UNIVERSITY OF CALGARY

Photon Pair Technologies for Quantum Communication

by

Joshua A. Slater

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

January, 2009

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Photon Pair Technologies for Quantum Communication" submitted by Joshua A. Slater in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Supervisor, Dr. Wolfgang Tittel
Department of Physics and Astronomy

Dr. Alexander Lvovsky
Department of Physics and Astronomy

Dr. Michal Okoniewski
Department of Electrical and Computer Engineering

January 16th, 2009
Date

Abstract

Quantum communication allows for many improvements over the communication limits imposed by classical physics. This thesis presents a series of new photon pair technologies developed as part of the on-going drive to exploit quantum entanglement and bring quantum communication to real-world applications: an exact model of the detection statistics of a probabilistic source of photon pairs from which a fast, simple and precise method to measure the source's brightness and photon channel transmissions can be derived; a source of hybrid photonic entanglement suitable for linking optical fibre quantum communication channels with free-space channels; a method that allows for characterization of time-bin and entangled time-bin qubits that goes beyond what has been accomplished before; and the first experimental demonstration of a fair, loss tolerant quantum coin flipping protocol, which is a quantum communication application that requires both entanglement and generalized measurements.

Acknowledgements

First, I want to thank the other students with whom I have persevered through graduate studies along side of: In particular, Henry Chen, Adam D'Souza, Paul Fairie, Melissa Gurney, Jyotsna Kashyap, Ofelia Rempillo, Michelle Seguin, Jean-Simon Corbeil, Yasaman Soudagar as well as the other members of IQIS and PHAS. I want to also thank the administration: Tracy Korsgaard for her help navigating the endless bureaucracy of graduate school, Hyejeong Hwang for her never-tiring support for our group, as well as Catherine Avramenko and Nancy Lu.

I want to thank all the QC2 group members from the past two and a half years who have made working here an incredible experience: Itzel Lucio Martinez, Gina Howard, Philip Chan, Steve Hosier, Ahdiyeh Delfan, Erhan Seglamyurek, Xiaofan Mo, Cecilia La Mela, Neil Sinclair, Jeongwan Jin, Terence Stuart, Vladimir Kiselyov, Sergey Moiseev, John Nguyen, Michael Underwood as well as Allison Rubenok for her incredible logistic support while I finished this work and especially Félix Bussières, with whom I have worked closely over the past two years. I know that his help and guidance thus far has had an important impact not just on my career but also on my life outside the lab. He is truly deserving of the title 'post-doc' we so often jokingly give him. Together they compose the best group I have had the pleasure of working with.

And, I want to thank my supervisor Dr Wolfgang Tittel. Of all the supervisors that I have worked under, I have never had the pleasure of working under one as patient, attentive and understanding, as Wolfgang. His seemingly unlimited supply of energy, incredible depths of knowledge and sense of fairness have been an inspiration to me.

Finally, I want to thank my family, Kim, Barb and Peter Slater, who have supported me and encouraged me throughout my life. I know you're all proud. One step closer to the 'Mr Transporter' you always wanted to see Dad.

Table of Contents

List of Tables

List of Figures

Glossary

μ	Brightness or mean number of photons per pulse
AE	Atomic Ensembles
ASE	Amplified Spontaneous Emission
BBBG	Coin flipping protocol by G. Berlin, G. Brassard, F. Bussières and N. Godbout
BS	Beam Splitter
CHSH	J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt
EPR	A. Einstein, B. Podolsky and N. Rosen
FWM	Four-Wave Mixing
$g^{(2)}(0)$	Second-order auto-correlation function
HBT	R. Hanbury Brown and R. Q. Twiss
HSPS	Heralded Single Photon Source
HWP	Half-Wave Plate
InGaAs	Indium Gallium Arsenide
MSF	Microstructured fibre
NIR	Near-Infrared
PBS	Polarizing Beam Splitter
PPLN	Periodically Poled Lithium Niobate
QC2	Quantum Cryptography and Communication labs
QKD	Quantum Key Distribution
QWP	Quarter-Wave Plate
Si	Silicon
SPDC	Spontaneous Parametric Down-Conversion
TDC	Time-to-Digital Converter

Chapter 1

Introduction

Communication can be described as the process of imparting information from a sender to a receiver via a certain medium [1].

1.1 The Classical versus Quantum World

At the end of the nineteenth century humankind thought it lived in a world governed by the laws of Newtonian mechanics, Maxwell's equations and other physical theories collectively known today as Classical Physics. To the best of humanity's knowledge, these physical laws held an iron-clad rule over the world and, as a consequence, impassible restrictions were placed on humanity's abilities - particularly in the areas of information communication.

One such area is the field of cryptography, which developed into a science in the mid twentieth century. If a sender, often named Alice, wants to send information over a public channel to a receiver, named Bob, without an eavesdropper, named Eve, learning the information, her options are limited [2, 3]. To encrypt information securely, either Alice and Bob must share a secret key that must be as large as the information itself or they must rely on one-way functions, which are functions designed to be simple to calculate one-way, but computationally difficult to invert and were developed in the later half of the century. Unfortunately, both techniques have serious drawbacks. The only solution for Alice and Bob to share a secret key is for them to meet beforehand and agree on the key. This becomes impractical over large distances or with large amounts of secret information or with many sender/receiver pairs in a network setting. The security

of one-way functions relies on Eve's inability to invert the function. This is a vulnerability as given enough time and computing power, it is always possible for Eve to eventually invert the function. The laws of classical physics require that Alice and Bob settle for either impractically or vulnerability.

Another capability restricted by classical physics is coin tossing. In general, coin tossing techniques are employed whenever Alice and Bob require a random bit, but Alice will win, and presumably gain something of value for one result, and Bob will win on the other result. It is therefore advantageous for one or both parties to choose the bit, rather than allow random chance to decide [4]. If the two parties are separated by some distance such that they cannot actually see a coin toss, and if neither party trusts the other, and they cannot agree on a trusted third player to toss the coin, then there does not exist a fair method to choose the random bit. With every method allowed by classical physics, it is possible for one party to cheat such that he or she always wins the toss.

A third area limited by classical physics is computation. The difficulty of computational problems can be classified in terms of the time (i.e. number of steps) and space (i.e. required memory), that a computer requires to complete the computation. Easy computations require a number of steps that grows polynomially, or slower, as the size of the input to the computation grows. Difficult problems, on the other hand, require a number of steps that grows exponentially, or faster, as the size of the computation grows. Although it has yet to be proved, the consensus of most experts is that certain computations, such as solving certain one-way functions used in cryptography, are difficult problems for computers based on classical physics. If true, these computations will always be impractical for large systems.

While the limits that the laws of classical physics imposed on our communication abilities were being understood, the limitations of these laws to explain the physical world were also being exposed. In the early twentieth century physics had revealed a

number of problems stemming from the classical laws - the ultraviolet catastrophe and the fact that electrons inexplicably held stable orbits around nuclei are examples of some of the problems that existed [5, 6, 7]. These quandaries were only finally resolved by the invention of the modern form of quantum mechanics in the 1920s. However, even as past problems were resolved the theory of quantum mechanics brought with it a collection of surprising features, often dubbed quantum weirdness, which, as will be demonstrated, have an important role to play in information and communication.

1.1.1 Bits, Qubits and Entangled Qubits

Classical information is usually represented in bits: an object that can be $'0'$ or $'1'$. In quantum mechanics, information is represented by the qubit: a particle that exists as a two-level system, (i.e. a system described by two orthogonal basis states) [7]. The basis states for the qubit are notated as $|0\rangle$ and $|1\rangle$. In quantum mechanics the particle can exist in both states simultaneously. This is known as a coherent superposition: $\cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$. Here, the parameters θ, with $\cos^2\theta$ and $\sin^2\theta$ being the probability to measure the particle in the corresponding basis state, and ϕ, a coherent phase relationship between the basis states, are sufficient to describe any qubit state, as seen in figure (1.1). This unique feature of quantum mechanics becomes apparent if one considers the coherent superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A measurement in the $[|0\rangle, |1\rangle]$ basis returns a result of 0 or 1 with 50% chance each, similarly for an incoherent, or probabilistic, mixture of $|0\rangle$ and $|1\rangle$. However, if one measures in the basis $[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]$ one would find the particle in the state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ with 100% certainty for the coherent superposition, but would still get a 50/50 mixture for the probabilistic mixture.

The weirdness of quantum mechanics continues as one begins to describe multiple particles. Two particles could exist in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, where the tensor product, $\otimes$, is the method used to mathematically combine two qubits. If

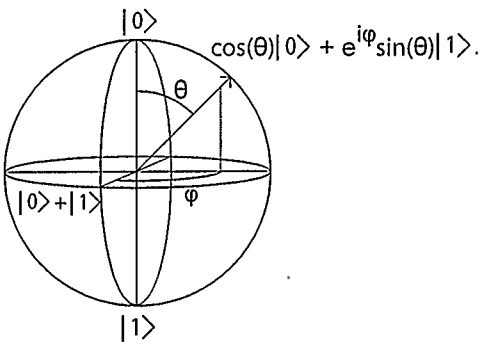

Figure 1.1: Qubit states represented on the Bloch sphere: The parameters θ and ϕ represent the polar and azimuthal angles of the vector on the Bloch Sphere that represents the qubit's quantum state. Coherent superpositions lie on the surface of the sphere. Completely incoherent mixtures exist as the center of the sphere.

one measures whether the particle is in the basis spanned by $|0\rangle$ and $|1\rangle$ then there is a 50/50 chance of each particle being detected in either basis state, independent of the other particle. However, the particles could exist in a more interesting state known as a Bell state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \tag{1.1}$$

This state has the property that there does not exist single particle states $|a\rangle$ and $|b\rangle$ such that the state of both particles can be written as $|\psi\rangle = |a\rangle \otimes |b\rangle$. Whenever the state of a composite system cannot be separated into a product of single qubit states the composite system is said to be entangled [7].

The full weirdness of entanglement becomes apparent in the thought experiment performed by Einstein, Podolsky and Rosen (EPR) in 1935 [8]. Imagine Alice and Bob each have one particle of a Bell state as described in equation (1.1). Before measuring their particles, Alice or Bob could perform *any* transformation to it (i.e. rotate the state around the Bloch sphere). Quantum mechanics predicts that correlations between their detections will still exist, regardless of whether Alice or Bob measured first and regardless of the distance between them. It is as if Alice's measurement instantaneously affects

the state of Bob's particle. EPR called this counter-intuitive property of entanglement 'spooky action at a distance'.

In 1964 John Bell took the EPR thought experiment further [9], as will be discussed in section 3.1.1, and proved that the correlations between entangled particles are stronger than correlations that can exist between classical particles.

Another unanticipated consequence of quantum mechanics is the no-cloning theorem. First discovered in 1982 [10], the theorem, simply put, states that an unknown quantum state cannot be copied perfectly. A strange result, considering how simple the copying of information is in the classical world that is at the heart of many of the gains quantum communication has over classical communication as discussed in the following sections.

It then took until 1991 [11] before physicists began to realize that communication with quantum systems is more powerful than communication with classical systems. A few tasks where quantum mechanics provides startling improvements are presented in the following sections.

1.1.2 Cryptography

As discussed earlier, one issue surrounding cryptography is having Alice and Bob share a secret key before their desire to transmit secret information. This is called the key establishment problem. With quantum mechanical systems, it becomes possible for the two parties to distribute a provably secret key from a distance. Quantum Key Distribution (QKD) was originally put forth in 1984 by C. H. Bennett and G. Brassard [12] and again in 1991 by A. Ekert [11]. The following protocol for QKD is based on a proposal by Bennett, Brassard and Mermin in 1992 [13].

Imagine that Alice has a source that produces qubits in an entangled Bell state, as in equation (1.1). Alice sends one qubit to Bob, over a public channel, and retains one qubit for herself. Alice and Bob each randomly choose one of two conjugate bases and

measure their qubit in that basis. Alice and Bob then compare their measurement bases, over an authenticated public channel, and keep results from measurements where they chose the same basis. In theory, these results will be perfectly correlated and can be used to form a secret key. However, due to experimental imperfections, such as detector noise, some errors will be introduced and the correlations may not be perfect.

If an eavesdropper, Eve, was present on the channel while Alice and Bob were trying to establish their secret key, the laws of quantum mechanics prevent Eve from learning the key without introducing errors. First, due to the no-cloning theorem, Eve cannot perfectly clone the qubit Alice sent to Bob and keep a copy for herself. She might imperfectly clone it; however this will disturb both the original qubit being sent to Bob, as well as her copy, and thus introduce errors. Another option is to perform a measurement on the intercepted qubit and then create another qubit to send to Bob. However, the qubit Eve creates will not be entangled with the qubit Alice originally kept and thus not generate perfect correlation between Alice and Bob. She cannot even replace the source with another source that produces results she knows in advance as this will also introduce errors. Thus, to ensure security, Alice and Bob will select a random subset of their measurements and compare results over a public channel. If an eavesdropper attempted to access information on a single qubit then Alice and Bob will find errors. In general, any deviation from perfect correlation is assumed to be the fault of an eavesdropper and, if the correlations between Alice and Bob are high enough, standard error correction techniques [14] can be used to create a perfectly correlated key and standard privacy amplification [15] techniques can be used to remove any information Eve might have about the key.

