}\}$, where L the length of each signature. The signature length is referred to as the signature half-bit length because there are two signature bits. L is an integer value which is dependent on the security required, and experimentally generated parameters. For a message k, the quantum signature is known as $Quantsig_k$ and the classical sequence of bits is called the $PrivKey_k = (b_1^k, \ldots b_l^k)$ is known as the *private key*.
2. Alice sends one copy of $Quantsig_k$ to each party in the protocol, for each possible message $k = 0, 1$.
3. Bob (Charlie) measure the signature elements sent by Alice, recording classically which phase-encodings are eliminated for a signature. This then gives a sequence of eliminated states (called the eliminated signature) which are used to authenticate or verify a message later on.
4. For each signature element l of $Quantsig_k$, Bob (Charlie) randomly chooses whether to keep it, or forward it onto Charlie (Bob). If Bob (Charlie) decides to keep the element, it becomes part of their quantum signature from Alice, if he decides to forward it on, the information is forgotten by Bob (Charlie) and becomes part of Charlie's (Bob's) signature.
5. In an ideal case, during the swapping of USE classical measurement outcomes, the number of elements Bob (Charlie) forwards onto Charlie (Bob) will be $L/2$. But due to asymmetric losses in transmission this is unlikely to happen, and therefore Bob (Charlie) have to set bounds on how many elements they receive before they abort a communication. Bob (Charlie) will abort if fewer than $L(1/2 - r)$ or more

than $L(1/2 + r)$ are elements are received, where L is the signature half-bit length and r is a bound defined by the verification threshold s_v given by $s_v = \frac{1}{16}(1 - 2r)$.

After stage 5 in the distribution stage, Bob (Charlie) will have a sequence of element measurements (eliminated signatures) corresponding to the signature elements sent by Alice, and a separate sequence of signature elements forwarded to him by Charlie (Bob).

Messaging stage

1. To send a signed one-bit message, m, Alice sends the private key ($PrivKey_m$) and the message (m) to the desired recipient, for this stage lets choose Bob, although Charlie would apply the same process.
2. Bob checks this private key sent by Alice ($PrivKey_k$) for mismatches against his stored eliminated signatures separately for both the signature sent to him by Alice previously, and the signature elements forwarded to him by Charlie. An authentication threshold, s_a, is applied to the matching to prevent forging. If fewer than $s_a \cdot L/2$ mismatches occur in both Alice and Charlie's eliminated signature, then the message is accepted. If otherwise, the message is rejected.
3. To forward the message to Charlie, Bob forwards the message and the private key (m $PrivKey_m$) sent to him by Alice.
4. Charlie also checks for mismatches, similarly to that carried out by Bob, but instead applies verification threshold, s_v. If less than $s_v \cdot L/2$ mismatches occur, the message is accepted. Otherwise it is rejected. The verification threshold is chosen $0 \leq s_a \leq s_v < 1$, so the verification threshold is always larger than the authentication threshold.

5.2.2 Unambiguous state elimination measurement

This new QDS protocol, like the previous experimental implementation [4], does not rely on any quantum memories (QM) for the state discrimination measurement, making use of a unambiguous state elimination (USE) measurement [19]. A description of the USE measurement process was presented in the previous Chapter, as it has not changed between the two different iterations of the protocol. However, the removal of the multiport for this new protocol means that the only remaining optical components are now similar to those used in phase basis set QKD [20].

5.2.3 Definitions of security and calculation process

The QDS protocol presented here is designed to prevent repudiation and forging malicious activities, and assumes the quantum channels between the parties cannot be tampered with or eavesdropped by a 3rd party [21]. The protocol also assumes that all classical communication channels are authenticated. The formal definitions remain the same as previously described in Chapter 3, section 3.4.2 [22], [23].

The formulations for the probability of malicious repudiation, forging, and the probability of an honest abortion of the protocol by Bob (Charlie) are given in Equation 5.1, Equation 5.2, and Equation 5.3 and are defined in the supplementary material of [21].

$$P(\text{repudiation}) \leq 2\exp\left(-\tfrac{1}{4}\left(s_{\text{v}}\text{-}s_{\text{a}}\right)^2 L\right) \qquad \text{Equation 5.1}$$

$$P(\text{forging}) \leq \exp\left(-\left(C_{\min}\text{-}s_{\text{v}}\right)^2 L\right) \qquad \text{Equation 5.2}$$

$$P(\text{honest abort}) \leq 2\exp\left(-\left(s_{\text{a}}\text{-}P_{\text{h}}\right)^2 L\right) \qquad \text{Equation 5.3}$$

Previous protocols [4], [5], [9], [16], [24], have always made these probabilities equal as there is no advantage in favouring security for one particular type of malicious activity and that is an assumption that will be continued here. Based on the equations above being equal, the authentication and verification thresholds are chosen to be Equation 5.4 and Equation 5.5 respectively. P_{h}, is the probability that a receiver will eliminate the state actually sent by Alice, which is calculated using the cost matrix generated by experimental measurements. g, is the gap, which is essentially the difference between the highest diagonal element of the cost matrix, and the lowest off-diagonal element, corrected for by the minimum error measurement that a malicious party can make, $P_{\min}$. P_{h}, g, and $P_{\min}$ will be defined in more detail later in the analysis.

$$s_{\text{a}} = P_{\text{h}} + {}^{g}/_{4} \qquad \text{Equation 5.4}$$

$$s_{\text{v}} = P_{\text{h}} + {}^{3g}/_{4} \qquad \text{Equation 5.5}$$

Finally, the minimum length of a signature half-bit L, which can be securely sent, based on the probabilities for repudiation, forging and an honest abort being equal is given by Equation 5.6. The security level in the equation refers to the probability of repudiation, forging, and honest abort.

$$L = -\frac{\ln\left(\frac{\text{Security level}}{2}\right)}{\left(\frac{g}{4}\right)^2} \qquad \text{Equation 5.6}$$

5.2.4 Experimental set-up

Figure 5.4 and Figure 5.5 show the optical and electrical experimental set ups used to implement the QDS protocol. The optical set-up will be explained first, followed by a description of how the electrical system drives the experiment. Following this, the experimental methods will be outlined, covering the experiment operation and data analysis.

The experimental set-up for this protocol is very similar to the one used in Chapter 4 [4], because it continues to use the USE measurement and polarisation routing. As can be seen in Figure 5.4, one of the obvious visual differences is that the requirement for the multiport has been lifted, allowing for varying lengths of optical fibre to be placed between Alice and Bob (Charlie). The use of non-PM standard telecommunications optical fibre (Corning SMF 28e [25]) as the quantum channel (and the continued use of polarisation routing [14]) meant Bob (Charlie) required polarisation controllers (in the form of static "bat-ear" polarisation controllers [26]) before each interferometer to compensate for polarisation drift. In fact, the optical system looks more akin to a QKD system than one of the originally proposed QDS [24], [27] systems. In reality, as will be seen in this section, it is only the classical processing that distinguishes this QDS protocol from a QKD protocol. As well as changes to the optical system there were many improvements made to the operation and analysis software.

Since all the information regarding the experimental system is covered in the previous Chapter (Section 4.2.4), only the differences will be highlighted in this Chapter. Although it is worth repeating that this system was operated at 100 MHz, with Alice using the same four phase-encodings as the Chapter 4.

The vertical-cavity surface-emitting laser (VCSEL) diode is no longer gain-switched through the Maxim drive board. It was found that electrically gain switching the VCSEL through a bias-tee (Picosecond Pulse Labs 5575A) with a stabilised DC source (Newport 505) could give equal performance (i.e. the spectral and temporal responses shown in Figure 4.10) with less experimental complexity and clutter.

At the output of Alice's unbalanced asymmetric Mach-Zehnder (UAMZ) interferometer, instead of sending her coherent state through the multiport, she then splits the intensity into two using a 50:50 beamsplitter (BS). This is an optical way of Alice generating her two identical copies of a quantum signature which can be sent to Bob and Charlie. The mean photon number ($|\alpha|^2$) for the experiment is defined at the outputs of the 50:50 BS and use inline optical attenuation (again based on knife edges) to ensure that the $|\alpha|^2$ is the same in both arms. The $|\alpha|^2$ is measured only for the signal pulses, as a large intensity ($|\alpha|^2 >>1$) is used for the reference pulse to preserve phase. It is possible for the correct pulse to be used for state tomography [28] at a receiver to assist in the security analysis but this process was not undertaken in these experiments.

In previous QDS protocols, after Alice, Bob and Charlie would take their coherent states and pass them through the multiport to perform the swap and comparison mechanism. Instead, as can be seen in Figure 5.4, the multiport is replaced with reels of optical fibre. In the experiment, reels of 500m, 1km, and 2km lengths were used. The reeled fibre was (8.2 μm core diameter) standard single-mode fibre designed for the telecommunications wavelengths of 1310 and 1550 nm (Corning SMF-28e+ [25]), which was pigtailed with short (<1 m) lengths of 4.4 μm core diameter single-mode fibre designed for a wavelength of 850 nm [29] to remove higher order modes before coupling to the PM fibre components. The different core sizes led to an extra loss of ≈0.8 dB per reel of fibre [12]. The experimental results presented in this Thesis refer to the actual reel length rather than an effective distance computed from channel losses, as it would be expected that coupling losses would be present in any real system.

After the reel of fibre, Bob (Charlie) performs the USE measurement using his two UAMZ interferometers. This construction of the interferometers and the USE measurement was described in the previous Chapter (section 3.2.2) and the optical set-up is shown in Figure 5.4. It should be noted that unlike the previous two QDS experiments both Bob and Charlie performed measurements of the phase-encoded coherent states sent them, where as previously only one receiver was tested. The photon events were also recorded on the commercially available thick junction PerkinElmer Si-SPADs [13].

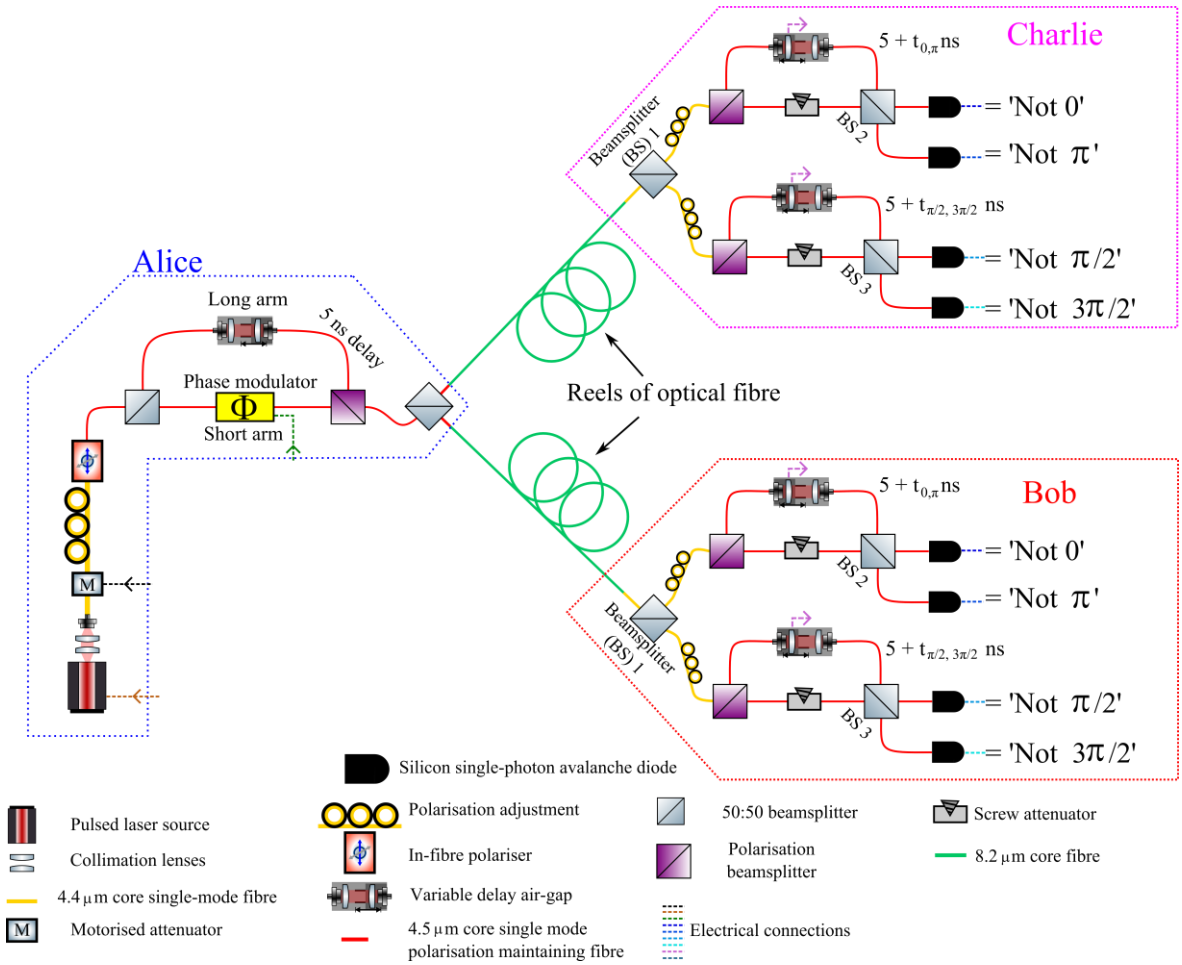


Figure 5.4 – The optical set-up for the kilometre range experimental realisation of quantum digital signatures. Alice, Bob and Charlie were physically separated to maximise to the distance between them on the optical bench.

The electrical system shown in Figure 5.5, like the optical system, was very similar to the electrical system used for previous experimental demonstrations of QDS [4]. The main difference was that two PCs are no longer required to run the experiment, one for monitoring the multiport, and one for recording the USE measurements. This reduced the complexity of the synchronisation of time-tag hardware, and simplifies the process of correctly initialising measurements.

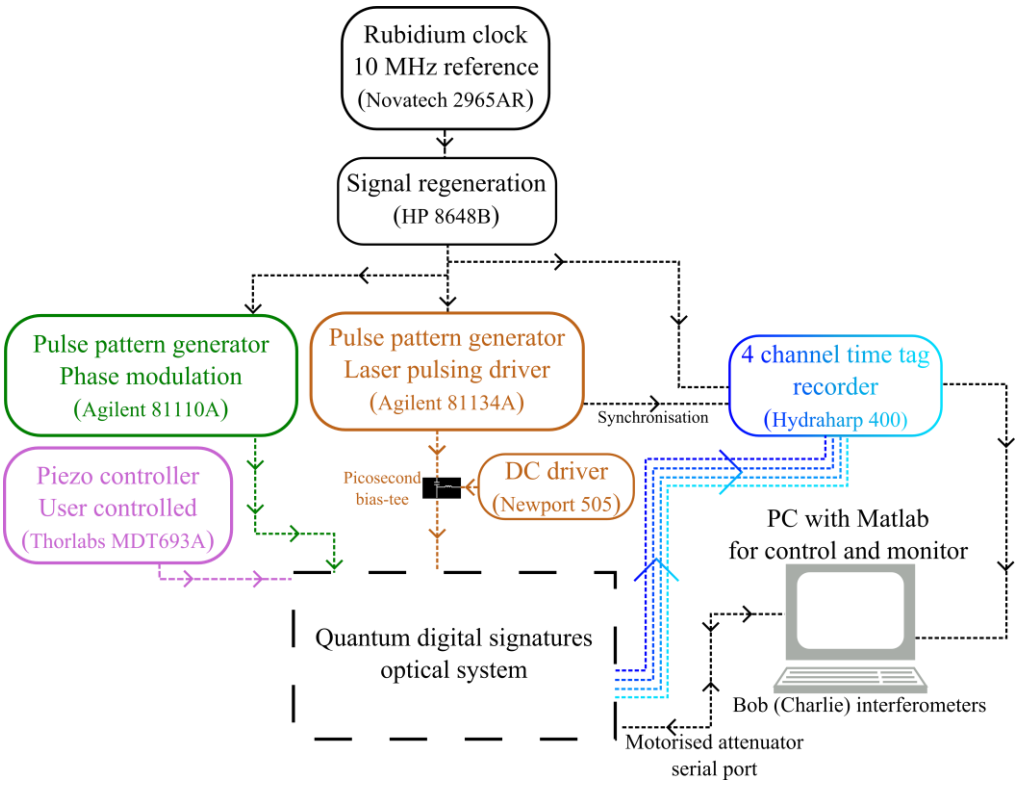


Figure 5.5 – The electrical set-up for the experimental realisation of kilometre range quantum digital signatures.

The rubidium clock [30] provided a 10 MHz reference which was then regenerated by the frequency synthesiser (Hewlett Packard 8648B) [31]. This was initially done to provide enough voltage for the reference to be used by so many devices, when two PCs were required. The 10 MHz reference was connected electrically to the Agilent 81110A and 81134A PPGs, as well as the time-tag hardware (HydraHarp 400 [32]).

A dual channel output PPG (Agilent 81110A) was used to drive the 100 MHz modulation of the lithium niobate ($LiNiO_3$) phase modulator (Photline NIR MPX800-LN-08 [33]). Each channel output provided two levels of modulation, resulting in the two non-orthogonal pairs. The outputs were added using an power combiner [34], which allowed a four level repeated pattern to be generated, which is shown in Figure 4.7. Ideally the four levels should be evenly spaced with flat tops to the waveform. As shown in Figure 4.7, there was some ringing and other imperfections in the signal which corresponds to ≈3° shift either side of the mean value, and the spacing between the mean values of the level is not equal, corresponding to ≈10° error in the initial setting of phase states. This error has some bearing on the final results when the measurements are analysed.

The Agilent 81134A PPG provided a 0.75 ns wide pulse at a 100 MHz clock rate with a ±1V signal into the bias-tee which is added to a 0.3 mA current from the dc driver (Newport 505). Each PPG can be electrically delayed internally, or externally to optimise the visibility of the measurement.

The time-tagging hardware collected the electrical signals from the Si-SPADs. (PerkinElmer) and using MATLAB [35] code would record time-tags, perform some preliminary filtering and save them to a hard disc for later analysis. Some preliminary analysis was performed in real-time during system operation which gave feedback on system visibility and provided an indication of the off-diagonal terms of the resulting cost matrix.

Methods

Initially the optical laser output pulse temporal and spectral profile was optimised for the experimental set-up. The losses of the interferometers were then calibrated so that Alice was sending weak coherent pulses for her signal and a large intensity reference pulses. Bob and Charlie's interferometers were loss balanced, and time synchronised for maximum visibility.

To perform measurements, Alice's outputs were connected to separate reels of fibre, depending on the distance chosen for the experimental run. The other end of the reel was connected to the receivers 50:50 BSs for the USE measurement. Bob (Charlie) could adjust their polarisation controllers to minimise the non-interfering peaks and therefore maximise the photons being routed correctly, which also affects the maximum visibility of the interferometers. All interferometers and reels of fibre were located in an air-conditioned laboratory, on the same optical bench.

The HydraHarp hardware only had 4 inputs, so only one receiver was measured at one time, as there were four detectors for each receiver. However the experiment was set-up and performed as if both receivers were being measured at the same time, although it is worth noting that the protocol does not formally require simultaneous measurements at Bob and Charlie. Both Bob and Charlie were optically connected to the system during any experiment, but the experiments were conducted twice – once with Bob's detectors connected to the HydraHarp and once with Charlie's detectors connected.

A custom MATLAB program (developed in-house by Robert Collins) controlled the time-tagging hardware, taking time-tag recordings from all four measurement detectors. The time-tags were used to generate histograms so that a user may view the evolution of the visibility of the interferometers, as the experimental conditions were altered. The visual feedback from the histograms allowed the user to fine-tune the interferometer path lengths using the piezo-electric controller. The histograms also gave the user visual feedback on any polarisation drift that had occurred during transmission as minor variations in environmental conditions affected the kilometre length reels of optical fibre. During configuration of the MATLAB program, the user was asked to define the position of the gating windows, where each histogram should be maximised or minimised and the location of the non-orthogonal peaks (which will be at 50% of the maximum intensity). Thresholds could be set on the acceptable visibility (typically >94%) and how equal the orthogonal, non-orthogonal pair's interference peaks were (i.e. how equal the two 50% peaks are). Once the thresholds were met or exceeded, the one second worth of time-tags used to form the histogram would be recorded, otherwise the time-tags were discarded and a fresh set collected, and the process repeated. Unlike the previous QDS system's control software which was written in LabVIEW and only allowed for a single-shot measurement, the revised MATLAB program refreshed the histogram with a new one-second duration of data so that repeated measurements could be rapidly collected after one configuration process, this allowed more efficient data collection.

A range of $|\alpha|^2$s were recorded from 0.1 to 1, in steps of 0.1. This was chosen to include the possible optimised gap position of ≈0.5 which was proposed earlier. The range also covers the $|\alpha|^2$s commonly used by QKD experiments, for example 0.1 to 0.5 [36], [37]. To sort the data from raw time-tags into gated format for checking correlations, a 1 ns wide gating window was placed either side of the defined peak positions, which were set by the user in MATLAB during data collection. One hundred, individual sets of 1 second's time-tag data recordings were taken for each $|\alpha|^2$, and each receiver. The gated detector event statistics from these time-tag data recordings (i.e. the USE success rates at each detector) were then averaged before being subjected to subsequent analysis to generate cost matrices, protocol thresholds, etc. which were then used in the later analysis to calculate the parameters needed to the signature half-bit length L.

5.3 Experimental results and analysis

As in the previous QDS Chapter, the presentation of the results and the analysis will start from the raw data, move onto the gated data, construct the necessary matrices and finally generate from the cost matrices the parameters required to calculate the signature half-bit length *L*. Unlike the previous QDS experiments, this analysis includes the results from Bob **and** Charlie, where before only one receiver was demonstrated, hence there are extra steps in the later stages allowing the security of the protocol to be defined by the worst performing user, as each user has slightly different measurement characteristics.

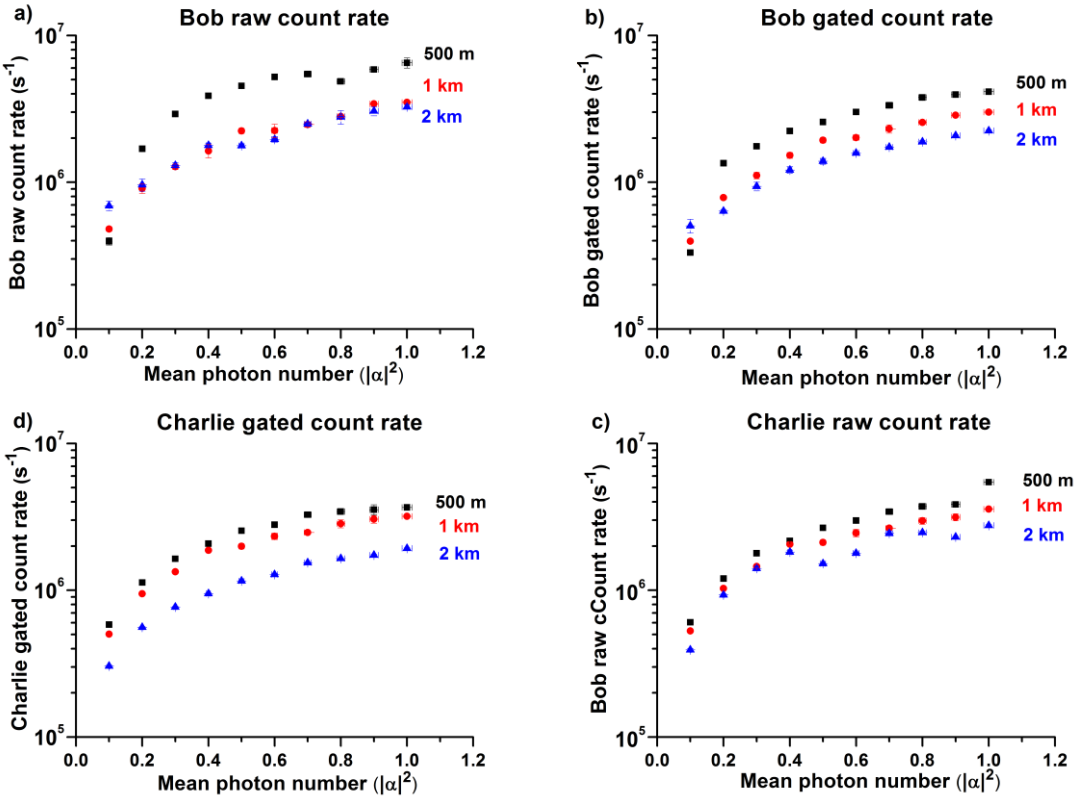


Figure 5.6 - Raw and gated rates for Bob (a, and b), and Charlie (c and d).

Starting from the raw time-tag data, Figure 5.6 a), and c) show the raw count rates for Bob and Charlie respectively. From a) it can be seen that the 2 km raw count rate was sometimes higher than the 1 km rate. This was due to optically misrouted photons (i.e. the non-interfering peaks) contributing to the background count levels. This was primarily due to inaccuracy of the static polarisation controller configuration, but also partly dependent on imperfections in the extinction ratio of the PBSs in the receivers. In Bob, the losses of the optical fibre for each distance are 2.2, 3.3, and 5.4 dB for 500 m, 1 km, and 2 km

respectively. For Charlie, the same reel of fibre was used for 500 m and 1 km as was employed by Bob (because of the high losses of the reels specifically purchased for Charlie), and 6.8 dB loss for 2 km. The losses of the various fibre lengths were found to be higher than the manufacturer's quoted attenuation of 2.2 dB/km. This was due to additional loss from the two splices (maximum of 0.3 dB each) and the differences between the fibre core sizes, which contributed loss due to modal mismatch of ≈0.8 dB. Standard telecommunication fibre (single-mode at 1310, 1550 nm, 9 μm core diameter) was used to connect sender and receivers so that the QDS system demonstrated compatibility with the existing telecommunications optical fibre infrastructure. But the PM fibre was single-mode for 850 nm (4.4 μm), so single-mode non-PM fibre at that wavelength was needed to strip any higher order modes [38] before returning to PM fibre.

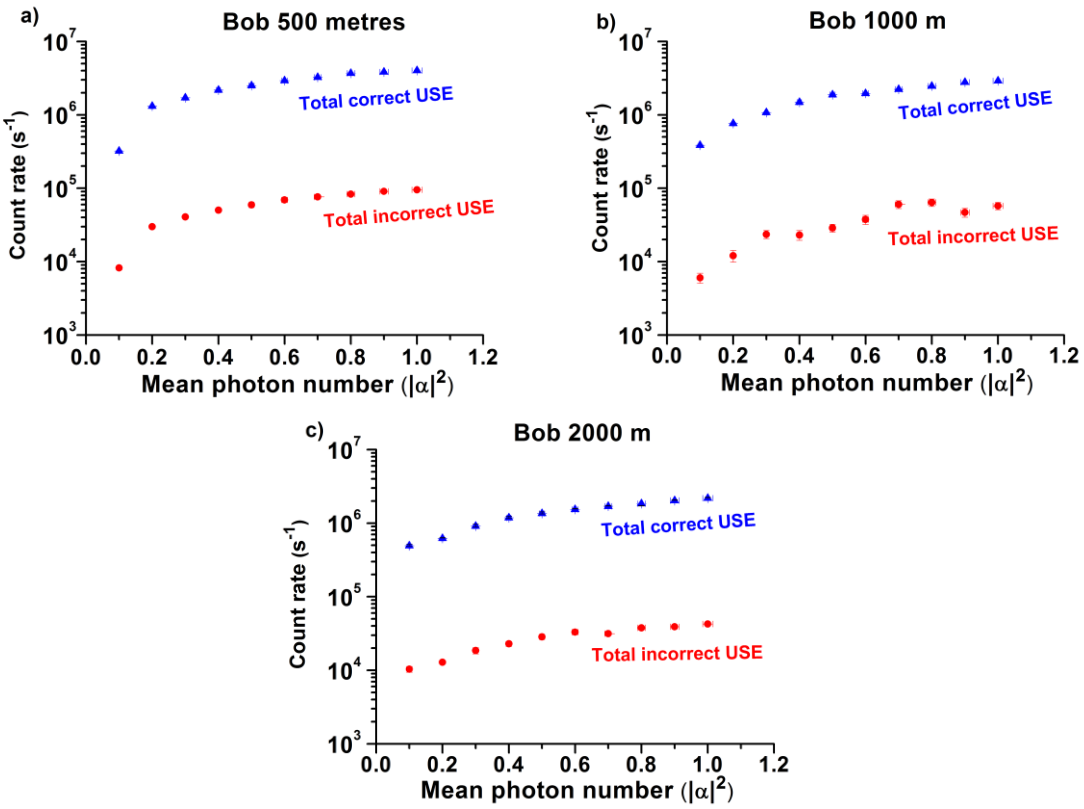


Figure 5.7- The correct and incorrect unambiguous state elimination (USE) rates for Bob at 500m, 1km, and 2 km, a), b), and c) respectively. The correct USE rates are > 95% of the total USE rate hence the total is not plotted.

Figure 5.6 parts b) and d), the gated count rates for Bob and Charlie respectively, show that even though the raw count rates for different fibre lengths sometimes over-lap, the gated

rates are all separated (except for an $|\alpha|^2$ of 0.1 in Bob). This confirms that it was the non-interfering peaks which were contributing to the raw count rate overlapping in the 1 and 2 km case in Bob. Over all the results for Bob and Charlie, the average gated rate was found to be 80 ± 13.4 % of the raw rate. This variation in values corresponds to the effectiveness of the polarisation routing for Bob and Charlie, although the visibility of the overall system was not heavily affected. This was surprising as the visibility is dependent on the polarisation of the states reaching the final beamsplitter. However, the PBS at Bob (Charlie) repolarises the coherent states at its output port. Therefore, if the static polarisation controllers are not set with perfect accuracy the resulting slightly incorrectly polarised input light will be repolarised to linear at the output of the PBS and, after rotation, the same parallel linear states will recombine on the final beamsplitter. If the presence of photon events in the non-interfering peak regions was primarily due to imperfections in the PBS, then the light at the final beamsplitter would have an orthogonally polarised component that would degrade the visibility.

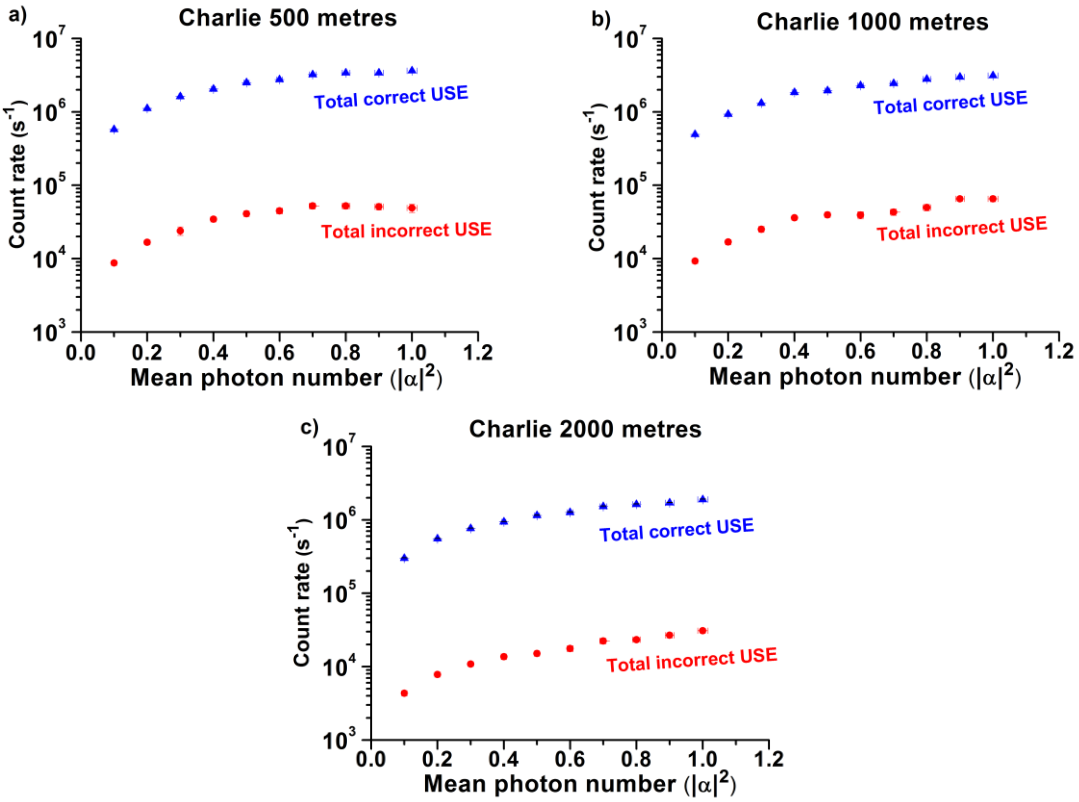


Figure 5.8 – The unambiguous state elimination (USE) rates for Charlie at 500m, 1km, and 2 km, a), b), and c) respectively. The correct USE rates are >98% of the total USE rate hence the total is not plotted.

The gated count rates all contribute to the USE measurement and cost matrix. From the previous Chapters description of the USE measurement, if Alice sends phase encoding π, Bob (Charlie) considers a correct USE measurement if he eliminates any state except for the π state, i.e. he does not have a photon event at his 'Not π' detector. For all the results for Bob and Charlie, the correct USE rate was on average 98 ± 0.35% of the total USE rate or, equivalently, 78.4% of the total raw rate. The 78.4% success probability is lower than the value of 83.84% seen in the previous Chapter [4] due to misrouting of the large intensity reference pulse. Small mismatches in polarisation in this experiment led to greater count rates in the non-interfering peaks in comparison to any mismatching in the previous experiment which used a reference pulse which was, relatively, more equal in intensity to the signal pulse. However, the correct USE rate of 98% of the total USE rate is higher than the previous experiment of 95.27% which is due to the improved visibility of the optical system. Figure 5.7 and Figure 5.8 show the USE total, correct and incorrect rates for Bob and Charlie respectively, at distances of 500 m, 1 km, and 2 km, in a), b), and c). All figures show the same general trend of increasing success rate with higher $|\alpha|^2$.The generation of the cost matrix, and subsequent analysis for this Chapter follows the follows the same process as the previous Chapter, so to save repetition this is not included in this Chapter. However extra analysis on the cost matrix is performed in this Chapter due to both receivers being analysed for the worst-case scenario, this is included as it is different.

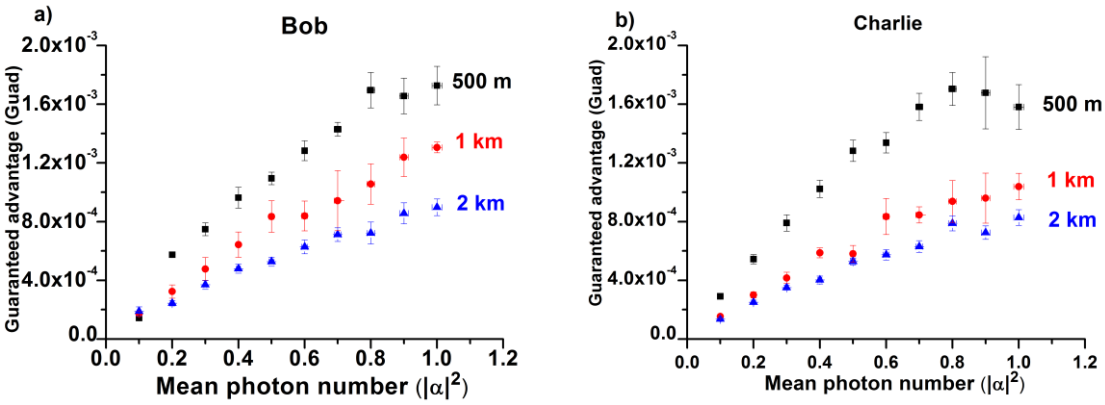


Figure 5.9 – Guaranteed advantage for Bob (a) and Charlie (b) over a range of mean photon number at the three different distances.