Thus, in the world of quantum communication, Alice and Bob can share a secret key with which to securely encrypt and exchange information and, unlike the classical world, Alice and Bob can prove the security of their key after distribution.

1.1.3 Coin Tossing

Coin tossing is another example of a task that can be performed better using qubits and quantum mechanics. As discussed earlier, if Alice and Bob need to agree on a random bit and it is advantageous for one or both parties to choose the bit (rather than allow random chance to decide) and if neither party trusts the other nor a third party to toss the coin, then they are at a stalemate. Classically there is no solution to this problem. But can a protocol exist in the quantum world? One figure of merit to assess this is the maximum winning probablity that a cheating party can create. All classical, non-relativistic, protocols have a maximum winning probability of 100% (i.e. a cheating player can always force victory) and are thus referred to as completely broken. In 1998 and 1999 two teams proved that a perfect quantum coin tossing protocol, that is a protocol with a maximum winning probablity of 50%, regardless of any cheating strategy, could not exist [16, 17]. Nevertheless, quantum coin tossing performs better than its classical counterpart.

The first attempt at a quantum coin flipping protocol was presented in 1984 by C. H. Bennett and G. Brassard [12], at the same time as QKD, although this turned out to be completely broken. In 2000 D. Aharonov, A. Ta-Shma, U. Vazirani and A. C.-C. Yao [18] presented the first quantum coin tossing protocol with a maximum winning probablity of 92%. Later, in 2004, A. Kitaev proved that the best possible quantum coin tossing protocol could have a maximum winning probability of $\frac{1}{\sqrt{2}} \approx 70.7\%$ [19], although the protocol is unknown. Clearly, quantum mechanics provides an improvement yet again. Unfortunately, the majority of protocols do not consider the losses that are present in any real implementation and would be completely broken in any real situation. In principle, quantum error correcting codes could be used to protect against loses but it is not known how to properly apply these codes to this game. In 2008 G. Berlin, G. Brassard, F. Bussières and N. Godbout (BBBG) [20] proposed the first protocol that was

tolerant to losses. The protocol is also 'fair', meaning that, if Alice cheats, her maximum winning probability is equal to Bob's maximum winning probability if he was cheating. The protocol, along with an experimental realization, is presented in chapter 4.

1.1.4 Other Tasks

On top of QKD and coin tossing there exists numerous other tasks where quantum mechanical properties, such as entanglement, allow for quantum protocols that perform better than classical protocols. Examples include:

- Quantum factoring algorithm, proposed by P. Shor in 1994 [21], which can invert some one-way functions described earlier in a polynomial number of steps and thus make classical cryptography based on these one-way functions insecure.
- Quantum bit commitment protocols, which allow Alice to send something to Bob that commits her to a bit value of her choice, A, in such a way such that Bob cannot determine A, but such that Alice can later prove what is A, are more secure, although not perfectly secure, than their classical counterparts [22].
- Quantum search algorithm, proposed by L. K. Grover in 1996 [23], which can search an unsorted quantum database faster than classical search algorithms can search an unsorted classical database.

It is clear that the quantum world provides many benefits over the classical world. Communication with quantum systems, such as qubits, provides clear advantages in many areas of communication. An important question though, is how does one actually implement communication with qubits?

1.2 Implementing Quantum Communication

Thus far the qubit has been described using a general theoretical model. To bring quantum communication to the real world an actual two-level physical system must be selected. The obvious choice for quantum communication is the same physical system that is used for classical communication - light. The telecommunications industry has developed communication technologies based on intense pulses of light for many reasons. Not only does light travel at the maximum speed limit of a material, but it also only weakly interacts with the environment as it travels and hence remains unperturbed or uncorrupted. Quantum communication can enjoy these same benefits, as well as piggy-back on the technological achievements of telecommunications industry, by using the single particle constituent of the strong laser pulse - the photon. The two-level qubit system, as described above, can be implemented using any of a number of photon properties including the simple two-level polarization modes that are natural to photons, or by selecting two modes of a continuous property such as emission time, spatial direction or frequency [24].

Other issues must be considered for implementations of quantum communication. Perhaps the most important is over what medium to transmit the photonic qubits. Telecommunication optical fibre is a nearly ideal option. Optical fibre technologies have been studied for decades by the telecommunications industry and are thus very well understood. It is inexpensive (a fraction of a cent per meter), has very low loss (0.2 dB/km at a wavelength of 1550 nm, see figure (1.2)) and is incredibly versatile (optical fibre can snake through buildings, travel underground between cities and even under oceans between continents). Unfortunately, optical fibre is birefringent and thus imparts a random polarization transformation on any quantum information encoded in the polarization modes of a photonic qubit. This birefringence also changes with changing temperature

and stress and thus an active polarization compensation would be required to use the polarization modes for quantum communication. A potentially easier type of encoding to use is the emission time of a photon source, more commonly known as time-bin encoding [25]. Perhaps the greatest advantage of optical fibre is the fact that huge optical fibre networks already exist thanks to the telecommunications industry. Thus, quantum communication over standard optical fibre is highly desirable and could be optimized using photons at 1550 nm with time-bin encoding. For these reasons, quantum communication with these properties has been implemented between cities and at distances over 100 km [2, 26, 27], and have even lead to commercial products [28].

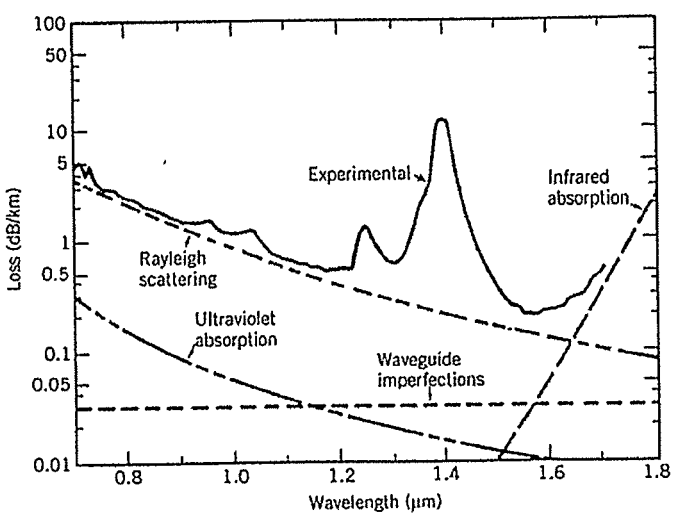

Figure 1.2: Losses in Optical Fibre: The various processes that contribute to the overall absorption inside standard optical fibre create an absorption minimum at 1550 nm wavelength [29].

On the other hand, it is impractical to install optical fibre between some communication users. Temporary structures and moving users such as ocean-faring ships and orbiting satellites cannot have optical fibre connections to communication networks. For these reasons, free-space links are required as well. Air has relatively little absorption in the near-infrared (NIR), see figure (1.3), and thus photons with wavelengths around

810 nm are desired. Air is also non-birefringent and thus the easy-to-use polarization encoding can be implemented as well. A fortunate coincidence is that single photon detectors for NIR wavelengths are about twice as efficient and have orders of magnitude less noise than their 1550 nm counter parts. Thus, over small inter-city links, free-space quantum communication has also been implemented [30, 31, 32, 33].

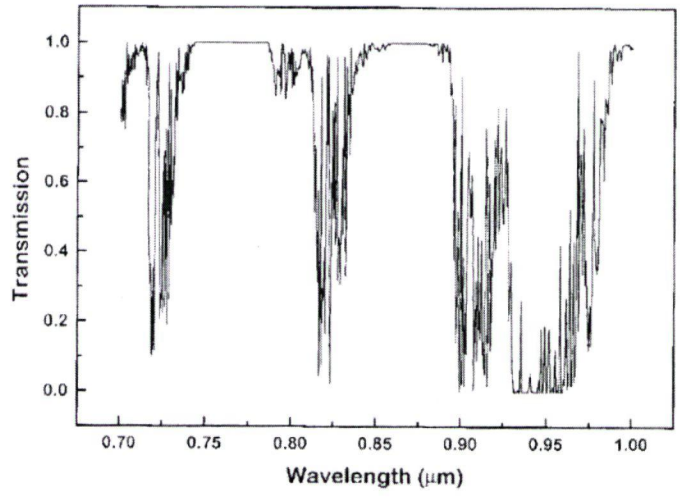

Figure 1.3: Losses in the Atmosphere: A transmission window appears just above 800 nm wavelength where single photon detectors are particularly efficient [34].

Therefore, to gain the communication benefits outlined earlier in this chapter, technologies to create entanglement between pairs of photons with the properties discussed here are required.

1.2.1 Long Distance Quantum Communication, Repeaters and Networks

In the future, as the distances over which quantum communication is attempted increases, the losses that are inherent in any medium will become an increasingly important issue. The telecommunications industry circumvented this problem by including repeaters in long links between users. These repeaters essentially amplify signals to overcome any signal loss. Unfortunately, this technique is not available in the quantum world due to

the no-cloning theorem. Instead, new technologies must be developed.

Current proposals for a quantum repeater require sources of entanglement and quantum memories to store entanglement reliably (for example, by reversably mapping the quantum state of a photon to an atomic excitation [35, 36, 37]), as well as another quantum feature known as teleportation [38]. Imagine two parties, Alice and Bob, each have one qubit of an entangled photon pair. Alice also has another qubit with a quantum state that she wants Bob to have. If Alice performs a two-qubit measurement and projects her two qubits onto an entangled Bell state, the quantum state will be teleported to Bob's qubit (modulo a correction operation that Alice can classically send to Bob). The idea of a quantum repeater is for two users to build-up a supply of shared entanglement and then teleport any quantum information when the need arises [39, 40]. Therefore, as the need for long-distance quantum communication develops so does the need for quantum repeaters, and thus quantum teleportation, and thus sources of entangled photon pairs.

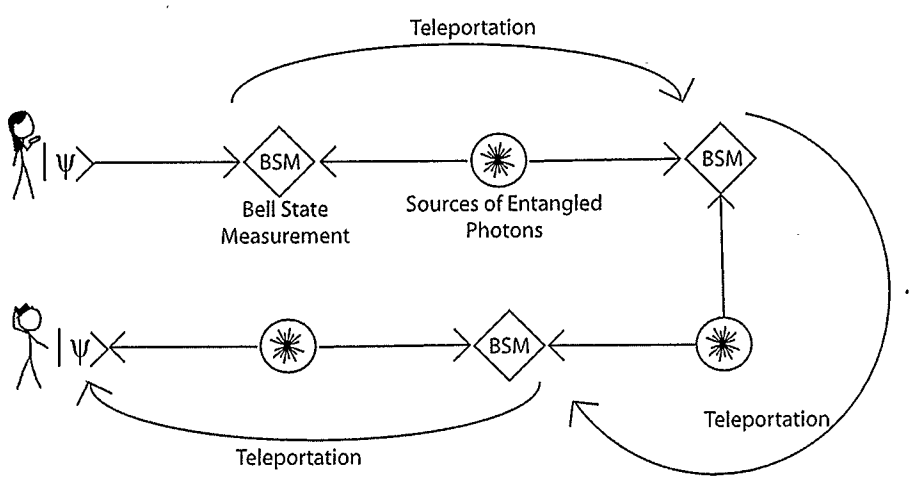

Figure 1.4: Quantum Repeaters: After the sources of entanglement distribute entangled photons around the network Alice's state can send her state to the next user in the network. Successive users teleport the state further until it reaches Bob. Alice and Bob courtesy of [41].

Similarly, quantum repeaters will become necessary as quantum networks consisting of different transmission media develop. If a user connected to an optical fibre network

needs to send a qubit to a user connected to a free-space network, some kind of quantum repeater will be required to 'convert' the quantum information from a photon suitable for fibre transmission to a photon suitable for free-space transmission. Thus, entangled photon pairs, with each photons at a desired wavelength, becomes a vital resource for any quantum network for quantum communication.

1.3 This Thesis

1.3.1 Motivation

As discussed in this chapter, quantum communication can provide many improvements over what can be achieved with classical communication techniques. In particular, the tremendous amounts of sensitive information that are now transmitted over public channels and secured by possibly breakable cryptographic techniques could be protected by QKD, which is the only proven technique for verifiable, unconditional security. Quantum communication also provides benefits for other communication tasks, such as coin tossing, over the best possible classical protocols. Therefore, strives to develop quantum communication technologies are necessary.