As a reminder, the Guad is the minimum difference between the largest diagonal element, and the smallest off-diagonal element, also known as the guaranteed advantage. Figure 5.9 a) and b) show the Guad as a function of $|\alpha|^2$ for Bob and Charlie respectively at the

different distances. The general trend for this is to increase with $|\alpha|^2$ however for Charlie's 500m values dropped at $|\alpha|^2 = 0.9$ and 1 due to a change in visibility. It can be seen that the average P_h value is decreasing from Figure 5.10. This suggests that the visibility of the system (defined in Equation 5.7) is increasing, but an off-diagonal element is decreasing in value. This increase in visibility leads to a smaller Guad value. This drift in visibility was caused by nonlinearities in the detectors at > 1 MHz raw count rates [39], also from the polarisation routing not being fully optimised.

The mean value of the diagonal minimum elements is called the probability for an honest elimination, P_h. It is the average probability in an honest scenario, where a receiver will eliminate the state actually sent by Alice, in this example the value is 1.48×10^{-4}. Figure 5.10 a) and b) show the P_h dependence with increasing $|\alpha|^2$ for Bob and Charlie respectively. P_h is primarily dependent on the visibility of interferometer and therefore some points are off the normal trend, seen in Bob's 1km data and Charlie's 500 m and 1 km data. In fact the P_h values for Charlie at1 km are better than the 500 m values at $|\alpha|^2$ of 0.9 and 1 - this is the result of increased visibility at those particular photon numbers due to better optimisation of the non-interfering peaks.

$$\text{Visibility}=\frac{(\text{Counts in maximum})-(\text{Counts in minimum})}{(\text{Counts in maximum})+(\text{Counts in minimum})} \qquad \text{Equation 5.7}$$

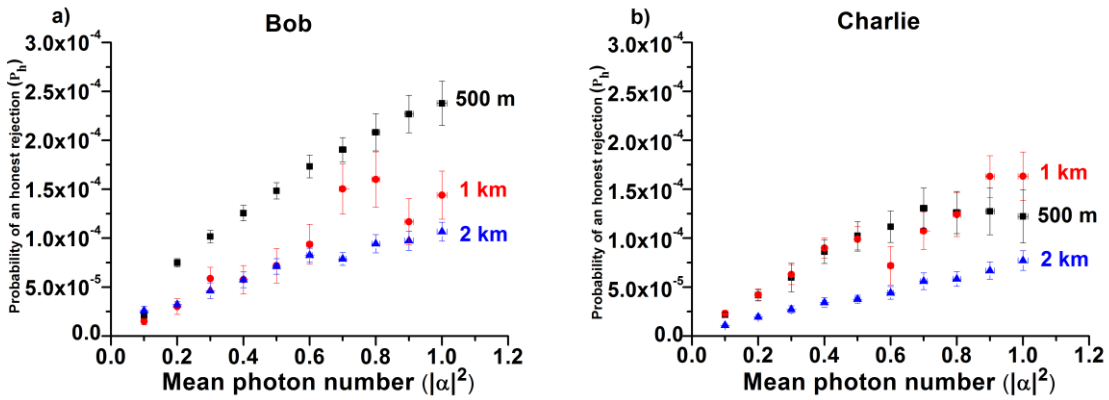


Figure 5.10– Average probability of an honest rejection, P_h, by Bob (a) and Charlie (b). P_h is directly related to the visibility of the interferometers which had a threshold visibility threshold setting of 94% on them.

As described in the previous Chapter's security analysis, the Guad is only a superficial value for the advantage a receiver has over a malicious attack, as a malicious party can perform some state distinguishing measurement(s) on photons sent by Alice. If there are a greater number of photons available for this distinguishing measurement then a malicious party can identify the state sent by Alice more accurately [40]. This is called the minimum error measurement P_{min} and is a correction factor which can be applied to Guad to give a more realistic advantage called the gap, g.

The minimum error measurement was discussed at the start of this Chapter in relation to the magnitude of the correction value. The formulations are the same for this Chapter as the previous, so to save repeating, the functions can be found at Equation 4.11. When $|\alpha|^2 \rightarrow 0$, $P_{min} \rightarrow 0.75$, when $|\alpha|^2 \rightarrow \infty$, $P_{min} \rightarrow 0$. This trend can be seen from Figure 5.1. For the experimental range of $|\alpha|^2$ used in this Chapter, an enlarged region of Figure 5.1 is shown in Figure 5.11. The P_{min} value for each $|\alpha|^2$ is indicated by the stars, and the trend is given as the dashed line, which decreases as the $|\alpha|^2$ increases. For the $|\alpha|^2 = 0.5$ used as the example, the P_{min} is 0.262.

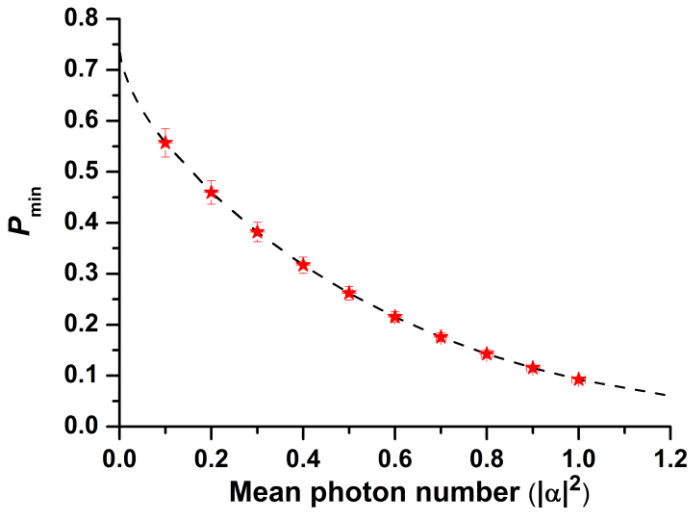


Figure 5.11 – The minimum error in a measurement for a malevolent party, $P_{min.}$ The relation of P_{min} to the $|\alpha|^2$ used by Alice in the QDS protocol can be seen.

The gap is created simply by multiplying the correction factor P_{min} by the Guad value from the experimental data, Equation 5.8. The values for the gap, for Bob and Charlie, are shown in Figure 5.12 a) and b) respectively, for each distance performed. As hypothesised from earlier analysis, the gap does indeed have an optimum value, due to nature of the P_{min} and Guad with $|\alpha|^2$. The value of the optimum gap ranges from $|\alpha|^2 = 0.4$ to 0.5. Therefore it is around the same value as the estimated optimised value from the beginning of this Chapter which was $|\alpha|^2 \approx 0.5$.

$$g = P_{min} \times \text{Guad} \qquad \text{Equation 5.8}$$

In the previous two implementations of QDS [4], [5], knowledge of the gap was sufficient information for the signature half-bit length to be calculated. This is because only Bob (or Charlie) was ever experimentally tested due to the high loss of one of the multiport outputs. Now that two receivers are being analysed, more processing needs to be performed to calculate L, as it must be equal for both parties. In simple terms, this is undertaken by, essentially, comparing the resulting values for each receiver and taking the worst-case scenario for the protocol.

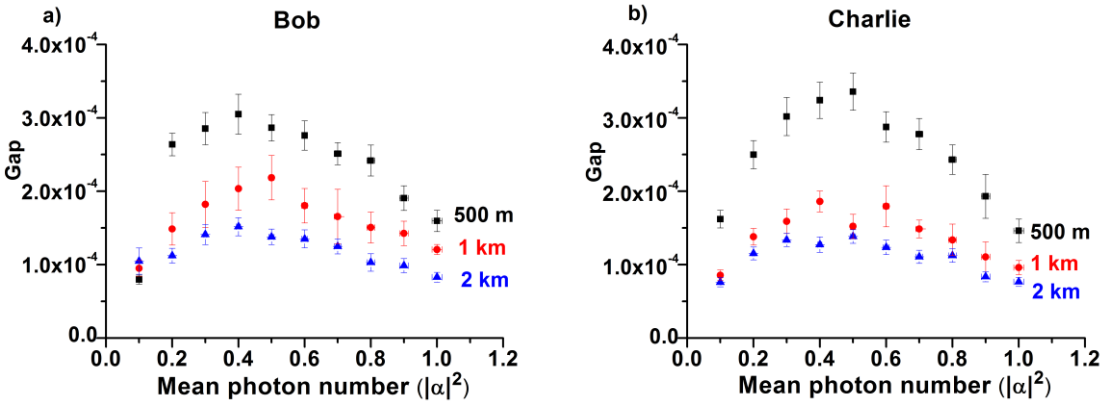


Figure 5.12 – The gap, g, for Bob (a) and Charlie (b) over the three distances measured. The optimised gap would be when it is maximal, i.e. the largest amount of advantage over a malicious attack.

The first new parameter is called the robustness of the protocol, which is directly related to P_h, as shown Equation 5.9. The maximum value of P_h for either receiver is taken as the robustness of the protocol, i.e. the matrix which has the highest diagonal elements (lowest maximum to minimum visibility) on average for a given $|\alpha|^2$. P_h is the probability that a

receiver will honestly eliminate a state actually sent by Alice. By taking the largest of the two values of P_h (Bob's P_h^B and Charlie's P_h^C), the protocol is taking into account the worst-case scenario where a malicious forging attack could have more signature elements accepted by the legitimate parties.

The robustness for the protocol is shown in Figure 5.13, and for the example $|\alpha|^2 = 0.5$, the value is 1.48×10^{-4}. This value is the P_h value from Bob, who had, on average higher diagonal elements. Robustness is the worst-case scenario of a forger getting an incorrect element accepted based on the measurement device alone.

$$\text{Robustness}=\text{Max}\left[P_h^B , P_h^C\right] \qquad \text{Equation 5.9}$$

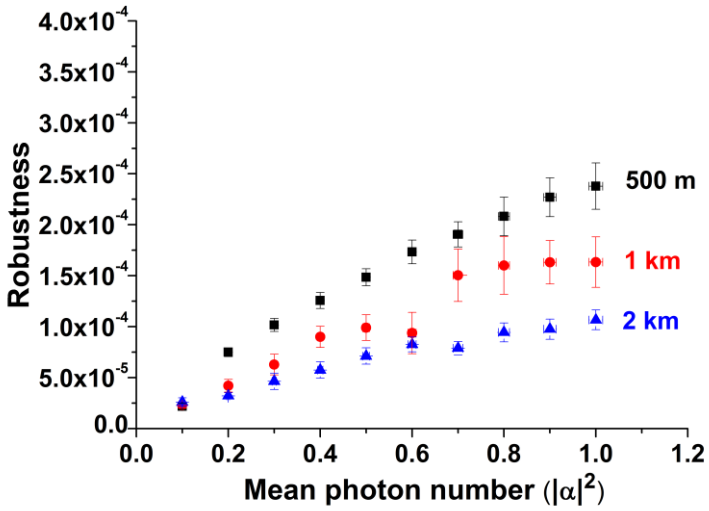


Figure 5.13- Protocol robustness. The worse-case scenario for a forger to get a guessed element accepted. It increases with $|\alpha|^2$ as the diagonal elements of the cost matrix increase in value.

Another new parameter is forge, the relation with $|\alpha|^2$ can be seen in Figure 5.14; for distances of 500 m and 2 km it has a maximum value at $|\alpha|^2 = 0.5$, while at 1 km the maximum occurs at $|\alpha|^2 = 0.4$, but the value with increasing $|\alpha|^2$ drops slightly and increases again after $|\alpha|^2 = 0.6$. Forge is the minimum off-diagonal element based on the diagonal average and the gap. The worst-case scenario is for forge is the smaller value of the receivers, Equation 5.10.

$$\text{Forge} = \text{Min}\left[P_h^B + g^B,\ P_h^C + g^C\right] \qquad \text{Equation 5.10}$$

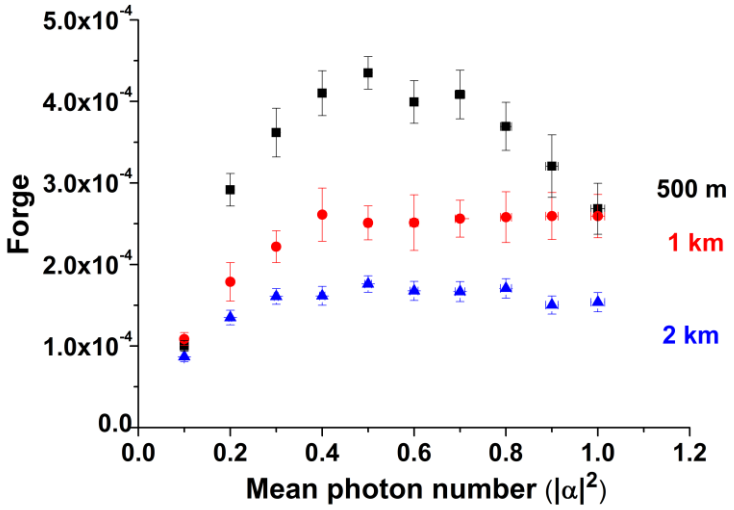


Figure 5.14- Protocol forging. The value is dependent on the diagonal minimum elements of the cost matrix and the gap. The diagonal elements increase with $|\alpha|^2$ while the gap has a shape shown in Figure 5.12.

The final new parameter required to calculate the signature half-bit length is the effective gap, g_{eff}, given in Equation 5.11. This gives the gap in a worst-case scenario for the two receiver protocol. The effective gap, similar to the gap, has an optimum value where it is largest, i.e. where the protocol will perform the best, and occurs at a $|\alpha|^2 = 0.4$ on average, which is a lower $|\alpha|^2$ than for the gap which occurred at $|\alpha|^2 = 0.5$.

$$g_{\text{eff}} = \text{Forge} - \text{Robustness} \qquad \text{Equation 5.11}$$

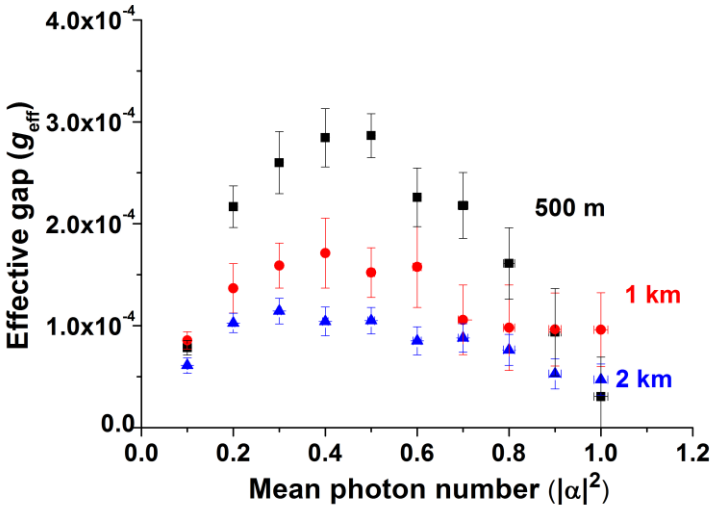


Figure 5.15 - Effective gap for the quantum digital signatures experiment, which takes into account the worst-case scenario for the protocol.

The signature half-bit length, previously given in Equation 5.6, is modified to replace the gap, g, with the effective gap, g_{eff} in Equation 5.12. This is done to give L for the worst case scenario across both receivers in this protocol, rather than just an L for a single receiver as was the case in both QDS protocols previously demonstrated. The signature half-bit length as well as being dependent on experimentally generated parameters is also dependent on the level of security selected for the protocol, which is the probability that a malicious activity will be performed successfully.

$$L = -\frac{\ln\left(\frac{\text{Security level}}{2}\right)}{\left(\frac{g_{\text{eff}}}{4}\right)^2} \qquad \text{Equation 5.12}$$

Figure 5.16 shows the signature half-bit length for the worst-case scenario of the experimentally realised protocol. As in previous protocols, the L has been calculated for a security level of 0.01%, which is shown in a) for the various distances used in this realisation. The change in L with different security levels was also investigated, with b), c) and d) being L for 500 m, 1 km, and 2 km respectively.

Signature half-bit length is dependent on the effective gap, which in Figure 5.15 was seen to be of a largely negative parabolic shape, leading to the generally parabolic shape of the

length with $|\alpha|^2$. The optimised gap is said to be the largest value, while in the case of the length, the smallest value is optimised case. Between $|\alpha|^2$ of 0.4-0.5 is where the optimised case would be, from the trend in data. In Figure 5.16 a) at 500m, $|\alpha|^2$ 0.1, 0.9, and 1 are affected by the non-linear response of the detector due to detector dead-time and count rate.

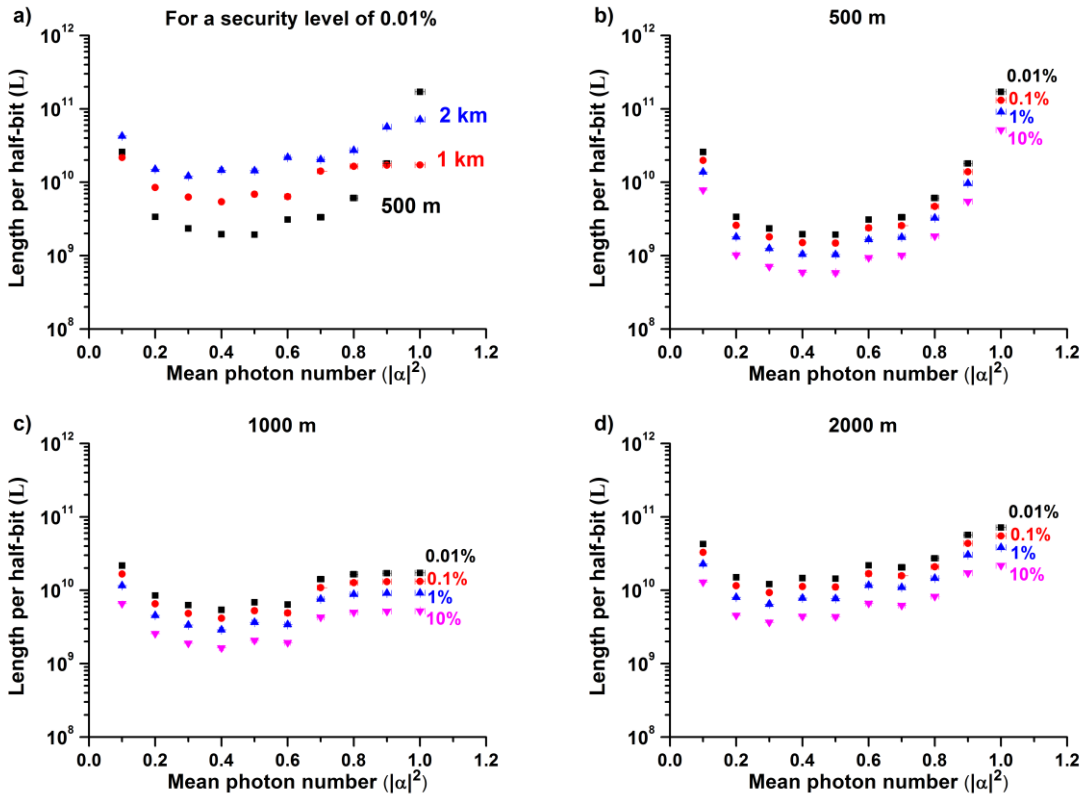


Figure 5.16 – The signature half-bit length L for the quantum digital signature protocol. a) The length comparison for distances for a security level of 0.01%. Length comparison for b) 500m c) 1km and d) 2 km at variety of different security levels.

Arguably the most important property of a secure communications system is an estimate of how long it would take for someone to send a secured signal. In our case that is the time taken to generate a signature of the required length *L*. As can be expected the time taken is strongly dependent on Alice's clock rate. The analysis of the results presented Collins *et al.* [4] suggests a time of >8 years for the signature to be sent, however this was calculated for a receiver to measure the number of signature elements, *L*, based on their USE rate. However, in the protocol, a receiver does not need to measure all the signature elements in

order for the protocol to work, if they do not make a measurement, they take note and ignore the element in the classical signature sent by Alice later. Therefore the time which is important is how long it would take Alice (the sender) to send the number of signature elements, which is based on the clock rate of Alice.

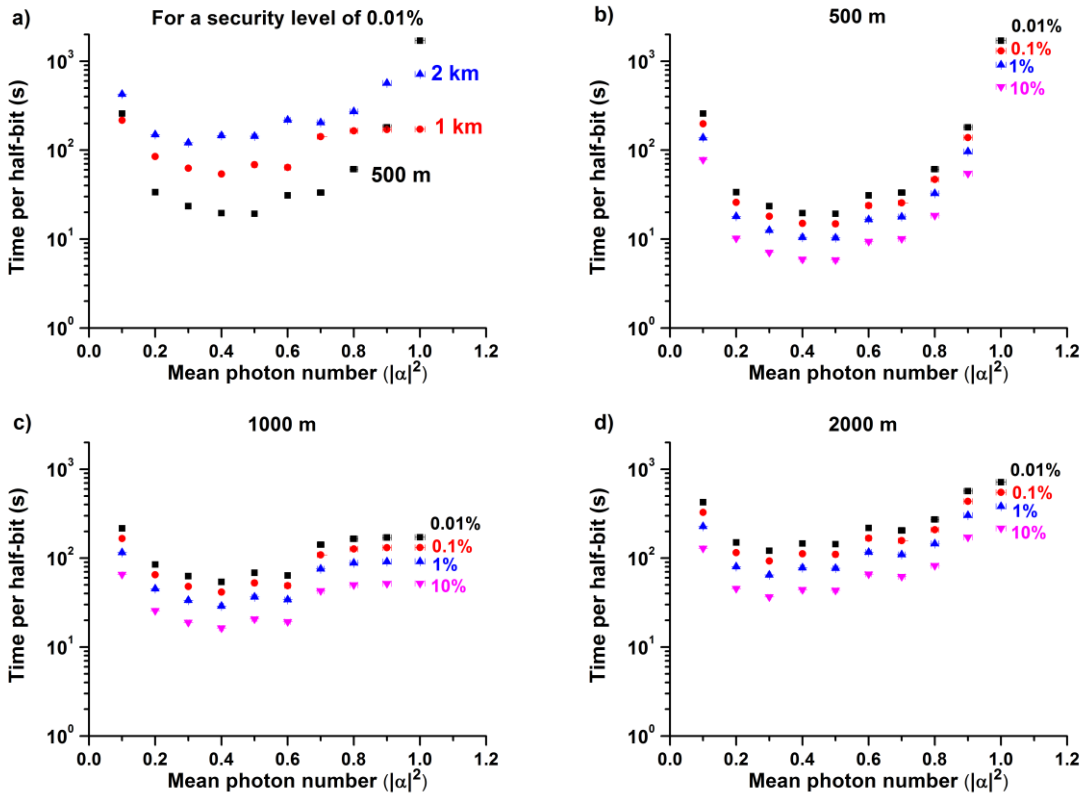


Figure 5.17 - The time taken for Alice to send one half-bit for the three distances tested at a security level of 0.01%. b), c) and d) are times taken for 500 m, 1 km, and 2 km respectively, for different security levels.

Figure 5.17 shows the time taken for Alice to send a signature half-bit, which is the signature half-bit length divided by Alice's clock rate of 100 MHz. Figure 5.17 a) shows a comparison of the times to send at different distances for a security level of 0.01%. Figure 5.17 b), c), and d) show the change in time with different security levels, at 500 m, 1 km, and 2 km respectively. The optimised values of $|\alpha|^2$ are the same for the time-taken as they are for the signature half-bit length, as the only difference is the division by 100 MHz.

5.4 Discussion and conclusion

At this stage it would be good to compare the past QDS experiments to the one presented in this Chapter. Table 5.1 gives some of the main parameters of interest for each experimental realisation, such as the range of $|\alpha|^2$, the transmission distance , the gap, signature half-bit length and the time taken (in seconds) for Alice to send a half-bit.

Protocol	$\|\alpha\|^2$ range	Distance range (metres)	Gap	Length (Elements)	Time to send half-bit (s)
Multiport and quantum memory [5]	0.04-0.28	≈5	8.03×10^{-4}	6.91×10^{7}	0.691
Multiport and USD/USE [4]	1-11.5	≈5	1.20×10^{-6}	5.13×10^{13}	5.13×10^{5}
Kilometre ranges with USD/USE [21]	0.1-1	≈2,000	2.84×10^{-4} (500 m)	1.93×10^{9}	19.3

Table 5.1 – Comparison of all the experimentally realised quantum digital experiments to date.

It can be seen from Table 5.1 that the first experimental implementation exhibits the shortest time taken to transmit the signature, albeit over a short distance of 5 m. This is due to two fundamental reasons. One is that the $|\alpha|^2$ range is very low, 0.04 to 0.28 in the experiment, meaning that the $P_{\min}$ values (0.64 to 0.4) are larger than the range used in the other experiments. This leads to a larger gap than the other protocols. Another reason is the use of phase modulator to decode the coherent states rather than passive USE measurements. This allows a better cost matrix to be generated, because if Alice is not sending phases which are 100% non-orthogonal, a receiver can compensate their measurement for greater visibility and consequently achieve better relative minima on the diagonal elements, while USE can only use what it is sent by Alice. However, the first experimental protocol required QM for it to work in a real set-up, making this approach unrealistic for application using current technology [1]–[3].

The second experimentally realised QDS protocol solved the problem of relying on QM, however the performance in terms of the time taken to generate the signature, was not

equal (or close) to the first experimental protocol which covered the same distance (≈5 m). This was due to the range of $|\alpha|^2$ used in the experiment (1 to 11.5), originally chosen to increase the unambiguous state discrimination rate, which required three photon correlations. However, this led to very small values of $P_{\min}$, meaning any benefits in increased detection rate led to a smaller gap. This also led to a large half-bit signature length and therefore time taken for Alice to send. In hindsight, a smaller range of $|\alpha|^2$ would have been better for showing the performance of the system. This would have been further improved when USE was adopted in later analysis to improve success rates. Although the second experimentally realised protocol did not require QM for operation, it did however still rely on the multiport, which limited the distance over which QDS can be carried out due to increased loss of the optical systems and the necessary proximity of Bob and Charlie in the shared interferometer scheme.

The experimentally realised protocol presented in this Chapter was designed to increase the distance over which QDS can be performed. This was achieved by performing the swap and comparison mechanism classically, rather than requiring the multiport to perform the action optically. This allowed greater distances of 500 m, 1 km, and 2 km to be demonstrated. The experimental hardware is akin to that used in QKD experimental systems, therefore potentially opening up QDS to application by existing systems. The experimental operation of the kilometre range QDS system itself benefited from a review of the previous system in the choice of $|\alpha|^2$ range. The range was also chosen as it included $|\alpha|^2$s generally used by QKD decoy state experiments [41].

QDS has been shown to be possible over kilometre distances, without the requirement for any complicated and high loss quantum technologies such as the QMs or the optical multiport. An optimised signature half-bit length at 500 m was found to be 1.93×10^9 for $|\alpha|^2 = 0.4$, taking Alice ≈19.3 s to send to a receiver.

5.5 Future work & improvements

In terms of future work there are several things to consider in moving forward from the QDS protocol presented in this Chapter. The choice of operating wavelength and the implementation of more efficient protocols are the main scope for moving forward with QDS, since we can perform the swapping mechanism classically in post processing.

As in all quantum informational experiments wavelength is an important property to consider when building an experimental quantum digital signature system, as it will determine the overall performance of a system. For instance, at an operational wavelength of 850 nm, there are a range of readily available sources, as well as silicon-based single-photon detection technologies that can be used [39], [42]. The disadvantage of 850 nm when used in fibre-optics communication with standard telecommunications fibre is the increased loss of 2.2 dB/km, making long distance implementations much more difficult.

Switching to a wavelength of 1550 nm or 1310 nm would (in principle) allow for an increase in distance due to the low loss of 0.2 dB/km using standard telecommunication optical fibre. However, the semiconductor-based single-photon detector technologies available at these wavelengths tend to have poorer performance in terms of reduced detection efficiencies, higher dead-time, a greater after-pulse probability and increased dark count rates, although improvements are always being made in technologies such as InGaAs/InP SPADs and superconducting nanowire single photon detectors [42], [43]. Currently the longest QKD implementations are all featured at 1550 nm [17], and if QDS protocols can be carried out using QKD hardware (as has been shown in this Chapter), then 1550 nm would be the obvious choice of wavelength to develop the next generation of QDS.

Throughout all the QDS protocols, analysis and generation of the signature half-bit length has come from the cost matrix. One of the key features in the cost matrix is the difference between the highest diagonal element, and the lowest off-diagonal element, as they are what really determine the signature half-bit length. The reason why they are not 50% can be narrowed down to two main factors, imperfect phase preparation by Alice, and the detection method used by a receiver.

It was found through basic simulations of phase preparation and imperfection of BSs that the optimised signature half-bit length could be reduced by around 50% by improving the phase preparation and visibility of the QDS experimental system. So any future QDS systems will have more consideration given to these properties during the design, assembly and calibration stages.

As well as general experimental improvements, new QDS protocols which improve the efficiency of QDS are currently in development [44]. This Chapter has shown that the use of a classical post-selection swap and comparison mechanism is possible, then this approach must be used if QDS is to be used at meaningful distances.

The next step for QDS is towards implementation of more efficient protocols allowing for greater distances to be covered. This protocol was presented by Amiri *et al.* in [44], which makes use of a decoy state BB84 based protocol with some adjustments to the post-processing (no need for error correction or privacy amplification) and propagation direction of quantum channel.

5.6 Acknowledgements

Dr Vedran Dunjko, Dr Petros Wallden, and Professor Erika Andersson developed the original protocols for QDS at kilometre ranges [16]. Mr Ryan Amiri analysed the results with help from the author and refined the security analysis with Vedran, Petros, and Erika. Dr Robert J. Collins helped in the optical design, and initially created the programs for acquiring and initially analysing data.

5.7 Bibliography

[1] A. I. Lvovsky, *et al.*, "Optical quantum memory," *Nat. Photonics*, vol. 3, no. 12, pp. 706–714, Dec. 2009.

[2] C. Simon, *et al.*, "Quantum memories," *Eur. Phys. J. D*, vol. 58, no. 1, pp. 1–22, Apr. 2010.

[3] F. Bussières, *et al.*, "Prospective applications of optical quantum memories," *J. Mod. Opt.*, vol. 60, no. 18, pp. 1519–1537, Oct. 2013.

[4] R. J. Collins, *et al.*, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[5] P. J. Clarke, *et al.*, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light.," *Nat. Commun.*, vol. 3, p. 1174, Jan. 2012.

[6] K. F. Reim, *et al.*, "Towards high-speed optical quantum memories," *Nat. Photonics*, vol. 4, no. 4, pp. 218–221, 2010.

[7] P. Wallden, *et al.*, "Minimum-cost quantum measurements for quantum

information," pp. 1–19, Dec. 2013.

[8] E. Andersson, *et al.*, "Experimentally realizable quantum comparison of coherent states and its applications," *Phys. Rev. A*, vol. 74, no. 2, p. 022304, Aug. 2006.

[9] V. Dunjko, *et al.*, "Quantum Digital Signatures without Quantum Memory," *Phys. Rev. Lett.*, vol. 112, no. 4, p. 040502, Jan. 2014.

[10] J. Noda, *et al.*, "Polarization-maintaining fibers and their applications," *J. Light. Technol.*, vol. 4, no. 8, pp. 1071–1089, 1986.

[11] Nufern, "Polarization Maintaining Short Wavelength Fibers." Nufern, East Granby, Connecticut, USA, 2013.

[12] Fiber-Optics.Info, "Connector Loss Test Measurements," *Fiber-Optics.Info*, 2015. [Online].Available:http://www.fiberoptics.info/articles/connector_loss_test_measurements. [Accessed: 10-Sep-2015].

[13] W. H. Steel, *Interferometry*, 2nd ed. Cambridge University Press, 1985.

[14] C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km.," *Opt. Lett.*, vol. 20, no. 16, p. 1695, Aug. 1995.

[15] K. Mochizuki, "Degree of polarization in jointed fibers: the Lyot depolarizer," *Appl. Opt.*, vol. 23, no. 19, p. 3284, 1984.

[16] V. Dunjko, *et al.*, "Quantum digital signatures with quantum key distribution components," *Phys. Rev. A*, vol. 89, no. 4, p. 022336, 2014.

[17] B. Korzh, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[18] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[19] F. E. Becerra, *et al.*, "Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states.," *Nat. Commun.*, vol. 4, no. May, p. 2028, Jan. 2013.

[20] M. Sasaki, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network.," *Opt. Express*, vol. 19, no. 11, pp. 10387–409, May 2011.

[21] R. J. Donaldson, *et al.*, "Experimental demonstration of kilometer-range quantum digital signatures," *Phys. Rev. A*, vol. 93, no. 1, p. 012329, Jan. 2016.

[22] R. J. Collins, *et al.*, "Supplementary information for Optical realisation of Quantum

Digital Signatures without quantum memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[23] P. J. Clarke, *et al.*, "Supplementary material: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nat. Commun.*, vol. 3, p. 1174, Nov. 2012.

[24] E. Andersson, *et al.*, "Experimentally realizable quantum comparison of coherent states and its applications," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 74, no. 2, pp. 1–11, 2006.

[25] Corning Incorporated, "Corning ® SMF- 28 e +® LL Optical Fiber," 2011.

[26] Thorlabs, "Manual Fiber Polarization Controllers User Guide," *Rev E*, 2014.

[27] D. Gottesman and I. Chuang, "Quantum Digital Signatures," *arXiv.org*, no. 0105032v2, 2001.

[28] M. Cramer, *et al.*, "Efficient quantum state tomography," *Nat. Commun.*, vol. 1, no. 9, p. 149, 2010.

[29] Thorlabs, "Single Mode Fiber : 450 to 600 nm Description," 2013.

[30] Novatech Instruments Inc, "Models 2960AR and 2965AR Disciplined Rubidium Frequency Standards," pp. 1–8, 2004.

[31] Agilent Technologies, "Agilent 8648A / B / C / D Signal Generators Spectral purity Internal reference oscillator," no. March 2007, 2012.

[32] Picoquant, "HydraHarp 400 Single Photon Counting System User's Manual and Technical Data," vol. 1.2.

[33] Photline, "NIR-MPX800 series phase modulator," 2010.

[34] Avtech Electrosystems Ltd., "AVX-SP AND AVX-CP SERIES."

[35] Mathworks, "MATLAB 2014b (8.4.0.118713)." The MathWorks Inc., Natick, Massachusetts, 2014.

[36] H.-K. Lo, *et al.*, "Decoy state quantum key distribution.," *Phys. Rev. Lett.*, vol. 94, no. September 2004, p. 230504, 2005.

[37] W. Tittel, *et al.*, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[38] K. J. Gordon, *et al.*, "A short wavelength GigaHertz clocked fiber-optic quantum key distribution system," *IEEE J. Quantum Electron.*, vol. 40, no. 7, pp. 900–908,

Jul. 2004.

[39] Perkin-Elmer Optoelectronics, “SPCM-AQRH Single Photon Counting Module,” *Perkin-Elmer Optoelectron. Datasheet*, pp. 1–10, 2002.

[40] N. Lütkenhaus and M. Jahma, “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack,” *New J. Phys.*, vol. 4, pp. 44.1 – 44.9, Jul. 2002.

[41] A. R. Dixon, *et al.*, “Continuous operation of high bit rate quantum key distribution,” *Appl. Phys. Lett.*, vol. 96, no. 2010, pp. 2008–2011, 2010.

[42] M. D. Eisaman, *et al.*, “Invited review article: Single-photon sources and detectors.,” *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, Jul. 2011.

[43] G. S. Buller and R. J. Collins, “Single-photon generation and detection,” *Meas. Sci. Technol.*, vol. 21, no. 1, p. 012002, Jan. 2010.

[44] R. Amiri, *et al.*, “Secure Quantum Signatures Using Insecure Quantum Channels,” *arXiv*, no. 1507.02975, Jul. 2015.

Chapter 6

Review of Conventional and Quantum Amplification

6.1 Introduction

Quantum key distribution (QKD) requires the use of either single photon sources, or highly attenuated coherent sources which are typically reduced to a mean photon number per pulse ($|\alpha|^2$) of <0.5, in order for the protocols to remain secure against eavesdropper attacks. This requirement inhibits the maximum transmission distance that can be achieved by QKD and other quantum communication protocols, such as quantum digital signatures (QDS), since a quantum channel will necessarily have a significant transmission loss, and any optical loss will greatly affect the performance of quantum communication protocols.