At the heart of all emerging quantum communication technologies is the requirement for photonic entanglement: QKD protocols, coin tossing protocols and future quantum repeaters all demand sources of entangled photon pairs. The first entanglement experiments were performed in 1972 [42] although the general consensus is that the first convincing demonstrations of entanglement and non-locality were performed in 1981 [43] but the entangled photons were difficult to create and use. In 1995 [44] more efficient and easier to use sources, based on spontaneous parametric down-conversion (see chapter 2), were developed and since then continued improvements in these sources have lead them to become staple commodities of quantum communication research. Sources producing po-

larization entangled photons at NIR wavelengths suitable for free-space transmission [32] and sources producing time-bin entangled photons at telecommunication wavelengths suitable for optical fibre transmission [27] have both become widely available. A much less considered component is a source of entanglement with one photon suitable for free-space transmission (NIR wavelengths with polarization encoding) and one photon for optical fibre transmission (telecommunication wavelengths with time-bin encoding) as required to link different networks together. We coined the term hybrid entanglement to describe such a source.

The ultimate goal of the quantum entanglement group of the Quantum Cryptography and Communication (QC2) Labs is to exploit sources of entanglement for applications that cannot be achieved with classical communication. This thesis details the beginning steps of these long term goals. Specifically, this thesis details the design, implementation and verification of a source of hybrid entanglement, as well as a novel method to characterize sources of photon pairs, novel techniques for the analysis of entanglement and an implementation of a quantum communication task: fair, loss-tolerant quantum coin tossing. To the best of our knowledge this is the first time that each of these four accomplishments have been demonstrated.

1.3.2 Organization

The organization of this thesis is as follows. Chapter 2 introduces methods to produce photon pairs, such as spontaneous parametric down-conversion, and an experimental indicator of pair production, the second-order auto-correlation function. Details on another method to produce pairs, four-wave mixing in optical fibre, are contained in appendix A. Next, a new model describing the statistics of pair production is presented along with how this model can be used to quickly characterize a source of photon pairs and predict measurement statistics. An experimental realization of a source is then presented along

with verification of this model.

In chapter 3 the theory behind producing, measuring and verifying entanglement is presented. Next, the source from chapter 2 is developed into a source of hybrid entanglement. This experimental realization is demonstrated through several measurements of signatures of entanglement, some of which are made possible by a new generalized time-bin analyzing interferometer that allows for a larger variety of measurements than the standard time-bin analyzing interferometer. Details on the design and alignment of the interferometers are contained in appendices B and C.

Chapter 4 introduces the BBBG fair, loss-tolerant quantum coin flipping protocol and then uses all the developments from previous chapters for the first experimental realization.

In chapter 5 a summary of these results is included along with a discussion of the future direction of these research projects.

1.3.3 Collaborations

These projects were completed in collaboration with several individuals. In particular, Félix Bussières has been involved in all the projects presented in this thesis. John Nguyen, Allison Rubenok and Terence Stuart, all former undergraduate students in QC2, and Vladimir Kiselyov, the QC2 engineer, contributed at different stages of these projects. The specific contributions of these individuals is presented below.

Félix and I, with some early assistance from Allison, built the source of photon pairs, as described in chapter 2. Original phase-matching calculations were performed by Allison (and later redone by Terence). Félix began work to develop a characterization model as in chapter 2. I developed the mathematics behind the model presented in section 2.2.1 and Félix and I developed the characterization technique presented in section 2.2.2. I developed the software used for this experiment (with early help from Terence).

In chapter 3, the idea of hybrid entanglement was first suggested by Félix. For the interferometers, I designed the pump interferometer and 810-conversion interferometer while Félix designed the 1550-conversion interferometer. We worked together on the construction of all three interferometers. John designed and constructed the 1550 time-bin interferometer. Félix and I integrated these into the existing optical setup while Vladimir built the custom electronics. I built the C++ software for these experiments while Félix build the Labview software and linked the two softwares together.

In chapter 4, I developed the software to play the coin flipping game.

More important than any specific result, Félix and I, as a team, put a tremendous amount of effort and time into the alignment, optimization and testing of the experimental setup so that the high quality results presented here were actually achievable.

Chapter 2

Sources of Photon Pairs

Before developing a source of hybrid entangled qubits for quantum communication the building blocks must first be put in place. The first step is to develop a source of photon pairs.

2.1 Theory and Background

The first sources of photon pairs were based on atomic cascades and were developed for fundamental tests of quantum mechanics [43]. These were based on two-photon decay paths via short-lived atomic states. Unfortunately, as the momentum of each emitted photon was uncorrelated, only very low collection efficiencies were possible. Improvements made by turning to other physical processes such as non-linear processes in materials and atomic ensembles, as described in the following sections, made photon pair sources useful for quantum communication.

2.1.1 Spontaneous Parametric Down-conversion

The next source of photon pairs to be developed was based on parametric amplification. This is a three-wave mixing process which depends on the $\chi^{(2)}$ non-linear coefficient of a material. Classically this process was used to amplify optical signals at a given wavelength. The signal and a pump beam can interact in a $\chi^{(2)}$ non-linear crystal such that the pump intensity is partially depleted while the intensity of the signal, as well as a third wavelength often called idler, are amplified. However, in the 1970s it was discovered that quantum mechanics allows for the amplification process to proceed even without a signal beam to seed the process [45]. There exists a finite probability for each pump

photon to interact with vacuum oscillations and produce a photon pair. This process now is known as spontaneous parametric down-conversion (SPDC).

The process can only occur if conservation laws are respected. The wavelengths of the pump and down-converted photons, λ_p, λ_s and λ_i respectively, must satisfy both energy and momentum conservation equations, the latter being referred to as phase-matching (here, $\overrightarrow{k}$ is the wavevector of the photon).

$$\frac{1}{\lambda_p} = \frac{1}{\lambda_s} + \frac{1}{\lambda_i} \tag{2.1a}$$

$$n_p\overrightarrow{k_p} = n_s\overrightarrow{k_s} + n_i\overrightarrow{k_i} \tag{2.1b}$$

In general it can be difficult to phase-match the three waves as the refractive indices in the material (n_p, n_s and n_i) depend on wavelength, crystal orientation and temperature. As the three waves propagate with different velocities, if phase-matching is not satisfied then the waves will move out of phase and begin to phase-match other non-linear processes. Overall, if phase-matching is not satisfied, than the probability of down-conversion will oscillate around zero and remain vanishingly small as the pump propagates through the crystal. To circumvent this difficultly birefringent crystals, where the refractive index depends on polarization as well, can be used. In this case, phase-matching is possible if both or one of the down-converted photons are polarized orthogonal to the pump beam. These are referred to as Type-I and Type-II phase-matching respectively and have been used extensively in the past [44, 46].

A newer phase-matching technique for SPDC known as quasi-phase matching was first investigated in 2001 [47, 48]. In this technique, the electric dipole moment is reversed periodically in order to guarantee phase-matching. The overall structure of the crystal becomes a periodic poled grating with a poling period Λ. The phase-matching equation for quasi-phase matching is modified by the poling period as below. In general, the poling

period's dependency on temperature must also be taken into account.

$$n_p \overrightarrow{k_p} = n_s \overrightarrow{k_s} + n_i \overrightarrow{k_i} + \frac{1}{\Lambda} \tag{2.2}$$

One major benefit to quasi-phase matching is that it allows for the use of non-linearities along propagation directions of crystals where birefringent phase-matching is not possible. Periodically poled lithium niobate (PPLN) has become a common crystal used with quasi-phase matching for photon pairs.

The three phase-matching regimes discussed above (perfect phase matching with birefringent crystals, quasi-phase matching with periodically poled crystals, and miss-matched phases) are compared in figure (2.1) assuming the non-linearities available to each were equal.

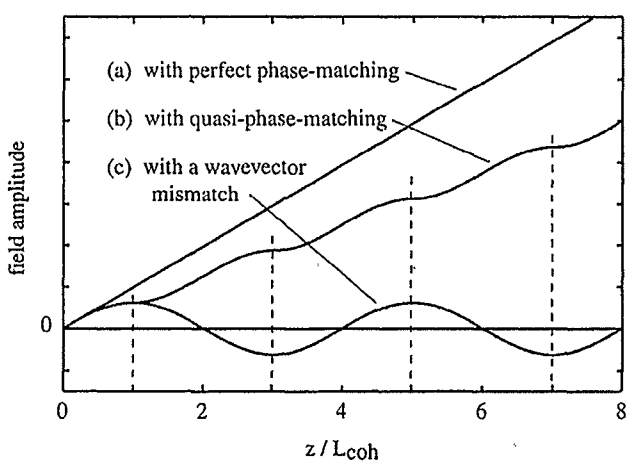

Figure 2.1: Quasi-Phase Matching: The intensity growth as a function of propagation distance through the crystal. Perfect phase-matching, as available in birefringent crystals, would perform better than quasi-phase matching if the non-linearities were equal [49]

2.1.2 Four-Wave Mixing and Atomic Ensembles

Crystals are not the only medium that can produce photon pairs. In general, any medium with sufficiently strong non-linear effects can be used. In particular, much work has

been done recently on the production of photon pairs directly inside optical fibre as this removes the issue of coupling photons from bulk crystals to optical fibres for transmission. Optical fibre, which is made of silica oxide, does not have a $\chi^{(2)}$ non-linearity but does have a third-order $\chi^{(3)}$ effect. This leads to four-wave mixing (FWM) processes where two pump beams can produce a photon pair. Standard telecommunication dispersion shifted fibre (DSF) has been used to produce photon pairs, with small wavelength separations from the pump beam, around telecommunication wavelengths (1550 nm) [50, 51] and novel microstructured fibre (MSF) designs have been used to produce photon pairs at wider separation in visible and NIR wavelengths (600 nm to 900 nm) [52, 53]. To date, no one has reported a photon pair source using optical fibre that produces photon pairs with one photon in the NIR (800 nm) and one photon at telecommunication wavelengths (1550 nm) although investigations have begun (see appendix A).

Producing photon pairs with atomic ensembles (AE) has also been explored [40] and experiments producing photon pairs at widely separated wavelengths (telecommunication and NIR wavelengths) have been achieved [54]. In these types of sources a collection of atoms with a lambda energy level system (i.e. two ground states labelled g and s and one excited state labelled e) are used. To prepare the AE a weak laser pulse is sent into the ensemble such that a single excitation from g to e is created and then decays to s. If this process occurred then one photon is emitted during the e to s decay and can be detected. Then when a second photon is required a second laser pulse, much stronger than the first, is sent through the ensemble such that the state s is guaranteed to form another single excitation in e and decay to g, thus emitting a photon.

2.1.3 Photon Pair Correlation

All aforementioned sources of photon pairs are of probabilistic nature as each photon in the pump beam has some probability to produce a pair (or excite an atom). Thus, the

number of emitted photon pairs per time unit follows a statistical distribution such as a Poissonian or thermal distribution. These different classical distributions can be identified through experimental measurements of the second-order auto-correlation function (here $I(t)$ refers to the intensity of the light field at time t while $\langle I \rangle$ corresponds to the expectation value of the measurement) [55]:

$$g^{(2)}(\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle\langle I(t+\tau)\rangle} \tag{2.3}$$

One interpretation of this quantity is that it is the normalized conditional probability that if intensity I is measured at time t it is also measured at time $(t+\tau)$.

If one considers the second-order auto-correlation function at zero time difference, $g^{(2)}(0)$, it is possible to show that for all classical light sources $g^{(2)}(0) \geq 1$ [55]. In particular, for a light field described by a Poisson distribution, as is the case for coherent light emitted by a laser, $g^{(2)}(0) = 1$ and for a light field described by a thermal distribution, as is the case for black body radiation, $g^{(2)}(0) = 2$.

In fact, the $g^{(2)}(0)$ can be used as a confirmation of a quantum mechanical source of photon pairs. In the quantum mechanical description (here I is replaced with the normally ordered $\hat{n}$, which is the an operator that gives the number of photons in a field [55]):

$$g^{(2)}(0) = 1 + \frac{\langle(\Delta\hat{n})^2\rangle - \langle\hat{n}\rangle}{\langle\hat{n}^2\rangle} \tag{2.4}$$

In this description, the classical results above are still true but now $g^{(2)}(0)$ can be calculated for photons as well as light fields. In particular, as photons can, in principle, exist as a single particle (i.e. a beam consisting of just one photon) it is possible to calculate the theoretical $g^{(2)}(0)$ with equation (2.4) and find that $g^{(2)}(0) = 0$ - A value not allowed by the classical description of light. Thus, $g^{(2)}(0) < 1$ is an indicator of a non-classical field of light.