For example, if the quantum channel loss is at least equal to the fraction of states an eavesdropper could be expected to perturb then a loss-less beamsplitter attack becomes possible (see Chapter 3 for details of this attack). This problem is not limited to quantum communication – the intensity of the transmitted light drops exponentially with transmission distance so conventional forms of communication are also affected. However, one major difference between the conventional and quantum communication is that conventional signals can be amplified to counteract the losses in the communication channel to be overcome. Although such amplifiers operate with a high fidelity (unity fidelity means the output properties are equal to the input) on conventional signals, use of such amplifiers in the quantum protocols, even if they do amplify the quantum state, would swamp the quantum signal with deterministic noise [1] and spontaneous emission from the amplifying process [2].

This Thesis has focused on optical communication through optical fibre cables, and the Chapters on quantum amplification will also concentrate on use of optical fibres. Figure 2.10 in Chapter 2 showed the percentage of the original signal intensity as a function of transmission distance in silica optical fibre. It can be seen that eventually the intensity reaching a receiver would be too low for a receiver to distinguish what is being sent. To overcome this problem conventional amplifiers are used to boost the signal which can

increase the maximum transmission distance. These amplifiers are generally placed every 30-60 km [3].

Quantum communication protocols are designed to utilise the fact that an unknown quantum state cannot be cloned deterministically without introducing noise or error [4], [5]. If we consider a classical laser pulse signal, composed of a large number of photons, it seems strange that while quantum mechanics tells us we cannot clone a quantum state perfectly, we can amplify classical signals with a high fidelity. Optical noise is added to the conventional signal when it is amplified, however the intensity of noise added is small relative to the gain of the signal- whereas the introduced noise would be comparable or greater than the quantum signal intensity.

Telecommunications systems can transmit over vast distances, and intercontinental (typically >1 500 km) transmission distances are achievable due to the use of all-optical amplifiers [6]. So far the furthest QKD experiment has been shown at 307 km [7], the improvements in transmission distance over the past few years have primarily been due to improvements in single-photon detector technology [8] rather than protocol improvements. However the T12 protocol, introduced by Toshiba is one protocol which is said to show improvements by implementing asymmetric basis set choice [9]. The relatively short transmission distance, in comparison to conventional telecommunications, is due to the quantum channel loss limitation, therefore any hope of intercontinental range will require a quantum amplifier/repeater, or radically different QKD/QDS protocols, where the bit rate does not fall off exponentially with distance. One way to combat this is to introduce low earth orbit satellites as transmission nodes, which can then interact with different ground-stations as the satellite orbit permits. However, there are many issues to be solved before an implementation is shown [10], [11].

6.2 Conventional optical amplifiers

In the early/mid 20th Century, many long distance (10-1000s of metres) communications were transmitted electronically via copper wire [12]. Electrical signals transmitted through copper wires have several benefits, such as potentially allowing a device to extract power for operation from the signal, and relatively cheap electronic components. However, the continuing growth in demand for bandwidth (bit rate) on these communication services led to a search for an alternative that offered a higher bandwidth [12].

After the invention of the laser in the 1960's [13], it was envisioned that these highly collimated monochromatic light sources could be used to transmit information using modulated light pulses. Development into low loss optical fibre systems was a major area of research which led to telecommunications today being performed at wavelengths around 1310 nm and 1550 nm because of the low-loss windows in silica glass [14]. A generic schematic of optical fibre communication line is shown in Figure 6.1.

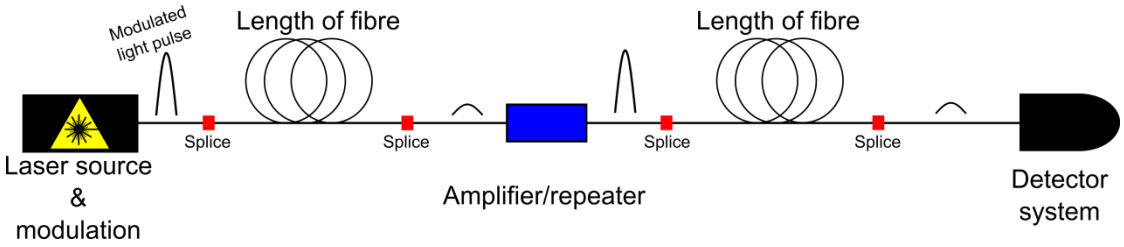


Figure 6.1 – Schematic of optical fibre communication line. Modulated light pulses are sent through a communication channel made up of several km of fibre to a receiver. After 30-60 km, due to losses inherent from the optical fibre and splices/connections the signal is amplified/repeated either by measure and resend, or optical amplifier methods.

Up until the early 1980's, repeater systems had been based on a measure and resend principle, where the optical signal is converted into an electrical signal (measured), electrically amplified, and used to re-modulate the original signal properties onto a new higher intensity laser pulse generated by a local laser source [3]. Although considered vital at the time, this measure/resend amplifier limits the bandwidth of the transmission because of the need for electronic circuitry for conversion/analysis. All-optical amplifiers, which do not require the conversion of the optical signal into an electrical pulse and then back again, were seen as a way to improve the bandwidth of a long-haul communications line.

Classical electromagnetic theory tells us that an electric-field E can be copied into a larger intensity signal gE, where g is the gain factor and is > 1[15]. The only limitation on this gain factor is the saturation of the gain medium, as the amplifier only has limited energy available.

System → / Feature ↓	**Semiconductor Optical Amplifier** [16], [17]	**Erbium-doped Optical Fibre Amplifier** [2], [16], [18]	**Raman Optical amplifier** [6], [19]
Maximum internal gain (dB)	30	30 - 50	30 (normally 10-15 to reduce Rayleigh scatter gain (amplified noise))
Insertion loss (dB)	6 - 10	0.1 - 2.0	≈1 (for circulator)
Polarisation sensitive	Weak	No	Yes
Pump	Electrical	Optical	Optical
Nonlinear effects	Small	No	Yes
Intrinsic noise (dB)	7 - 12	3 - 5	<5.5 (depending on gain)
Noise type	Amplified Spontaneous Noise (ASE)	ASE	ASE, phonon stimulated, double Raleigh scatter (leading to gain of ASE), short life-time of upper-state
Notes	Low cost, with signal distortion, and mode coupling problems for multimodal fibre optics..	Needs special fibre for integration.	No special fibre needed, as regular fibre shows nonlinear properties. Requires low temperature and can be expensive.

Table 6.1 – Summary of classical amplifiers reviewed in this Chapter.

Optical amplifiers use stimulated emission of an excited gain medium to increase the optical power of the signal pulse. The gain medium for an optical amplifier could be doped fibre/crystal or a semiconductor material, excited by a pump source (optically or electrically) just before the expected arrival time of a signal pulse. The incoming pulse causes stimulated emission of the excited elements, amplifying the pulse in a similar way to a laser. The process for stimulated emission can, however, also add noise to a signal due to spontaneous emission, which can then be amplified at a proceeding amplifier. In conventional optical signals this noise does not impede state distinguishability because the intensity of noise added is small in comparison to the signal intensity. However, in the case of quantum signals the introduced noise is comparable (or even greater) in intensity to

the signal. The introduction of spontaneous emission into the signal is one of the main reasons why conventional amplifiers are not suitable for quantum state amplification [4].

The three main contenders for optical amplifiers are semiconductor optical amplifiers [16], [20], rare-earth-metal doped fibre amplifiers (such as erbium-doped [2], [18], [21], [22]) and Raman amplifiers [19]. As with all technologies, each method has its own merits and demerits.

A semiconductor optical amplifier can be an inexpensive approach, however there can be some signal degradation from Fabry-Pérot resonances in the device [16]. The rare-earth-metal doped fibres may be sought after where amplifiers are required and the optical fibre is easily accessible, such as a local exchange [2]. A Raman optical amplifier has the greatest benefit in intercontinental and sub-sea applications where the installation is more permanent and inaccessible because it can use the standard optical fibre as a gain medium rather than requiring specialised components. A summary of the main features of these optical amplifiers is given in Table 6.1.

Conventional all-optical fibre amplifiers have benefited the telecommunication industry greatly, allowing an increase in bandwidth and transmission distance. Added noise can be an issue, but conventional detector systems can usually discriminate the signal over the noise, because generally the noise intensity is still much lower in comparison to the signal, typically by several 10's of decibels [6].

The gain of conventional linear amplifiers can be determined by a gain coefficient γ which is dependent on the gain medium and wavelength to be amplified [19]. If the gain medium operates as a linear amplifier the total gain G is determined by $G = \exp(\gamma L)$, where L is the length of the gain medium [23].

The amount of noise added to a signal is determined by the amplifier noise figure F_n seen in Equation 6.1, where SNR is the signal to noise ratio of the input and out signals [23], [24]. The ratios of signal to noise can be shown to be $2-(1/G)$ for coherent states [25]. Equation 6.1 is the general equation for the noise figure of a linear amplifier in decibels (a commonly used unit in telecommunications).

$$F_n = 10\log_{10}\left(\frac{SNR_{in}}{SNR_{out}}\right) \approx 10\log_{10}\left(2-\left({}^{1}/_{G}\right)\right) \qquad \text{Equation 6.1}$$

Equation 6.1 for large G gives a limit of 3 dB (approximately equal to a factor of 2) this means that of the total signal, 3 dB of that will be noise. This means that the signal to noise ratio of the output is small than that of the input. Optical amplifiers generally operate at G ≥30 dB, and from 6.2 it can be seen that even at G = 25 dB the noise figure will be very close to the 3 dB limit value.

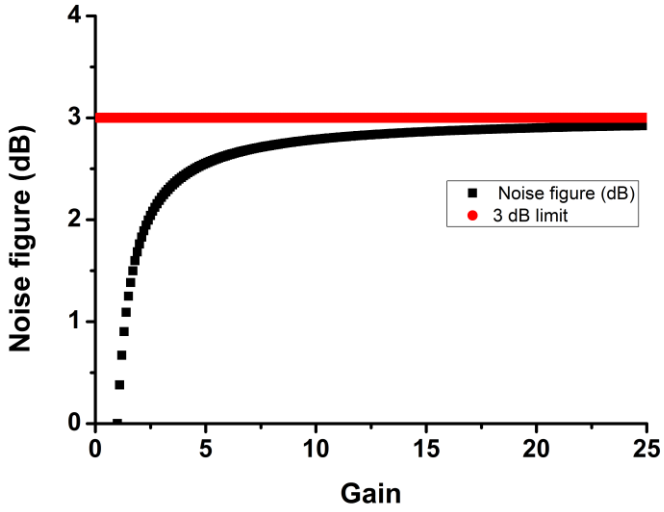


Figure 6.2 – The noise figure for a linear optical amplifiers approaching 3 dB as gain value increases.

Nonlinear optical amplifiers, such as the Raman amplifier, have higher noise figures than linear amplifiers because of a term in the noise figure which integrates over the length of the fibre. The more active length the Raman amplifier has, the larger the noise figure become which is generally >3 dB [26].Therefore there during the optical amplification there is inherent noise added to a signal using a conventional optical amplifier. The amount of noise is dependent on the gain of the amplifier, and whether it is linear or nonlinear in operation.

6.3 Quantum amplification and repeaters

As with conventional signals, it would be beneficial to be able to amplify quantum states for either communication purposes, or even to boost the number of photons before a

measurement. Increasing the amplitude of a state $|\alpha\rangle$ linearly would give $|\alpha\rangle \rightarrow |g\alpha\rangle$, where g is a gain factor >1. This is unphysical for quantum mechanics as doing this deterministically will violate the no-cloning theorem [5]. Following on from that it was shown that amplifying a quantum signal in a linear way would give a noise figure g^2-1 [1].

While noiseless deterministic cloning is not possible, the quantum-information community has instead been working on probabilistic, non-deterministic cloning methods, based on post-selection of data. This idea was first presented in 2008 by T.C. Ralph and A.P. Lund to provide quantum amplifiers and repeaters for quantum key distribution [27]. Post-selected nondeterministic amplifiers and repeaters are probabilistic devices because a party cannot know if the quantum state has been amplified until certain conditions have been met, normally through the presence or absence of detection events. Therefore a party cannot predict whether the conditions for successful amplification will be met until the process has actually happened. This is different from conventional deterministic amplifiers and repeaters which are expected to be able to amplify correctly on demand. This probabilistic condition of the amplifier limits the noise that can be added to the signal during the amplification process.

Figure 6.3 shows the phasor diagram for the possible amplification processes that could occur for coherent state. A conventional optical amplifier will add noise to the amplified signal based on the gain of the amplifier creating a noisy state.

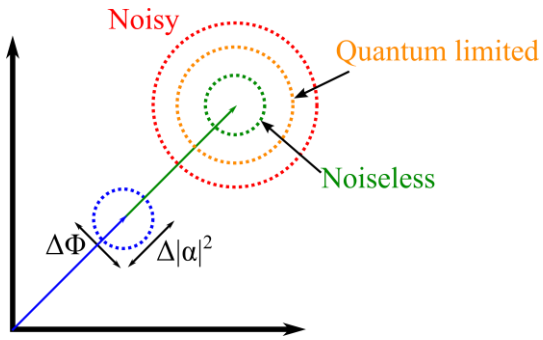


Figure 6.3- Phasor diagram for the amplification of a coherent state. Ideally a noiseless amplifier would not increase the minimum amount of noise a coherent state. The quantum limited amplifier amplifies the minimum noise and introduces additional noise. A conventional optical amplifier adds more noise on top of the quantum limited case. [28]

At this stage it is worth noting the difference between a quantum amplifier and repeater, which in this thesis is primarily determined by the configuration of the system, although there are no formal definitions outside this Thesis in regards to quantum amplifiers. If the mode of increasing the maximum transmission distance possible is performed by adding photons into the signal in some way, meaning the original optical signal from Alice is a constituent of what reaches Bob, then this can be classed as an amplifier. If the original signal from Alice is used to make a measurement at some point in the transmission channel and the measurement outcome reaches Bob, then the device can be classed as a repeater. Repeaters generally operate using entangled pair sources. A comparison between example amplifier and repeater systems is shown in Figure 6.4 a) and b) respectively.

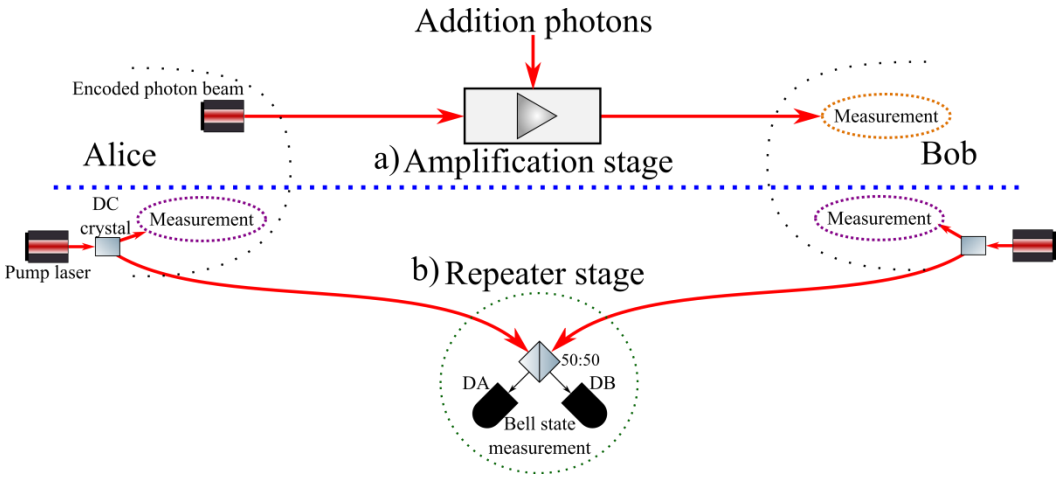


Figure 6.4 – a) A schematic for a quantum optical amplifier. b) A schematic for a quantum optical repeater

There are several methods which can be used in quantum amplification protocols for non-deterministic amplification, including: photon addition and subtraction; quantum scissors; and entanglement swapping. The photon addition and subtraction protocols are classed as amplifiers because of the addition of photons to the original signal, while the quantum scissors and entanglement swapping devices are classed as repeaters because they measure the original signal at the node. Each method is described, giving experimental methods, recent publications and a summary of advantages/disadvantages.

6.3.1 Photon addition and subtraction

Photon addition and subtraction devices are relatively simple devices to understand. As the name suggests, the original signal from Alice has photons added to it in some way. After the addition process, a subtraction stage uses a low reflectivity beamsplitter (BS) to subtract a small portion of the amplified signal for measurement to demonstrate that the amplified state does indeed have greater intensity.

The photon addition stage allows photons to be added to the signal pulse, these photons amplify the intensity of the original signal sent by Alice. The addition can be performed by several different methods and recent experimental implementations and simulations have shown photon addition using thermal noise sources [29], [30], stimulated spontaneous parametric down-conversion (SPDC) [31]–[33], and also doped fibre [34], [35] - examples of experimentally realised devices are given in the following sub-sections. Some of these addition stages require a single-photon detector to monitor whether an addition has been successful or not, which can be one of the post-selection conditions. These post-selection conditions depend upon the type of photon addition, as these may, or may not, require a photon detection. It should be noted that the photon addition provides gain to the original signal, essentially amplifying it.

After the photon addition stage, a subtraction stage (generally consisting of a low reflectivity BS and a single-photon detector) is used to improve the fidelity of the amplified quantum state, and also verify that there is greater than 1 photon present after the addition stage. As mentioned only some addition stages feature a detector for monitoring, and post-selection, therefore the subtraction stage is the only post-selection condition to confirm the amplification. A low reflectivity BS is used because the overall gain of the amplifier is affected by the subtraction stage removing photons from the amplified state and reducing the output intensity. However the low reflectivity also affects the maximum success probability of overall device as the general post-selection condition is that the detector at the low reflectivity output must register a photon count. The fidelity and gain are also affected by the reflectivity of the subtraction BS. Photon subtraction detection statistics are linked to the statistics of the photon stream not reflected, therefore given certain post-selection conditions can change the relative intensity of the output.

Random noise source

Amplification based on the addition of random noise to the signal has been investigated using simulation [29], where the noise was from a thermal source. An experimental realisation of a device was recently shown with random phase noise generated by randomising the phase of pulses generated from a continuous-wave beam [30]. Figure 6.5 shows a schematic of such schemes. In both cases, the additional photons are randomised in phase, i.e. their phase is from the continuous 0-2π range, and therefore the success probability of the devise is low because of the wide range of phase values possible. While Müller *et al.* [30] showed the randomisation from pulse generation of a continuous-wave coherent beam, random phase noise can also be achieved by a thermal source with super-Poissonian statistics as simulated by Marek and Filip [29].

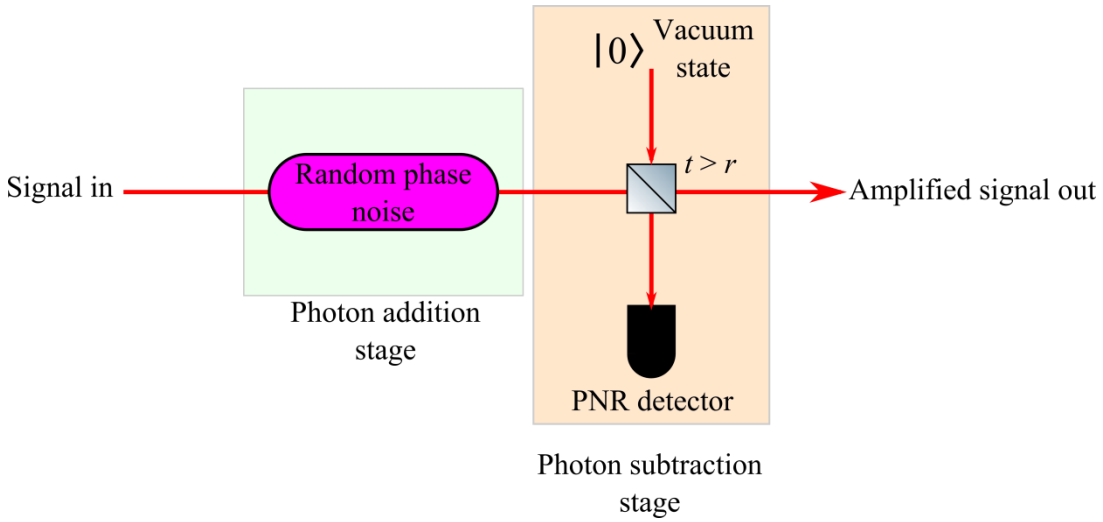


Figure 6.5. – Schematic diagram of a random phase noise experimental apparatus. Many photon addition and subtraction devices employ a photon number resolving (PNR) detector in the subtraction stage to add further post-selection conditions. [29], [30]

In the experimental implementation of Müller *et al.* [30] the phase randomised additional photons were generated from an auxiliary beam using electro-optic modulators which featured variable electrical delays to set the phase of the pulse generated. This system was designed to test the 1→2 cloning of a quantum state where one state was generated from an strong optical beam, phase randomised and then another state was generated later from the same strong optical beam. The test was to see if these two generated states would be the same. In a deterministic experiment, this would lead to low fidelity, but using non-

deterministic methods with post-selection, the fidelity is higher. The polarisation of the generated photons was orthogonal to the original beam and could be separated by a polarisation beam splitter before the subtraction stage. No detection conditions were assigned to the addition stage, the conditioning was only carried out based on events at the subtraction detector which tapped off a portion of the amplifier beam using a low reflection BS.

The subtraction stage in the experiments of both [29], [30] consisted of a highly transmitting (low reflectivity) BS with a photon number resolving (PNR) detector on the reflection side. The use of such a detector allowed for variable gain and fidelity because knowing the transmission and reflectivity coefficients of the BS allows some information about the photon number statistics of the transmitted pulse to be inferred from the photon number statistics of the reflected pulse. In the post-selection stage the user can select conditions on the subtraction stage, only accepting time instances when the number of photons detected at the PNR detector (M) are above a certain threshold, which in the work of Müller *et al.*[30] was $M \geq 1$, 2, 3, 4, and 5. Increasing the number of photons required at the PNR detector will lower the success rate of the amplifier, as it will become increasing unlikely that more than one photon will be detected given the low reflectivity of the BS and the low detection efficiency of PNR detectors, see the review in Chapter 2. In the work of Müller *et al.*[30], the success rate for $M = 1$, for a mean photon number per pulse ($|\alpha|^2$) of 2 was 0.1 correlations per second, while the success rate for $M = 5$ was 1×10^{-4} per second. Simulations from Marek and Filip [29] showed the gain could theoretically increase from 2 to 4.5 for $M = 1$ to 6, but in the work of Müller *et al.*[30] a gain was not investigated, as only the $1 \rightarrow 2$ cloning was of interest, i.e. the nominal gain of 2 for the $M = 1$ case.

While it is useful to have variable gain, fidelity and success probability, PNR detectors are generally large structures, extremely complex to construct and operate, as well as having high initial and maintaining costs. At present, PNR detectors, such as the transition edge sensor [36], typically have poor overall detection efficiencies of around 1-3% (Chapter 3) therefore the success probability for an amplifier is reduced significantly. The more commonly available single photon detectors, which are generally more efficient, work in a Geiger detection mode (although some have been adapted to have a level of PNR properties by having an array of single devices [37]) and users may be more confident

using these devices for real world applications since they are widely commercially available [38]–[42], although this would negate the variable gain of such devices.

Many quantum optical amplifier applications are aimed at use in quantum communication, more specifically phase-encoding QKD protocols implemented in optical fibre, which generally use a known phase-encoding alphabet of four non-orthogonal states (0, $^{\pi}/_{2}$, π, and $^{3\pi}/_{2}$). The use of a fully randomised phase source (i.e. over all 0-2π phase space) does not take advantage of the situation that the phase-alphabet is known. The success probability could be increased if the amplifier was restricted to the phase-alphabet and could pick randomly between the elements in the alphabet (if a secure protocol allowed for this) as there would be a smaller spread of possible phases and the success probability is inversely related to the number of phases.

Stimulated spontaneous parame*t*ric down conversion

Stimulated spontaneous parametric down conversion (SPDC) is another method of photon addition, where the additional photons are generated in a non-linear crystal by the SPDC process [43]. If the signal photons from Alice are in the vicinity of the generated pair properties of the signal are shared with the generated pair. The SPDC process generates photon pairs, each has a signal and idler photon, the signal is used to amplify the Alice's signal, while the idler is measured by a single photon detector to prove that SPDC has occurred.

Phase-matching in a SPDC crystal, which is the relation of the wavelength of the signal and idler to the emission direction, is a key property for creating amplification as a crystal not optimally aligned will not generate as many photons pairs with the desired wavelengths [23]. The stimulated nature of the emission means that the phase, and polarisation properties of the photon-pair are equal to the photon state that was being amplified.

A single-photon detector is required to measure the idler photon emitted from the pair which travels a different optical path to the signal. A triggered event at the addition stage is one of the post-selection conditions. The generation of SPDC pairs is dependent on the pump power used, therefore it is possible to generate more than one pair for greater amplification. For a single photon source used in quantum communication, more than one photon pair is a problem, but in amplification a higher pump power can be useful for

generating a greater number pairs to increase the gain of the amplifier and success probability.

SPDC optical amplifiers have been experimental realised by at least three groups [31]–[33]. A schematic diagram of the experiment reported by Zavatta *et al.* [32] is shown in Figure 6.6. A barium borate (BBO) crystal was used as the gain medium, which was pumped by a coherent source (wavelength = 786 nm) at a repetition rate of 82 MHz. The photons propagating from the quantum channel (Alice's signal) were made collinear with the signal propagating from the pair generation, while the idler was detected by a gated photon detector coupled to the crystal using a single-mode optical fibre. After the photon addition stage there was a subtraction stage using a 90:10 BS, to indicate if it was likely there was >1 photon in the amplified beam. The detection conditions in post-selection for this beam were detection events at the addition stage and the subtraction stage. A range of $|\alpha|^2$ were tested from 0.2 to 1.4, the fidelity was then checked against a mode locked reference and found to be ≈1 up to $|\alpha|^2$ of 0.5, dropping to ≈ 0.3 at $|\alpha|^2$ of 1.5. The effective gain of the system was found to be, ≈1.9 up to $|\alpha|^2$ of 0.2, dropping off to ≈1.4 at $|\alpha|^2$ of 1.4. A success rate of 20-70 bits s^{-1} was found for $|\alpha|^2$ 0.2 to 1.

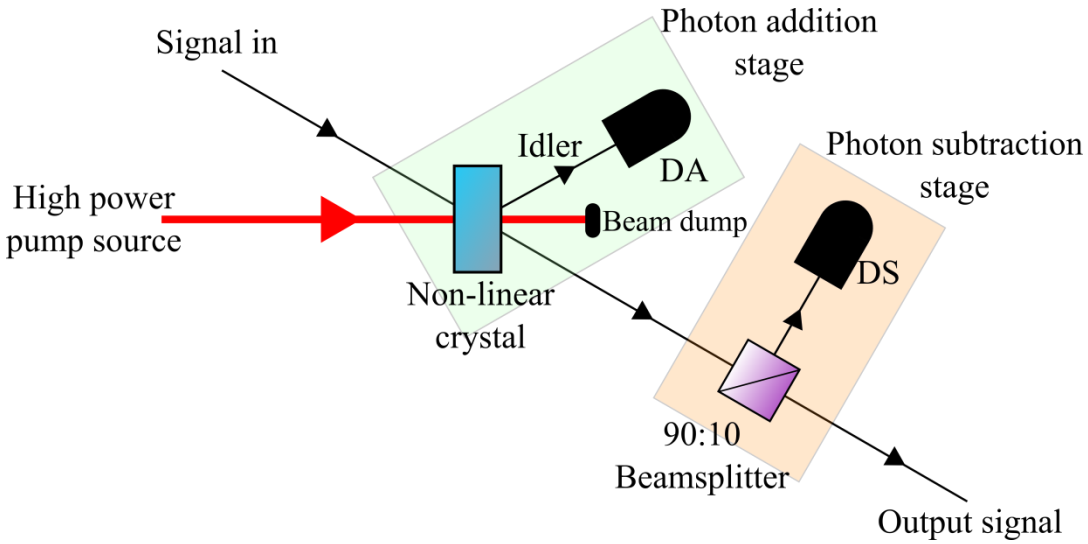


Figure 6.6 –Schematic of stimulated spontaneous parametric down-conversion amplification (SPDC) scheme. [32]

One of the major advantages of the SPDC device is that the amplifier node does not know any information about the original state other than it has been amplified; meaning no

information about the state is recorded by the amplifying station. One drawback for the experimental devices shown is that they are all implemented in free-space, requiring optical fibre quantum communication protocols to be coupled into free-space for amplification and then re-coupled into optical fibre, potentially leading to significant additional losses.

Unfortunately the success probability of the work reported by Zavatta *et al.* [32] is very low (of the order of 1×10^{-6}) making it unsuitable for most communication applications. This low success probability is primarily due to the SPDC process and the use of single mode optical fibre for coupling to the detectors. The SPDC process emits pairs in a cone shape [44], [45], therefore the probability that a pair(s) is generated propagating collinear with the signal from Alice is small. A guided device which limits the pair propagation direction, in a waveguide for instance, could perhaps improve the success probability and such devices were discussed in Chapter 2.

6.3.2 Heralded scissor devices

Heralded scissor or entanglement swapping devices are frequently of the schematic configuration which is shown in Figure 6.7. These devices were first introduced by Pegg, *et al.* [46] in 1998 and subsequently shown experimentally by many groups [47]–[53]. The 'scissor' style device uses two BS, one a 50:50 to perform a Bell-state measurement [54], with the other a variable BS where the entanglement swapping occurs. A single photon source is coupled to the variable BS which sets up a superposition of states. This single photon is generally generated by type-1 SPDC (the generated pair have the same polarisation), although other single photon sources could be used, such as quantum dots [55]. The magnitude of the superposition is determined by the splitting ratio of the variable BS. The reflected part of the variable BS is interfered with an input signal. The Bell-state measurement is successful (i.e. the input photon and the amplifier photon are indistinguishable) if there is a photon detection at D+ and no detection at D-. If successful, the properties of the signal pulse are passed onto the transmitted single photon. The single-photon source and Bell-state measurement do not need to be located in the same 'amplifying station' and can be separated by long distances or high loss channels, because the entanglement is said to be robust [56].

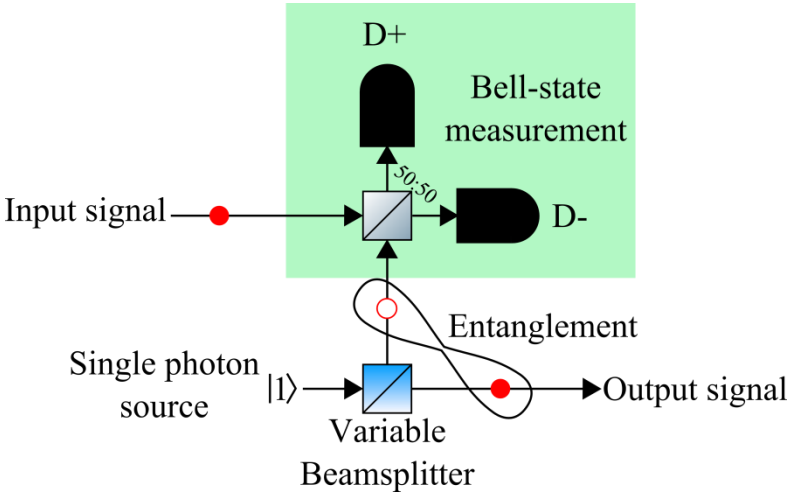


Figure 6.7 – Schematic for a heralded scissor/entanglement swapping device. [53]

Recent simulations using an entanglement swapping device were performed by NICT, Japan [56]. The team had recently been looking into the limitation of QKD protocols due to high loss turbulent mediums because of their interest in satellite QKD communications [56]. The gain is altered by changing the transmission of the variable BS. The simulation used a standard scissor set-up as shown in Figure 6.7. These simulations showed high fidelity, between 0.85 and 0.95, over a range of gains 0.5 to 3.

Heralded-scissor devices have been experimentally realised: Bruno *et al.* [48] showed that a gain between 1 and 100 is possible depending on the transmission of the variable BS, although a higher transmission was found to substantially lower the success rate because of the low amplitude intensity for the Bell-state measurement. Variable BS transmissions of 0.87, and 0.7 showed coincidence rates of 780 and 1400 s^{-1} respectively. Osorio *et al.* [53] showed a range of gain from 0.4 to 2 with lower success rates. The post-selection conditions for each case was detection of the idler photon, confirming a photon pair was generated by the SPDC process, then a detection event at D+.

These heralded scissor entanglement swapping devices have shown a success probability of the order of 1×10^{-5}, a factor of 10 greater than the photon addition and subtraction devices. The success probability could be improved with a more efficient way of generating the single photons at the variable BS. It was mentioned by Bruno *et al.* [48]

that the probability of generating a pair was 0.01 and this pair then needs to be confirmed by detection of the idler photon, which could be very inefficient.

The design shown in schematic form in Figure 6.7 could be carried out in free-space or optical fibre configurations, making it useful for ground and satellite applications.

Qubit amplifiers

A very recent modification of the heralded amplifier has come in the form of a qubit amplifier [57] which makes use of type-II SPDC process where signal and idler photon are different polarisations. Instead of the post-selection being based on the idler being detected and the result of the Bell-state measurement, only the Bell-state measurement is used to non-deterministically determine whether there was amplification. Qubit amplifiers were first proposed in 2010 [50], and further discussed in 2011 [58] as a way of extending the transmission distance for device independent quantum key distribution (DI-QKD) and (at least partially) closing the Bell-test loophole.

The experimental device, shown in schematic form in Figure 6.8, is similar to the scissor device with two main differences. The first is the use of type II SPDC instead of type I; this generates the photon pairs in orthogonal polarisations, where in type I they are collinear. The use of type II means the Bell-state measurement is now carried out with four detectors to identify the polarisations, as perpendicular polarisations will no longer interfere at the 50:50 BS.

In the experimental realisation [57], gains of 0.2 to 9 were tested, based on the transmission distance, with a higher gain used for longer distances. The fidelity of the states remained high >97% for the Bell-state measurement. A 4-fold coincidence based on the Bell-state measurement, successful herald by Alice, and measurement of the amplified state lead to a success rate of in the order of ≈0.2 per second, which for a 4-fold coincidence is rather good. This experiment was mainly used to test the qubit amplifier for use as a DI-QKD device, and has shown that transmission distances of 80 km could be achieved, in principle.

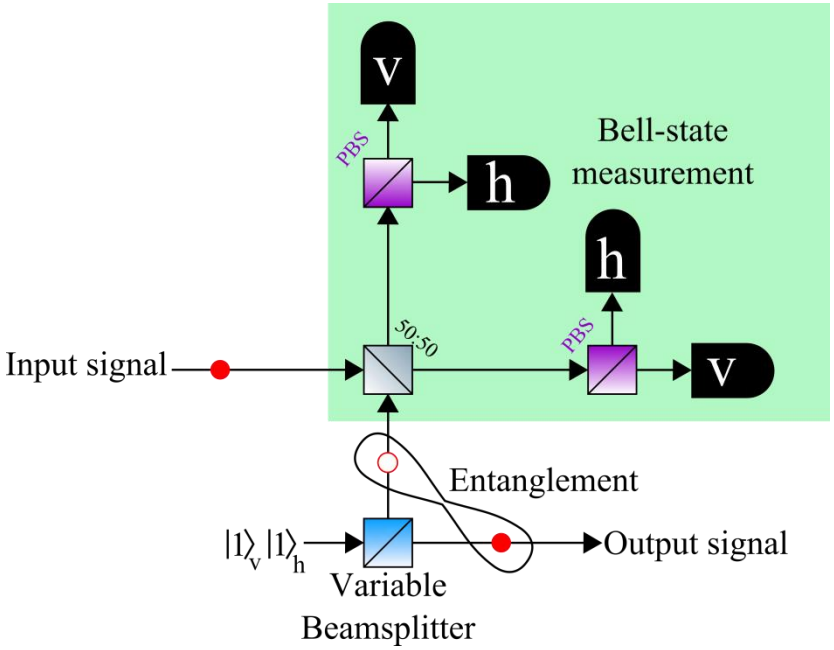


Figure 6.8 – Schematic for a qubit amplifier, which can be seen to be a modified version of the heralded scissor device. A more thorough Bell-State measurement is performed, because of the two different polarisation used in the protocol. [57]

6.3.3 Entanglement repeater and relays

The entanglement repeater is a quantum optical repeater based on a measurement device independent QKD (MDI-QKD) [59]–[61]. The schematic of this system is already shown in Figure 6.4 b), where Alice and Bob, who control their own spontaneous parametric down-conversion sources, measure their idler photon from the pair to determine the properties (which are entangled to the signal photon) while the signal photon is sent down the quantum channel to be measured in a Bell-state measurement with the signal photon from the other party. This basic system, shown in Figure 6.4 b), already theoretically increases the transmission distance of QKD by a factor of 2, because the Alice and Bob in principle only send one signal photon at a time, any measurement by Eve on either of them will break the entanglement and cause the Bell-State measurement to fail.