As part of the characterization of a source of photon pairs we define an operational

definition of the $g^{(2)}(0)$, in line with previous work [56], for the following setup. The two photons of each photon pair produced by a source are deterministically separated. One beam is immediately sent to a single photon detector (detector H) while the second beam is split again at a 50/50 beamsplitter before the photons are detected by one of two single photon detectors (detectors A and B - note that detectors H, A and B response is either 'detected nothing' or 'detected something'. Their response is the same whether they detect 1, 2 or 10^6 photons). Only when the first detector reports a detection are the second detectors activated. This detector is said to herald the presence of light at the other detectors. This setup is known as the Hanbury Brown and Twiss (HBT) setup [57]. The single photon $g^{(2)}(0)$ can then be defined as the normalized conditional probability that, if a photon is detected at A, another photon will be detected at B:

$$g^{(2)}(0) = \frac{p_{AB|H}}{p_{A|H} \times p_{B|H}}, \tag{2.5}$$

This definition follows the properties discussed above. $g^{(2)}(0) = 1$ for uncorrelated photons following a Poisson distribution, $g^{(2)}(0) = 2$ for stimulated photons following a thermal distribution and $g^{(2)}(0) = 0$ for a source that emits single photons. For a probabilistic source of photon pairs that emits pairs with a Poisson or thermal distribution, like the non-linear crystals described earlier, one may think that the $g^{(2)}(0) = 1$ or 2 with this definition. This is not true because the heralding feature of detector H removes the vacuum component from detectors A and B and thus alters the statistics. That is why this setup is often referred to as a Heralded Single Photon Source (HSPS). Although it is not a perfect single photon source, the heralding signal indicates the presence of at least one photon, and, for this reason, HSPSs have been used for quantum communication tasks in the past [58, 59, 60, 61].

2.2 Characterization Model

In most applications, it is beneficial or even essential to know the mean number of photon pairs μ emitted per unit of time, a quantity that is here referred to as the *brightness*. For entanglement based QKD, Ma *et al.* have shown that both the secret key generation rate and the maximum distance over which a secret key can be established can be maximized by properly tuning the brightness [62]. Another example is the security of QKD based on HSPS, which relies on the ability of the sender to assess the photon statistics in a precise way [58, 59, 60, 61]. Also, de Riedmatten *et al.* have shown that the visibility in Bell-state measurements, which is a key element of proposed quantum repeaters, crucially depends on the brightness [63]. Most recently, H. C. Lim *et al.* created a model that permits an entanglement distributor in a quantum network to determine the brightness that optimizes the entanglement visibility (see sections 3.1.1,3.3) for any pair of users in a quantum network, when given user-specific parameters such as the single photon transmission to each user [64].

Assessing the brightness of a source of photon pairs is a non-trivial task when limited to lossy channels and non photon-number-resolving detectors. This problem can be solved provided one knows the exact value of the total transmission of all photon channels. However, evaluating the loss associated with coupling a single photon from free-space to a single mode fibre is not simple. One technique requires mode-matching a probe laser to the single photon mode, but this can be imprecise and unpractical (see [65, 66, 67] as examples). The brightness can also be inferred from measurements of the second-order autocorrelation function, $g^{(2)}(0)$ [68]. However, as the time required for $g^{(2)}(0)$ measurements depends on three-fold coincidence detection stemming from two simultaneously generated pairs, such measurements are time consuming to implement (see [69] and [70] as examples). Therefore, a method from which the brightness and the

losses of the transmission lines can be determined with precision, speed and simplicity is necessary.

To this end, the following sections detail how one can assess the brightness and the photon channel transmissions of a source of photon pairs by solely measuring single and two-fold coincidence detections stemming from photons belonging to one pair. This makes this method very fast and efficient.

2.2.1 Model

To assess the properties of a source of photon pairs, we developed an exact model of the detection statistics of the experimental setup detailed in figure (2.2) [71].

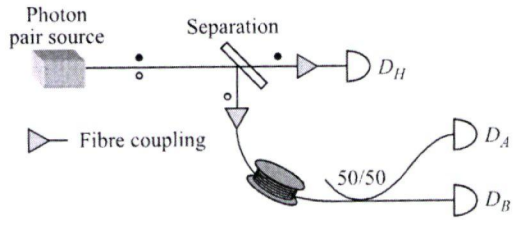

Figure 2.2: The sources of photon pairs we consider comprise all probabilistic sources, including those based on nonlinear crystals, optical fibres or atomic ensembles. The distribution of the number of produced photon pairs per measurement time window can be given by any distribution such as Poissonian or thermal and is assumed to be known in advance. The pairs are deterministically separated, potentially by a dichroic beamsplitter in the case of collinear generation with non-degenerate wavelengths, or by non-collinear generation, into two separate channels. Each beam is filtered to remove all pump light and then the pairs are coupled into optical fibres. One beam is split again at a 50/50 beamsplitter before the photons are detected by non-photon number resolving single photon detectors D_H, D_A and D_B. It is important to note here that the 50/50 beamsplitter and D_B used in this setup is not required to determine the brightness and the transmissions. Indeed, to assess the brightness and the transmissions only the detectors D_H and D_A are necessary. In this work, the beamsplitter and D_B were added only to provide a way to verify the validity of the predictions through the $g^{(2)}(0)$ measurement. Modifying the model (vector $\mathbf{P}$ and matrices, see below) to accommodate for a setup with no beamsplitter and D_B is straightforward.

To model the detection statistics of this experimental setup we construct a column

vector $\mathbf{P}$, as shown in equation (2.6), which describes the joint state of the detectors:

$$\mathbf{P} = \left(p_{\bar{A}\bar{B}\bar{H}} \; p_{A\bar{B}\bar{H}} \; p_{\bar{A}B\bar{H}} \; p_{\bar{A}\bar{B}H} \; p_{AB\bar{H}} \; p_{A\bar{B}H} \; p_{\bar{A}BH} \; p_{ABH} \right)^{\mathrm{T}} . \tag{2.6}$$

Each element of $\mathbf{P}$ describes the probability that a set of detectors clicked or not per measurement time window. The measurement time window is defined as the elementary observation time for which detections are considered for statistical analysis (i.e. a finite time window centered on one pump pulse; see later) and thus, $\mathbf{P}$ describes the state of the detectors after receiving the photons contained within one measurement time window. For example, $p_{A\bar{B}\bar{H}}$ is the probability that detector D_A clicked, during the measurement time window, and D_H and D_B did not. The goal is to determine how this vector, initially in state $\mathbf{P}_0 = (1\ 0\ \ldots\ 0)^{\mathrm{T}}$, is affected by single and multiple photon pair emissions as well as detector dark counts during one measurement time window. First, we describe the interaction of *one* photon pair with the detectors using the following transition matrix:

$$M_\eta = \begin{pmatrix} 1-\eta_H+(\eta_A+\eta_B)(\eta_H-1) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \eta_A(1-\eta_H) & (1-\eta_B)(1-\eta_H) & 0 & 0 & 0 & 0 & 0 & 0 \\ \eta_B(1-\eta_H) & 0 & (1-\eta_A)(1-\eta_H) & 0 & 0 & 0 & 0 & 0 \\ \eta_H(1-(\eta_A+\eta_B)) & 0 & 0 & 1-(\eta_A+\eta_B) & 0 & 0 & 0 & 0 \\ 0 & \eta_B(1-\eta_H) & \eta_A(1-\eta_H) & 0 & 1-\eta_H & 0 & 0 & 0 \\ \eta_A\eta_H & \eta_H(1-\eta_B) & 0 & \eta_A & 0 & 1-\eta_B & 0 & 0 \\ \eta_B\eta_H & 0 & \eta_H(1-\eta_A) & \eta_B & 0 & 0 & 1-\eta_A & 0 \\ 0 & \eta_B\eta_H & \eta_A\eta_H & 0 & \eta_H & \eta_B & \eta_A & 1 \end{pmatrix} . \tag{2.7}$$

Each element of M_η describes the probability for a pair to cause a transition of the three detectors. Each term is written as a function of η_H, η_A and η_B which are the overall transmissions of each channel, from the photon pair source to D_H, D_A and D_B respectively, including all optical losses, fibre coupling losses, detector inefficiencies, and the 50/50 beamsplitter. For example, $M_\eta(1,1)$ is the probability for the system to make a transition from $\bar{A}\bar{B}\bar{H}$ to $\bar{A}\bar{B}\bar{H}$ (i.e. to remain in the state where no detectors clicked), which must equal: $p_{\bar{A}\bar{H}} + p_{\bar{B}\bar{H}} = (1 - \eta_H - \eta_A + \eta_A\eta_H) + (1 - \eta_H - \eta_B + \eta_B\eta_H) = 1 - \eta_H + (\eta_A + \eta_B)(\eta_H - 1)$. Similarly, $M_\eta(2,1)$ is the probability to make a transition from $\bar{A}\bar{B}\bar{H}$ to $A\bar{B}\bar{H}$ (i.e. no detectors clicked before and, provided one photon pair arrives, only D_A clicks), which equals $\eta_A(1 - \eta_H)$. All the upper diagonal elements

are equal to 0 as photons cannot make detectors "unclick". The rest of the matrix is constructed following the same physical reasoning. Furthermore, to conserve the total probability, each column of M_η sums to 1. The result of *one* photon pair interacting with the detectors is thus given by $M_\eta \mathbf{P}_0$.

Second, the evolution of the system when i photon pairs are created during the measurement time window is described by $(M_\eta)^i \mathbf{P}_0$, as the detectors are not number resolving and losses and the beamsplitter choice for individual pairs in multi-pair emission are independent.

In addition to the absorption of a photon, thermal excitations can also cause detector clicks. These dark counts can be taken into account by constructing another matrix M_{dc}. Thus, the evolution resulting from dark counts and i photon pairs is described by $M_{dc}(M_\eta)^i \mathbf{P}_0$. Noting the dark count probabilities per measurement time window as d_H, d_A and d_B, we get

$$M_{dc} = \begin{pmatrix} (1-d_A)(1-d_B)(1-d_H) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ d_A(1-d_B)(1-d_H) & (1-d_B)(1-d_H) & 0 & 0 & 0 & 0 & 0 & 0 \\ (1-d_A)d_B(1-d_H) & 0 & (1-d_A)(1-d_H) & 0 & 0 & 0 & 0 & 0 \\ (1-d_A)(1-d_B)d_H & 0 & 0 & (1-d_A)(1-d_B) & 0 & 0 & 0 & 0 \\ d_A d_B(1-d_H) & d_B(1-d_H) & d_A(1-d_H) & 0 & 1-d_H & 0 & 0 & 0 \\ d_A(1-d_B)d_H & (1-d_B)d_H & 0 & d_A(1-d_B) & 0 & 1-d_B & 0 & 0 \\ (1-d_A)d_B d_H & 0 & (1-d_A)d_H & (1-d_A)d_B & 0 & 0 & 1-d_A & 0 \\ d_A d_B d_H & d_B d_H & d_A d_H & d_A d_B & d_H & d_B & d_A & 1 \end{pmatrix}. \quad (2.8)$$

Thus, when an unknown number of photon pairs are incident, it is possible to calculate the final vector $\mathbf{P}$ through

$$\mathbf{P} = \sum_{i=0}^{\infty} p_i M_{dc}(M_\eta)^i \mathbf{P}_0, \quad (2.9)$$

where p_i is the probability to create i photon pairs per measurement time window. Provided that the probability distribution for p_i is known this equation holds for all distributions, such as Poissonian, thermal or any distributions between the two [72]. Note that all matrices commute so the order in which they are applied does not matter. The construction of the matrices ensures that all elements of $\mathbf{P}$ are bounded individually between 0 and 1 and that the elements of $\mathbf{P}$ sum to 1 (i.e. the total probability is conserved). We note that the model is exact and there are no approximations.

2.2.2 Determining channel transmissions

With this model one can precisely determine the values of μ, η_H, η_A and η_B by measuring single and two-fold coincidence detection probabilities stemming from single pairs only. However, these measurements require that the pump power (or equivalently the brightness of the photon pair source) is low enough so that multi-pair events are negligible: $p_i \ll p_1$ for $i > 1$. Fortunately, this model also allows an experimental verification of this condition. The verification arises from correlations in detections on D_A and on D_H. To measure this, p_H is defined to be the heralding probability, i.e. the probability for D_H to click independent of the other detectors, $p_H = p_{\bar{A}\bar{B}H} + p_{A\bar{B}H} + p_{\bar{A}BH} + p_{ABH}$, and similar expressions are defined for p_{AH} and p_A. We then define a parameter $G = p_{AH}/(p_H p_A)$ quantifying the strength of the correlation between detections at D_A and D_H. The model described by equation (2.9) predicts that, for Poisson, thermal and in between distributions, the value of G equals one at a very low brightness, when the coincidences are dominated by dark counts and detections are uncorrelated, and equals one again at high heralding probabilities, when the coincidence detections stem mostly from multi-pair emissions and correlations are smeared out. In between, the value of G can go well above 1 and this is an indication that multi-pair emissions are negligible. As we show here, this allows one to experimentally obtain an upper bound for μ when proceeding as follows.