This idea for MDI-QKD can be expanded upon in order to make this system a repeater as shown in Figure 6.9. The addition of one repeater node requires an extra source of photon pairs in which to perform two Bell-state measurements, therefore as well as additional repeater nodes, sources nodes are also required to generate the photon pairs. If both Bell-

State measurements are successful Alice and Bob will be able, from their measurement of their idler photon, to generate an encryption key. In Figure 6.4 the addition of one repeater stage allowed for a theoretical doubling of transmission distance, while in Figure 6.9 the maximum distance is quadrupled. Adding a repeater node, *n*, the maximum distance of entanglement based QKD protocols can be increased by a factor of 2*n*.

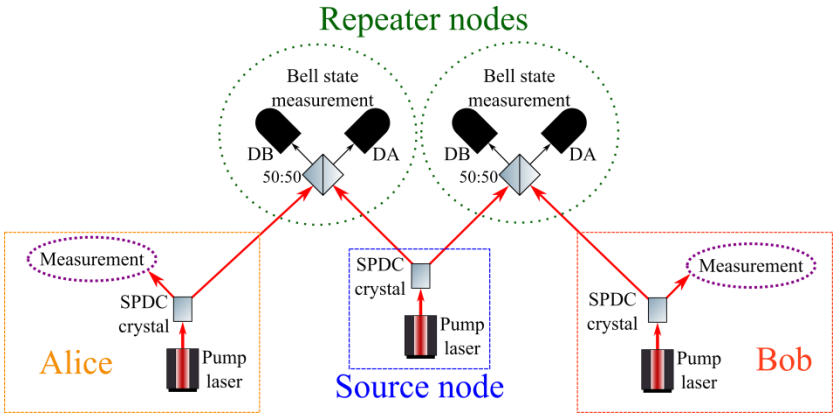


Figure 6.9 – An example schematic of how an entanglement repeater would work for a two stage repeater.

Although entanglement repeaters theoretically look like a promising way to increase the maximum distance of quantum communication protocols, there are several issues which need to be addressed before they can be regarded as practical. Quantum communication requires the probability of greater than one photon per pulse to be low, in order to do this with SPDC sources, the pump power must be reduced, as the emission of SPDC is super-Poissonian. This means that the probability of emitting one pair in the first place can be <1%. Given that the probability of a pair being emitted is low, the probability that simultaneous pairs are emitted at the same time from Alice, Bob and the source nodes is extremely low. On top of that, the photons which are measured by the repeater station need to actually make it there through the high loss transmission medium. Given all of these technological limitations this experiment is a challenging prospect and, to the best of my knowledge, only one experimental realisation has been attempted with limited success [62]. The experimental realisation followed a double pass generation of photon pairs at the repeater node which sent photons to Alice, Bob and the Bell-state measurement. Only pair generation rates were reported in the paper, limiting any real prospect of an in-depth analysis being presented here. The success probabilities of such devices are likely to be extremely low, growing smaller with each additional node introduced. However, with the

increasing efficiency of spontaneous parametric down-conversion sources, now able to emit photon pairs in the MHz range, another experimental implementation is overdue.

6.3.4 Summary of quantum amplifiers

It has been shown that non-deterministic noiseless quantum amplification has been an area of active research over the past decade with many different protocols and experimental implementations of varying success. Three types of devices were reviewed, addition and subtraction, heralded scissor and entanglement swapping devices. Table 6.2 gives a general summary of each device described.

Device type	Source of photons	Success probability	Nominal gain	Notes
Addition and subtraction	Spontaneous parametric down-conversion (SPDC), single photons, coherent or thermal source	1×10^{-6} to 1×10^{-9}	>1	- Photon number resolving subtraction stage can increase gain. - Low success probability due to continuous range of possible phase values.
Heralded scissor device	SPDC	1×10^{-5}	>1	-Use of heralded source gives low success probability. - Herald sources make the device robust against high loss channels.
Entanglement repeater	SPDC	$>>3 \times 10^{-5}$	1	-Multiple entangled heralded sources for many Bell-State measurements make the success probability low.

Table 6.2 – General overview of the three quantum optical amplifier devices.

Addition and subtraction devices have low success probabilities because the addition photons have random properties, i.e. phase, which spans over 0-2π space. The gain, fidelity and success probability can be adjusted by using a photon number resolving detector and post-selection conditions on the number of photons detected at one time. A fixed phase alphabet is generally used in quantum communication protocols , for example the BB84 protocol of quantum key distribution uses 0, $\pi/2$, π, and $3\pi/2$ [63], therefore it makes sense to restrict the amplification process to these values rather than trying to

amplify using a source which equally covers the entire phase space. This could be one method to increase the success probability above heralded scissor devices.

Heralded scissor devices were shown to have improved success probability over the addition and subtraction devices, also with a larger gain range. DI-QKD was shown to favour these devices to help increase the transmission distance using entangled heralded sources [57] so these quantum amplifiers already have an application. The gain could be varied to accommodate large losses by using variable transmission:reflection ratio BS in the device. Although these devices look promising, the use of heralded sources inhibits the achievable success probability because of the low probability of a pair being generated in the SPDC process.

Entanglement swapping repeaters using heralded entangled sources are favoured by many as the future of long distance QKD. The repeaters rely on a Bell-state measurement which can confirm if the states sent were distinguishable or not. The gain is set at unity because the device is a repeater and does not amplify any signal. The predicted success probability will be related to several factors, including losses between parties and the repeater station, and the probability that heralded pairs are emitted at the same time. SPDC sources can now generate pairs more efficiently [64] than the source in the first experimental realisation [62], therefore the success probability of any subsequent experimental implementation will have risen. As well as requiring pairs to be generated simultaneously and not be lost during transmission to the repeater, there may also be a need for some form of quantum memory (or delay) so that the states arrive at the Bell-state measurement at the same time. This will be high loss and will lower the success probability for each repeater node.

Although there have been many successful experimental implementations of quantum optical amplifiers, many have disadvantages which are not easily fixed. The requirement for single photon sources generated by SPDC or quantum dots, which are inefficient and sometimes experimentally difficult to maintain for long periods, means that success probabilities are generally low for quantum optical amplifiers.

For quantum amplification to become a real solution for quantum communication protocols, higher success probabilities, high fidelity, and >1 gain devices are required. In

the next Chapter, a newly proposed device which is based on photon addition and subtraction, called the state comparison amplifier (SCAMP) is described, providing a higher success probability than previous devices, with high fidelity output.

6.4 Bibliography

[1] C. M. Caves, "Quantum limits on noise in linear amplifiers," *Phys. Rev. D*, vol. 26, no. 8, pp. 1817–1839, Oct. 1982.

[2] A. W. Naji, *et al.*, "Review of Erbium-doped fiber amplifier," *Int. J. Phys. Sci.*, vol. 6, no. 20, pp. 4674–4689, 2011.

[3] A. Ghatak and K. Thyagarajan, *An Introduction to Fiber Optics*. 1998.

[4] V. Scarani, *et al.*, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Nov. 2005.

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

[6] M. N. Islam, "Raman amplifiers for telecommunications," *IEEE J. Sel. Top. Quantum Electron.*, vol. 8, no. 3, pp. 548–559, 2002.

[7] B. Korzh, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photonics*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[8] B. Korzh, *et al.*, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," *Appl. Phys. Lett.*, vol. 104, no. 8, p. 081108, Feb. 2014.

[9] M. Lucamarini, *et al.*, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express*, vol. 21, no. 21, pp. 24550–24565, 2013.

[10] E. Meyer-Scott, *et al.*, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," *Phys. Rev. A*, vol. 84, no. 6, pp. 1–9, 2011.

[11] D. E. Bruschi, *et al.*, "Spacetime effects on satellite-based quantum communications," *Phys. Rev. D*, vol. 90, no. 4, p. 045041, Aug. 2014.

[12] K. Ward, "A Short History of Telecommunications Transmission in the UK," *J. Commun. Netw.*, vol. 5, no. 1, pp. 30–41, 2006.

[13] T. H. Maiman, "Stimulated Optical Radiation in Ruby," *Nature*, vol. 187, no. 4736. pp. 493–494, 1960.

[14] J. Wilson, *et al.*, *Optoelectronics: an introduction*. Prentice Hall Europe, 1998.

[15] V. Scarani, *et al.*, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Nov. 2005.

[16] M. J. Connelly, *Semiconductor Optical Amplifiers*, 1st ed. Kluwer Academic Publishers, 2002.

[17] J. Simon, "GaInAsP semiconductor laser amplifiers for single-mode fiber communications," *J. Light. Technol.*, vol. 5, no. 9, pp. 1286–1295, 1987.

[18] C. R. Giles and E. Desurvire, "Modeling erbium-doped fiber amplifiers," *J. Light. Technol.*, vol. 9, no. 2, pp. 271–283, 1991.

[19] B. Utreja and H. Singh, "A review paper on comparison of optical amplifiers in optical communication systems," vol. 2, no. 11, 2011.

[20] A. Rostami, *et al.*, "Nanostructure Semiconductor Optical Amplifiers," pp. 163–183, 2011.

[21] E. Desurvire, *et al.*, "High-gain erbium-doped traveling-wave fiber amplifier.," *Opt. Lett.*, vol. 12, no. 11, pp. 888–890, 1987.

[22] R. J. Mears, *et al.*, "Low-noise erbium-doped fibre amplifier operating at 1.54μm," vol. 23, no. 19, pp. 1026–1028, 1987.

[23] M. Fox, *Quantum Optics: An introduction*, 1st ed. Oxford: Oxford University Press, 2006.

[24] G. Kweon, "Noise Figure of Optical Amplifiers," *J. Korean Phys. Soc.*, vol. 41, no. 5, pp. 617–628, 2002.

[25] H. Haus, "The noise figure of optical amplifiers," *Photonics Technol. Lett. IEEE*, vol. 10, no. 11, pp. 1602–1604, 1998.

[26] R. Kaur and K. Kaur, "Analysis and Investigation of Noise Figure of Fiber Raman Amplifier," *Int. J. Electron. Comput. Sci. Eng.*, pp. 3–7, 1998.

[27] T. Ralph and A. Lund, "Nondeterministic noiseless linear amplification of quantum systems," *arXiv Prepr. arXiv0809.0326*, pp. 1–4, 2008.

[28] E. Eleftheriadou, "Quantum optical state comparison amplifier," University of Strathclyde, 2015.

[29] P. Marek and R. Filip, "Coherent-state phase concentration by quantum probabilistic

amplification," *Phys. Rev. A*, vol. 81, no. 2, pp. 022302Marek, P., & Filip, R. (2010). Coherent–stat, Feb. 2010.

[30] C. R. Müller, *et al.*, "Probabilistic cloning of coherent states without a phase reference," *Phys. Rev. A*, vol. 86, no. 1, p. 010305, Jul. 2012.

[31] J. Fiurášek, "Engineering quantum operations on traveling light beams by multiple photon addition and subtraction," *Phys. Rev. A*, vol. 80, no. 5, p. 053822, Nov. 2009.

[32] A. Zavatta, *et al.*, "A high-fidelity noiseless amplifier for quantum light states," *Nat. Photonics*, vol. 5, no. November 2010, p. 5, 2010.

[33] J. A. Levenson, *et al.*, "Quantum optical cloning amplifier," *Phys. Rev. Lett.*, vol. 70, no. 3, pp. 267–270, 1993.

[34] S. Fasel, *et al.*, "Quantum cloning with an optical fiber amplifier.," *Phys. Rev. Lett.*, vol. 89, no. 10, p. 107901, 2002.

[35] M. I. Dzhibladze, *et al.*, "Regenerative glass-fiber neodymium quantum amplifier," *Sov. J. Quantum Electron.*, vol. 14, no. 1, pp. 85–88, 2007.

[36] F. Group, "Transition edge sensors (TES)," 2014. [Online]. Available: http://web.mit.edu/figueroagroup/ucal/ucal_tes/. [Accessed: 09-Nov-2015].

[37] M. J. Applegate, *et al.*, "Efficient and robust quantum random number generation by photon number detection," *Appl. Phys. Lett.*, vol. 107, no. 7, 2015.

[38] Excelitas Technology, "Single Photon Counting Modules," 2015.

[39] Micro Photon Devices, "InGaAs SPAD - gated," 2014.

[40] ID Quantique, "Visible single-photon detection module with high timing resolution and low dark count rate.," 2015.

[41] ID Quantique, "Infrared single-photon counting system ID210 advanced system for single-photon detection with 100 MHz gated mode and free-running mode.," 2002.

[42] Princeton Lightwave, "High Speed Single Photon PGA-600HSU," no. 1, 2011.

[43] H. Di Lorenzo Pires, *et al.*, "Type-I spontaneous parametric down-conversion with a strongly focused pump," *Phys. Rev. A*, vol. 83, no. 3, p. 033837, 2011.

[44] M. P. Edgar, *et al.*, "Imaging high-dimensional spatial entanglement with a camera," *Nat. Commun.*, vol. 3, no. May, p. 984, 2012.

[45] R. E. Warburton, *et al.*, "Single-photon position to time multiplexing using a fiber

array," *Opt. Express*, vol. 19, no. 3, pp. 2670–2675, 2011.

[46] D. Pegg, *et al.*, "Optical State Truncation by Projection Synthesis," *Phys. Rev. Lett.*, vol. 81, no. 8, pp. 1604–1606, Aug. 1998.

[47] S. Babichev, *et al.*, "Quantum scissors: Teleportation of single-mode optical states by means of a nonlocal single photon," *EPL (Europhysics Lett.*, vol. 1, 2003.

[48] N. Bruno, *et al.*, "A complete characterization of the heralded noiseless amplification of photons," *New J. Phys.*, vol. 15, 2013.

[49] S. Kocsis, *et al.*, "Heralded noiseless amplification of a photon polarization qubit," *Nat. Phys.*, no. 3, pp. 1–6, 2013.

[50] N. Gisin, *et al.*, "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier," *Phys. Rev. Lett.*, vol. 105, no. 7, p. 070501, Aug. 2010.

[51] H. M. Chrzanowski, *et al.*, "Measurement-based noiseless linear amplification for quantum communication," *Nat. Photonics*, vol. 8, no. 4, pp. 333–338, Mar. 2014.

[52] F. Ferreyrol, *et al.*, "Implementation of a Nondeterministic Optical Noiseless Amplifier," *Phys. Rev. Lett.*, vol. 104, no. 12, p. 123603, Mar. 2010.

[53] C. I. Osorio, *et al.*, "Heralded photon amplification for quantum communication," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 86, no. 2, pp. 1–4, 2012.

[54] Y.-H. Kim, *et al.*, "Quantum Teleportation of a Polarization State with a Complete Bell State Measurement," *Phys. Rev. Lett.*, vol. 86, no. 7, pp. 1370–1373, 2001.

[55] S. Buckley, *et al.*, "Engineered quantum dot single-photon sources.," *Rep. Prog. Phys.*, vol. 75, p. 126503, 2012.

[56] J. S. Neergaard-Nielsen, *et al.*, "Quantum tele-amplification with a continuous-variable superposition state," *Nat. Photonics*, vol. 7, no. 6, pp. 439–443, May 2013.

[57] N. Bruno, *et al.*, "Heralded amplification of photonic qubits," *Opt. Express*, vol. 24, no. 1, p. 125, Jan. 2016.

[58] M. Curty, *et al.*, "Heralded-qubit amplifiers for practical device-independent quantum key distribution," *Phys. Rev. A*, vol. 84, no. 1, p. 010304, Jul. 2011.

[59] H.-K. Lo, *et al.*, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012.

[60] T. Ferreira, *et al.*, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, no. 5, p. 052303, 2013.

[61] Y.-L. Tang, *et al.*, "Measurement-Device-Independent Quantum Key Distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, no. 19, p. 190501, Nov. 2014.

[62] Z. Zhao, *et al.*, "Experimental realization of entanglement concentration and a quantum repeater.," *Phys. Rev. Lett.*, vol. 90, no. 20, p. 207901, 2003.

[63] Y.-C. Jeong, *et al.*, "An experimental comparison of BB84 and SARG04 quantum key distribution protocols," *Laser Phys. Lett.*, vol. 11, no. 9, p. 095201, Sep. 2014.

[64] L. A. Ngah, *et al.*, "Ultra-fast heralded single photon source based on telecom technology," *arXiv:1412.5427*, vol. 5, no. 2, p. 5, 2014.

Chapter 7

Experimental Demonstration of a Quantum Optical State Comparison Amplifier

7.1 Introduction

This Chapter presents an experimentally realised quantum amplifier which shows an improved success probability over all previously realised quantum amplifiers. This amplifier does not rely on complex quantum resources for implementation, making it a relatively simple experimental set-up compared to other quantum amplifiers. This Chapter will introduce the quantum amplifier device and its general operation. Following this Chapter, the next will give a further characterisation of the state comparison amplifier (SCAMP) device with variations made to the operation and construction.

The SCAMP was first introduced by Eleftheriadou *et al.* in 2013 [1]. The experiments reported here constitute the first demonstration of the SCAMP approach, and some of these results were published in 2015 [2].

7.1.1 Background and protocol

SCAMP is an addition and subtraction quantum optical amplifier. Although it works in a very similar way to the other photon addition and subtraction devices described in the previous Chapter, there are two key differences which allow SCAMP to have a higher success probability, as described below.

The photon addition and subtraction devices' success probabilities mainly relied on the random phase properties of the addition photon, which uniformly span over the entire 0-2π of phase. Quantum cryptography experiments such as quantum key distribution (QKD), or quantum digital signatures (QDS) can use a number of phase-encodings (N) in their protocol. The number of phase-encodings selected depends on the protocol used, and typically ranges from $N = 2$ to 8 [3]–[5]. Instead of adding photons which have a random phase over 0-2π range, it makes sense to only choose within the small subset of phase-encodings being implemented in the protocol.

The first improvement SCAMP makes over existing devices is that it employs a known phase-alphabet, *N*, consisting of the possible phase-encodings that Alice will implement in her quantum communication protocol. However this does not mean the amplifier will know exactly what states will be sent by Alice and is therefore only guessing between one of the possible *N* values. The probability of the amplifier guessing correctly will be 1/*N*. The use of the known phase-alphabet means that SCAMP is required to be a trusted node, meaning that information from the amplifier's guess states and detection outcomes could allow an eavesdropper some advantage during communication if it were not trusted.

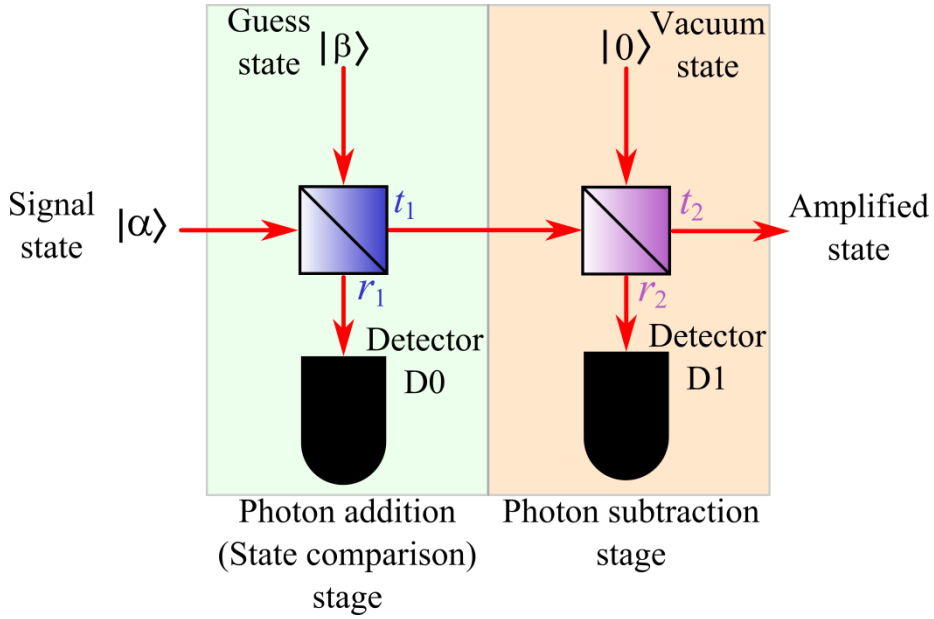


Figure 7.1 – State comparison amplifier schematic showing the addition and subtraction stages.

The second improvement over previous amplifiers is that SCAMP does not rely on any complex quantum sources, or photon number resolving (PNR) detectors. Many quantum amplifiers have relied on spontaneous parametric down-conversion to generate single-photon pairs for amplification [6]–[8]. In practical terms, this is a complex process in which it can prove difficult to maintain stability. Also, the required correlations in the amplification also meant that the idler was one of the correlated events, this greatly reduces the probability of success [6], [8]. PNR detectors can be used as a discriminator in the device subtraction stage to allow greater gain or improved fidelity [9]. However these detectors are cryogenically cooled to reduce the gain noise, sometimes as low as milli-kelvin for transition edge sensors [10], [11]. The addition photons in the SCAMP device

can be created by an attenuated coherent laser source [12], and the detection can be performed by compact commercially available detectors, such as a silicon single-photon avalanche diode (Si-SPAD) [13], [14].

The basic setup for SCAMP is shown in Figure 7.1. The device works in two parts, first the state comparison, which performs an addition of coherent state intensity for the signal by a guess coherent state. This stage provides the optical gain for the SCAMP device.

The second part is a photon subtraction with a low reflectivity beamsplitter (BS) which is used to improve the fidelity of the output. This improved fidelity comes at the expense of lowering the overall success rate of the amplifier. Coherent states are eigenstates of the annihilation operator, so the subtraction does not have an effect on the coherent state properties other than reducing the intensity [15].

For the input and guess states $|a\rangle$ and $|b\rangle$, the coherent amplitude in the nominal vacuum output is $t_1\alpha - r_1\beta$, and the other beamsplitter output passes to the subtraction stage. The amplitude in the subtraction arm is therefore $-r_2(t_1\beta + r_1\alpha)$, and the output amplitude is $t_2(t_1\beta+r_1\alpha)$. We assume that the input and guess are chosen from probability distributions over the coherent states,

$$\hat{\rho}_{in} = \int d^2\bar{\alpha} P(\bar{a}) |\bar{\alpha}\rangle\langle\bar{\alpha}|,$$

$$\hat{\rho}_{in} = \int d^2\bar{\beta} P(\bar{\beta}) |\bar{\beta}\rangle\langle\bar{\beta}|,$$

and calculate the output state and the fidelity based on these and the properties of the device. The fidelity is,

$$F = \int d^2\alpha P(\alpha) \langle g\alpha | \hat{\rho}_{out} | g\alpha \rangle,$$

where $\hat{\rho}_{out}$ is the output state conditioned both on the input state distributions from ($\hat{\rho}_{in}$ and $\hat{\rho}_{out}$) and on the successful operation of the device. This is the probability that the output state passes a measurement test comparing it to the amplified version of the input state and can be written as

$$F = P(T|S) = \frac{P(T|S)}{P(S)},$$

$$= \frac{\int d^2\bar{a} \int d^2\bar{\beta} P(T|S, \bar{\alpha}, \bar{\beta}) P(S|\bar{\alpha},\bar{\beta}) P(\bar{a}) Q(\bar{\beta})}{\int d^2\bar{\alpha} \int d^2\bar{\beta} P(S|\bar{\alpha}, \bar{\beta}) P(\bar{a}) Q(\bar{\beta})},$$

where P(T|S) is the probability that the output state will pass the fidelity test given that the device operates successfully.

Single-photon detectors are used to record events for correlation in post-selection. The input signal, from Alice, is compared against the guess state from the node that selects one of the possible *N* phase-encodings from the known alphabet. If the signal and node state are indistinguishable the state is amplified and passed through to the subtraction stage. If the states are distinguishable then there is a mixed output, leading to photon events being sometimes recorded at the D0 detector.

The post-selection conditions for a successful amplification in SCAMP are detection at the subtraction stage (D1) and no detection at the addition stage (D0). The node claims a successful amplification when D0 does not measure an event (the signal and guess are thought to be indistinguishable), and a recorded event at D1 (the pulse exiting the amplifier likely contains more than one photon). Figure 7.2 shows the possible amplification processes for SCAMP in the case of two guess states. For two possible non-orthogonal guesses which are π out of phase, the state is either amplified or not. However in the case of imperfect visibility some coherent state could still pass through the state comparison stage. This would likely be low amplitude and not likely to trigger the correct post-selection conditions.

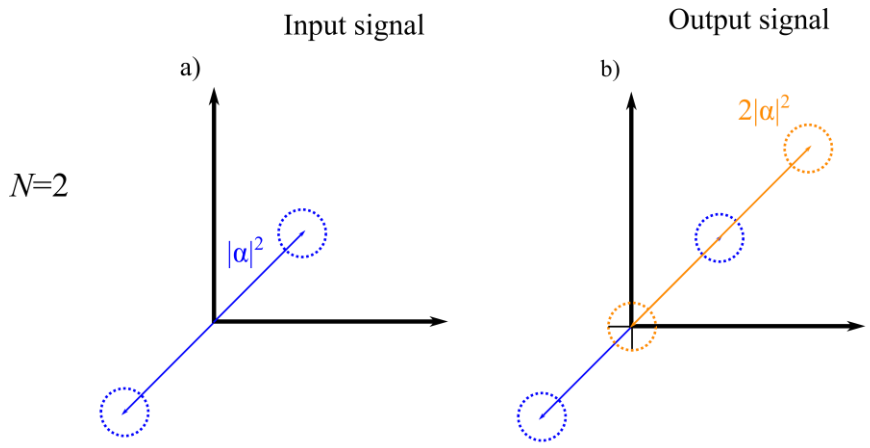


Figure 7.2- Amplification processes for the state comparison amplifier (SCAMP). a) and b) are the input and output states for the state comparison for two possible phase state, N *for a gain of 2.*

In the case where more than two guess states are possible the amplification can results in a mixed state output, i.e. there is mixed interference at the state comparison stage. This will result in coherent state passing through the amplifier. The subtraction stage is more likely to click for the larger amplitude correct states, rather than the lower amplitude mixed state that comes from a greater number of possible guess states, and therefore the conditional output of the amplifier is increased in fidelity compared to the non-conditioned output. This will become apparent later when the detector post-selection conditions are applied to the visibility of the amplifier output.

The nominal gain (theoretical gain) of SCAMP is given by Equation 7.1, where t_2 is the transmission coefficient of the subtraction stage and r_1 is the reflection coefficient of the addition stage. The subtraction stage will generally always be a low reflectivity BS (approximately 5 or 10 %), to improve the fidelity of the amplified state. The gain of the SCAMP device can be varied primarily by changing the reflection coefficient of the addition stage.

$$g_{\text{nom}} = t_2 / r_1 \qquad \text{Equation 7.1}$$

7.2 Experimental implementation

This Chapter focuses on the experimental implementation of the theoretical SCAMP protocol [1]. This experimental implementation shows a device which has a $g_{\text{nom}} = 1.8$, t_2=0.90, r_1=0.50. In the following sub-Sections, the experimental set-up is first introduced along with the method of operation, this gives a general explanation of how SCAMP operates, which can also be referred to for Chapter 8's experiments as well.

The results are analysed to show the gain, conditional visibilities, and the fidelity of the output. Results are also analysed for the purposely introduced noise to show how robust SCAMP is to noise in a communication channel.

7.2.1 Experimental set-up

The experimental set-up revolves around the amplification stage shown in Figure 7.1 and the expanded system diagram can be seen in Figure 7.3 which shows in more detail how the optical system is set out to perform the experiment. Figure 7.4 is complementary to

Figure 7.3, showing the electronic components, and connections to the optical set-up (linked by equal colours).

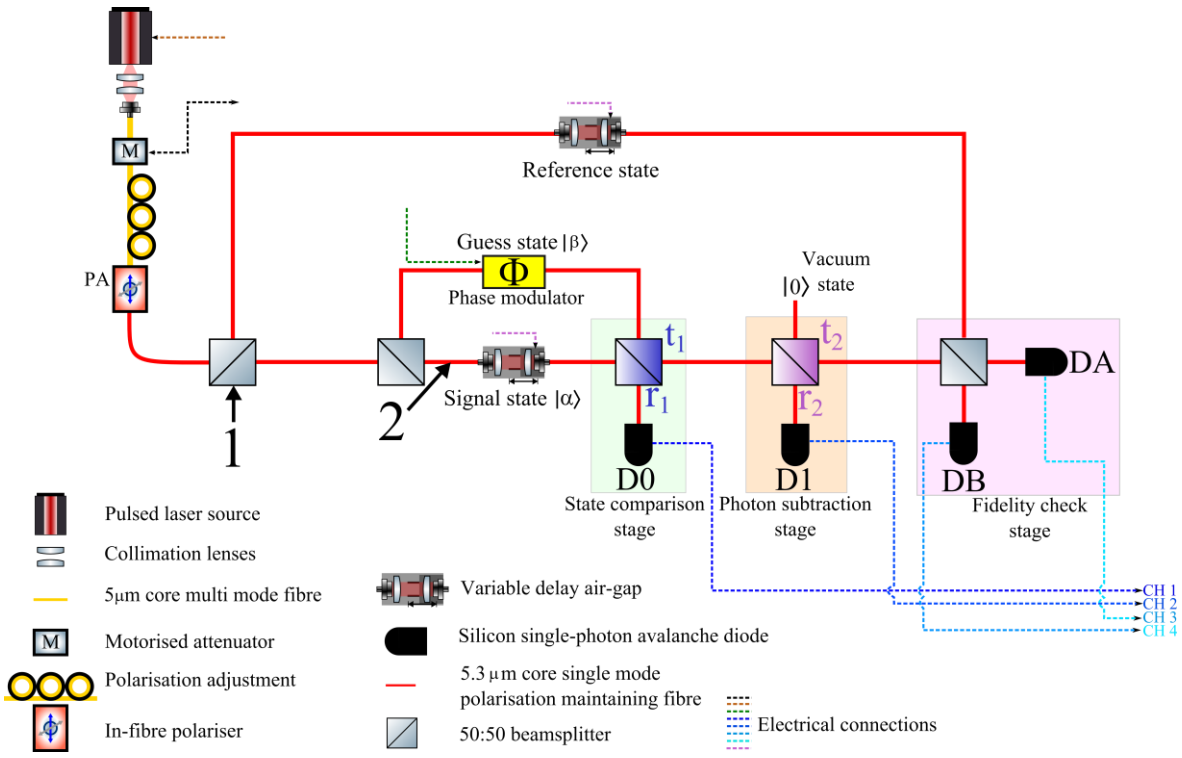


Figure 7.3 – The optical experimental set-up used for the state comparison amplifier. Number 1, and 2 denote where the noise addition was introduced. 1 being for the 850 nm LED, while 2 is for the white light noise.

A 10 MHz clock reference (Novatech [16]) was regenerated by a signal synthesiser (Hewlett-Packard [17]), this provided a lower jitter, and larger amplitude 10 MHz reference signal. The reference signal provided a common electrical clock for other instruments to phase lock to, allowing instruments to operate together in synchronisation. The electrical reference signal was split into four and connected to three pulse pattern generators (PPGs) and the time-tagging hardware (HydraHarp 400) [18]. Two Agilent 81110A PPGs [19] were employed as electrical drivers used to drive the phase modulator (Photline [20]) with a known repeating phase-encoding pattern of length N (N being the number of possible values in the phase-alphabet).

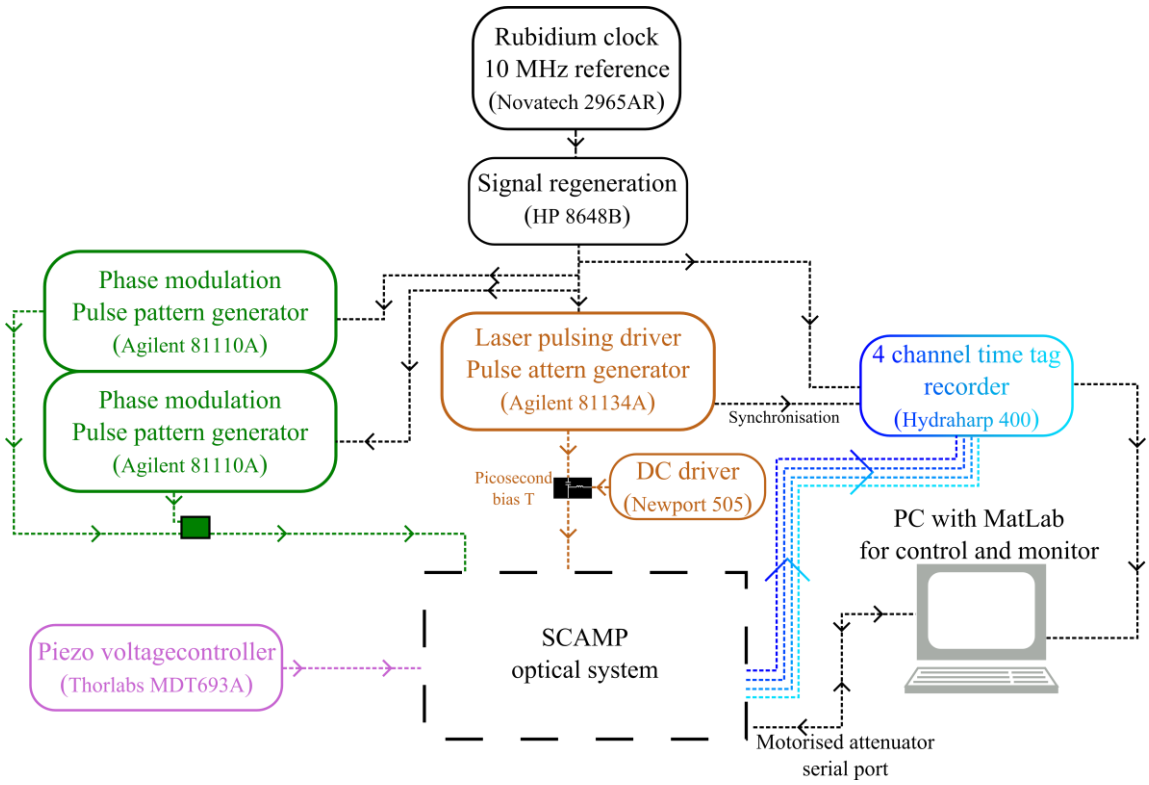


Figure 7.4 – Electrical experimental set-up for SCAMP.

To drive the vertical-cavity surface-emitting laser (VCSEL) (the same device and set-up used in the previous Chapters [21]), a DC offset generated by the DC driver (Newport [22]) was combined with the Agilent 81134A PPG 1 MHz pulsed output on a bias-tee. An electrical synchronisation was also sent from the Agilent 81134A to the HydraHarp 400 for sampling of the Geiger-mode detectors.

In this test-bed demonstration of the principles of a SCAMP system, the single optical path from the laser was split into two paths at the first 50:50 BS. The transmitted path was used in the SCAMP process while the reflected path was left unaltered and used as a reference state for fidelity checks on the final 50:50 BS.