1. The dark count probability per measurement time window for each detector is measured (d_H, d_a, d_b).

2. The pump power is lowered and the transmissions are optimized until a value of G significantly higher than 1 is measured ($G \gg 1$).

3. A plot of G versus μ is produced numerically assuming that the fibre coupling is perfect and that there are no additional optical losses, thereby setting the values

of η_H and η_A equal to the specified detection efficiency of the detectors.

4. An upper bound for μ is obtained from the plot by identifying the largest value of μ that produces a value of G equal to the measured value.

They key point is that, for a given μ and dark count probabilities, G is decreased towards 1 when the transmissions are decreased. Thus, using this method, the true value of μ must be smaller than the upper bound as the transmissions are overestimated. This, in return, allows one to obtain a lower bound for the ratio, $r = p_1/p_{i>1}$, of the probability of single pair emissions, p_1, over the probability of multi-pair emissions, $p_{i>1} = 1 - p_0 - p_1$. As an illustration, using $\eta_H = 60\%$ and $\eta_A = 25\%$, corresponding to the detection efficiencies of our detectors, and using their respective measured dark count probabilities (see section 2.4.2), we produced the solid line shown on figure (2.3) where we assumed a Poisson distribution, $p_i = \exp(-\mu)\mu^i/i!$.

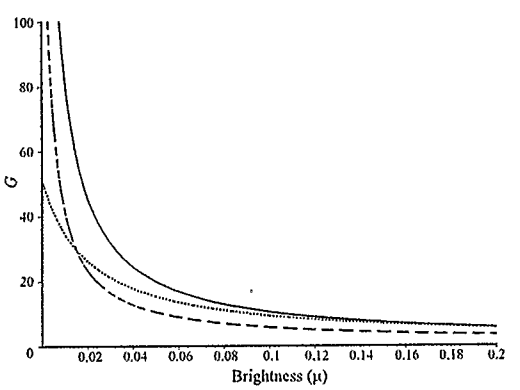

Figure 2.3: Correlation strength G versus brightness μ. The solid line corresponds to $\eta_H = 60\%$ and $\eta_A = 25\%$. It reaches a maximum value at very low μ and then sharply decreases to 1 for $\mu = 0$ (not visible). The meanings of the dotted and dashed lines are discussed in section 2.4.2 and [71] respectively.

Once the pump power is properly set and the lower bound on r is sufficiently high, equation (2.9) can be truncated to $i = 1$ and one can show that the probability for D_H to click on a photon and not a dark count is given by $p_H^{(1)} = (p_H - d_H)/(1 - d_H)$. Similarly,

we get $p_A^{(1)} = (p_A - d_A)/(1 - d_A)$ and the equivalent for $p_B^{(1)}$. In the same way, we can get expressions for the coincidence probabilities p_{AH} and p_{BH}. Then, using these expressions and an experimental data collection run with a heralding probability that guarantees negligible multi-pair events, one can solve for the four unknowns μ, η_H, η_A and η_B, since the dark count probabilities can be measured directly. These unknowns can be calculated through equations (2.10) through (2.12). The equivalent set for D_B is constructed by replacing η_A and $p_A^{(1)}$ by η_B and $p_B^{(1)}$, respectively:

$$\eta_H = \frac{p_{AH} - p_H^{(1)} d_A(1 - d_H) - p_A^{(1)} d_H(1 - d_A) - d_A d_H}{p_A^{(1)}(1 - d_A)(1 - d_H)}, \tag{2.10}$$

$$\eta_A = \frac{p_{AH} - p_H^{(1)} d_A(1 - d_H) - p_A^{(1)} d_H(1 - d_A) - d_A d_H}{p_H^{(1)}(1 - d_A)(1 - d_H)}, \tag{2.11}$$

$$p_1 = \frac{p_H^{(1)}}{\eta_H} = \frac{p_A^{(1)}}{\eta_A}. \tag{2.12}$$

Note that these predictions apply to any statistical distribution for which the multi-pair events can be neglected (for example, through the method described above). However, to determine the value of the brightness, one must have prior knowledge of the distribution and how to relate it to the measured value of p_1. In the case of a Poissonian source, we have $p_1 \doteq \mu \exp(-\mu)$ which can be solved numerically for μ. The case of a thermal distribution is similar with $p_1 = (\tanh\sqrt{\mu}/\cosh\sqrt{\mu})^2$.

Once the transmissions are precisely known, one can use equation (2.9) to find the brightness that corresponds to any measured heralding probability. This will then allow one to predict the complete detection statistics vector $\mathbf{P}$.

2.2.3 Application to a Heralded Single Photon Source

The transmissions and the brightness, along with the knowledge of the pair distribution type, can be used to predict the $g^{(2)}(0)$ of an HSPS for any desired heralding probability p_H, in an HBT experiment [57]. As stated earlier, the distribution of the number of

photons in that mode follows the distribution of the number of photon pairs created by the source except for a reduced vacuum component, p_0, due to the heralding. A $g^{(2)}(0) < 1$, which is achievable with a HSPS, implies a nonclassical source (for a perfect single photon source $g^{(2)}(0) = 0$). Alternatively, a $g^{(2)}(0) \geq 1$ describes a classical source (for Poissonian $g^{(2)}(0) = 1$ and for thermal $g^{(2)}(0) = 2$, see section 2.1.3). As an experimental test of the model, predictions can be compared with real measurements of the $g^{(2)}(0)$. In this experiment, which can be seen as measuring a subset of equation (2.9), detectors D_A and D_B are activated only when D_H clicks. The $g^{(2)}(0)$ is defined as

$$g^{(2)}(0) = \frac{p_{AB|H}}{p_{A|H} \times p_{B|H}}, \tag{2.13}$$

where $p_{AB|H}$ is the probability that both D_A and D_B click provided that D_H clicked, etc.

For a specific heralding probability p_H, one can directly measure $g^{(2)}(0)$ using the setup of figure (2.2) by keeping only the events where D_H clicked. On the other hand, the $g^{(2)}(0)$ can also be predicted for the same heralding probability using equation (2.9). The experimental results of this verification are presented in the next section.

One interesting theoretical result regarding optimization of an HSPS can be derived from this model. Considering a Poissonian distribution at low brightness and assuming that dark counts are negligible, one can derive from equation (2.9) that $g^{(2)}(0) = \mu(2 - \eta_H)$. Similarly, for a thermal distribution the $g^{(2)}(0)$ is higher by a factor of 2: $g^{(2)}(0) = 2\mu(2 - \eta_H)$. In the case of spectral and/or spatial correlations, where the coincidence detection probability $\eta_{HA} = c\eta_H\eta_A$ is decreased by a factor c [71], and with a Poissonian source, $g^{(2)}(0) = \mu(2/c - \eta_H)$. This indicates that for a HSPS, the transmission to the heralding detector is a crucial parameter to optimize.

2.3 Experimental Setup

The experimental setup is shown in figure (2.4) and is detailed in the following sections.

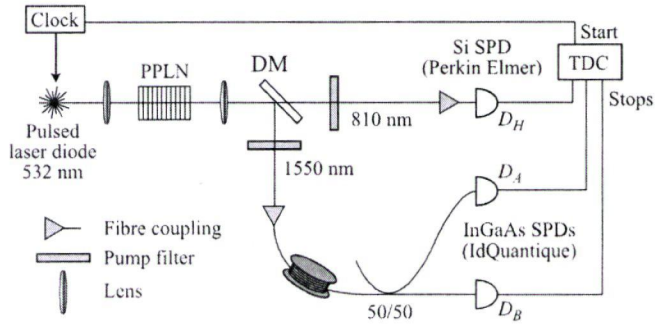

Figure 2.4: Experimental setup.

2.3.1 Optical setup

To produce photon pairs, a 1 cm long periodically poled lithium niobate ($LiNbO_3$) crystal (PPLN) with a three available grating period of 7.05 μm, 7.10 μm and 7.15 μm designed by Stratophase (SFG2-10) was purchased. Using the Sellmeier equation $LiNbO_3$ coefficients from [73] and assuming a 530.6 nm pump laser, phase-matching curves can be calculated for the crystal, as seen in figure (2.5) [74, 75]. Based on these calculations, the crystal was heated to 176 °C using an oven and PID temperature controller from Thorlabs (PV10 and TC200 respectively). Then, with the 7.05 μm poling period collinear SPDC to one or several photon pairs can occur, with each pair consisting of one 807 nm and one 1546 nm photon.

For the pump laser, a pulsed diode laser from PicoQuant (PDL-800-B) that creates 50 ps pulses at 530.6 nm was selected. The diode emits at 1061 nm and was frequency doubled to 530.6 nm. Afterwards, excess 1061 nm light is filtered using a dispersive prism from Thorlabs (PS851). Light was then focused onto the PPLN and afterwards a dichroic

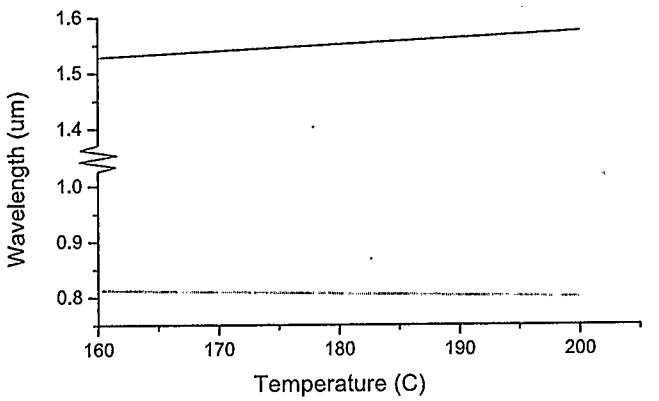

Figure 2.5: Phase matching calculation for PPLN with a 7.05 μm grating period pumped with a 530.6 nm laser.

mirror from CVI Melles Griot was used to separate the down-converted photons. After excess pump light was removed with Thorlabs long-pass colour filters (FGL715 followed by FGL780 with cutoff wavelengths at 715 nm and 780 nm respectively to minimize fluorescence problems) the photons were coupled into SMF28 optical fibres.

The 810 nm photons were sent towards D_H, a free-running silicon (Si) single photon counting module from Perkin-Elmer (SPCM-AQR-14-FC). This detector has a 60% single photon detection efficiency (quantum efficiency) at 800 nm, is rated to have under 100 false detections (dark counts) per second and is engineered to have a maximum deadtime of 40 ns (32 ns typical). The 1550 nm photons were sent through a 50/50 fibre beamsplitter designed and constructed by the Fibre Optics Laboratory at École Polytechnique de Montréal. Afterwards the photons reached one of D_A or D_B, which were gated Indium Gallium Arsenide (InGaAs) single photon detectors from IdQuantique (id201). These detectors can be set to have quantum efficiencies between 10% to 25% but due to excess dark counts these detectors can only be activated (gated) for a short time window centered around the expected arrival time of the photons. This time window width was set to 5 ns and the detector deadtime was set to 10 μs.

2.3.2 Electronics setup

The detection statistics were recorded using a Time-Digital-Converter (TDC) from ACAM (ATMD-GPX). This device can monitor nine channels (one start channel and eight stop channels) for electrical signals and reports the time difference from the start pulse to each stop pulse with 80 ps resolution, which can be continuously downloaded to a computer. The start pulse for the TDC was provided by the clocking signal which was produced by a delay generator from Stanford Research Systems (DG535). The clocking signal was also used to trigger the pulsed laser diode and the InGaAs detectors. The stop pulses collected by the TDC included the detection signal from the Si detector, two detection signals from the InGaAs detectors and two *gate-out* signals also from the InGaAs detectors. Each InGaAs detector emits a gate-out pulse when it is triggered if the detector is not currently in deadtime due to a previous detection. These gate-out signals were collected so that events where one or both detectors were dead could be discarded from analysis. The detections on the Si detector were considered valid only if they arrived within a 5 ns window centered on the expected arrival time of the photons, as measured by the TDC. These data were transferred to PC via application drivers specially designed by ACAM for our application and were analyzed in real-time using in-house C++ and Labview software. Due do low data rates between the TDC and the PC the clocking signal triggering the laser and InGaAs detectors was set to 30 kHz while determining the transmissions. This low repetition rate ensured that the saturation effects in the detection electronics were avoided.