The reference path featured a variable delay air-gap to match the arrival time of the unaltered reference with the signals at the final fidelity check BS. A piezo-electric actuator (Thorlabs [23]) was placed in the variable delay air-gap allowing a user to adjust for nanometre scale variations in the path length, in real time.

The transmitted path was further split into two paths, a "guess" path and "signal" path, which were then recombined at the state comparison stage of the amplifier. Ideally the guess state in the amplifier would not have used energy from the same laser as the signal but instead have had its own laser source which was indistinguishable from the signal (such as a pair of temperature tuned narrow spectral line-width distributed feedback lasers [24]). In this test-bed the same coherent source was used for both signal and guess due to the experimental complexity of two indistinguishable sources.

The signal path featured a variable delay air-gap with screw-adjustable attenuator and piezo-electric actuator which provided adjustment of the path length. Apart from the variable air-gap and attenuation, the signal was left unaltered, and was used to simulate a phase-encoded signal coming from Alice in a QKD/QDS style experiment.

The guess state arm only features the phase modulator, which was used to select the 'guess' state. The phase-alphabet of the possible guess states, N, for experiments here, was 2, 4 or 8. The phase modulator was electrically modulated by the Agilent 81110A PPGs, each of which had two channel outputs that could modulate one non-orthogonal pair, hence two PPGs were required to generate $N = 8$. The output of these were combined using high-speed electrical combiners (Avtech [25]).

The guess and signal state were then compared on the amplifier stages, where photon detectors D0 and D1 recorded events. All detectors used in the experiment were Excelitas Geiger-mode silicon single-photon-avalanche diodes (Si-SPADs) [14].

The fidelity of the amplified outcome was then tested on the final 50:50 BS, the interference was recorded on detectors DA and DB. The HydraHarp 400 records the measurements taken by D0, D1, DA, and DB in time-tag mode, which records the time instance in which a detector measured an event. Although not strictly necessary for the correct operation of the amplifier, the electrical output of each SPAD was subject to electrical delays from measured lengths of cables timed to ensure that electrical events triggered by fractions of the same light pulse reached the HydraHarp simultaneously. This synchronisation was performed to simplify testing of the amplifier system in the laboratory.

7.2.2 Methods

The methods used to operate and analyse the results will be described in this section.

Calibration and set-up

Initially the optical laser output pulse waveform was optimised to give a good temporal and spectral profile. The SCAMP experiment could be described as an interferometer inside another interferometer, so the SCAMP device was referred to as the inner interferometer, and the fidelity check the outer interferometer. Each interferometer was calibrated separately so that the losses in the different optical paths were equal when the phase modulator was set to zero phase difference from the signal. A visibility of >96 % was achieved on both interferometers during calibration.

Before making a set of measurements the phase modulator was configured to send a repeating pattern for one of the three investigated phase-alphabets (N = 2, 4, or 8). For N = 2, one electrical channel was set to switch on and off, giving the two levels for 0, and π, therefore each state occurs half the time (500,000 times per second), the same idea follows for N = 4, and 8 with each state occurring $^{\nu}/_{N}$ times per second, where ν was the clock frequency of 1 MHz. The output of the driving electronics for the phase modulator was not uniformly level for the entire duration of one period and exhibited some distortion, including overshoot and damped ringing. As the duration of the laser pulse was relatively short compared to the period of the electrical driving signal for the phase modulator, the timing offset of the periodic laser pulse train was adjusted so that the laser pulses occurred at times which gave optimum visibility in the inner interferometer (hence optimising the outer interferometer as well).

The four single-photon detectors employed in this test-bed demonstration of SCAMP, D0, D1, DA, and DB, sent photon events to the HydraHarp 400 which recorded the events in time-tag mode (when an event occurs the associated macro-time, relative to the start of the measurement process, of the event is stored). A computer program written in MATLAB [26] then processed this into four histograms which updated once every second, one for each detector. The histograms allowed visual feedback for the user who could adjust the voltage over the piezo-electric actuators in the inner and outer interferometer to improve the visibility of the system.

Threshold visibilities were set for the inner and outer interferometers, once the threshold was reached, or exceeded, the MATLAB program would save the one second duration measurement of raw time-tagged data which had been used to create the histograms. There were two threshold visibilities taken into account in the experiment which needed to be reached on each interferometer, the standard maximum and minimum visibility, and the ratio of the counts in each detector for the non-orthogonal phase-encodings (i.e. how equal the peaks are in terms of integrated counts in the histogram). The standard visibility threshold was set to take about 90% in both the inner and outer interferometers, while the threshold ratio for the non-orthogonal states was set to (1 ± 0.1):1. The MATLAB code saved 100 individual 1 second duration sets of time-tag measurements for each $|\alpha|^2$.

After data acquisition the saved time-tag data was gated (or temporary filtered) by discarding events that occurred outside of a ±2 ns window centred on a periodic occurrence determined by the position of the peaks in the histogram. The gated time-tags were then processed for time-correlations and the average of the 100 individual sets computed for later analysis.

7.3 Results

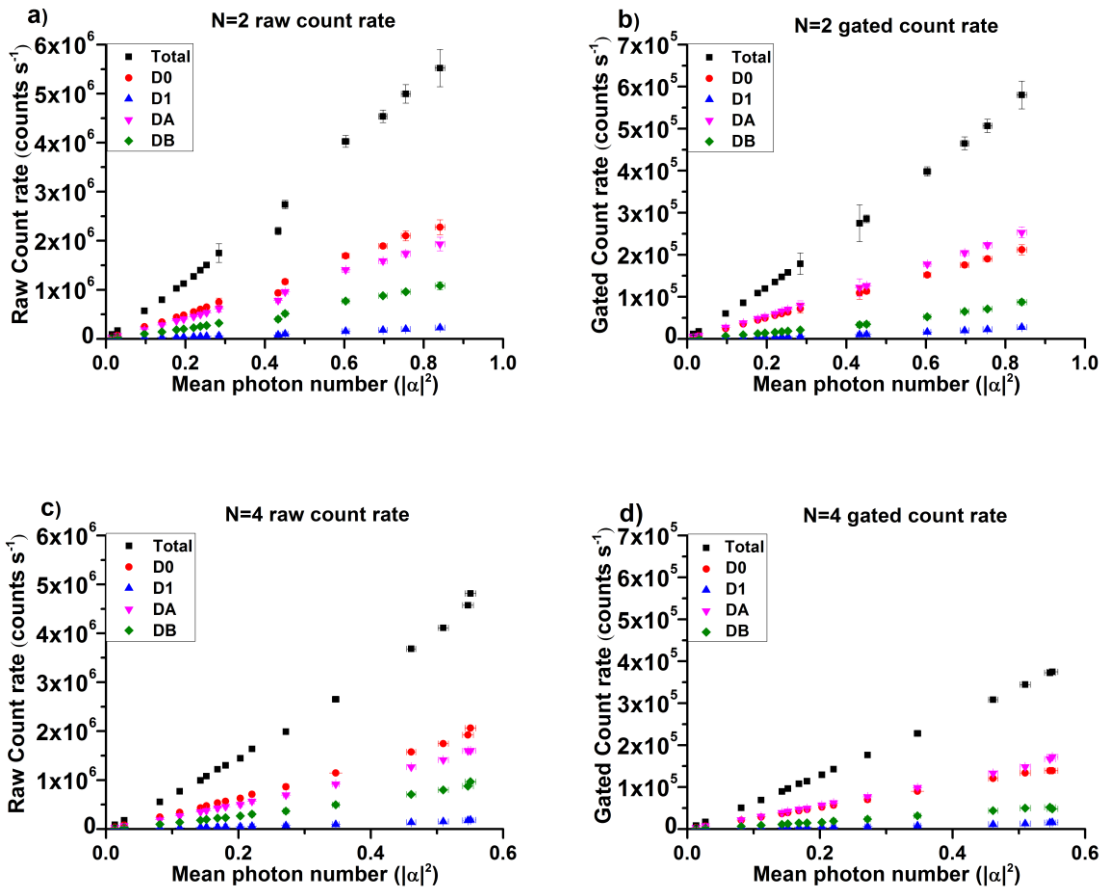
This section will be used to present processed time-tag data that was acquired from the SCAMP experimental system. The initial configuration of SCAMP featured a 50:50 comparison BS at the state comparison stage, and a 90:10 BS at the subtraction stage, giving a nominal (theoretical) gain of 1.8 (from Equation 7.1). In the original theoretical paper [1] it was proposed that this configuration would provide a modest gain with high fidelity output.

Two sets of results are analysed: first experiments were performed with no additional noise, merely investigating the SCAMP. Secondly to test the noise resistance of SCAMP, additional photon noise was inserted into various parts of the experiment by coupling into fibre-fibre splices, or extra fibre couplers on a BS.

All experiments were carried out over a range of $|\alpha|^2$ for possible phase-alphabets $N = 2$, 4, and 8. The same MATLAB code was used for all experiments, with only minor changes made to the visibility saving thresholds due to the impurity in phase-encodings at higher N values.

7.3.1 State comparison amplifier with 1.8 nominal gain

Raw count rates for each detector are plotted in Figure 7.5, a) c) e) for $N = 2$, 4, and 8 respectively, these are the average total number of measured events recorded over the whole 1 second data acquisition period. The gated count rates for each detector are shown in Figure 7.5 b), d), and f) for $N = 2$, 4, and 8 respectively. The gated count rate is the number of measured events within the 4 ns gating window over the 1 second data acquisition period. On average, the gated count rate was 4.2 ± 0.3 %, 8.7 ± 0.4 %, and 3.1 ± 0.1% of the raw rate for $N = 2$, 4, and 8 respectively. This variation in the gated percentage comes from the $|\alpha|^2$ range and phase-alphabet used. Because of the use of a laser pulse repetition frequency of 1 MHz, the raw count rate is dominated (>90%) by background noise, this lead to inaccuracies in the $|\alpha|^2$ set for each phase-alphabet, the variation is picked up in the gated rate for each N.



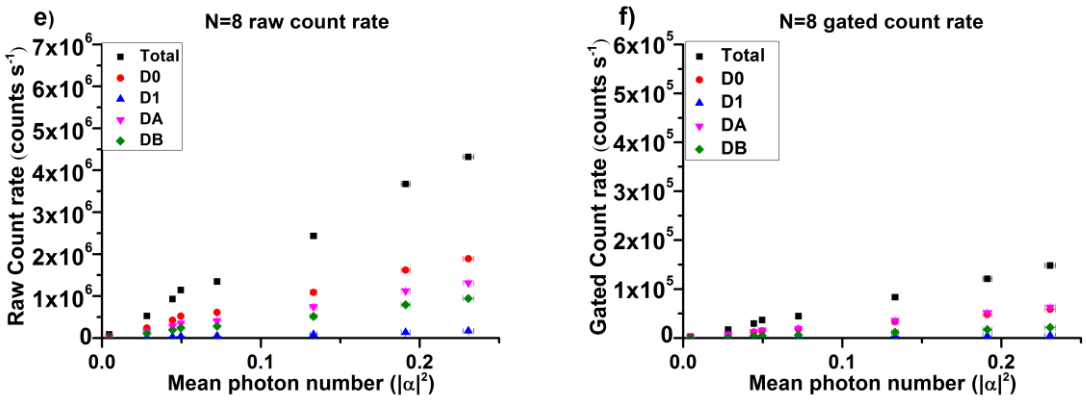


Figure 7.5 - Raw and gated count rates for experimental SCAMP experiment with nominal gain of 1.8

Calculation of the $|\alpha|^2$ was based on Equation 7.2, which is a back-calculation from the gated count rates on the addition detector (D0). $|\alpha|^2$ was estimated from the using the raw count rate output of an ID Quantique Si-SPAD [27], after back calculation the initial estimated values were found to be incorrect because small changes in the over-all raw count rate on the detector meant large variations in the $|\alpha|^2$ set. It can be seen in a), c), and e), of Figure 7.5 that the total raw count rate approximately the same for the different ranges of $|\alpha|^2$, because the $|\alpha|^2$ change was hidden by the small change in overall raw count rate.

$$|\alpha|^2 = \frac{\text{Maximum} + \text{Minimum}}{2 \times \text{SPDE} \times l_{comp} \times \text{Repeated pattern frequency}} \qquad \text{Equation 7.2}$$

Equation 7.2 takes into account the maximum and minimum peaks of the D0 (addition stage) histogram. This count rate is then compensated for loss between the point of $|\alpha|^2$ and the single-photon detector, l_{comp}, single-photon detection efficiency (SPDE), and the intensity equalisation (a factor of 2, because half of the light intensity is coming from the signal state, the half the guess state). The frequency of the maximum pulse is also taken into account, for $N = 2$, 4, and 8, the repeated pattern frequency is 0.5, 0.25, and 0.125 MHz, respectively. The formula could be extended to include all other peaks from the histogram, but the outcome would be approximately the same.

It can be seen in the gated count rates that DA has over taken D0 in count rate, which initially suggests measureable gain in the system. However, the larger gated count rate on

detector DA is due to the 50:50 reference splitting when there are no amplified states present, rather than actual gain from the amplifier.

The range of $|\alpha|^2$ used for the experiment was thought to have remained constant for $N = 2$, 4, and 8, although it can be seen by the x-axes in Figure 7.5 that the $|\alpha|^2$, when back calculated from the gated count rates, has dropped for increasing N. The value of raw count rate for detector D0 for $N = 2$, 4, and 8 does not change wildly as can be seen from Figure 7.5 a), c), and e). However when the gated count rate is analysed, it can be seen there is a huge difference between the gated rates (and associated $|\alpha|^2$ range), Figure 7.5 b), d), and f). Unlike the previous experimental Chapters, this experiment was performed at 1 MHz, the fraction of a second that the gate is open is small, leading to a gated rate of only <10% of the measured raw count rate. Small changes in the raw rate corresponded to large changed in the gated rate. This was put down to drifting laser power during experimentation which was not picked up by the monitoring.

SCAMP is a noiseless non-deterministic amplifier, which works based on probabilistic success in post-selection. The effect of post-selection on the measurement can be shown by applying various conditions to the visibility of the final fidelity stage BS, where the amplified state is interfered with an unaltered reference state.

Standard visibility of an interferometer is calculated using Equation 7.3. 'correct guess' refers to the integrated counts under the constructive interference peak, and 'incorrect guess' the integrated counts under the destructive interference peak. This equation only takes into account two states which are π out of phase. A modified visibility calculation taking into account all the of other non-orthogonal phase pairs in the alphabet is shown in Equation 7.4. 'All possible guesses' refers to the counts in all peaks corresponding to the entire phase-alphabet.

$$\text{Visibility} = \frac{(\text{correct guess} - \text{incorrect guess})}{(\text{correct guess} + \text{incorrect guess})} \qquad \text{Equation 7.3}$$

$$\text{SCAMP conditional Visibility} = \frac{(\text{correct guess} - \text{incorrect guess})}{\sum \text{All possible guesses}} \qquad \text{Equation 7.4}$$

The SCAMP conditional visibility is based on the time gated time-tag correlations, with all Si-SPADs time synchronised. The post-selection SCAMP conditional visibilities are as follows and are plotted in Figure 7.6 a), b), and c) for N = 2, 4, and 8 respectively.

- *No comparison or subtraction (black data points)*:
    - Correct – Detection at detector DA.
    - Incorrect – Detection at detector DB.
- *Comparison only (red data points)*:
    - Correct –Detection at DA and no detection at D0.
    - Incorrect - Detection at DB and no detection at D0.
- *Subtraction only (blue data points)*:
    - Correct –Detection at DA and detection at D1.
    - Incorrect - Detection at DB and detection at D1.
- *With comparison and subtraction - the full SCAMP (pink data points)*:
    - Correct – Detection at DA and D1, with no detection at D0.
    - Incorrect – Detection at DB and D1, with no detection at D0.

From Figure 7.6 a), b), and c), it can be seen that as more post-selection conditions are applied to the Equation 5.4, the visibility improves. Each sub-figure shows four conditions which were investigated during post-selection, 'No comparison or subtraction' (black data points), 'Comparison only' (red data points), 'Subtraction only' (blue data points) and 'Comparison and subtraction' (pink data points). The visibility of the system increases as more strict conditions are applied. However the difference between the 'subtraction only' and 'comparison and subtraction' is very small, with the 'comparison and subtraction' being only marginally larger. The question might arise "why even bother conditioning with the subtraction and comparison detectors to give a fully conditioned amplified state?" The answer is that the information about the state comparison lets an amplifier node know whether or not its guess state was correct or incorrect, the information could be used later for use in quantum cryptography protocol. The discussion will continue later when the success rate/probability of the amplifier is presented.

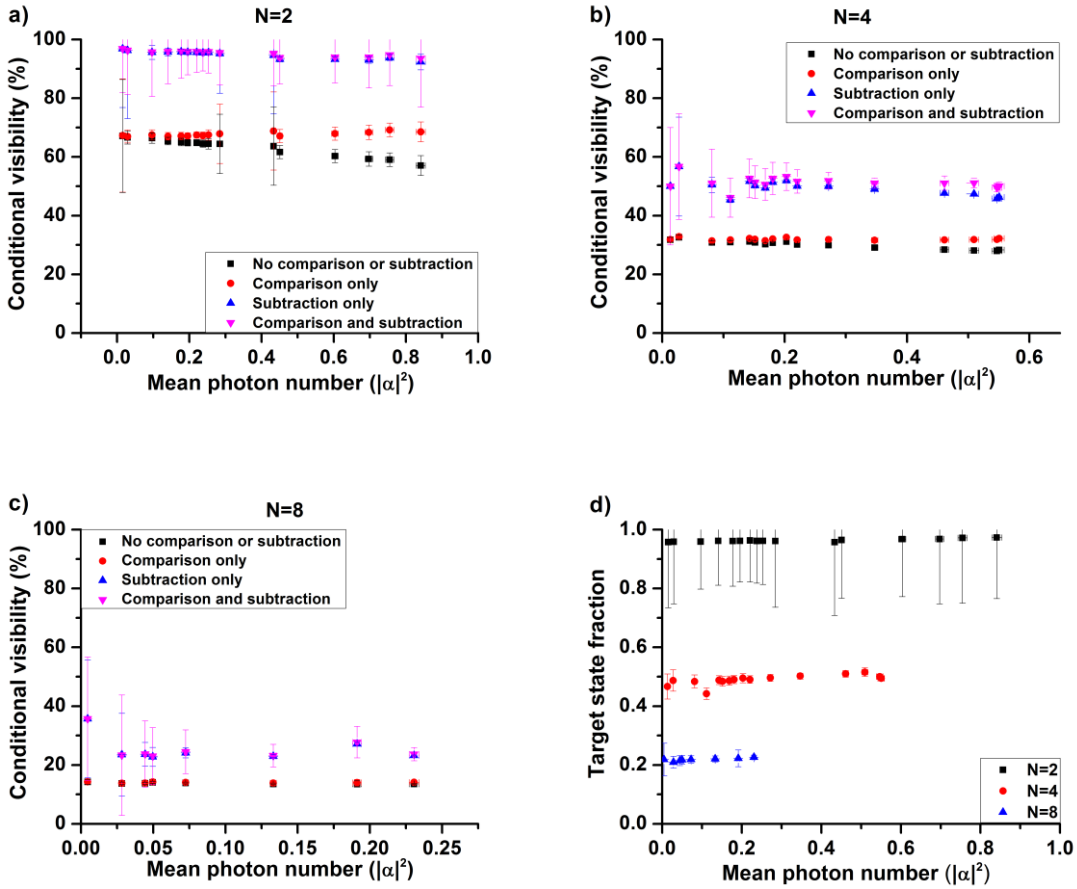


Figure 7.6 – Conditional visibilities of the outer interferometer for N = *2, 4 and 8 (a, b and c) set-up based on post-selection and Equation 7.4. d) the Target state fraction (TSF).*

The target state fraction (TSF) is the percentage of the overall successfully amplified states which are amplified using the right guess state. The limit of target state fraction is given by $^{2}/_{N}$. From use of SCAMP conditions settings, the amplification TSF is on average 0.96, 0.49, and 0.22 respectively, showing that the limit is almost reached, but due to some experimental imperfections, such as imperfect visibility, the TSF is just short of the limit. The TSF is calculated using Equation 7.5, and is plotted in Figure 7.6 d). The experimental uncertainty in the TSF for $N = 4$, and 8 is small in comparison to in case of $N = 2$. This is due to the threshold settings in the experiment. $N = 2$ only has a visibility threshold ($\gtrsim$ 96%) whereas the $N = 4$, and 8 have threshold bounds based on their other non-orthogonal pair respective heights, which is a tighter threshold to stay in than simply greater than a set visibility. Therefore the $N = 2$ values generally have a greater uncertainty in the TSF.

$$\mathrm{TSF}=\frac{\text{Conditioned correctly guessed amplified states}}{\sum \text{All conditioned amplified states}} \qquad \text{Equation 7.5}$$

Success rate and probability are two important properties of an optical quantum cryptography amplifier. As seen in the summary from the previous chapter (Table 6.2) previously experimentally realised quantum optical amplifiers had success rates which were low, <1% of the clocking frequency. Figure 7.7 a), b), and c) show the total success rate for N = 2, 4, and 8 respectively. The total success rate, Figure 7.7 d), is shown as well to indicate that each N's range of $|\alpha|^2$ follow the same trend. In a), b), and c), the total number of amplified states is given, along with the correctly guessed amplified successes, and the other amplified states, which are incorrectly guessed.

For N = 2 the difference between the correctly and incorrectly amplified states is greatest, because the guess is either correct or not, the number of incorrectly amplified states is only dependent on the visibility of the state comparison and fidelity stages. As more non-orthogonal pairs are added to the phase-alphabet, incomplete interference takes place, so some portion of intensity can carry on through the amplifier which is why the number of correctly and incorrectly amplified states is approximately equal for N = 4, and there are more incorrectly amplified states for N = 8.

An amplifier, as the name suggests, amplifies a signal. For this initial experimental implementation, the nominal (theoretical) gain was said to be 1.8 because of the BS configuration. After back calculation from the state comparison stage, Equation 7.6, and the fidelity stage, Equation 7.7, the estimated effective gain is then calculated using Equation 7.8, and plotted against the $|\alpha|^2$ in Figure 7.8 a). l_{comp} and l_{fid} are estimated losses from the single-photon detectors to before each beamsplitter.

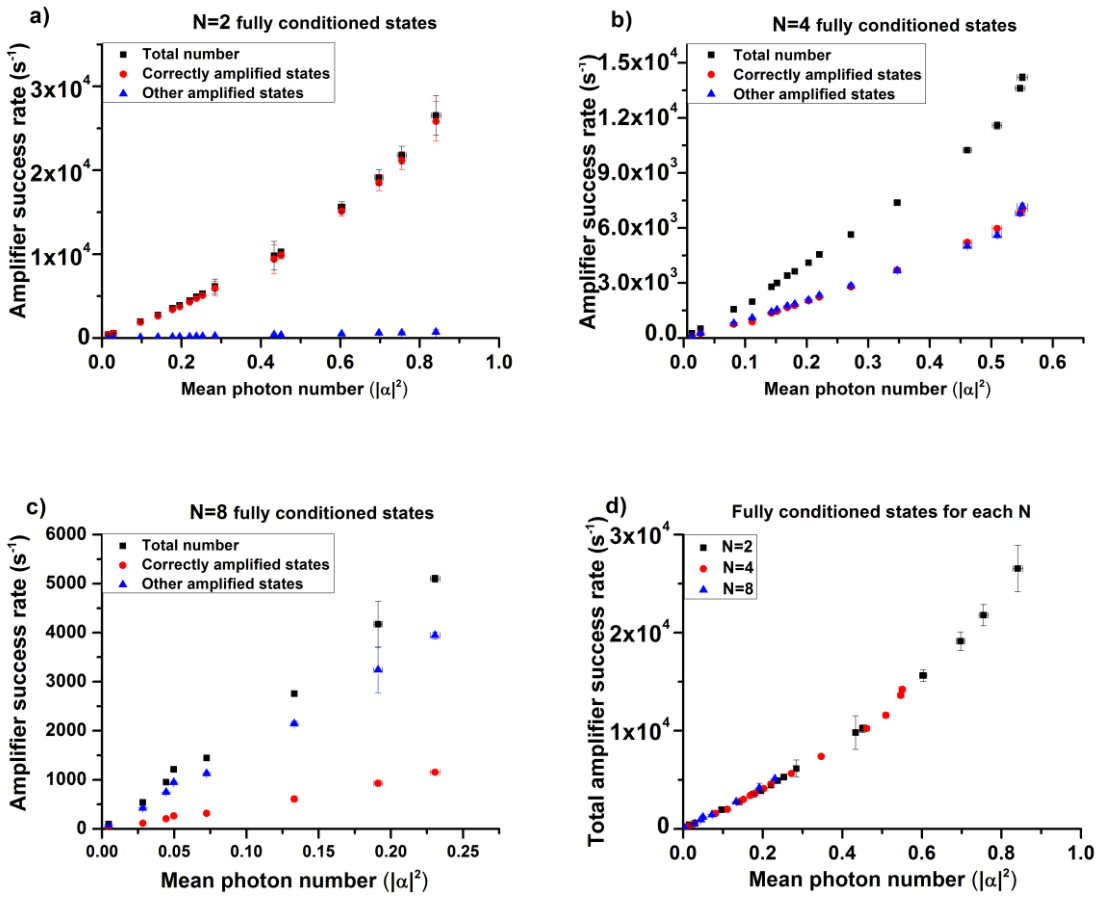


Figure 7.7 - Success & failure rate of N = 2, 4 and 8. a), b) and c). d) shows the total success rate. The success rate depends on correlated events of D0 and D1 only, and not on events at Da and Db.

It can be seen that the estimated effective gain of the amplifier is unfortunately <1. Given that the nominal gain of 1.8 corresponds to 2.55 dB of gain, experimental component loss may explain why gain fell below 1. The loss from the input of the 50:50 state comparison stage to the output of the 90:10 subtraction stage is approximately 2.82 dB, due to splice, and inherent component loses, therefore our gain comes to 0.27 dB loss. The gain actually estimated in Figure 7.8 a), found a lower value of gain than the 0.27 dB loss. This can be accounted for by further losses in the system at the fidelity stage. The large uncertainties in the $N = 2$ case compared to the $N = 4$, and 8, gain values comes from the threshold settings on the visibility for both interferometers ($\gtrsim$96%), which allows for large variation in some conditioned count rates. While in the $N = 4$ and 8 cases, the thresholds include other non-orthogonal states which are required in the visibility calculation, the bounds on these are tighter.

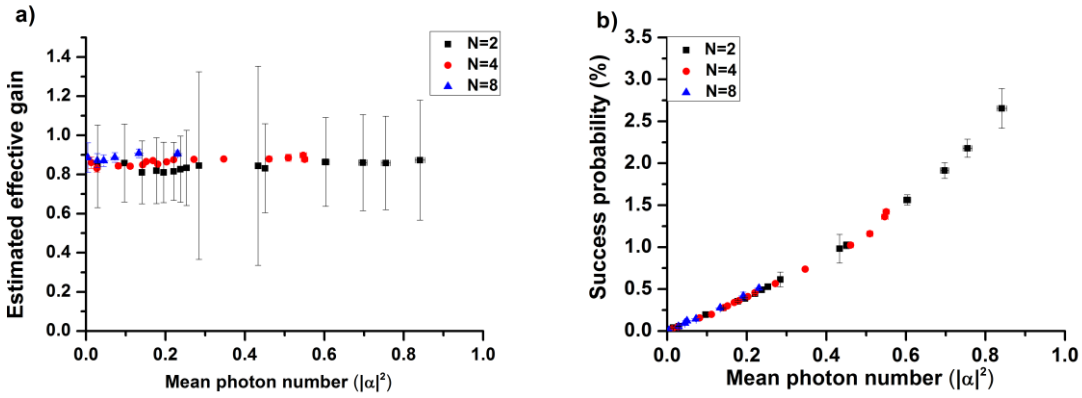


Figure 7.8 – a) estimated effective gain based on Equation 7.8, b) and the success probability.

$$Count\ rate\ from\ signal = \frac{D0_{Maximum} + D0_{Minimum}}{(2 \times SPDE \times l_{comp})} \qquad \text{Equation 7.6}$$

$$Count\ rate\ from\ amplifier = \frac{DA_{Maximum} + DB_{Minimum}}{(2 \times SPDE \times l_{fid})} \qquad \text{Equation 7.7}$$

$$G_{\text{eff}} = \frac{Count\ rate\ from\ amplifier}{Count\ rate\ from\ signal} \qquad \text{Equation 7.8}$$

The amplifier's probability of success is plotted in Figure 7.8 b) and is the total number of successfully amplified states divided by the clock frequency of the system, 1 MHz. The probability is found to increase almost linearly with increasing $|\alpha|^2$ (over the range used in the experiment).

Initial experimental investigations of SCAMP using the nominal gain of 1.8 configuration has shown a non-deterministic amplifier which has a success probability (>1% for $|\alpha|^2 > 0.4$), which depends linearly with $|\alpha|^2$. This high success probability leads to impressive success rates (> 10 k, for $|\alpha|^2 > 0.4$) which are higher than previously shown realisations. This success rate can be increased easily by increasing the clock rate of the system to >1 MHz. However, the estimated effective gain ($g_{\text{eff}} = 0.858 \pm 0.020$) of the device based on back calculation shows that this device cannot be used for amplifying as the loss of the device means that the gain < 1 in this configuration. However, replacing the existing standard off-the-shelf commercial optical components with customised low loss

components and ensuring minimum loss splices while assembling the system could lead to a gain of >1.

7.3.2 Added noise

After the initial investigation of the SCAMP device properties without added noise, the same experiments were carried out again, with noise purposely added into the system to see its effects on the conditional visibilities and success rates. SCAMP works in post-processing, depending on correlations of detections, therefore it was predicted that the added noise would not have much effect on the outcome, as the noise added is from non-coherent sources, so the probability of correlations is low.

Figure 7.3 has two positions in the experiment, denoted 1 and 2, where the added noise was introduced into SCAMP to test the system for noise robustness using the nominal gain of 1.8 set-up.

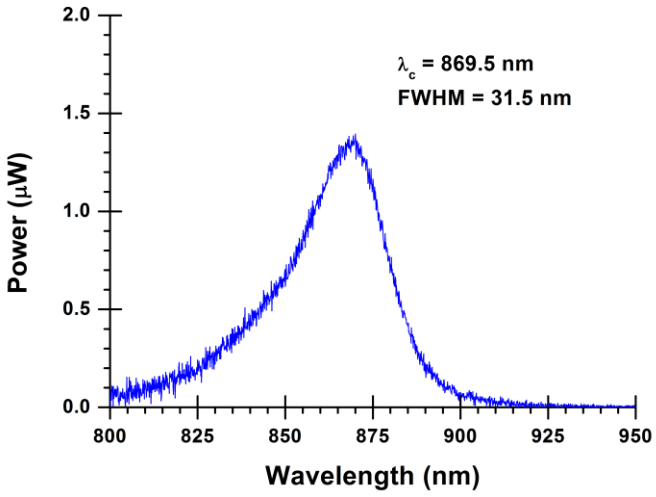


Figure 7.9 – Spectrum of the "850 nm" Thorlabs M850F2 light emitting diode source taken in the lab. [28]

Position 1 was where an 850 nm wavelength optical fibre coupled LED (Thorlabs M850F2) was added, the spectrum of which is shown in Figure 7.9. The emitted light from the LED was attenuated using an optical variable attenuator and coupled into the first 50:50 BS. This coupled noise light into every channel. Although the LED had a narrow

bandwidth (FWHM of 31.5 nm Figure 7.9), it is a sufficiently broadband and incoherent light source that the interferometric visibility of the noise introduced is still effectively 0%.

Position 2 was a free-space coupled broadband white light source, a projector bulb. Some of emitted light from the quartz-halogen bulb (100 W Philips FocusLine Type 7023 projection lamp – colour temperature 3400 K, giving emission in the visible and infrared [29]) was focused into a large multimode fibre bundle enclosed in a metal gooseneck, the output of which was pointed towards a splice in the signal state arm of the inner interferometer. The light had a small probability of being coupled into the core or cladding of the fibre, allowing it to propagate through the rest of the system. The broadband white light will have an interferometric visibility of essentially 0% in the interferometers that comprise the SCAMP system and consequently will not undergo any intensity variations at the detectors due to changes in the optical path lengths.

The experimental method was the same as before with the same post-selection conditions. The only difference to the method was setting the attenuation of the noise, the modified method was as follows:

- A mean photon number ($|\alpha|^2$) was selected.
- Measurements were taken when no added noise was present.
- Measurements were taken when noise was purposely added using a noise source. The level of noise is measured using the raw count rate on the D0 detector.
    - 0.5, 1, 1.5, and 2 mega-counts total (signal + noise) raw on D0.

In these experiments the HydraHarp 400 measuring the raw time-tags was connected by a USB 2.0 connection to the computer which limited the total combined raw count rate from the detectors to approximately 4 $MCounts^{-1}$ [30], a low enough count rate to ensure that a FIFO (first in, first, out) overflow could not take place . A FIFO overflow happens when the internal FIFO buffer in the HydraHarp has filled faster than events could be transferred and events are lost due to lack of buffer space). The HydraHarp aborts a measurement if a FIFO overflow occurs and does not allow access to any data remaining in the buffer. No more than 1 mega-counts per second of noise per detector could be handled, which limits the number of measurements performed as the $|\alpha|^2$ is increased. The main results primarily

follow the $N = 4$ phase-alphabet, as it is most applicable to the quantum communication protocols today which generally feature a 4 phase-encoding alphabet (BB84 decoy-states).

White light noise

The total raw count rate is plotted in Figure 7.10 a), it can be seen that the total count rate for 'no added noise' measurements follows a linear trend with increasing $|\alpha|^2$ while the measurements with noise purposely added follow a flat trend, because the measurements were made for a constant raw count rate on the D0 detector of 0.5, 1, 1.5, or 2 mega-counts per second. The gated count rates in Figure 7.10 b), c), d) and e) show that added noise does not affect the overall gated count rates very much, apart from at the subtraction stage (D1 c)), which shows that the gated count rate increases significantly at lower $|\alpha|^2$ as the noise is added. This increase in gated counts at the D1 detector has implications for the total success rate of the system, which is shown in Figure 7.10 f). SCAMP success is defined as a detection at D1, and no detection at D0, therefore an increased gated count rate at D1, and relatively little change in the D0 gated count rate will lead to an increased total success rate, which has been shown in f).

From the gated count rates and total success rate, it can be seen that added noise will have the effect of increasing the total success rate of an amplifier. Conditional visibility of the system is a better indication of how noise affects the amplification of the state as this directly shows the effects of increased count rate on the D1 detector. It was shown in the previous results section that the visibility of the final fidelity stage could be improved by adding more post-selection conditions, given that the noise is uncorrelated the same condition should show the same effect.