2.4 Experimental Results

2.4.1 Bandwidth Measurements

The first measurements of the photon pair source were measurements of the coherence length l_c of the downconverted 810 nm photons. We built a balanced, free-space Michelson interferometer in the path of the 810 nm photons and coupled the output of one arm into fibre. We controlled the path length of one arm with a nanomax translation stage while the path length of the other arm could be continuously varied using a piezo-electric actuator. At each step of the translation stage we measured interference visibility by observing count rates on the Si detector as the piezo was continuously scanned. From these visibility measurements the coherence length was measured to be 90 μm. From these measurements we calculated the bandwidth to be $\Delta\lambda_{810} \approx 7\,\text{nm}$.

$$\Delta\lambda_{810} = \frac{\lambda^2}{l_c} \approx 7\text{nm} \tag{2.14}$$

Based on energy conservation of the SPDC process, the bandwidth of the 1550 nm photons is $\Delta\lambda_{1550} \approx 27\,\text{nm}$.

$$\Delta\lambda_{1550} = \lambda_{1550}^2\left(\frac{\Delta\lambda_{810}}{\lambda_{810}^2} + \frac{\Delta\lambda_{532}}{\lambda_{532}^2}\right) \approx \frac{\lambda_{1550}^2}{\lambda_{810}^2}\Delta\lambda_{810} = 27\text{ nm} \tag{2.15}$$

As the downconverted photons' coherence time, which equals $l_c/c = 0.27$ ps, is much smaller than the pump pulse duration, which is 50 ps, one can confidently assume that this source of photon pairs follows Poissonian statistics [72].

2.4.2 Confirmation of Model

We first measured dark count probabilities to be $d_A = 2.87 \times 10^{-4}$, $d_B = 3.84 \times 10^{-4}$ and $d_H = 2.5 \times 10^{-7}$ per 5 ns. Next, we lowered the pump power using neutral density filters in order to increase the correlation strength between D_H and D_A to a value of $G = 20.6 \pm 1.0$, corresponding to a heralding probability of $0.287 \pm 0.001\%$. Intersecting this value with

the solid line of figure (2.3) gives an upper bound of $\mu \leq 0.0480 \pm 0.0013$, yielding $r \geq 41.0 \pm 2.2$, which was considered sufficiently high to continue. Next we measured single and coincidence detection probabilities and calculated the following values: $\eta_H = 0.1212 \pm 0.0031$, $\eta_A = 0.0145 \pm 0.0005$, $\eta_B = 0.0162 \pm 0.0005$ and $\mu = 0.02375 \pm 0.00016$, corresponding to $r = 83.5 \pm 0.6$. The G curve corresponding to these values is plotted as the dotted line on figure (2.3), and the predicted value of G at $\mu = 0.02375$ is 23.9 ± 0.5, which is close to the measured value of 20.6.

Using these values together with equation (2.9), we produced a plot of the predicted $p_{AB|H}$, $p_{A|H}$ and $p_{B|H}$ for a wide range of the brightness (and consequently, of the heralding probability). We compared these predictions to the measured values on figure (2.6a) and (2.6b). Next we compared predicted and measured $g^{(2)}(0)$, as shown on figure (2.7a). On the same figure we plotted the value of the brightness μ corresponding to each heralding probability. In all cases, the agreement between the predicted and measured values is excellent. We note that for these measurements, the repetition rate was increased to 5 MHz and the InGaAs detectors were activated for 5 ns only when the Si detector clicked synchronously (within a 5 ns window) with the pump, as required for $g^{(2)}(0)$ measurements in the HBT setup. This resulted in an average detection rate of 30 kHz, with randomly distributed time differences, for the InGaAs detectors and was thus sufficient to ensure that saturation effects in the detection electronics was not an issue.

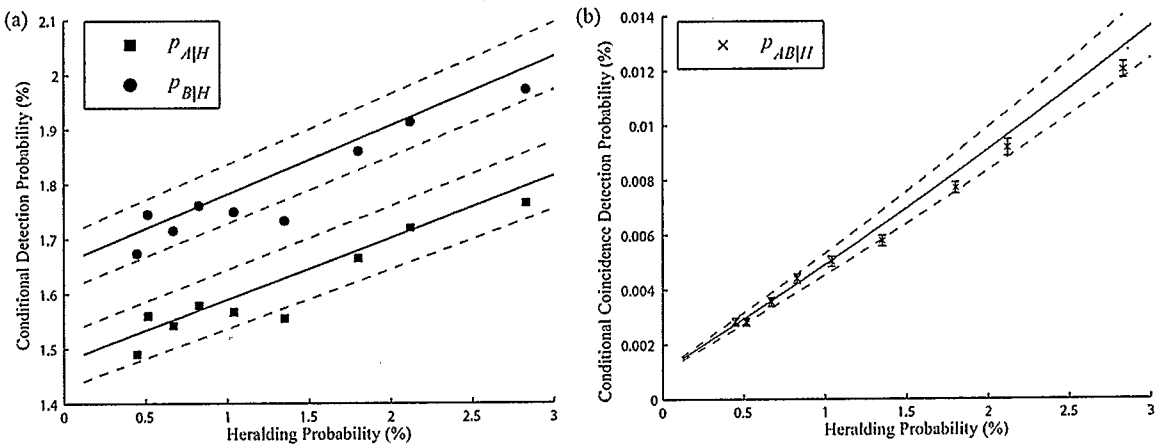

Figure 2.6: (a) Predicted (solid lines) and measured (points) conditional detection probabilities $p_{A|H}$ and $p_{B|H}$. (b) Predicted (solid line) and measured (points) conditional coincidence probability $p_{AB|H}$. The dashed lines on both plots are the one standard deviation uncertainty bounds on the predicted values which were generated using the uncertainty bounds on the measured transmissions.

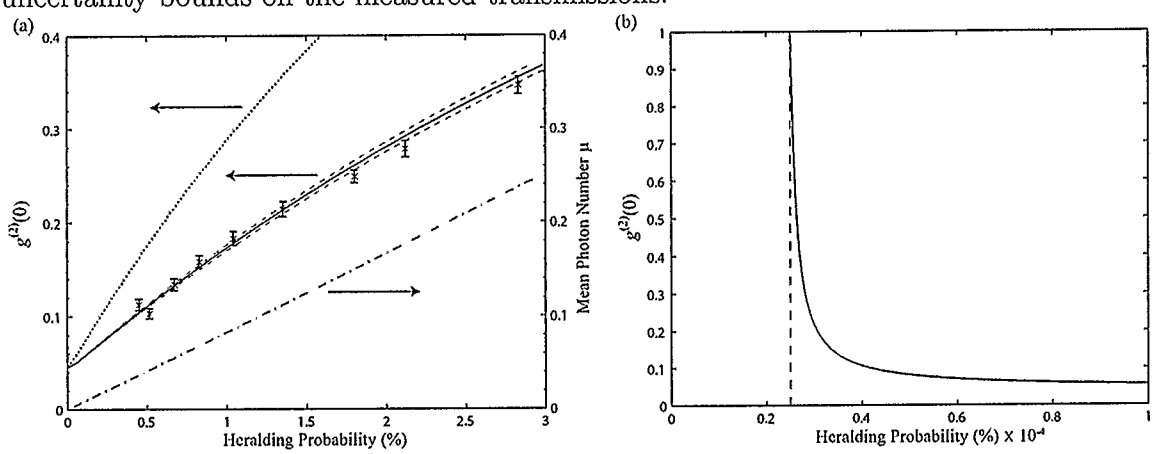

Figure 2.7: (a) Predicted autocorrelation $g^{(2)}(0)$ for Poissonian (solid line) and thermal (dotted line) distributions, measured values (points), and the corresponding brightness μ (dash-dotted line). The measured data agrees very well with the Poissonian distribution. Arrows indicate which scale corresponds to which line and dashed lines are the one standard deviation uncertainty bounds on the predicted values. (b) As the heralding probability reaches the noise level of D_H (dashed line), the model correctly predicts that the $g^{(2)}(0)$ approaches one, as uncorrelated dark counts begin to dominate over photon clicks.

2.5 Discussion

This method drastically reduces the time needed to characterize the source as measurements of single and two-fold coincidence detections at a low heralding probability are sufficient to determine the transmissions. These can then be used to predict the brightness of a photon pair source and the $g^{(2)}(0)$ of a HSPS for any heralding probability. In contrast, a single direct measurement of the $g^{(2)}(0)$ at a given heralding probability requires three-fold coincidence detections stemming from multi-pair emissions, which are less likely to happen. In this experiment, at a heralding probability of 0.287%, two-fold coincidences were approximately 700 times more likely than three-fold coincidences. Consequently, a direct $g^{(2)}(0)$ measurement required much more time.

This model allows an entanglement distributor in a quantum network to quickly and precisely tune the brightness on demand as required to optimize the performance of entanglement based QKD, to assess the security of HSPS-based QKD or to optimize quantum repeater error rates and distances, all in the context of fluctuating experimental conditions such as photon channel transmissions. Finally, in [71], we showed that our model correctly reproduces the detection statistics even if the photons are spectrally and/or spatially correlated, and that this only leads to an overestimation of the brightness of the source and thus does not affect security of QKD. The simplicity of the proposed method makes it very attractive for the field of quantum communication in general.

Chapter 3

Sources of Entanglement

3.1 Theory and Background

One of the unique, and most important, features of quantum mechanics is entanglement. Simply put, two particles are said to be entangled if the state of a composite system cannot be separated into a product of single qubit states [7]. The two particles in the state

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_a}|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_b}|1\rangle) \tag{3.1}$$

are not entangled because one can easily say that particle one is in the state $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_a}|1\rangle)$ and particle two is in the state $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_b}|1\rangle)$. Each particle can be fully described independently of the other. However, the state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle \tag{3.2}$$

cannot be factorized into two separate states and thus the full description of either particle's state requires the other particle. This state is an entangled state.

Entanglement has profound affects on statistical correlations one can observe in experimental situations. Imagine that one has a source that emits the entangled Bell state described by equation (3.2). If one projects the first qubit onto $|0\rangle$ (i.e. measures whether the particle is in the state $|0\rangle$), one will have a 50% chance of a detection. The same holds for particle two. This is akin to projecting onto the north pole of the Bloch sphere in figure (3.1). If one projects both particles onto $|0\rangle$ one will either detect both particles or neither particle. Detections of the particles are perfectly correlated.

However, the above thought experiment could be reproduced with a completely clas-

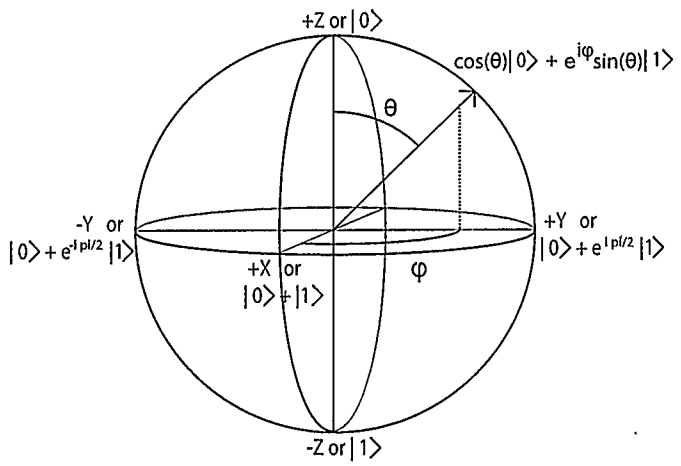

Figure 3.1: Qubit states represented on the Bloch sphere: The parameters θ and ϕ represent the polar and azimuthal angles of the vector on the Bloch Sphere that represents a qubit's quantum state. Another commonly used notation is to describe the quantum state by its relation to the Z, Y and X axes. For instance, $|0\rangle$ and $|1\rangle$ are the states $+Z$ and $-Z$ and form the Z-axis.

sical source of particles. Imagine a second source that emits both particles in the state $|00\rangle$ with a probability of 50% or both particles in the state $|11\rangle$ also with a probability of 50%. If one projects both qubits onto $|0\rangle$ one will again see perfect correlation: either both particles are detected or neither particle is detected. To demonstrate that there exists a difference between the entangled Bell State and the classical mixture one can use the density matrix formalism. A density matrix is defined as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{3.3}$$

where p_i is the probability that a source emits the state $|\psi_i\rangle$. Calculating the density

matrix of the state emitted by each source described above yields the following result:

$$\begin{aligned}\rho_{\text{entangled source}} &= 1 \times |\Phi^+\rangle\langle\Phi^+| \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}\end{aligned} \tag{3.4}$$

$$\begin{aligned}\rho_{\text{classical source}} &= 0.5 \times |00\rangle\langle 00| + 0.5 \times |11\rangle\langle 11| \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\end{aligned} \tag{3.5}$$

The density matrices are clearly different and therefore there must exist projection measurements that lead to different measurement results.

3.1.1 Visibility and CHSH

There are two widely used experiments to assess the non-classical nature of qubit pairs. These are known as coincidence visibility measurements and violations of the CHSH inequality, both of which are described here.

Instead of the states described by equations (3.4) and (3.5), imagine that we have a single source that emits the entangled Bell state with probability V and the classical mixture with probability $(1 - V)$.

$$\rho = V|\Phi^+\rangle\langle\Phi^+| + (1 - V)(0.5|00\rangle\langle 00| + 0.5|11\rangle\langle 11|) \tag{3.6}$$

And instead of projecting each particle onto $|0\rangle$, imagine that we project each particle onto an equal superposition of $|0\rangle$ and $|1\rangle$ with a different phase for each particle ϕ_1 and

ϕ_2: $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_i}|1\rangle)$ (this is akin to projecting each particle onto a state somewhere on the equator of the Bloch sphere in figure (3.1)). The probability to measure a coincidence detection will equal (with $\phi = \phi_1 + \phi_2$):

$$\text{P(coincidence detection)} = \frac{1}{4}(1 + V\cos(\phi)). \tag{3.7}$$

Therefore, the probability of a coincidence detection depends on the phase settings of each measurement and, more importantly, if one scans the phase of one measurement (which is akin to rotating the projection around the equator in figure (3.1)) the coincidence detection probability will vary sinusoidally with a maximum value of $\frac{1}{4}(1+V)$ and a minimum value of $\frac{1}{4}(1-V)$. In particular, we see that the visibility, as defined in equation (3.8), equals

$$\begin{aligned} \text{visibility} &= \frac{\text{maximum value - minimum value}}{\text{maximum value + minimum value}}. \\ &= V \end{aligned} \tag{3.8}$$

Thus, as a maximally entangled state will have a visibility of 1 and with the measurements described above the quality of source of entanglement can be assessed by measuring these visibility curves. If $V > \frac{1}{3}$ then, due to the Peres criterion [76], the two particles must be entangled.

More generally, for a maximally entangled state, if one particle is projected onto a fixed state and the projection of the second particle is scanned around a full circle on the Bloch sphere in figure (3.2), the visibility will be maximized if the fixed projection of particle one lies on the circle scanned by the projection of particle two. Conversely, if the projection of particle two remains perpendicular to the fixed projection of particle one then the measured visibility will be zero. The visibility can take values between zero and one for intermediate cases.

The second common experiment used to verify the non-classical nature is a test of the CHSH inequality. This test is based on the work of John Bell [9] in 1964 and Clauser,

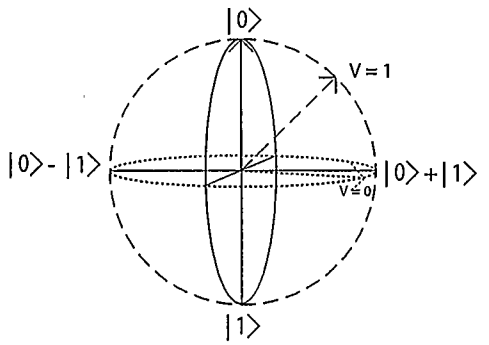

Figure 3.2: Two Entanglement Visibility Curves on the Bloch Sphere: The projection of particle one (solid arrow) is fixed at $|0\rangle$ while the projection of particle two (dashed and dotted arrows) traces one of two circles on the Bloch sphere. In one case the circle (dashed) passes through the fixed projection of particle one and the resulting visibility is maximized ($V = 1$). In the other case (dotted circle) the projection of particle two remains perpendicular (i.e. on the equator of equal superposition) to the fixed projection of particle one and the visibility is zero.

Horne, Shimony and Holt (CHSH) [77] in 1969 and allows identifying if the correlations under test must be explained using theories that do not obey local realism (see later). It is actually stronger than the Peres criterion and visibility curves as not all entangled states will violate the inequality; however all states that do violate the inequality are entangled. The description here is the CHSH form of Bell's inequality.

To perform this experiment one must be able to perform a certain projective measurement. Mathematically, one must measure the observable $M = +|\psi\rangle\langle\psi| - |\psi^{\perp}\rangle\langle\psi^{\perp}|$, where $|\psi\rangle$ and $|\psi^{\perp}\rangle$ are some pair of basis states. Now, imagine that one has a source of two particles. If one performs a projective measurement on the first particle in one of two bases (a and b) and the second particle in one of two other bases (c and d) one can measure a quantity known as the correlation coefficient, as in equation (3.9), for each combination of bases. Here, α and β determine the bases chosen for each particle (i.e. $\alpha = a$ or b, $\beta = c$ or d) and P_{+-} is the probability to project particle one onto $|\psi\rangle$ and

particle two onto $|\psi^{\perp}\rangle$, in their respective bases (similarly for P_{++}, P_{--} and P_{-+}).

$$E(\alpha, \beta) = P_{++} + P_{--} - P_{+-} - P_{-+} \tag{3.9}$$

CHSH demonstrated that if this experiment is preformed with a classical mixture, similar to the one described earlier, then the following inequality is true (S is typically referred to as the S-parameter).

$$S = |E(a, c) + E(b, c) + E(b, d) - E(a, d)| \leq 2 \tag{3.10}$$

It was also demonstrated that with a source of perfect entanglement as described earlier in equation (3.2), and the correct measurement settings, one can violate this inequality and achieve $S \leq 2\sqrt{2}$. Therefore, an experiment with a proper set of four measurement settings that produces $S > 2$ can be used to verify that a source emits entangled particles. Specifically, if one projects onto the equator of the Bloch sphere, $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$, one set of four measurement settings that would allow one to violate the CHSH inequality are:

$$\begin{aligned} a &\rightarrow |\psi\rangle = |\phi = -\pi/4\rangle \\ b &\rightarrow |\psi\rangle = |\phi = \pi/4\rangle \\ c &\rightarrow |\psi\rangle = |\phi = 0\rangle \\ d &\rightarrow |\psi\rangle = |\phi = \pi/2\rangle \end{aligned} \tag{3.11}$$

Countless articles regarding interpretations of Bell's inequality and the numerous experiments confirming that entanglement, as allowed by quantum mechanics, violates the inequality have been written. The general consensus is that entanglement violates one (or both) of the following two assumed properties of the physical world, which are required for the derivation Bell's inequality. The first assumption is that a measurement of one particle does not affect the state of the other particle. This is known as locality. The second assumed property is that both particles are emitted with definite states

although these may be unknown to the experimenter. This is known as realism. A source of a classical mixture is well described by local realism while a source of entanglement can only be described by violating at least one of these assumptions. Extensive articles have been written on these features (for example, see [24] for a discussion of experimental loopholes) but it is sufficient here to say that a violation of Bell's inequality is a signature of entanglement.

Finally, to connect visibility measurements to Bell's inequality it is important to note that $S = 2\sqrt{2}V$ if certain conditions are met. These conditions are that the coincidence curve is a sinus and that the probability to detector a particle does not depend on the measurement basis (and that the loopholes discussed in [24] are closed). Therefore, to ensure that all local realistic models of the measured state are ruled out, visibilities of the measured state need to be $V > 1/\sqrt{2} \approx 0.707$.

3.1.2 Producing and Measuring Entanglement

In general, to produce a source of entangled photons, something must be added to a pre-existing source of photon pairs. This something must be added such that there exists two possible methods in which a photon pair could be produced. If these two methods produce orthogonal states, and when a pair is produced it is impossible to know which of the two methods occurred, then the resulting state is entangled.

With the Type-I down-conversion crystals discussed in Chapter 2 producing entanglement in the polarization degree of freedom of the downconverted photons can be straightforward. An early example was demonstrated by Kwiat *et al.* [46] in 1999 by placing two identical Type-I crystals back to back, but with the optical axis of the second crystal at 90° with respect to the first, as in figure (3.3). Then, pump light polarized at 45° with respect to each of the optical axes is equally likely to down-convert in either crystal. If down-conversion occurs, and the crystals are thin enough, it is impossible to

know in which crystal the downconversion occured and thus polarization entanglement, as in equation (3.12), is achieved.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + e^{i\phi}|VV\rangle) \tag{3.12}$$

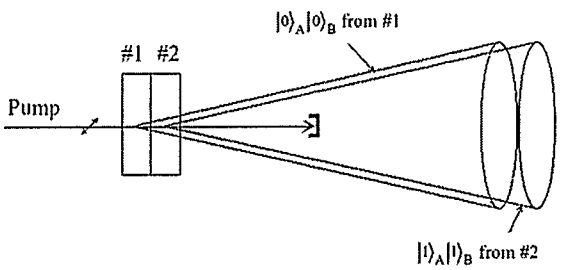

Figure 3.3: Entanglement generation with type-I spontaneous parametric down-conversion: The two crystals produce photon pairs in orthogonal polarization directions. If they are placed back-to-back then a pump polarized such that SPDC can occur in either crystal will produce entanglement. Image from [24]

Notice the similarity between equation (3.12) and equation (3.2). The horizontal polarized component, $|H\rangle$, is mapped to $|0\rangle$ and vertical, $|V\rangle$, to $|1\rangle$. The same polarization entangled state has been generated with periodically polled crystals [78], optical fibre [51] and atomic ensembles [79] in cleverly designed experiments in which the method of generating each polarization state is indistinguishable.

Measuring a polarization qubit is a straightforward task. Each photon can be projected onto any polarization state, anywhere on the Bloch sphere, by using a quarter-wave plate (QWP), half-wave plate (HWP), polarization beam splitter (PBS) and detector.

Another type of entanglement, which is compatible with all sources of photon pairs, and was first demonstrated by Brendel *et al.* in 1999 [25], is time-bin entanglement. The pump light is first passed through an interferometer with a large path-length difference, and phase ϕ_p, such that two pulses exit the interferometer at two different times (these are commonly labeled as early, short, or t_0, and late, long, or t_1), as in figure (3.4). If

down-conversion occurs in the source of photon pairs it is impossible to know which pulse created the photon pair and thus time-bin entanglement is created.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|t_0 t_0\rangle + e^{i\phi_p}|t_1 t_1\rangle) \tag{3.13}$$

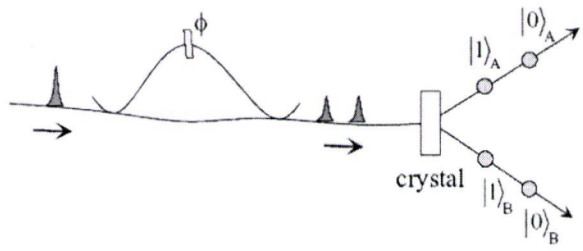

Figure 3.4: Entanglement with an interferometer: Two pulses exit the interferometer and as each are equally likely to cause down-conversion in the crystal time-bin entanglement is created. Image from [24]

Again, notice the similarity to equation (3.2). The early component, $|t_0\rangle$, is mapped to $|0\rangle$ and late, $|t_1\rangle$ to $|1\rangle$. A full mathematical description of these time-bin states could be expressed via a Gaussian distribution, at the central time of the wavepacket, with an extension given by the coherence length of the photon. If the time difference between $|t_0\rangle$ and $|t_1\rangle$ is larger than the coherence time of the photons then the overlap between between these basis states is arbitrarily close to zero (i.e. $\langle t_0|t_1\rangle = 0$).

Measurements on a a time-bin qubit are more challenging than on a polarization qubit. One could simply measure the arrival time of the photon but then one can only project onto $|t_0\rangle$ and $|t_1\rangle$ and thus there is nothing to continuously vary to generate visibility curves or violate the CHSH inequality. A better method is to pass each photon through another interferometer with the same path-length difference, and phase ϕ, as the pump interferometer in figure (3.4). The following equation details this action on a time-bin qubit (notationally, the time-bin inside the ket is the time-bin the photon belonged to after creation and the subscripted time-bin is the time-bin that the photon

exists in after leaving the measurement interferometer):

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi_p}|t_1\rangle) \\ \rightarrow\ & \frac{1}{2}(|t_0\rangle_{t0} + e^{i\phi}|t_0\rangle_{t1} + e^{i\phi_p}|t_1\rangle_{t1} + e^{i(\phi_p+\phi)}|t_1\rangle_{t2}) \\ & = \frac{1}{2}(|t_0\rangle_{t0} + (e^{i\phi}|t_0\rangle + e^{i\phi_p}|t_1\rangle)_{t1} + e^{i(\phi_p+\phi)}|t_1\rangle_{t2}) \end{aligned} \tag{3.14}$$

Each component of the time-bin state has a equal probability of traveling through each arm of the measurement interferometer. Thus, the photon exits the measurement interferometer in one of three time-bins. A detection in the first time-bin corresponds to a projection onto $|t_0\rangle$, with the photon having traveled through both interferometer's shorter arms, and a detection in the third time-bin corresponds to a projection onto $|t_1\rangle$, with the photon having traveled through both interferometer's longer arms. A detection in the middle time-bin corresponds to a projection onto $\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i(\phi_p-\phi)}|t_1\rangle)$ and interference between the paths long-short and short-long. This is a projection measurement onto the equator of the Bloch sphere in figure (3.1) and follows the mathematics developed in equations (3.6) through (3.8). Therefore, by scanning the phase of the measurement interferometers one can verify the presence of entanglement by generating visibility curves and violating the CHSH inequality, as described in section 3.1.1. It should be noted that as only the phase difference, $(\phi - \phi_p)$, appears in any measurement terms the phase of the pump interferometer can be taken as the reference phase. Thus, ϕ_p is set to zero for the remainder of document.