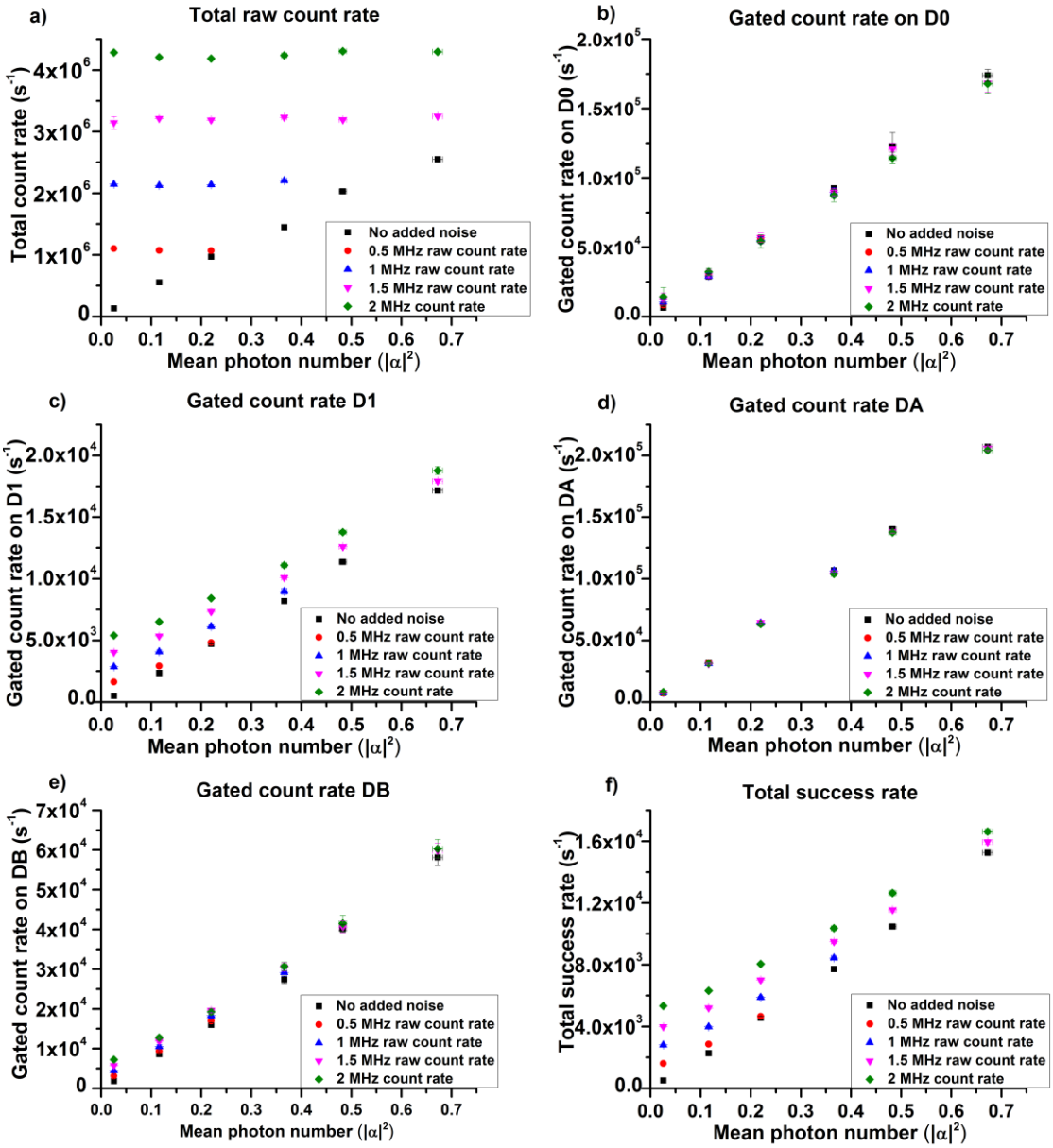


Figure 7.10 – Raw, gated and success rates with added white light noise.

Figure 7.10 shows the conditional visibilities for $N = 4$ for 'no comparison or subtraction', 'comparison only', 'subtraction only', and 'comparison and subtraction', a), b), c) and d) respectively, plotted against the raw count rate on D0. It can be seen that as the noise level increases (the raw count rate on D0 increases) that the conditional visibility decreases. This decrease is more significant in the lower $|\alpha|^2$ cases because the level of noise added is considerably greater than the signal intensity. Therefore, increasing the $|\alpha|^2$ provides a more robust means of counteracting a noisy channel. The large uncertainties in the subtraction only c), and comparison and subtraction d) come from the error propagation of the large standard deviation with respect to the mean value [31]. Relatively small number

of correlations occur which varied largely with separate runs, because it relies on 3 or 4 detection correlations.

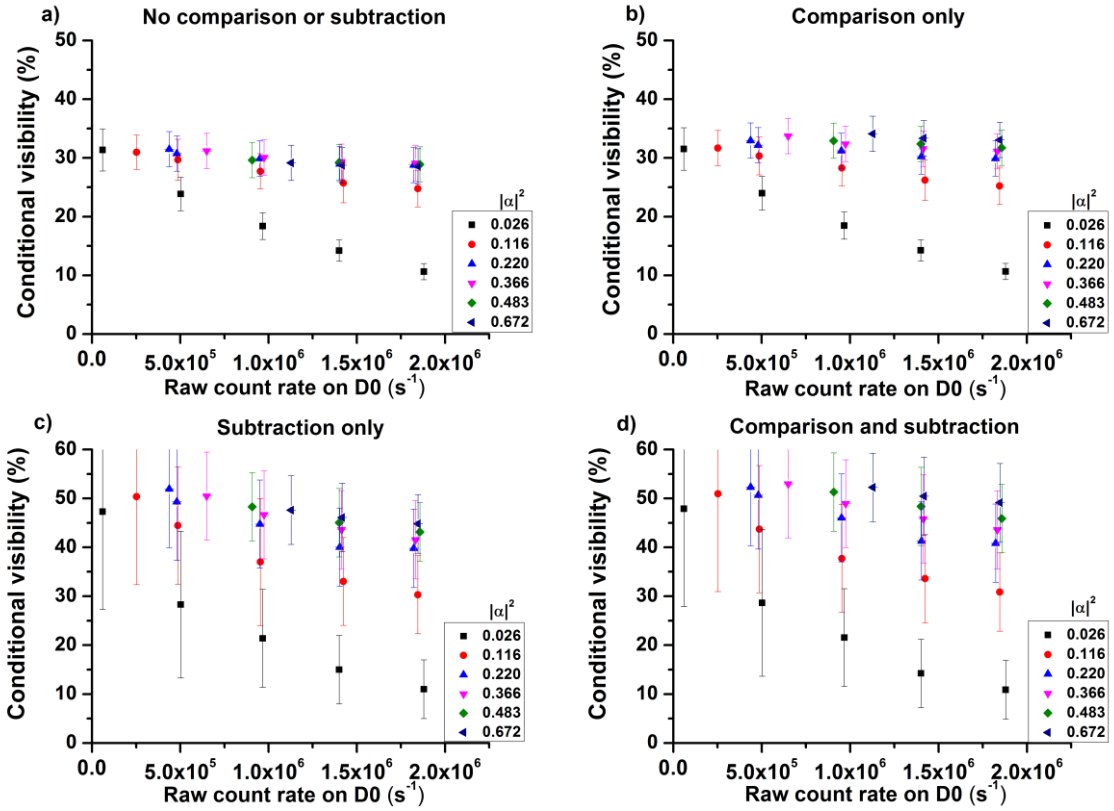


Figure 7.11 – Conditional visibilities of N = 4 with added noise from a white light source. The first point for each trend is the measurement without any added noise.

The conditional visibilities are based on Equation 7.4 and are largely determined by the number of correctly and incorrectly guessed amplified successes. Figure 7.12 shows how the fraction of correct/total fully conditioned states changes with increased noise in the experiment. In all phase-alphabets it can be seen that at low $|\alpha|^2$, the fraction of correct/total drops significantly with increasing noise, showing that incorrect amplifications are becoming more dominant at the amplifier output. However, as the $|\alpha|^2$ increases, the fraction comes closer to the no added noise case seen in the previous results.

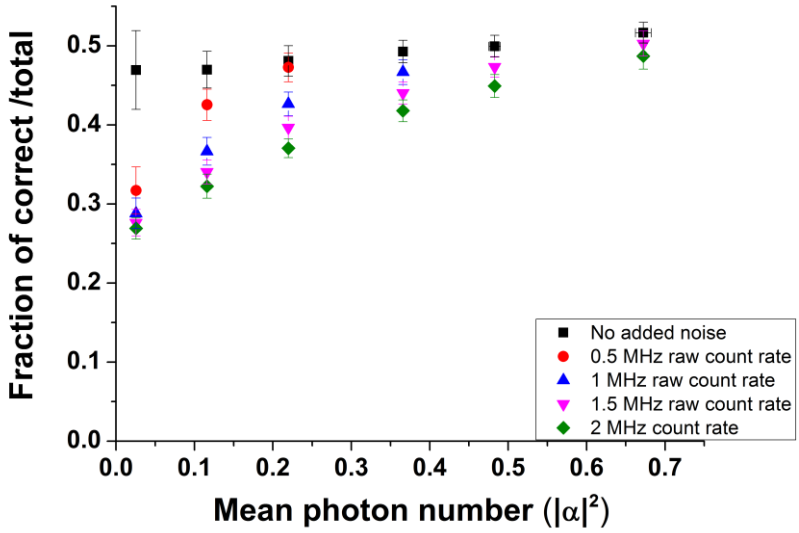


Figure 7.12 – Fraction of correct over total amplified states for N = 4. For N = 4, the ideal fraction should be 0.5.

The state comparison amplifier has been shown to operate moderately successfully even with a white light source employed to create added noise. White noise does affect the conditional visibility of SCAMP depending on the excess noise level added. This is because the wavelengths that make up the broadband light will see different reflection coefficients, meaning the 50:50, and 90:10 BS may not have the same transmission and reflection coefficients at other wavelengths. The detectors also have different detection efficiencies at other wavelength. For the Si-SPAD, the detection efficiency increases with lower wavelength (to a certain point, see Figure 7.13), so broadband spectral noise is more efficiently detected, especially at lower wavelengths. This effect was mostly seen on the D1 detector which has a critical role in confirming a successful amplification. Increasing $|\alpha|^2$ allows an amplifier to better compensate the added noise, but it is not ideal to increase the $|\alpha|^2$ used in quantum communication protocols because of the increased risk of eavesdropping attacks such as the photon number splitting [32].

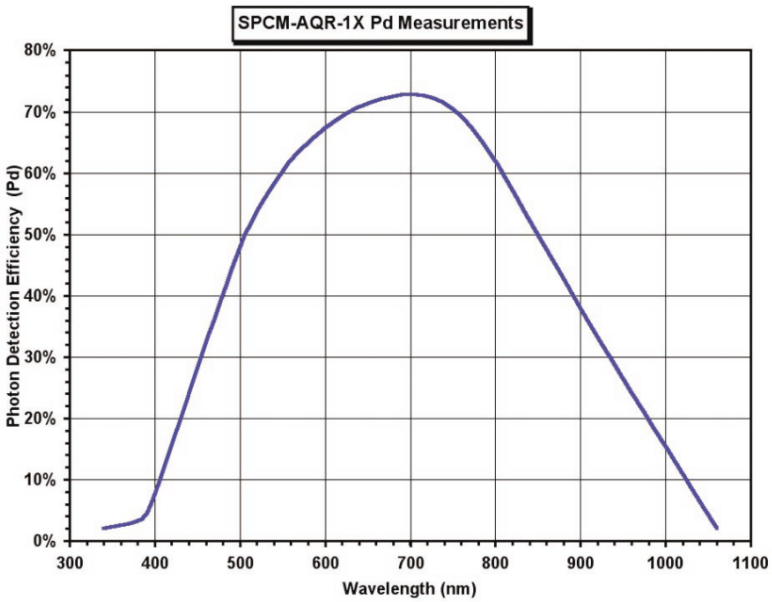


Figure 7.13 – Single-photon detection efficiency versus wavelength for a typical thick-junction silicon single-photon avalanche diode used in these experiments. [13]

850 nm wavelength light emitting diode noise

Although the experimental investigation of additional channel noise showed that it did have an effect on the conditional visibility and fraction of correctly amplified states to all amplified states it was thought that a broadband white light source was not the ideal way to test a noisy channel because in a real quantum channel, the noise is more likely to be of the same wavelength or close the signal wavelength if a filter is placed before entry to the device. The discrepancies between reflection co-efficient of the BSs, and detection efficiencies make the effect of the white light noise more evident, as it was found that the subtraction detector had the greatest respective increase in gated count rate.

Another set of measurements replaced the white light source with an 850 nm wavelength LED which was incident on the first 50:50 BS, as shown in Figure 7.3 position 1. The level of noise added was controlled by a motorised attenuator, allowing for similar noise level measurements to those of the white light source.

Measurements using the 850 nm wavelength LED noise source were performed for a range of $|\alpha|^2$ trying to remain consistent with those used in the white light noise measurements.

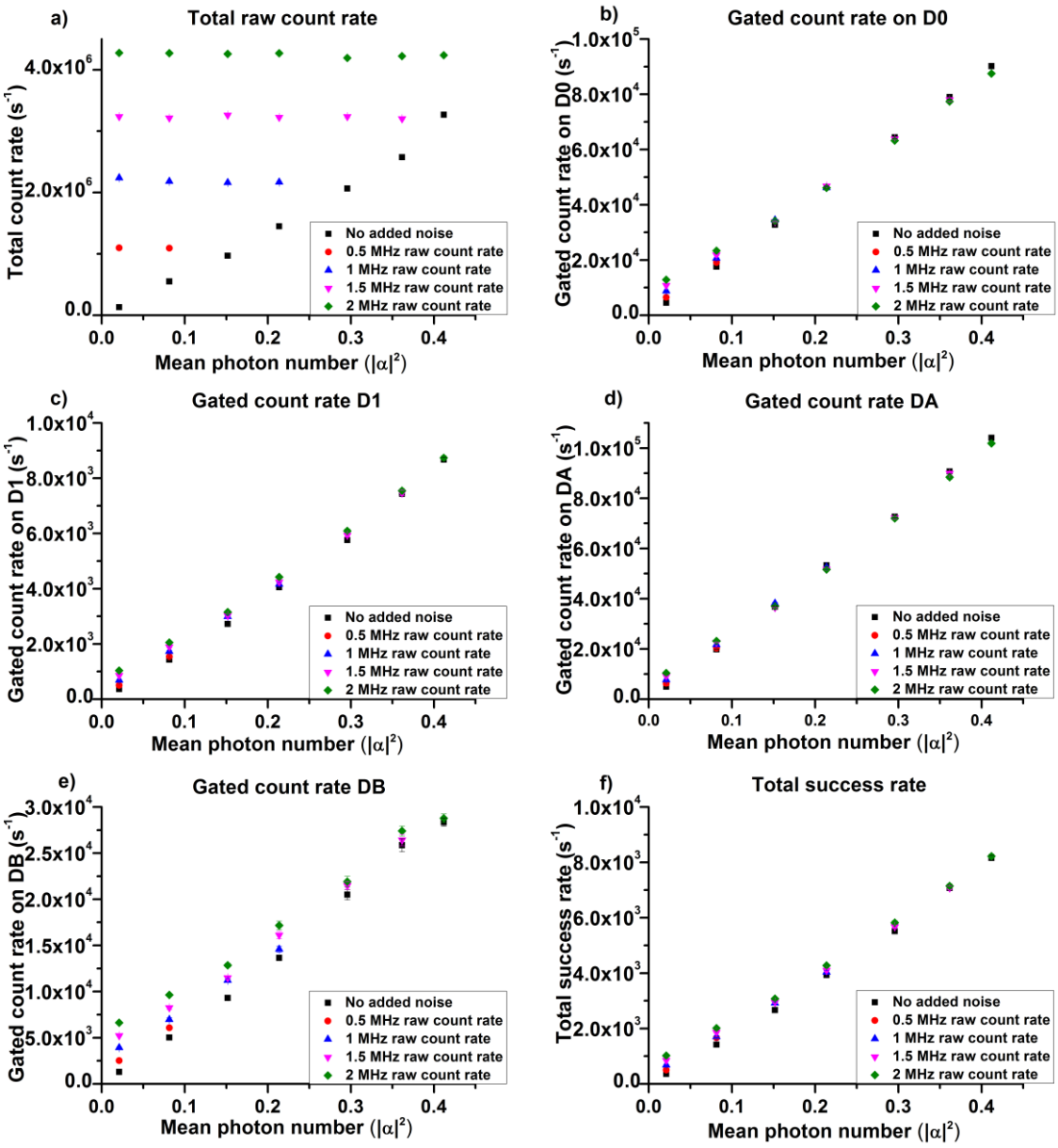


Figure 7.14 - Raw, gated and success rates with added 850 nm wavelength incoherent noise.

The total raw count rate over all detectors is shown in Figure 7.14 a), as before the case with no noise added follows a linear trend with $|\alpha|^2$, whereas the cases with added noise remain flat with changing $|\alpha|^2$. The gated count rates for D0, D1, DA, and DB are shown Figure 7.14 b), c), d), and e) respectively. Unlike the white noise addition, each detector sees a similar increase in the gated count rate, therefore it is likely that the effect of the 850 nm wavelength added noise will be less than that of the white light noise because in the white light added noise the D1 detector received a significant increase, while others only seen minor increases. This is shown in the total success rate plotted in Figure 7.14 f)

which shows that the additional noise from an 850 nm wavelength LED has a very small increase on the overall success rate, whereas the white light noise showed a large increase, even at large $|\alpha|^2 = 0.7$.

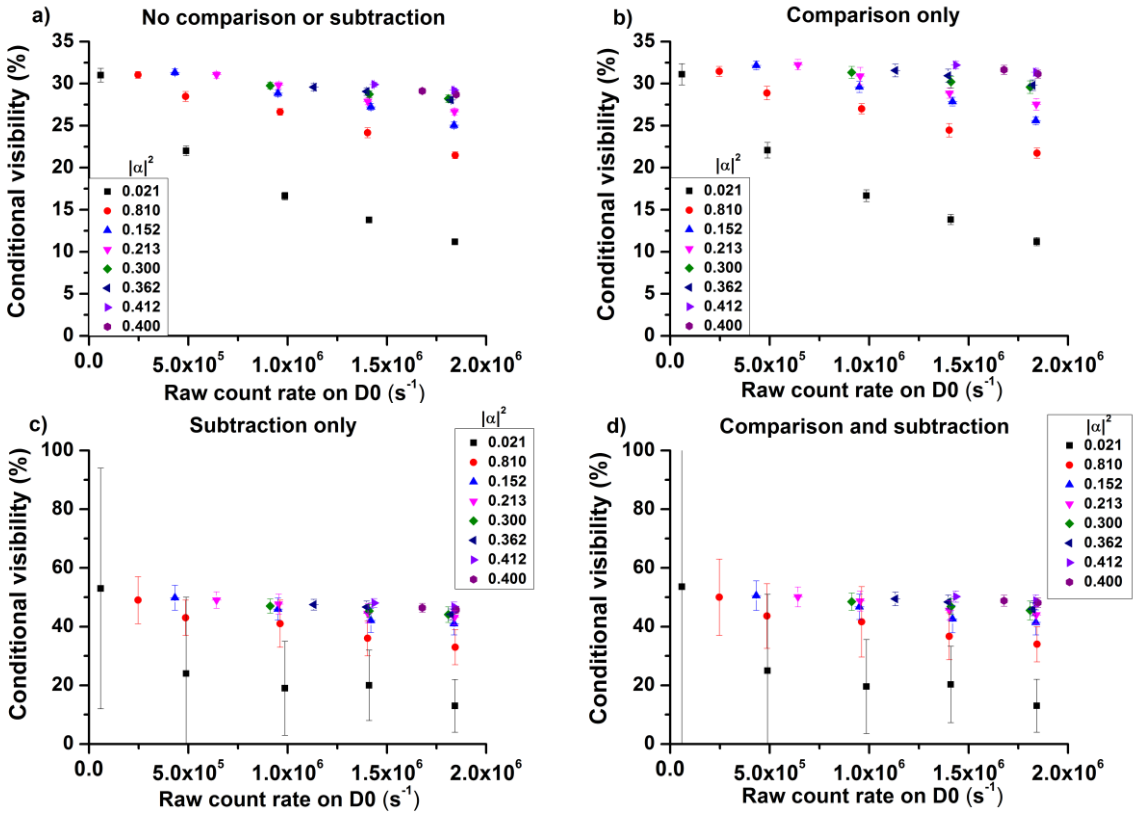


Figure 7.15 - Conditional visibilities of N = 4 with added noise from an 850 nm wavelength incoherent source. Again, the first point in each of the trends is the value without added noise

As was shown in the addition of white light noise experiment, increased count rate on the D1 detector can decrease the conditional visibilities of the system due to Equation 7.4's dependence on the fraction of correct over total successfully amplified rates. The conditional visibilities are shown in Figure 7.15, for the four possible post-selection conditions, a) no comparison or subtraction, b) comparison only, c) subtraction only, and d) comparison and subtraction. The conditional visibility is on the *y*-axis, and the raw count rate on the D0 state comparison detector is on the *x*-axis. For each trend the point at the lowest raw count rate on D0 is the measurement conducted with no additional noise. The larger uncertainties in c) and d) come from the large standard deviations present in the data [31]. The correlations are for 3, and 4 detector correlations respectively and at low

MPNs the probabilities of these occurring are low meaning that the standard deviations are respectively larger than for a) and b).

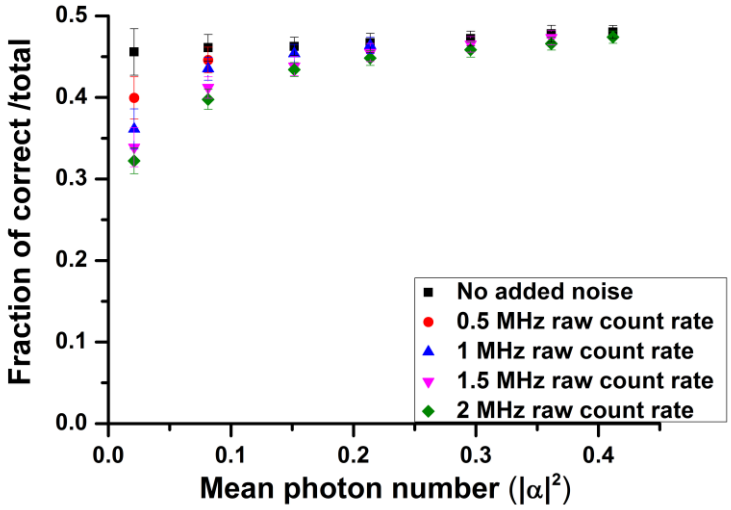


Figure 7.16 - Fraction of correct over total amplified states for N = 4. For N = 4, the ideal fraction should be 1, but due to an non-unitary visibility the fraction will always be lower than 0.5.

Similar to the addition of white light noise, the conditional visibility starts to drop, as the raw count rate on the D0 detector starts to increase. Increasing $|\alpha|^2$ of the signal state causes a reduction in the magnitude of the drop. However, unlike in the white light noise results, here the drop in conditional visibility is primarily due to the increase in the gated DB count rate (decreasing the visibility of the final BS), rather than the increase in D1. It can be seen in Figure 7.16 that the fraction of correct to total successfully amplified states recovers quicker with increased $|\alpha|^2$ than the white light noise results shown in Figure 7.12. By $|\alpha|^2 = 0.2$ the 850 nm wavelength noise results show the additional noise and no added noise are almost comparable while in the white light noise results at $|\alpha|^2 = 0.2$ the no additional noise, and noise results are very much distinguishable.

7.3.3 Discussion

Initial result for the state comparison amplifier device (SCAMP) with a theoretical nominal gain of 1.8 showed that the effective experimental gain (g_{eff}) of the device turned out to be 0.858 ± 0.020 due to losses in the amplifier device caused by splice connections and

inherent optical component loss. The gain remained fairly constant over the range of $|\alpha|^2$ used in the experiment. The highest achieved success probability was found to be > 2.5%, at a $|\alpha|^2 = 0.83$ for $N = 2$, and was also found to be linearly dependent on the $|\alpha|^2$ of the signal state. The post-selection conditions also allowed an increase in the overall visibility of the final fidelity measurement stage. The highest success probability corresponds to > 25k success rate achieved by the amplifier. This is significantly higher than other quantum amplifiers due to the classical light source used.

Noise is an inherent part of communications, this can come from the spontaneous emission of a laser source, scattering in the channel, and background noise which is coupled into the channel. If SCAMP is to be used as an amplifier in any sort of quantum cryptography protocol, then it must be robust to these added sources of noise.

Initial experiments with a broadband white light source showed that noise does affect the success probability, conditional visibility, and the fraction of correct to total successfully amplified states, even with post-selection conditions. This was primarily due to the broadband wavelength of the white light source, and the wavelength dependency of the detection efficiencies which increases at shorter wavelength in the visible regime. The subtraction BS which is 90:10 at $\lambda = 850$ nm would not be uniformly 90:10 over a broader wavelength range because of the optical coatings on the BS itself - it is suspected that at lower wavelengths the BS is more reflective. The higher reflectivity at the shorter wavelengths, and the higher detection efficiencies of the Si-SPAD at shorter wavelengths meant a significant increase in count rate was measured at the D1 subtraction stage. The post-selection conditions for a successful amplification are no photon detection at D0 (the state comparison stage) and a detection at D1. With little increase in the gated count rate at D0, but a significant increase in the D1 gated rate, the number of "successful" amplifications has increased, and lowered the conditional visibility.

Although a communications channel may indeed have broadband noise due to exposed fibre or other input mechanisms, in practice, to minimise the effects of the noise, a series of optical filters would be placed either before the detectors or the SCAMP device, therefore only a small bandwidth of wavelengths would be propagating in the device, and incident on the detectors. To test SCAMP with such noise, the 850 nm wavelength LED source was used to simulate background noise in a communications channel from spontaneous

emission and scattering. This noise was present in all channels, the signal channel, guess from amplifier, and the fidelity stage, the very worst case with noisy components.

The SCAMP device showed that it was it was more robust to added noise with a wavelength of 850 nm for lower $|\alpha|^2$, as the fraction of correct to total successful amplification recovered quicker (i.e. the difference in fraction with added noise became smaller with increasing $|\alpha|^2$ faster) than for the white noise case, as can be seen in Figure 7.12 and Figure 7.16 for the white noise and 850 nm wavelength noise respectively. Therefore if a narrow bandwidth spectral filter(s) is (are) placed into the SCAMP device it will improve the robustness against out-of-band noise. Narrow temporal gating can also assist.

Increasing $|\alpha|^2$ for the signal state showed that the amplifier could be more robust against noise, however increasing the $|\alpha|^2$ is not ideal for quantum communications experiments, as it may allow for successful eavesdropping attacks, such as the photon number splitting attack [33]. In any case the $|\alpha|^2$ reaching the amplifier is very likely to be <0.5 as that is the largest $|\alpha|^2$ currently used in BB84 decoy state QKD experimental protocols [34]. Of course, losses in the communications channel mean the MPN will drop before reaching the amplifier so in reality the input $|\alpha|^2$ will be < 0.5.

7.4 Conclusion & future work

This Chapter introduced the state comparison amplifier (SCAMP), which fits into the category of addition and subtraction quantum optical amplifiers. The device was characterised for different nominal gains, and also tested for robustness against added background noise.

Table 7.1 shows a comparison of some general quantum amplifier properties for comparison with SCAMP. It can be seen that SCAMP has greater success probability, primarily due to the use of a restricted phase-alphabet rather than a continuous range of phase values. The success probability was also linearly dependent on the $|\alpha|^2$ used in the experiment and was observed to reach values >2% for $|\alpha|^2 > 0.7$. It can also be seen that the source technology required for a SCAMP implementation is far simpler than other quantum amplification methods which can require single-photon sources or pair emission from spontaneous parametric down-conversion (SPDC).

Device type	Source of photons	Success probability (%)	Nominal gain	Notes
Addition and subtraction	Spontaneous parametric down-conversion (SPDC), single-photons, coherent or thermal source	1×10^{-4} to 1×10^{-7}	>1	- Photon number resolving subtraction stage can increase gain. - Low success probability due to continuous range of possible phase values.
Heralded scissor device	SPDC	1×10^{-3}	>1	- Use of heralded source gives low success probability. - Herald sources make the device robust against high loss channels.
Entanglement swapping	SPDC	$>>3 \times 10^{-3}$	1	- Multiple entangled heralded sources for many Bell-State measurements make the success probability low.
State comparison and subtraction (SCAMP)	Coherent source	Linear dependence on mean photon number (>2% observed)	>1	- Simple use of off-the-shelf linear optics, detectors and sources. - Shown to be robust against noise of similar wavelength. - Required to be a trusted node.

Table 7.1 – State comparison amplifier comparison table.

Although the theoretical nominal gain of the SCAMP device was 1.8, the effective gain was 0.858 ± 0.020, meaning the device acted as an attenuator that additionally provides some information on the transmitted states. This was due to inherent loss in the optical components and splicing. The losses could be reduced by using purpose built components or even a waveguide construction, although certain waveguide materials have shown high loss at 850 nm, therefore a change in wavelength may be required to take full advantage of this approach.

The robustness of SCAMP with added noise was investigated using two different noise sources, a broadband white light source and 850 nm LED. The white light was shown to have a noteworthy effect on the device performance in terms of success probability and fraction of correct to total successfully amplified states, as the subtraction stage detector saw a significant increase in gated count rate. A photon detection at the subtraction stage was one of the conditions for post-selection so a significant increase in post-selected events would create incorrect amplification events. This substantial increase on the subtraction stage was primarily due to the wavelength dependence of the reflection coefficient and detection efficiency. It was judged that the use of narrow bandwidth optical filters was a requirement, to discard any other wavelengths of noise and therefore further measurements were taken with 850 nm noise. SCAMP was found to be more robust at lower $|\alpha|^2$ for this noise, as the increase in gated count rate was noteworthy.

The first experimental implementation of SCAMP showed a significant improvement in performance over existing experimental implementations in terms of success probability, and therefore success rate.

Future work

One of the main targets of SCAMP, and indeed many other quantum optical amplifiers/repeaters, is to increase the overall transmission distance of quantum communication protocols. This would help quantum communication technologies to be considered in more real world applications. Many previously presented quantum optical amplifier devices have only focused on the amplification of coherent states at high $|\alpha|^2 > 0.5$ with little consideration to the how a device would perform in a realistic communications channel. Therefore future analysis of SCAMP would consider operation in an optical channel. The optimal position for SCAMP in a communication channel, and the number of devices to employ are both factors that would have to be considered. Consideration should be made to other SCAMP configurations, and feedforward mechanisms which could help increase the success probability, conditional visibilities, and the gain.

Indistinguishable sources

While in the SCAMP experiments presented here the laser source was simulated by splitting the signal into two paths, phase modulating one of the paths to provide a “guess

state", and then recombined on the state comparison BS (essentially operating as an interferometer) in practice a quantum amplifier node would be a self-contained device with its own laser source providing the photons for the "guess state".

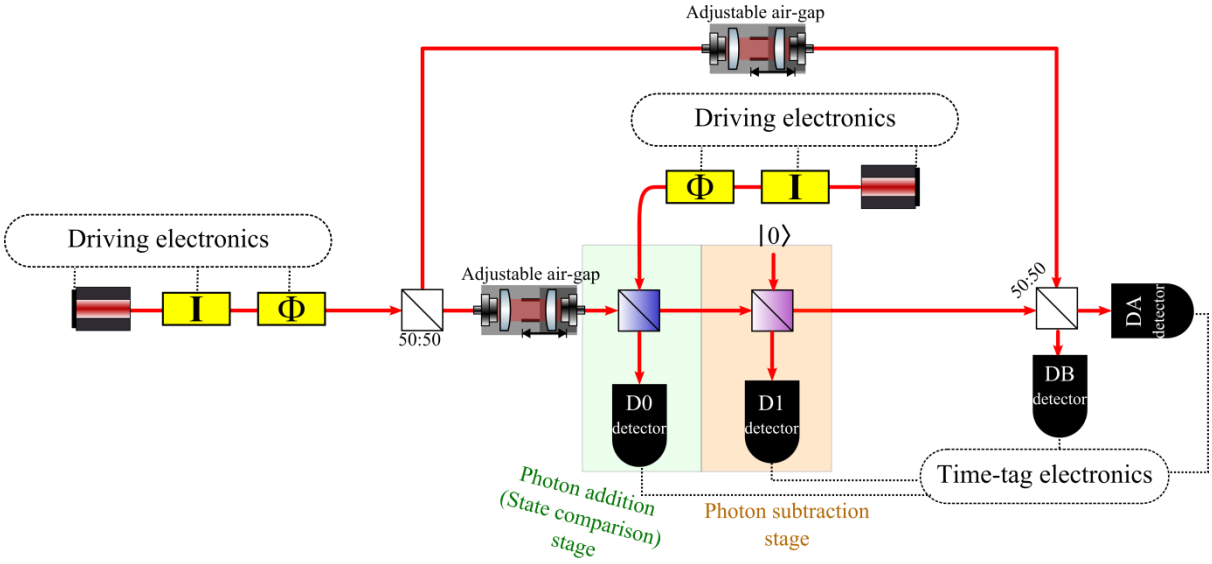


Figure 7.17 – A schematic design of how the state comparison amplifier could be tested in the laboratory with two independent indistinguishable sources. Each source would have separate driving electronics and controls, to drive the laser source, intensity modulator, and phase modulator.

In future work a SCAMP system could be tested with two independent indistinguishable sources, such a two narrow spectral band-width distributed feedback lasers which are known to be wavelength tuneable [24]. A simple schematic of how a test system might look is shown in Figure 7.17, which looks similar to the system used in this experiment, except the guess state coherent state source is now generated by a separate source. Difficulties arising from the use of two independent and indistinguishable sources will come from the monitoring and control of the wavelengths and pulse generation from each source, as this will greatly affect the visibility of the state comparison and final fidelity stages, as high visibility requires the states to be indistinguishable, a slight change in wavelength will reduce the visibility dramatically [35].

Applications of the state comparison amplifier

Like the laser at first introduction, SCAMP may be a device which is a solution looking for a problem. This section discusses some of the possible applications for SCAMP.

Quantum fingerprinting

Quantum fingerprinting involves three parties Alice, Bob, and a referee [36], [37]. The aim of the protocol is to check whether Alice and Bob have the same message, or code word, by sending less information for a comparison than needs to be sent by a classical equivalent [37].

Alice and Bob each have a message, apply an error correction code (to increase any mismatches) and covert that into a sequence of encoded coherent states. They send their sequences to the referee who performs a state comparison and measures the outcome.

The quantum fingerprinting protocol does not appear to have dependence on bit rate, more the quality of the information reaching the referee. If this is the case, a SCAMP device could be used in the communications channel to help extend the transmission distance of the correctly guessed states. The post-selection events could be correlated with detection events at the receiver to show that the amplifier gave amplification, and the states received where either equal or not for the N=2 case.

However, the low success probability of SCAMP at the low mean photon numbers typically used in quantum fingerprinting may mean that more information (coherent states) is required to be sent by Alice and Bob, meaning SCAMP actually causes the protocol to perform worse.

Continuous-variable quantum key distribution (CV-QKD)

An ideal application for quantum amplification would be to help increase the transmission distance of quantum communication protocols. CV-QKD, briefly described in Chapter 3, uses a continuous range of mean photon numbers and phase quadrature values relying heavily on classical reconciliation and privacy amplification. CV-QKD uses coherent states of $|\alpha|^2 > 1$, much greater than discrete variable protocol [38]. These higher |a|2 values may mean SCAMP could find a use in CV-QKD.

It was shown that as $|\alpha|^2$ values increased the success probability of SCAMP also increased. However this would still be around 4-5% for this SCAMP configuration, too low for a benefit to be seen.

The success probability could be increased by using more efficient single photon detectors, and also a feedforward mechanism to correct for any known mistakes .

Other applications

SCAMP has been shown to operate at high clocking frequencies with a high fidelity output, something other quantum amplifiers have not shown as of yet. However at present no immediate applications fit into the niche characteristics that SCAMP provides.

The device also features the following properties:

- Works with a known phase-alphabet and guesses between the values.
- Post-selection of detection events to give noiseless amplification.
- Success probability is linearly dependent on the $|\alpha|^2$ value incident on the amplifier node.
- Can operate at MHz repetition frequencies.
- High fidelity output for correctly guessed states.

A quantum information scenario which requires amplification, but the performance is not dependent on an information transfer rate would be an idea application for SCAMP.

7.5 Acknowledgements

Professor Stephen Barnett, Dr John Jeffers, and Dr Electra Eleftheriadou, worked on the initial theoretical proposal for the state comparison amplifier. Their discussions with Professor Gerald Buller, Dr Robert Collins and the author led to the experiments' initial design. Robert initially wrote the MATLAB code that performed the data acquisition and initial time-tag analysis.

7.6 Bibliography

[1] E. Eleftheriadou, *et al.*, "Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.*, vol. 111, no. 21, p. 213601, Nov. 2013.

[2] R. J. Donaldson, *et al.*, "Experimental Implementation of a Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.*, vol. 114, no. 12, p. 120505, 2015.

[3] N. Gisin, *et al.*, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[4] H. Bechmann-Pasquinucci, *et al.*, “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,” *Phys. Rev. A*, vol. 59, no. 6, pp. 4238–4248, 1999.

[5] K. Tamaki, *et al.*, “Security of the Bennett 1992 quantum-key distribution against individual attack over a realistic channel,” *Phys. Rev. A*, p. 16, 2002.

[6] N. Bruno, *et al.*, “Heralded amplification of photonic qubits,” *Opt. Express*, vol. 24, no. 1, p. 125, Jan. 2016.

[7] G. Y. Xiang, *et al.*, “Heralded noiseless linear amplification and distillation of entanglement,” *Nat. Photonics*, vol. 4, no. 5, pp. 316–319, 2010.

[8] N. Bruno, *et al.*, “A complete characterization of the heralded noiseless amplification of photons,” *New J. Phys.*, vol. 15, 2013.

[9] P. Marek and R. Filip, “Coherent-state phase concentration by quantum probabilistic amplification,” *Phys. Rev. A*, vol. 81, no. 2, pp. 022302Marek, P., & Filip, R. (2010). Coherent–stat, Feb. 2010.

[10] A. E. Lita, *et al.*, “High-Efficiency Photon-Number-Resolving Detectors based on Hafnium Transition-Edge Sensors,” vol. 351, no. 2009, pp. 351–354, 2009.

[11] D. Fukuda, *et al.*, “Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling.,” *Opt. Express*, vol. 19, no. 2, pp. 870–875, 2011.

[12] L. A. Coldren and B. J. Thibeault, “Vertical-Cavity Surface-Emitting Lasers,” in *Optical Fiber Telecommunications IIIB*, Elsevier, 1997, pp. 200–266.

[13] Perkin-Elmer Optoelectronics, “SPCM-AQRH Single Photon Counting Module,” *Perkin-Elmer Optoelectron. Datasheet*, pp. 1–10, 2002.

[14] Excelitas Technology, “Single Photon Counting Modules,” 2015.

[15] E. Eleftheriadou, *et al.*, “Quantum Optical State Comparison Amplifier,” pp. 1–5, 2013.

[16] Novatech Instruments Inc, “Models 2960AR and 2965AR Disciplined Rubidium Frequency Standards,” pp. 1–8, 2004.

[17] Agilent Technologies, “Agilent 8648A / B / C / D Signal Generators Spectral purity

Internal reference oscillator," no. March 2007, 2012.

[18] Picoquant, "HydraHarp 400 Single Photon Counting System User's Manual and Technical Data," vol. 1.2.

[19] Agilent Technologies, "Agilent 81110A 165/330 MHz Agilent 81104A 80 MHz Pulse/Pattern Generators," 2000.

[20] Photline, "NIR-MPX800 series phase modulator," 2010.

[21] J. Tatum and J. Guenter, "Modulating VCSELs," *Honeywell Int.*, pp. 1–19, 1998.

[22] Newport, "Model 500B Series Laser Diode Drivers," *Model 500B Ser. User's Man.*, vol. 1, 2003.

[23] Thorlabs, "Thorlabs Piezoelectric-actuator Specification Sheet," *Rev C*, 2013.

[24] H.-F. Liu and W. F. Ngai, "Nonlinear dynamics of a directly modulated 1.55 μm InGaAsP distributed feedback semiconductor laser," *IEEE J. Quantum Electron.*, vol. 29, no. 6, pp. 1668–1675, Jun. 1993.

[25] Avtech Electrosystems Ltd., "AVX-SP AND AVX-CP SERIES."

[26] Mathworks, "MATLAB 2014b (8.4.0.118713)." The MathWorks Inc., Natick, Massachusetts, 2014.

[27] ID Quantique, "Visible single-photon detection module with high timing resolution and low dark count rate.," 2015.

[28] Thorlabs, "Fiber-Coupled High-Power LED," *Rev A*, pp. 0–1, 2013.

[29] Koninklijke Philips N.V. (Royal Philips), "Halogen non-reflector," 2015.

[30] Intel, Compaq, *et al.*, "Universal Serial Bus Specification," *Group*, p. 650, 2000.

[31] L. Kirkup, *Experimental Methods: An Introduction to the Analysis and Presentation of Data (Physics)*, 1st ed. John Wiley & Sons, 1995.

[32] K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 71, no. 4, pp. 3–6, 2005.

[33] M. Dušek, *et al.*, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Opt. Commun.*, vol. 169, no. 1–6, pp. 103–108, 1999.

[34] L. O. Mailloux, *et al.*, "Quantum key distribution: examination of the decoy state protocol," *IEEE Commun. Mag.*, vol. 53, no. 10, pp. 24–31, Oct. 2015.

[35] H.-K. Lo, *et al.*, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012.

[36] J. M. Arrazola and N. Lütkenhaus, "Quantum fingerprinting with coherent states and a constant mean number of photons," *Phys. Rev. A*, vol. 89, no. 6, p. 062305, Jun. 2014.

[37] F. Xu, *et al.*, "Experimental quantum fingerprinting with weak coherent pulses," *Nat Commun*, vol. 6, Oct. 2015.

[38] D. Huang, *et al.*, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Opt. Express*, vol. 23, no. 13, p. 17511, 2015.

Chapter 8

Further Characterisation of the State Comparison Amplifier

8.1 Introduction

The state comparison amplifier (SCAMP) was shown to be an interesting device in the previous Chapter, with higher success probability that any other experimentally realised non-deterministic quantum amplifier, implementing less complex experimental components and methods [1], [2]. This Chapter follows on from the previous Chapter's work, providing a further investigation on the SCAMP device including:

- Increasing the nominal gain from 1.8 to 9 by changing the state comparison beamsplitter (BS).
    - Also investigating robustness with added noise at a wavelength of 850 nm.
- Adding an extra subtraction stage after the nominal gain of 9 SCAMP, to improve the conditional visibilities and fidelity.

The reasons behind the experiments are discussed in following paragraphs, followed by the experimental implementation, results and discussion. Given that the experimental implementation and methods are very similar to the previous Chapter of SCAMP, only the differences will be highlighted in this Chapter, to save repetition.

As mentioned in the previous Chapter, the original design of SCAMP had a nominal gain of 1.8. When experimentally tested, it was found that the device was not actually working as a 'true' amplifier due to only having an estimated effective gain, $g_{\text{eff}} \approx 0.87$ (or, a loss of 0.13). This was due to inherent losses in optical components and construction.

Two ways of improving g_{eff} could be, constructing a device with low loss components, or increasing the nominal gain to overcome the losses. The latter was chosen as the approach for the experiments carried out in this Chapter. A beamsplitter (BS) with a 90:10 BS ratio was chosen to replace the 50:50 state comparison BS. This would give the device a nominal gain of 9, following $g_{\text{nom}}=t_2/r_1$, where r_1 is the reflection of the state comparison BS, and t_2 is the transmission of the subtraction stage. This should show true gain (i.e. $g_{\text{eff}}>1$) even in the presence of the expected system losses.

As before, the robustness of the SCAMP device is tested against different levels of channel noise. Only the 850 nm wavelength LED is implemented in the experiment as it was concluded from the previous Chapter that a narrowband width filter could be used to block most broadband wavelength noise, as it was seen that white light noise greatly affected the SCAMP success rates.

The introduction of an extra subtraction stage, allows an extra post-selection condition to be added. From Chapter 6, the photon addition and subtraction experiments similar to the configuration of SCAMP were known to contain photon number resolving (PNR) detectors [3], [4]. This allowed these experiments to alter the gain factor and also fidelity. By introducing an extra subtraction stage it is possible for an improved fidelity SCAMP output without the requirement for PNR detectors.

8.2 Experimental implementation

All experiments were carried out at a source repetition rate of 1 MHz, using a very similar experimental set-up to that used in the previous Chapter. An experimental diagram of the optical system is shown in Figure 8.1 illustrates how similar the set-ups were (Figure 7.2 is the previous system). The electrical system is the same for this Chapter as well, Figure 7.3 in the previous Chapter. Only changes to the experimental set-up are mentioned here as all other details can be found in the previous Chapter.

The first change made was the swapping of the 50:50 state comparison BS with a 90:10 BS. This meant re-calibration of the optical losses and path lengths. Leading to the guess intensity from the amplifier being ≈10× greater than the signal intensity, this is not seen as a problem because the amplifier node would have its own attenuated coherent source which could provide enough power.

For the added noise experiment, the 850 nm wavelength LED (spectral FWHM 30 nm [5]) added noise was introduced by free-space coupling into the signal channel only, unlike the previous Chapter where it was introduced into all channels. It was chosen only to be added into the signal channel to simulate noise in the signal channel only, since the noise from the local source of the comparison stage is likely to be considerably less.

Like the previous Chapter's noise measurements the mean photon number ($|\alpha|^2$) was selected without any noise present. When noise was to be added, the vertical-cavity surface-emitting laser (VCSEL) diode source for the experiment was blocked, the LED was turned on, and the level of power adjusted and monitored on the D0 state comparison stage detector. Three different noise levels were set for measurement during the experiment, ≈ 0.1, 0.5, and 0.9 MHz noise only raw count rate on the D0 detector. Once the level was set the VCSEL diode was unblocked and the experiment continued as normal, for a particular phase-alphabet.

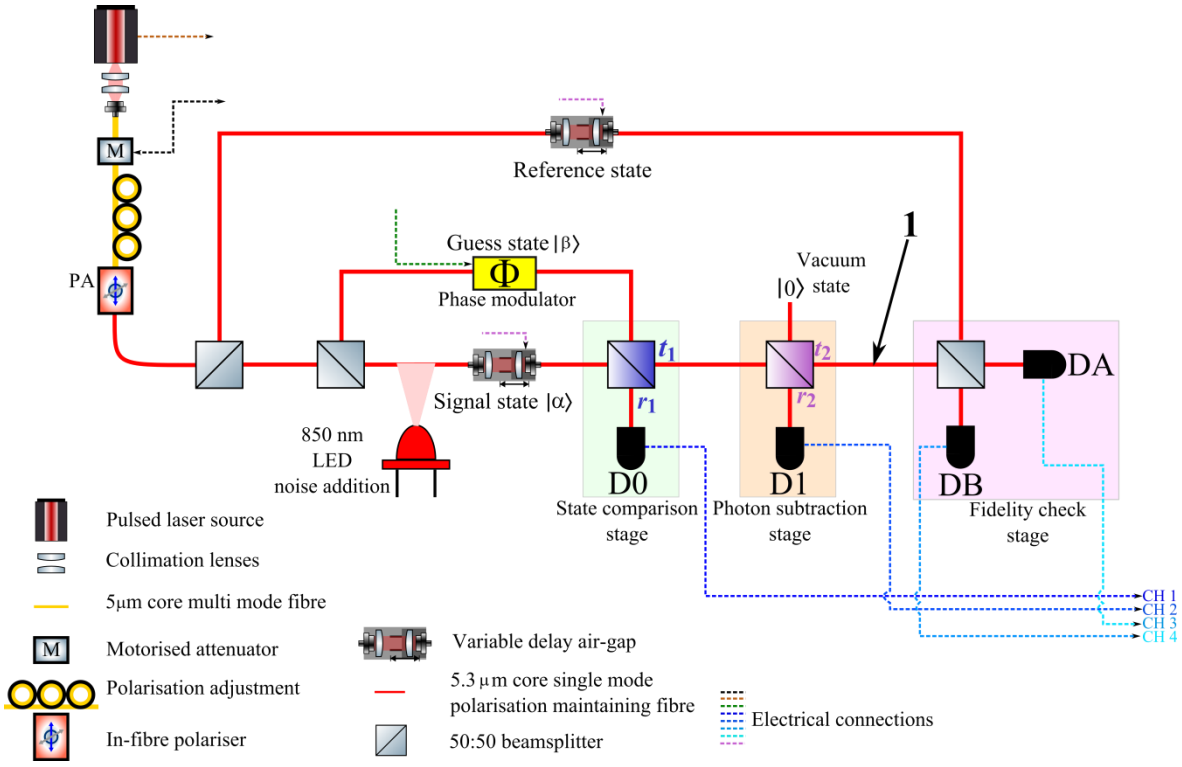


Figure 8.1 – A modified version of experimental diagram from the previous Chapter showing where the additional noise for the 90:10 BS experiments was added, and also the position of the extra 90:10 beamsplitter which was used for photon subtraction denoted 1.

The extra subtraction stage was introduced after the first stage, denoted as position 1 in Figure 8.1. The extra subtraction stage was a 90:10 BS. This experiment was carried out after the 90:10 BS replacement in the state comparison stage, therefore all three BSs acting as the SCAMP node are 90:10. The extra subtraction stage required another single-photon detector, which was the same design of silicon single-photon avalanche diode used for

every other experiment in this Thesis, the Excelitas SPAD [6]. This extra BS also required the system to be recalibrated for loss and optical path length. It also required some editing of the MATLAB [7] code, to include the extra subtraction stage for data acquisition and processing.

8.3 Nominal gain of 9 results

Estimation of $|\alpha|^2$ for this experiment was calculated using Equation 8.1, a modified version of Equation 7.2 from the previous Chapter which is scaled to compensate for the 90:10 ratio of the BS now used for the state comparison: This also takes into account the single-photon detection efficiency (SPDE) and loss from the point of $|\alpha|^2$ before the comparison BS to the single-photon detector (l_{comp}).

$$|\alpha|^2 = \frac{\text{Maximum} + \text{Minimum}}{2 \times \text{SPDE} \times l_{comp} \times \text{Repeated pattern frequency}} \times \frac{10}{9} \qquad \text{Equation 8.1}$$

Raw and gated count rates for N = 2, 4, and 8 are shown in Figure 8.2, with the left sub-figures for raw count rates, while the gated count rates are on the right. As can be seen when the gated and raw are compared, between 70-90% of the raw count rate is retained in the gating process, showing significant improvement over the previous results with the 50:50 state comparison BS which was <5%. The increase in retained raw rate is because of improved laser stability and lower background. It can also be seen that the range of $|\alpha|^2$ is more consistent between phase-alphabets, because of the improved laser stability.

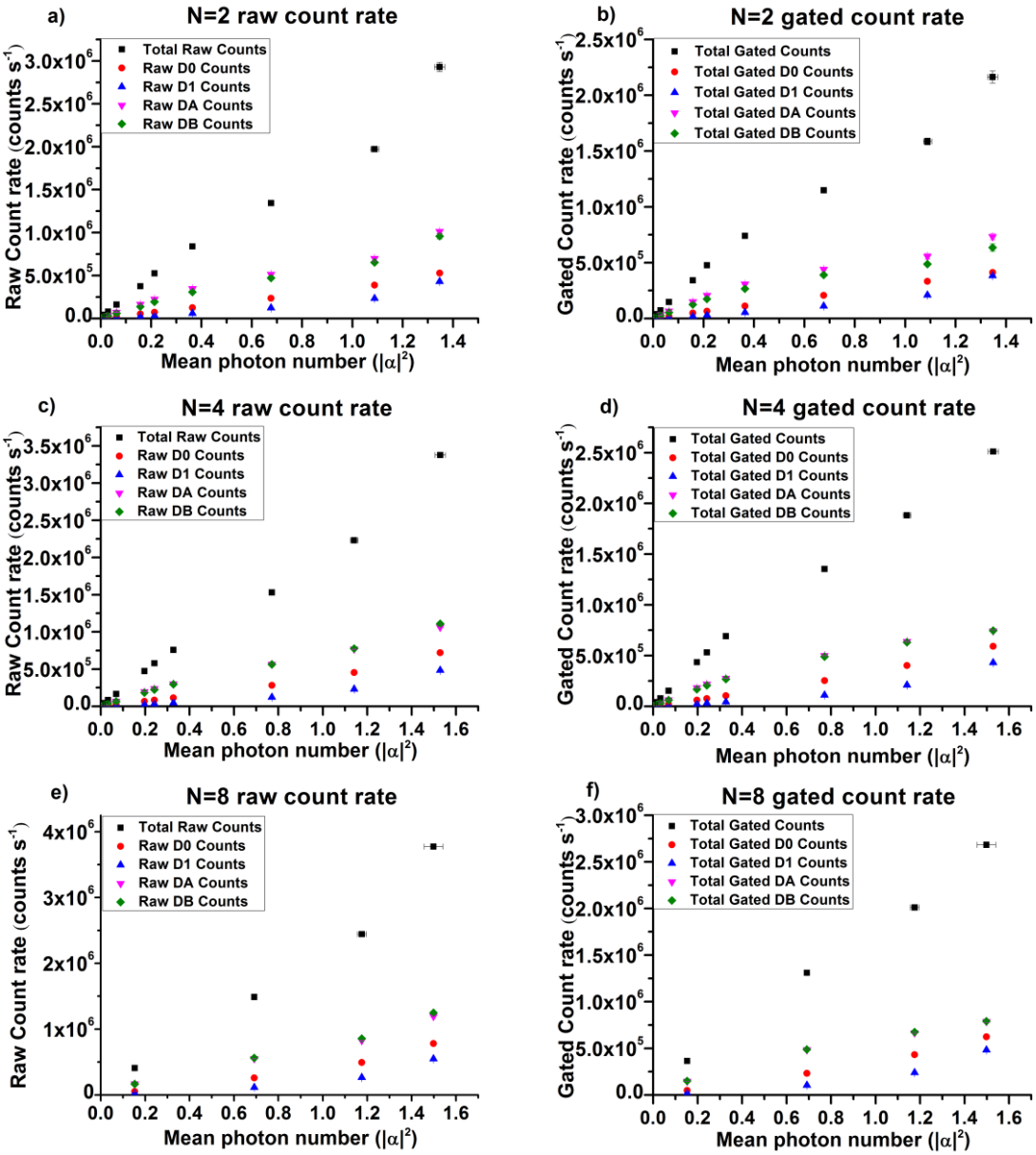


Figure 8.2- 1 MHz 90:10 state comparison beamsplitter (BS) raw and gated count rates for N = *2, 4, and 8. The left side are the raw count rates, while the right are the gated count rates.*

Figure 8.3 a), b) and c), corresponding to $N = 2$, 4, and 8 respectively, show how the conditional visibility described in the previous Chapter (Equation 7.4) changes as different conditions are applied - from no comparison or subtraction to a comparison or subtraction only, to full comparison and subtraction.

Interestingly, while in the 50:50 state comparison BS experiment the 'comparison only' condition was only a marginal improvement over the 'no comparison or subtraction' case,

and the 'comparison and subtraction' only marginally improved upon the 'subtraction only', whilst for the 90:10 state comparison BS this was not the case across the full range of $|\alpha|^2$. At $|\alpha|^2$ <0.2 this is still true, however, at $|\alpha|^2 \geq 0.2$ the 'subtraction only', and 'comparison only' overlap and cross. For the 50:50 state comparison BS, the loss balancing on the state comparison BS meant that when a guess was π out phase with signal, all the photons would be routed to the D0 detector, while in the 90:10 case, photons will still be routed through the amplifier. The increase in detections at D1 will lead to a lower conditional visibility, while a good visibility on the state comparison will still mean the guess right will not be routed to the D0 detector. Therefore at higher $|\alpha|^2$ the comparison only events are more significant.

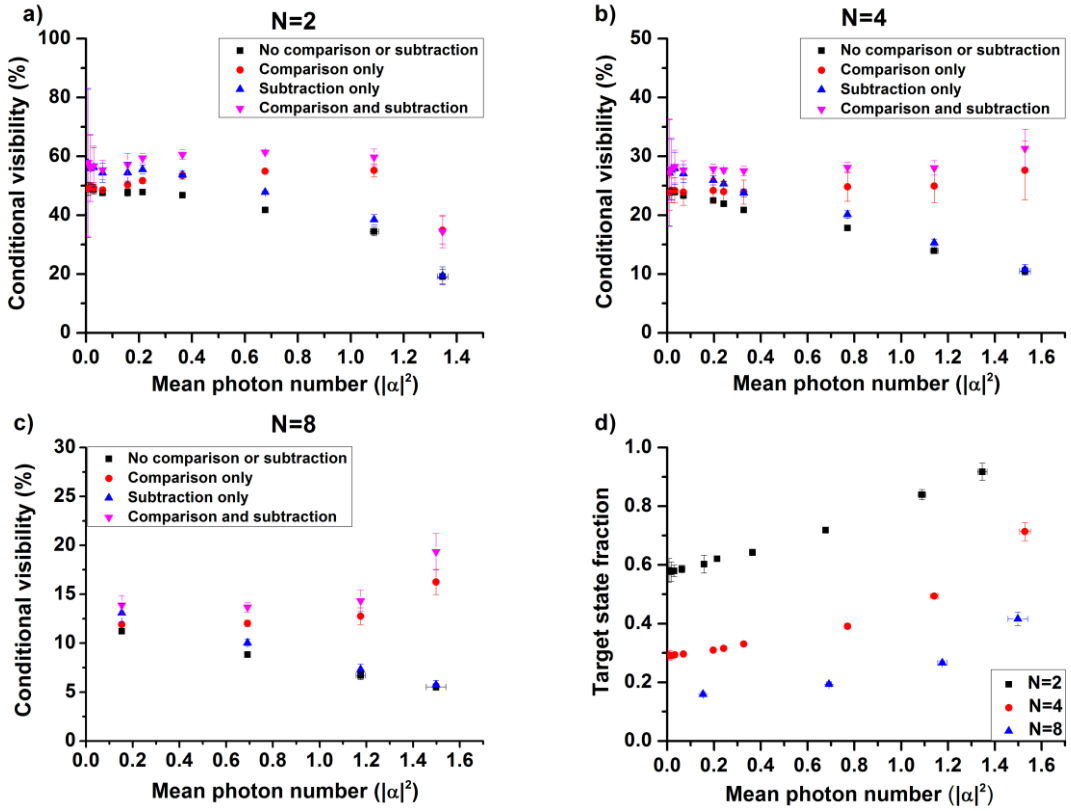


Figure 8.3 – 90:10 state comparison beamsplitter (BS) conditional visibilities calculated using Equation 6.5 for N = *2, 4, and 8.*

The conditional visibility for N = 2, 4, and 8 increases with $|\alpha|^2$, however the final point in N = 2 drops off unexpectedly. The detectors at these $|\alpha|^2$ are counting at >1 MHz, so there may be some nonlinear effect taking place in the detectors [6].

The target state fraction (TSF), plotted in Figure 8.3 d), following Equation 7.5, is the fraction of successful amplification events which are guessed correctly. The TSF remained constant for the 50:50 state comparison configuration aside from at very low $|\alpha|^2$ where the count rate was approaching the dark count rate, while in this experiment the TSF increases as the $|\alpha|^2$ increases. This is thought to be due to non-linearity effects in the detectors for the greater intensity pulses.

Following on from the TSF, Figure 8.4 shows the total success rates, with correctly and incorrectly guessed successes for $N = 2$, 4, and 8, a), b), and c) respectively. It can be seen that at higher $|\alpha|^2$ (>1), the other guessed success rate tails and drops off. This is thought to be caused by the recovery of the detectors at the high photon counting levels at these high $|\alpha|^2$ levels. This effect is largely seen in the $N = 4$, and 8 figures, which is why the total success rate tails off for those two phase-alphabets as is seen in Figure 8.4 d).

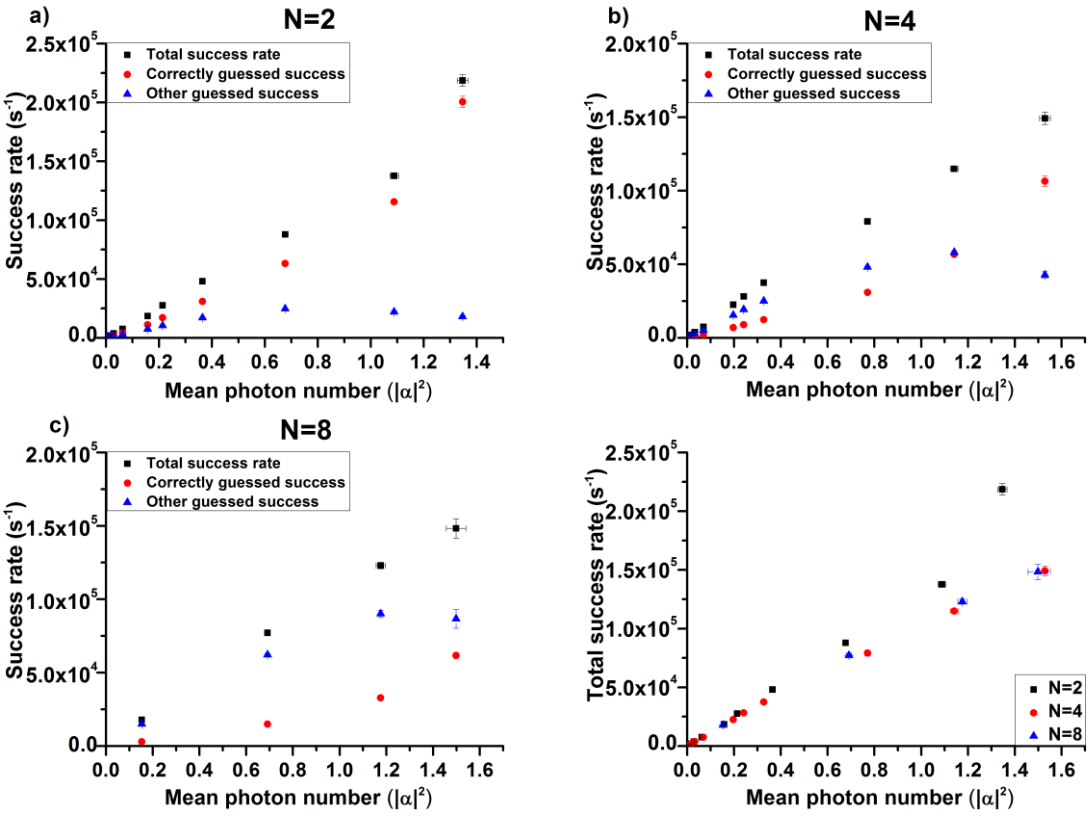


Figure 8.4 – Success rates for N = *2, 4, and 8 in a), b), and c). The total success rates placed together for comparison in d).*

The estimated effective gain, g_{eff}, of the 90:10 SCAMP amplifier is shown in Figure 8.5 a), following Equations 7.6, 7.7, and 7.8 and taking into account the state comparison BS ratios. The figure shows that g_{eff} is >1, indicating that is does indeed work as an amplifier, unlike the previous configuration. The decreasing trend with increasing $|\alpha|^2$ comes from non-linear detector response and dead-time in the detectors at higher $|\alpha|^2$, although even then the estimated effective gain is still >1.

The success probability, as given in Figure 8.5 b), has been shown to reach a value of >5% for $|\alpha|^2$ >0.4. The success probability is defined as the number of successful correlations from the SCAMP amplifier (i.e. time correlations when there are no measured events at D0, and a measured event at D1) divided by the clock frequency of the system, which in this case is 1 MHz. It can be seen that the success probability can reach as high as 21.8 ± 0.48% from $N = 2$, at a $|\alpha|^2 \approx 1.4$. This corresponds to a success rate of >200 KHz, a factor of 10 greater than seen in the previous experiment. The trends for success probability are equal across the different N values for $|\alpha|^2 < 0.7$, however $|\alpha|^2 > 0.7$ $N = 2$ follows a separate trend to the $N = 4$, and 8 case. This is thought to be caused by the clock frequency of the laser which was so high that the detectors were unable to recover at such high photon counting levels, causing the 'other amplification successes' to be missed, reducing the overall success probability.

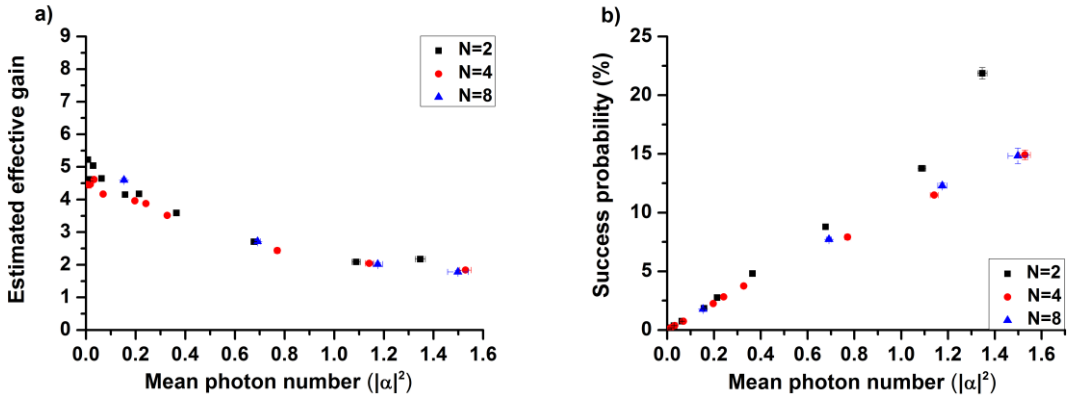


Figure 8.5 – Estimated effective gain, a), and the success probability, b).

If a comparison between the 50:50 BS, 1 MHz results are taken, for $|\alpha|^2 = 0.238$, the success probability is 0.491%, where as in the 90:10 BS case for a similar $|\alpha|^2 = 0.213$, the success probability is 2.76%, a significant increase in the success probability.

One of the primary improvements the 90:10 state comparison BS SCAMP device has shown is the increased estimated effective gain of >1. The g_{eff} value is ≈ 4.7, however this decreased with increasing $|\alpha|^2$ due to the fidelity stage DA, and DB, where non-linear detector responses occurred due to high peak intensities of the amplified beam. Significantly higher success probabilities were also shown, having a linear relationship with increasing $|\alpha|^2$ until limitation of visibility and non-linear detector response caused some deviation at higher $|\alpha|^2$ (i.e. >0.5).

8.3.1 90:10 state comparison beamsplitter noise analysis

The results presented in this section are for the $N = 4$ case like the previous Chapter.

Figure 8.6 shows the a) total raw count rate, b-e) gated rates for each detector and f) the total success rate for $N = 4$, with no added noise, and the three other levels of added noise.

In Figure 8.6 a), the total count rate, it can be seen that the no noise measurements follow an almost linear trend with $|\alpha|^2$. With the addition of noise, an offset is added that increases with the increasing noise.

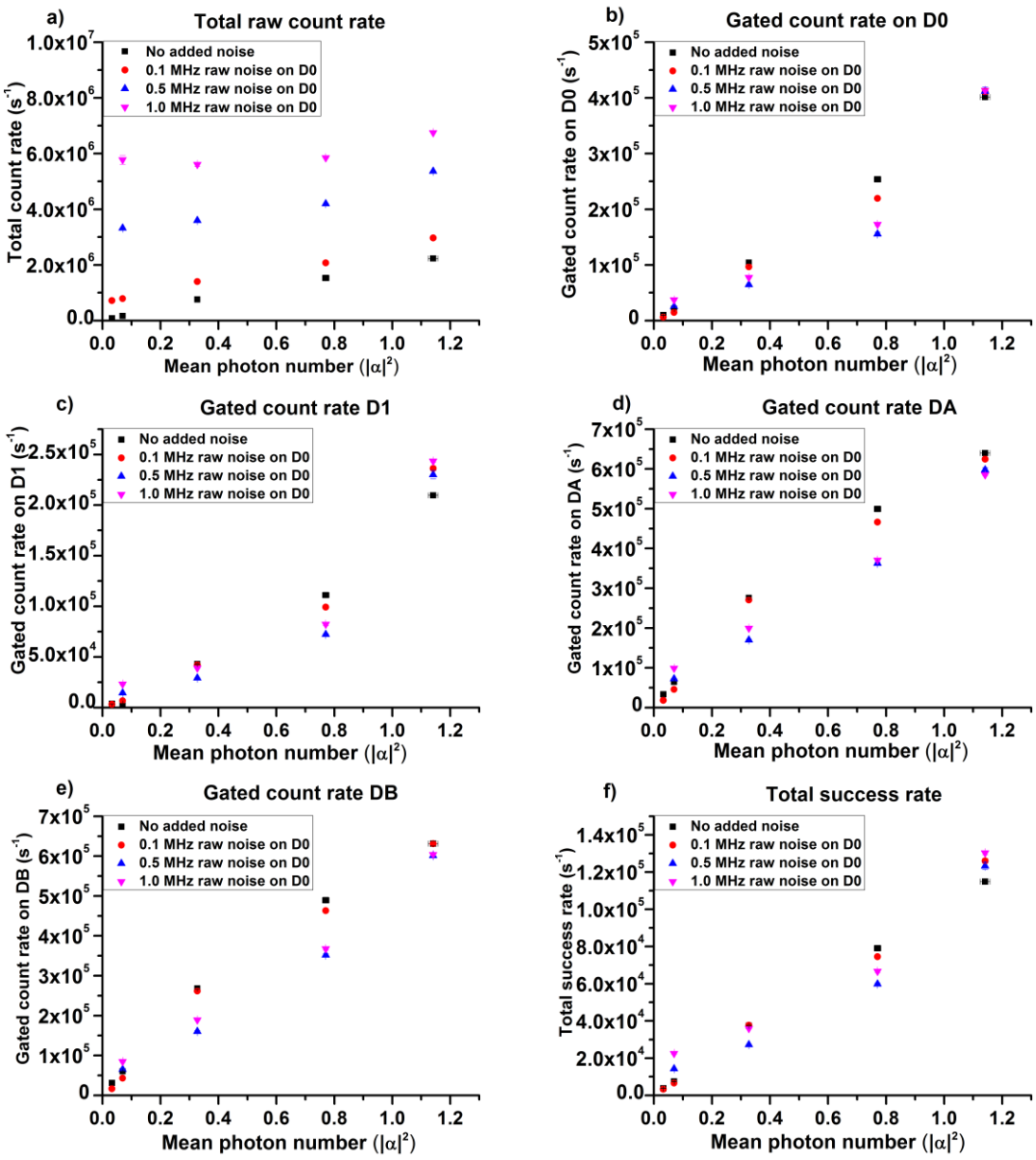


Figure 8.6 – Added 850 nm wavelength LED noise to the 90:10 state comparison beamsplitter (BS) set up a) raw count rates, b-e) gated count rates, and the total success rate for N = 4.

The general trend for the gated count rate with added noise is to decrease with increased level. Because the noise is essentially a constant background, the number of increased events outside the gating region is causing the number of events in the gated region to drop. This is because an event outside the gating region will cause the detector to reset. The reduced gated rate leads to a reduced total success rate, seen in Figure 8.6 f).

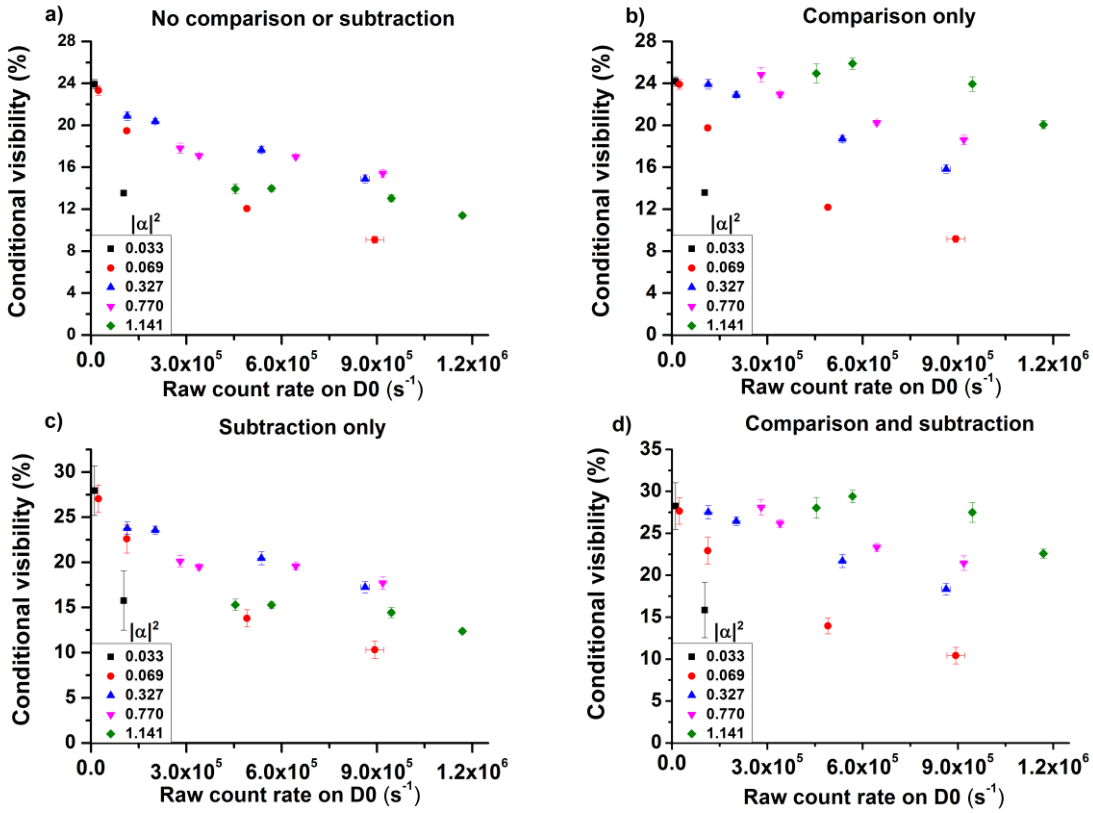


Figure 8.7 – N=*4 850 nm noise conditional visibilities calculated using Equation 6.4, the four different conditional visibilities, 'no comparison or subtraction' a), 'comparison only' b), 'subtraction only' c), and 'comparison and subtraction' d).*

Conditional visibility trends with no noise are shown in Figure 8.3 b) for $N = 4$. It was found that as $|\alpha|^2$ increased, the trends for 'no comparison or subtraction' and 'subtraction only' were to decrease, while the trends for 'comparison only' and 'comparison and subtraction' were to increase with $|\alpha|^2$. Figure 8.7 shows the results for $N = 4$ with a sub-figure for each condition. The first point in each trend is the no noise measurement for that $|\alpha|^2$ and it can be seen that for the no noise measurements the sae trends are seen as in Figure 8.3. As expected from the previous Chapter's noise results, the increased level of noise reduces the conditional visibility. However increasing $|\alpha|^2$ allows for some compensation.

It was shown from Figure 8.4, the fraction of correct/total successful amplifications for $N = 2$, 4, and 8, increased with greater $|\alpha|^2$, i.e. the fraction of correct over total successfully amplified states increased. This was found to be due to a decrease in

incorrectly guessed successes because of nonlinear detector properties and dead-time. It can be seen from Figure 8.8 that the added noise at $|\alpha|^2$ <1 tends to decrease this fraction, as the added noise creates false events on the D0 detector making the decreasing the number of correctly guess successful states. At the highest $|\alpha|^2$ it can be seen that the noise has a varied effect on the fraction, probably because there are so many events on the D1 subtraction stage, and the effect of the added noise (i.e. adding counts into the D0 detector) is not as significant as at lower $|\alpha|^2$.

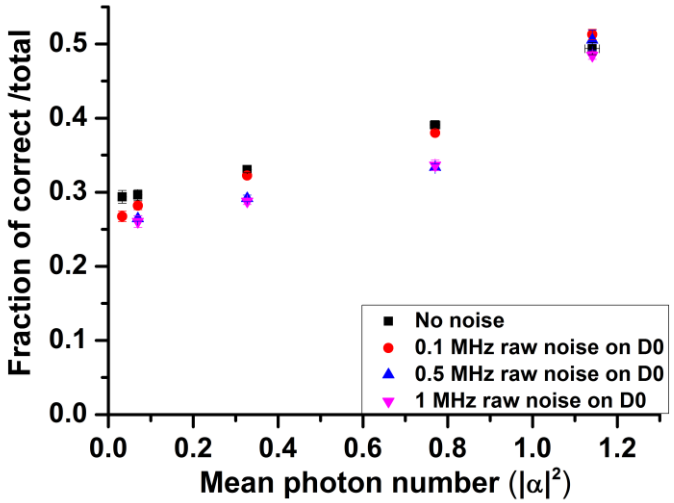


Figure 8.8 – Fraction of the correctly guess successful amplifications over the total number of successful amplifications for N = *4.*

8.4 Extra subtraction stage

As mentioned previously an extra subtraction stage, (following the original subtraction stage) was introduced to increase the fidelity and conditional visibilities of the 90:10 state comparison amplifier output, in a similar way to how photon number resolving (PNR) detectors [8] could be conditioned to post-select events with *M* numbers of photons for variable fidelity and gain [4].

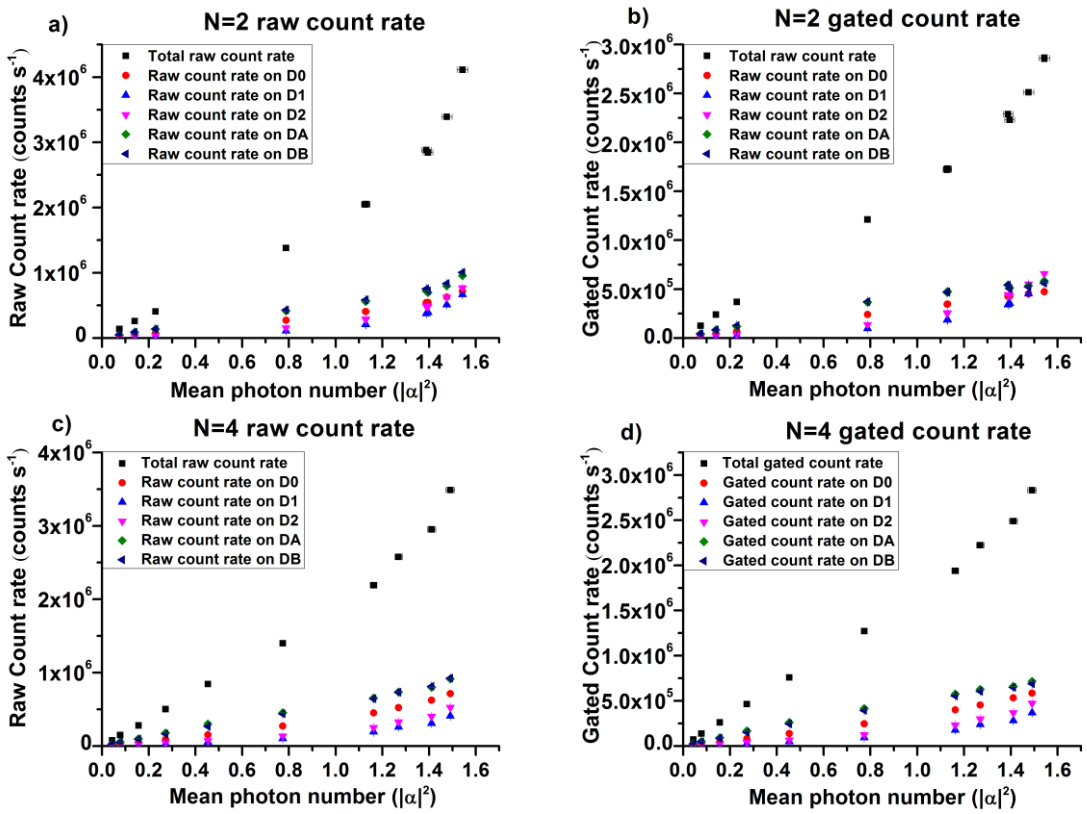


Figure 8.9 – The raw and gated count rates for N = *2, and 4.*

The raw and gated count rates are shown in Figure 8.9 for $N = 2$ (a and b), and 4 (c and d). Phase-alphabet $N = 8$ was not considered for these experiments as it has been seen in all other SCAMP experiments that it follows that same trends as N=2 and 4, just at different values.

The extra subtraction stage detector is denoted D2 detector and it was found that it had a higher gated (and raw) count rate than the first subtraction stage (D1), this could be because of extra losses between the first subtraction stage BS and its corresponding detector.

The extra subtraction stage introduces additional loss, from splices and inherent component loss, so it can be seen that DA, and DB detectors have a lower raw count rates than seen earlier in the Chapter. The gating process retained on average 87.3 ± 0.7 % of the raw count rate, which is on par with the 90:10 results presented earlier in the Chapter, which were found to be 70 - 90%.

The conditional visibilities are presented in a different manner to those presented previously. This change in presentation is to give the reader a full appreciation of the improvement the second subtraction stage conditions give to the fully conditioned visibility over just one subtraction stage.

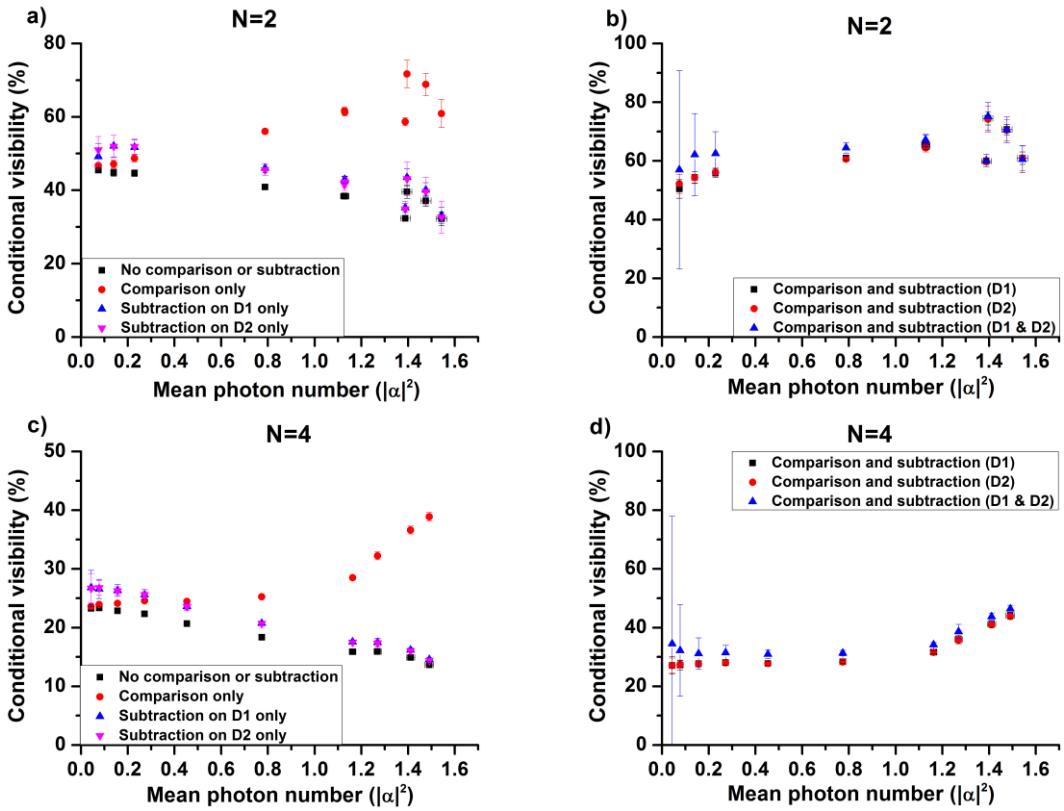


Figure 8.10 – The conditional visibilities for N = *2 and* N = *4 calculated using Equation 7.4.*

Figure 8.10 shows four sub figures where a), and b) are for $N = 2$, also c), and d) for $N = 4$. a) and c) represent the four post-selection conditions which require either 1, or 0 correlations with the DA, and DB events. Two different 'subtraction only' events can occur based on either the D1 or D2 subtraction detectors firing. The correlations follow the same trends as the 90:10 BS presented earlier in, with the 'comparison only' and 'subtraction only' visibilities intersecting at a $|\alpha|^2 \approx 0.4$. Figures b) and d) show the post-selection conditions for fully amplified correlation (no detection at D0, and a subtraction at either D1, or D2), and the fully amplified correlations where both subtraction detectors measure and event, with no detection at D0. It can be seen that the extra subtraction stage post-selection condition (i.e. requiring both subtraction stages to trigger events) improves

the post-selected visibility by up to 5% at the low $|\alpha|^2$ values over the standard one subtraction stage event. Therefore adding addition subtraction stages with post-selection conditions can improve the conditional visibility of the system, and therefore the fidelity.

It should be noted that large uncertainties that occur for $|\alpha|^2$ <0.3 because the number of correlations for both D1 and D2 subtraction stages firing are only a few correlations (which can be seen in the success rates Figure 8.11 d), so fluctuations create large standard deviations, creating the large uncertainty observed [9].

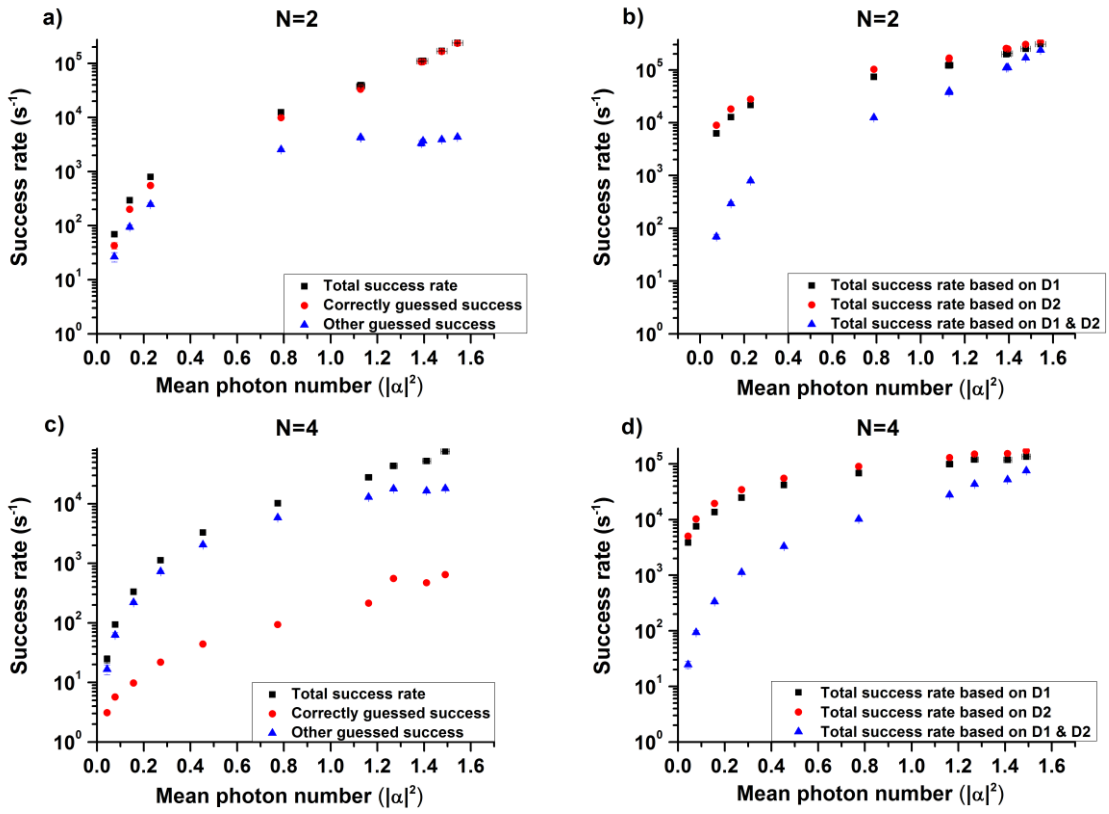


Figure 8.11 - Success rates for the state comparison amplifier (SCAMP).

The success rates for $N = 2$, and 4 are shown in Figure 8.11, where a), and b) correspond to $N = 2$, and c), and d) correspond to $N = 4$. a) and c) show the total success rate, correctly guessed success and other guessed states successes for the success time-correlations of D0 not measuring an event, and both subtraction detectors (D1 and D2) measuring an event. $N = 2$ shows a dominance of correctly guessed success states, however $N = 4$ shows the reverse, that there are a lot more "other" guessed states being amplified than the correct.

This feature was also seen in the 90:10 results shown in Figure 8.4, however the percentage of 'other' states is much greater with the extra subtraction stage.

Sub-figures b) and d) show the total success rates for the amplifier based on the D1 only events, D2 only events, and correlations with D1 and D2. These, of course, take into account the required absence of a detection event at D0 as well. The single detection event rates of D1, and D2, alone, are very similar. However the total success rate of D1 and D2 correlations show a significant decrease in the success rate, especially at the lower $|\alpha|^2$ of the investigated range, i.e. <1. This is because of the decreasing likelihood of having two photons in the pulse even with the amplification, and also detecting two simultaneously on separate detectors.

The extra subtraction stage adds some changes the ultimate transmission of the device, meaning the new nominal gain of the SCAMP device is now 8.1 (because of the extra 90:10 subtraction BS, essentially giving $t_2 = 0.81$). As well as a lower nominal gain, extra loss due to inherent component losses and fusion splicing during construction also lowers g_{eff}. Figure 8.12 a), and d), show g_{eff} for the SCAMP device with an extra subtraction stage for $N = 2$, and 4. This was calculated using Equations 7.6, 7.7 and 7.8 from the previous Chapter. Both g_{eff} follow the same trend of dropping with increasing $|\alpha|^2$, as was also seen in the base 90:10 results, Figure 8.5.

The success probabilities for $N = 2$, and 4 are shown in Figure 8.12 b) and d). It can be seen that the success probability for a state comparison and subtraction correlation based on D1 or D2, are almost equal. Success probability based on D2 is slightly higher due to its increased success rate maintaining the idea that there is extra loss in D1 subtraction stage leading to the detector itself. The success probability for correlations based on a detection at D1 and D2 are substantially lower for $|\alpha|^2 < 0.8$ where they are below 1 %. The success probability does start to increase nonlinearly with $|\alpha|^2 > 0.8$, but is still always lower than the success probability of the system with one subtraction stage.

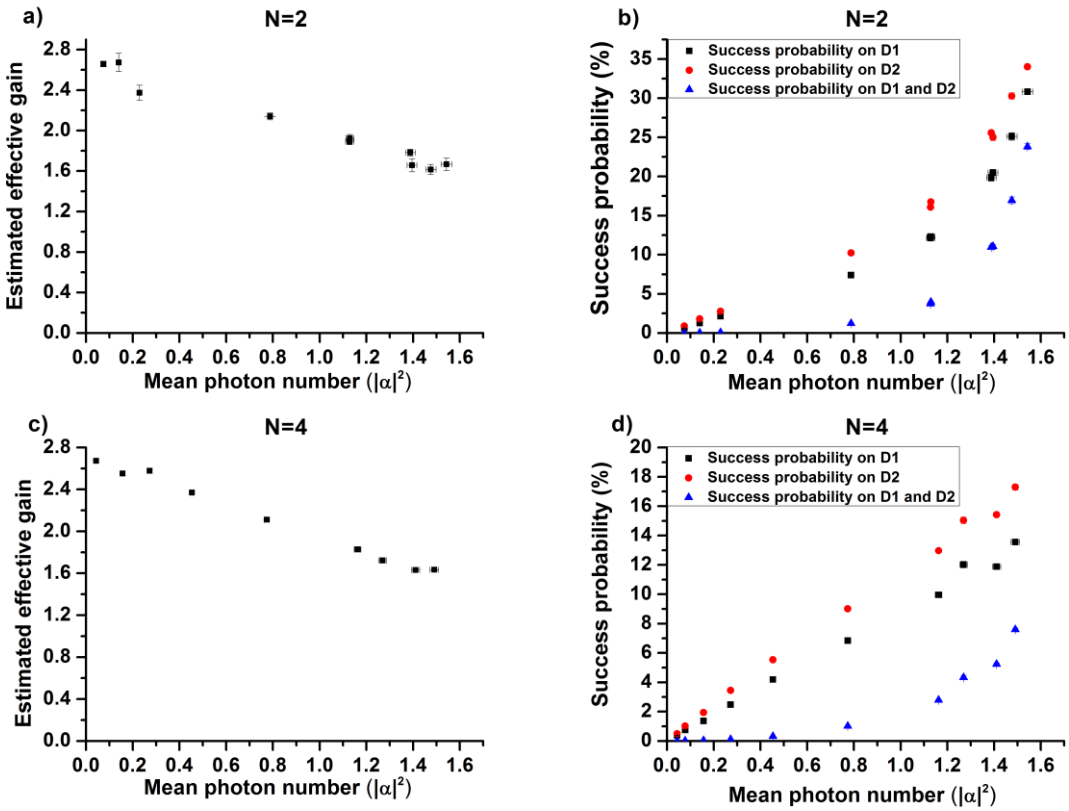


Figure 8.12 – The estimated effective gain, a) and c), and also the success probability, b) and d), for N = *2 and 4 respectively.*

Overall, the extra subtraction stage has shown some interesting properties. It does show reduced estimated effective gain, however it still works very much as an amplifier with a value of >1.6. The extra subtraction stage showed an increase in the state comparison and subtraction conditional visibility, by up to 5 %, however the fully conditioned success probability was lower. For $N = 4$ it was shown that the 'other' guess states had an increased success rate over the 'correct' guess states, relative to the previously shown 90:10 results.

8.5 Summary

Replacing the 50:50 BS at the comparison stage of the previous design iteration with a 90:10 BS gave a nominal gain of 9 but also showed a reduced conditional visibility, which was to be expected, as the amplifier is now always sending an output, even when guessing wrong. It was found that the output of the 'comparison only' case followed the same trend as 'comparison and subtraction' while the 'subtraction only' case followed the trend of 'no comparison or subtraction'. This is the reverse of what was observed in the 50:50 state

comparison BS experiment, but it is not unexpected. The amplifier will always be giving an output even when making an incorrect guess, this means the condition based on the D1 subtraction stage becomes more common for right and wrong guesses, making its effect in the conditional visibility less significant, while the D0 detector events become more significant because of the high maximum and low minimum for the right and wrong guess. The 'comparison only' and 'subtraction only' were also found to have a crossover at an $|\alpha|^2 \approx 0.4$, showing that increasing the $|\alpha|^2$ changes the significance of the conditions as more photons are added to the device as the detection a D1 is becoming more common than a detection at D0 leading to less significance in the conditional visibilities.

Noise was purposely added into the higher nominal gain SCAMP using a 90:10 BS to simulate noise in a communication channel. The way in which the noise was introduced was modified to give a better simulation of noise in a communications channel. The same 850 nm wavelength LED as used in the previous added noise experiment was shone free-space onto the signal channel splice, which allowed coupling of 850 nm photons into the core and cladding. The addition of noise in this way allowed it to be added to the signal channel only, simulating noise from the communications channel only. In the previous addition of noise experiment the 850 nm noise was added into all channels, but this was seen as unrealistic, because the fidelity reference, and coherent source at the amplifier node should have low, or no excess noise. Again the 850 nm wavelength noise was chosen because it is presumed a quantum optical amplifier node would have an optical bandwidth filter to block broadband wavelength noise.

As in the previous set of added noise results, SCAMP was shown to be robust to additional noise with higher $|\alpha|^2$ (i.e. >0.5). However, low levels of noise 0.1 MHz (raw noise on the D0 detector) were shown to be acceptable even at $|\alpha|^2$ <0.5. The conditional visibility was the most affected property due to lower visibility on the outer interferometer, and slightly increased gated rate on the D1 detector.

The addition of the extra subtraction stage to the 90:10 BS experiment showed that the conditional visibilities could be improved by as much as 5% for the post-selection condition of no detected events at the state comparison stage, and a detection event at both subtraction stages. This improvement was over the post-selection condition of no detected events at the state comparison stage, and a detection event at one subtraction stage. This

improved conditional visibility does come at a cost to the overall system performance however, as it was seen the success probability dropped by up to 5% also the estimated effective gain dropped by a factor of 2 because of extra losses, and lower nominal gain, over the previous 90:10 results.

8.6 SCAMP device conclusion and future work

Table 8.1 shows the collated summary of the various experiments performed with SCAMP from this Chapter and the previous. The results in Table 8.1 focus on the $N = 4$ phase-alphabet, as it equivalent to the BB84[10] type protocols commonly used in quantum communications [1], [11], [12] and therefore is the most relevant for real world applications. Also included for reference are the general properties of the photon addition and subtraction devices that have been experimentally demonstrated prior to the SCAMP experiment. The comparison to these devices is made because the SCAMP device fits into the category of photon addition and subtraction devices.

Device type	Clock frequency (MHz)	$\|\alpha\|^2$ range	Success probability (%)	Effective gain	Notes
50:50 state comparison	1	0.013 – 0.551	0.026 – 1.42	0.858 ± 0.020	- Good success probability, however <1 gain factor
90:10 state comparison	1	0.01-1.53	0.10 – 14.98	4.46-1.83	- Success probability seen higher in $N = 2$. $N = 4$ values are for reduced visibility.
Extra subtraction stage	1	0.043 – 1.49	0.0025 – 7.60	2.67 – 1.63	- Increased conditional visibility due to more significant detection for post-selection.
Addition and subtraction (general)	-	0-2	1×10^{-4} - 1×10^{-7}	>1	- Photon number resolving subtraction stage can increase gain. - Low success probability due to continuous range of possible phase values.

Table 8.1 –Collated results for N = *4 for all SCAMP experiments performed in this Thesis.*

It can be seen that all SCAMP configurations have significantly improved success probability over previous photon addition and subtraction devices. This is primarily due to the fixed phase-alphabet incorporated into the photon addition stage, which limits the phase space in which the amplifier can randomise its guess photons. A secondary, but arguably equally important factor, is the experimental simplicity of the SCAMP device over previously demonstrated devices, because it does not use complex quantum resources (such as spontaneous parametric down-conversion) for the photon sources, or complex photon number resolving detectors.

The initial 50:50 state comparison BS device showed an improved success probability over previously shown photon addition and subtraction devices, however the estimated effective gain was found to be less than 1, making it an attenuator.

To improve the estimated effective gain, the 50:50 state comparison BS was replaced with a 90:10 BS, which showed an improved success probability and gain. However the conditional visibilities dropped as a result because the amplifier always produces an output even if the guess is wrong.

An extra subtraction stage was introduced to compensate for the decrease in conditional visibilities with the 90:10 BS, resulting in a drop in the gain and success probability, however, these were still higher than the 50:50 state comparison BS based device.

Overall SCAMP has been further characterised to show a high success probability, >1 estimated effective gain, and high conditional visibilities. The device far outperforms other photon addition and subtraction devices, and indeed all other previously experimentally realised quantum optical amplifiers.

Future work

Similar to the previous Chapter's future work section, this Chapter will mention that a SCAMP device which implements two indistinguishable independent sources is a key experiment for showing an independent amplifying node. All SCAMP experiments have been shown with the same source, where an interferometer has split the power into two paths, and then had them recombined. This simulates two indistinguishable sources,

however showing that it really does work with two separate sources would show that the SCAMP device could possibly be used as a remote quantum amplifier.

Improving the success probability of the quantum amplifier is also an important feature of quantum amplifiers. As quantum communication is a possible application for quantum amplifiers, low success probabilities will actually lower the key generation rate and maximum transmission distance making their implementation a hindrance. One novel way to improve the success probability could be to incorporate some sort of feedforward mechanism, which allows an amplifier node to correct any known mistakes it has made during amplification.

For instance, take the 50:50 state comparison stage for $N = 2$ (phase-encodings 0 and π). In this case, when the amplifier node guesses wrong, all photons are routed to the D0 detector, and none pass through the amplifier, in a high visibility case. If the guess is right, all photons are routed through the amplifier. Therefore if an amplifier makes a guess, and detects a photon at D0, they know they are wrong and can make another guess which is correct. This relies on information being transferred forward, so that the same pulse can still be amplified. This will rely on fast electronic switching, and also some form of low-loss photon delay mechanism, such a lengths of silica optical fibre, which can delay a photon pulse by 1 ns for every ≈ 0.2 m of optical-fibre, with a loss of 0.2 dB/km.

8.7 Acknowledgements

This work follows on from Chapter 7, with the same team involved. The author acknowledges additional discussions with Dr Luca Mazzarelli, University of Strathclyde.

8.8 Bibliography

[1] R. J. Donaldson, *et al.*, "Experimental Implementation of a Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.*, vol. 114, no. 12, p. 120505, 2015.

[2] E. Eleftheriadou, *et al.*, "Quantum Optical State Comparison Amplifier," *Phys. Rev. Lett.*, vol. 111, no. 21, p. 213601, Nov. 2013.

[3] C. R. Müller, *et al.*, "Probabilistic cloning of coherent states without a phase reference," *Phys. Rev. A*, vol. 86, no. 1, p. 010305, Jul. 2012.

[4] P. Marek and R. Filip, "Coherent-state phase concentration by quantum probabilistic

amplification," *Phys. Rev. A*, vol. 81, no. 2, pp. 022302Marek, P., & Filip, R. (2010). Coherent–stat, Feb. 2010.

[5] Thorlabs, "Fiber-Coupled High-Power LED," *Rev A*, pp. 0–1, 2013.

[6] Excelitas Technology, "Single Photon Counting Modules," 2015.

[7] Mathworks, "MATLAB 2014b (8.4.0.118713)." The MathWorks Inc., Natick, Massachusetts, 2014.

[8] G. S. Buller and R. J. Collins, "Single-photon generation and detection," *Meas. Sci. Technol.*, vol. 21, no. 1, p. 012002, Jan. 2010.

[9] L. Kirkup, *Experimental Methods: An Introduction to the Analysis and Presentation of Data (Physics)*, 1st ed. John Wiley & Sons, 1995.

[10] W. Tittel, *et al.*, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[11] M. Sasaki, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network.," *Opt. Express*, vol. 19, no. 11, pp. 10387–409, May 2011.

[12] V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without Quantum Memory," *Phys. Rev. Lett.*, vol. 112, no. 4, p. 040502, Jan. 2014.

Chapter 9

Conclusions and Future Work

9.1 Conclusions

Chapter 2 introduced technology that can used to experimentally realise theoretical quantum communication protocols. Coherent sources, silicon single-photon avalanche diodes are common technologies used throughout the thesis because they are commercially available and easy to use. Other technologies such as single-photon sources and quantum memories (QM) are not directly implemented in the experiments, however they were described in overviews to illustrate why they were not used. They are simply not experimentally mature enough to be realistically used in quantum communication technologies.

Chapter 3 introduced both conventional and quantum cryptography and digital signatures. Commonly used public-key cryptography were said to be at risk from attacks from quantum computers running one of the known quantum search algorithms. Quantum safe protocols, both conventional and quantum were described. Conventional quantum-safe protocols still rely on one-way functions which are currently secure against known search algorithms, however like public-key cryptography are at risk from possible future breakthroughs in search algorithms. Quantum protocols, on the other hand, are made secure by the laws of quantum mechanics, which have been rigorously tested over many years, and are therefore more likely to be safe from future breakthroughs.

Chapter 4 described the first experimental implementation of quantum digital signatures which did not require a quantum memory for the swap and comparison mechanism, or the discrimination of the phase-encoded quantum states sent by Alice. While the predecessor experiment required QM for the state discrimination measurement, Chapter 4 introduced unambiguous state discrimination and elimination, a passive state discrimination measurement. For a 0.01% probability of forging, the shortest signature half-bit length was found to be 5.13×10^{13} for a $|\alpha|^2 = 1$. This gave a time for Alice to send of 5.13×10^5 seconds, which is approximately 5.94 days. The signature half-bit length, and time taken for Alice to send was also found to increase with $|\alpha|^2$.

Chapter 5 described the next stage in removing the experimental complexities of quantum digital signatures by removing the lossy and bulky multiport which performed the swap and comparison mechanism in all previous experimental realisations. By removing the requirement for quantum memory in the state discrimination measurement, the receivers could store their sent signature elements classically, this meant they could perform the swap and comparison mechanism classically in post-processing, rather than using the optical multiport which limits the achievable transmission distance to several metres. This was shown up to a transmission distance of 2 km in optical fibre with two receivers, Bob and Charlie. An optimised signature half-bit length at 500 m was found to be 1.93×10^9 for $|\alpha|^2 = 0.4$, taking Alice ≈19.3 s to send to a receiver.

Chapter 6 moved away from QDS and introduced the next topic of the Thesis, quantum amplification. Conventional telecommunication amplification was introduced, and an explanation why these amplifiers cannot be directly used in quantum communications was given, essentially because of the added noise. Non-deterministic quantum amplifiers were introduced, these allow the added noise to be overcome by post-selection of photon events at the expense of success probability.

Chapter 7 introduced a relatively new quantum amplifier, the state comparison amplifier (SCAMP). This device has similarities to other devices in the photon addition and subtraction category, however as was seen there are many difference in the technology used in practice. The use of commercial available technology and fixed phase-alphabets allowed the state comparison amplifier to perform much better than all previously demonstrated quantum amplifiers. Success probabilities of >2% were observed for mean photon numbers ($|\alpha|^2$) >0.7. SCAMP was also shown to be robust to additional noise if $|\alpha|^2$ was increased, however it was shown to less robust to broadband wavelength noise due to an increased detection rate on the subtraction detector. Although the nominal gain was said to be 1.8, the loss of the device actually attenuated the signal with a gain of 0.858.

Chapter 8 was a further investigation into the characteristics of the SCAMP device. The first investigation was to increase the nominal gain of the device from 1.8 to 9, in order to show a device that actually had gain. This actual gain was found to be up to 4.46, with a success probability of >14% at $|\alpha|^2$ >1.0, corresponding to >140 kHz success rate. This device configuration was also shown to be robust to noise as $|\alpha|^2$ is increased. An extra

subtraction stage was also added onto the SCAMP device to increase the output fidelity, this was shown to reduce the gain and success probability, however the conditional visibility (directly relatable to fidelity) was shown to increase marginally.

9.2 Future work

As was discussed in at the end of Chapters 5, one of the limiting factors in the achievable distance is the choice of wavelength. At 850 nm the loss in standard telecommunication optical fibre is 2.2 dB/km. Add to this coupling losses and mode mismatches will only shorten the maximum achievable distance. The primary reason for this choice of wavelength was the silicon detector technology available which has moderate detection efficiency, low dark count rates and 10's of ns dead-time. However a move to a wavelength in the telecommunication region 1550 nm would allow optical loss of $\leq$0.2 dB/km, and minimal coupling and mode matching losses. The downside of switching to 1550 nm is that the detection efficiencies for InGaAs/InP detection technology tends to be lower, also with higher dark count rates. However the detection technology for 1550 nm is an active area of research, so detector characteristics are improving.

Whether or not the move from 850 nm to 1550 nm is made, another future step for QDS which could improve the achievable distance is to implement more efficient protocol. This could be performed by the protocol presented by Amiri *et al.* in [1], with some adjustments to the post-processing and propagation direction of quantum channel.

The state comparison amplifier was shown to have significant improvements over all other quantum optical amplifiers, to the best of my knowledge. Although a solid application for SCAMP is not currently known one of the desired applications for quantum amplifiers is in quantum communication protocols, to either help improve the transmission distance, or simply improve the probability of detecting a certain quantum state. As well as investigating applications in quantum communications other applications need to be found.

Experiments carried out with SCAMP in this Thesis were carried out using the same coherent source which was split and then recombined using an interferometer. For SCAMP to be tested as a real device, experiments using two indistinguishable sources, one for a sender, and the other as the amplifiers node must be performed.

Recent trends in quantum communication has been to move from bulky optical components spliced together, to integration on chip [2]. This gives optical systems which can be cheaper, have increased stability, and be more compact. In the right material the optical systems can also be less lossy as well. SCAMP is a relatively simply device, a coherent source, two beamsplitters and two detectors, however it is quite bulky. Moving to an integrated device will give a more compact device which is more robust to environmental changes and has the potential to have reduced losses and be more cost-effective.

Although the success probability of SCAMP is higher than other quantum amplifiers, it can be improved further by a feedforward mechanism. For instance if two phase-encodings were implemented in SCAMP, in the nominal gain of 1.8 set-up, the state comparison is either right or wrong, with all photons going through the amplifier or to the detector. In the wrong case, a second guess can be made which corrects the initial guess. Or in the right guess, another correct guess can be made to increase the gain. This feedforward will rely on optical delays long enough for the detector electronics to trigger (or not trigger) and event, and then also encode the phase of the second guess. This could be up several hundred nanoseconds or even into microsecond delays.

9.3 Bibliography

[1] R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure Quantum Signatures Using Insecure Quantum Channels," *arXiv*, no. 1507.02975, Jul. 2015.

[2] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based Quantum Key Distribution," pp. 1–5, 2015.