Other degrees of freedom of photons, including momentum or mode entanglement [80] and energy-time entanglement [81, 82, 83], have been used to create entanglement.

3.1.3 Hybrid Entanglement

As discussed in Chapter 1 polarization encoding at 810 nm is useful for free-space transmission while time-bin encoding at 1550 nm is useful for optical fibre transmission. How-

ever, to link free-space and fibre quantum channels a source of hybrid entanglement, an 810 nm polarization qubit entangled with a 1550 nm time-bin qubit, is required. The following details how to create hybrid entanglement when starting with time-bin entanglement.

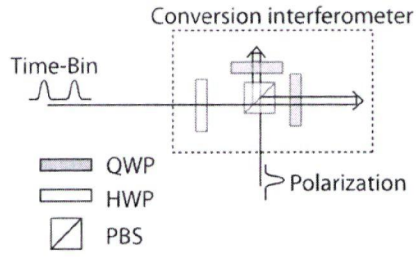

Figure 3.5: A time-bin to polarization conversion interferometer made from a folded Mach-Zehnder design

To convert a time-bin qubit to a polarization qubit one needs another interferometer. However, instead of beamsplitters this interferometer must be built with polarization beam splitters and be preceded by a HWP, as in figure (3.5). Each arm of the interferometer must also contain a QWP. The HWP is aligned such that each basis state of the qubit is split equally at the PBS, as both time-bin states have the same polarization. Specifically, horizontally polarized light traverses the long arm while vertically polarized light traverses the short arm. Thus, the horizontal component is delayed in time, and acquires a phase shift, with respect to the vertical component. The QWP in each arm is aligned such that the polarization of light in each arm is rotated 90° and all light is emitted out the same arm of the interferometer. As the input light was composed of two time-bin states and there are two paths in this conversion interferometer there are three possible time-bins for the output light, if the time difference imposed by the conversion interferometer is equal to the time difference of the input time-bins states. By post-selecting only the middle time-bin the net effect of the conversion interferometer is to

convert the time-bin qubit into a polarization qubit, as shown in the following equations.

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|H\rangle_{t0} + |H\rangle_{t1}) \\ \rightarrow\ & \frac{1}{2}(|V\rangle_{t0} + |H\rangle_{t0} + |V\rangle_{t1} + |H\rangle_{t1}) \\ \rightarrow\ & \frac{1}{2}(|V\rangle_{t0} + e^{-i\phi}|H\rangle_{t1} + |V\rangle_{t1} + e^{-i\phi}|H\rangle_{t2}) \\ \rightarrow\ & \frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi}|V\rangle) \end{aligned} \tag{3.15}$$

This new polarization qubit can then be analyzed using the polarization optics described in the previous section. In principle this conversion process can be made deterministic (i.e. without requiring post-selection) using optical switches.

Interestingly, there are two possible interpretations to this conversion interferometer. If the conversion interferometer is seen as part of the source of entangled photons (i.e. with Alice along with the source of photon pairs) then the source can be interpreted as producing hybrid entanglement. However, if the conversion interferometer is seen as part of the measurement (i.e. with Bob along with the polarization optics) then the source produces standard time-bin entanglement and one does not have hybrid entanglement. Instead, what one has is a generalized way to measure and analyzing time-bin entanglement. As described in the previous section, the standard time-bin interferometer allows only for projections onto the poles and the equator of the Bloch Sphere ($|t_0\rangle$, $|t_1\rangle$ and $\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi}|t_1\rangle)$, see figure (3.1)). This new type of interferometer, in combination with the polarization optics, allows for continuous measurements along any circle around the Bloch sphere - a feat never before achieved with time-bin qubits.

3.2 Experimental Setup

The experimental setup for the production of entanglement is shown in figure (3.6). This setup is similar to the setup of figure (2.4) in section 2.3 but contains the interferometers

required to produce and analyze entanglement. These differences are detailed in the following sections.

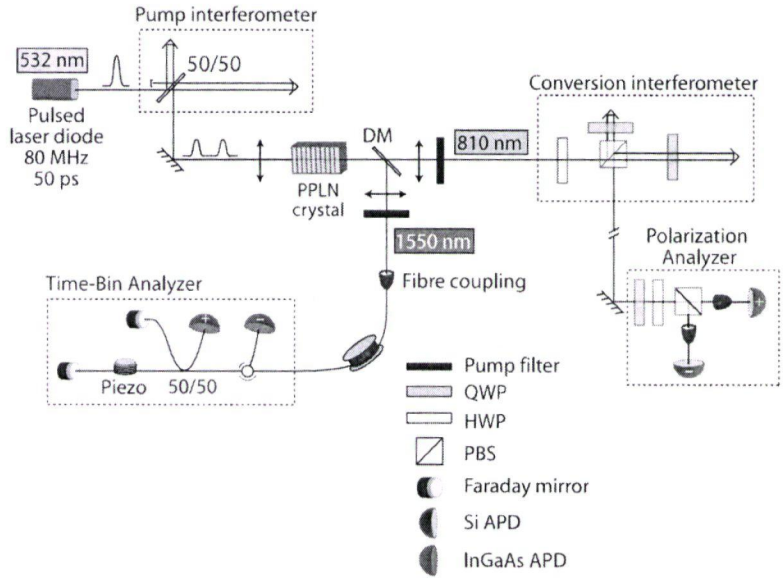

Figure 3.6: Experimental setup

3.2.1 Optical setup

The optical setup was the same as described in section 2.3.1 except for the addition of four interferometers used to create and analyze time-bin entanglement: one interferometer to create the time-bin state in the pump beam and three interferometers to analyze the time-bin qubits. For the 810 nm light we built an interferometer that converts the time-bin qubit to a polarization qubit instead of the standard time-bin analyzing interferometer. For the 1550 nm light we built both the standard analyzer and a conversion interferometer. These interferometers are hereafter referred to as the 810-conversion interferometer, the 1550 time-bin interferometer, the 1550-conversion interferometer and the pump interferometer respectively. Their design, construction and alignment are detailed in appendix B. After the output of the 810-conversion interferometer the 810 nm photons were sent through a QWP, HWP and PBS (Edmund Optics NT46-554, NT46-

555 and NT47-779). Each output of the PBS was coupled into SFM28 optical fibre and sent to a separate Si single photon detector. The 1550 nm photons were coupled into polarization maintaining fibre and then sent through either the 1550 time-bin interferometer or the 1550-conversion interferometer. The SMF28 output of the 1550-conversion interferometer was sent through a home-made fibre polarization controller and then through a fibre PBS (General Photonics PBS-001-P-03-SM-NC). The outputs of this PBS (or the two outputs of the 1550 time-bin interferometer) were sent to separate InGaAs single photon detectors.

3.2.2 Electronics setup

The electronic setup was the same as described in section 2.3.2 except for the following changes. Detection signals from the Si SPDs were combined in an OR gate and the result was combined in an AND gate with a clocking signal from the laser. This signal was used to trigger the InGaAs SPDs. The gate-out signals from the two InGaAs (see section 2.3.2) were combined in another AND gate and the result was used to start the TDC. This ensured that data was only collected when at least one Si SPD registered a detection at the expected time and both InGaAs detectors were not in the middle of deadtime. These improved electronics allowed us to trigger the pump laser at between 5 MHz and 10 MHz. Detections were considered valid only if they appeared within a 320 ps window as measured by the TDC. This reduction from 5 ns used in section 2.3.2 was necessary as our time-bins were separated by 1.44 ns. Statistics were again collected with in-house C++ and Labview software developed for these experiments.

3.3 Experimental Results

3.3.1 With Standard Time-Bin Interferometer

For the first set of measurements the 810 nm photons were sent through the 810-conversion interferometer and then the HWP, which was set at 22.5° (the QWP was removed), followed by separation at the PBS. A detection in a Si detector then corresponded to a projection onto the X-Y circle of the Bloch sphere (i.e. an equal superposition of two linear polarization states: $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi_{810}}|V\rangle)$ or, equivalently, between the two time-bin states: $\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi_{810}}|t_1\rangle)$ - see figure (3.1) for a description of the Z, X, Y notation to describe quantum states) with a phase given by the interferometer. A detection in the other Si detector corresponded to a detection of the orthogonal state. The 1550 nm photons were sent through the 1550 time-bin interferometer and thus a detection in an InGaAs detector also corresponded to a projection onto the X-Y circle (i.e. an equal superposition of the two time-bin states with a phase given by the interferometer: $\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi_{1550}}|t_1\rangle)$). This is the standard time-bin measurement as described in section 3.1.2. As our setup includes two detectors for each photon there are four visibility curves (i.e. one for each pair of detectors). An average entanglement visibility of $90.2 \pm 1.8\%$ was measured by scanning the phase of the 1550 time-bin interferometer, as seen in figure (3.7).

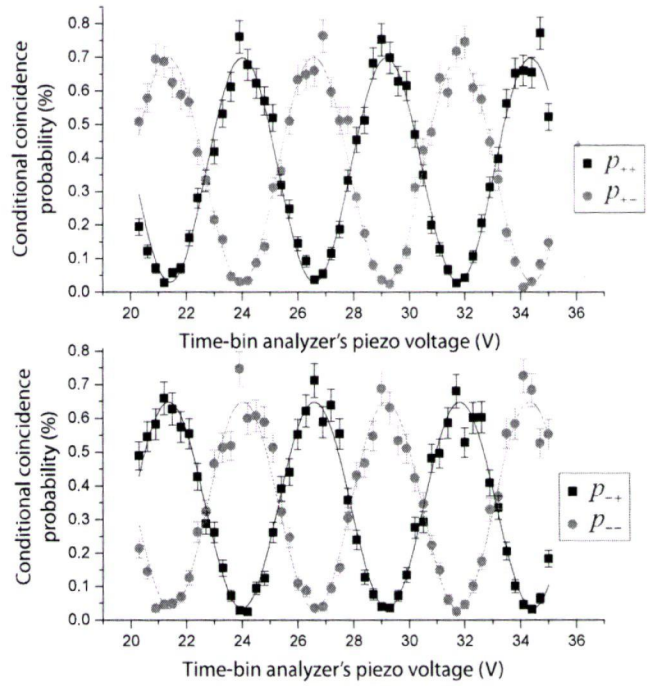

Figure 3.7: Entanglement visibility results using 810-conversion interferometer and 1550 time-bin interferometer, while scanning the phase of the latter. Experimental points are squares and vertical lines are one standard deviation uncertainty bounds. Curves show an average visibility of $90.2 \pm 1.8\%$.

For the second set of measurement results the CHSH version of Bell's inequality was violated. The 810 nm photons were sent through the 810-conversion interferometer and the 1550 nm photons were sent through the 1550 time-bin interferometer. The four settings used for the CHSH violation and the four correlation coefficients are presented below in table (3.1) and (3.2) (note that a HWP angle of θ rotates a state by 4θ on the Bloch sphere). These values give an S-parameter of $S = 2.61 \pm 0.14$, which is a clear violation of the inequality.

Table 3.1: Measurement settings for CHSH violation

810 nm HWP Settings	1550 nm Voltage Settings
$a = \phi = -\pi/16$	$c = \phi = 0$
$b = \phi = \pi/16$	$d = \phi = \pi/2$

Table 3.2: Results demonstrating CHSH violation

	a	b
c	-0.686 ± 0.035	-0.641 ± 0.035
d	0.657 ± 0.035	-0.628 ± 0.035

3.3.2 With Conversion Time-Bin Interferometer

The 810 nm photons were sent through the 810-conversion interferometer and the 1550 nm photons were now sent through the 1550-conversion interferometer. As discussed in section 3.1.3, the following visibility measurements can be thought of as analyzing time-bin qubits by projecting onto states on circles around the Bloch sphere not always accessible with the standard time-bin analyzing interferometer. Here, we use the Z,Y,X notation as described in figure (3.1). For circles 1 through 3 the 1550-conversion interferometer was set to project the 1550 nm photons onto $\pm X$ (i.e. equal superpositions of $|t_0\rangle$ and $|t_1\rangle$). For each curve, the QWP was set such that rotating the HWP projected the 810 nm photon onto states on one of three orthogonal circles on the Bloch sphere, as described in figures (3.8) through (3.10) and described more fully in appendix C. For circles 4 through 6 the 1550-conversion interferometer was set to project the 1550 nm photons onto $\pm Z$ (i.e. $|t_0\rangle$ and $|t_1\rangle$) and then measurements were taken with the same three QWP settings as before, as described in figures (3.11) through (3.13) and also described more fully in appendix C. These measurements were designed such that maximal visibility would be measured on circles 1, 2, 4 and 5 and zero visibility on circles 3 and 6. All results are summarized in table (3.3). Background counts were not subtracted.

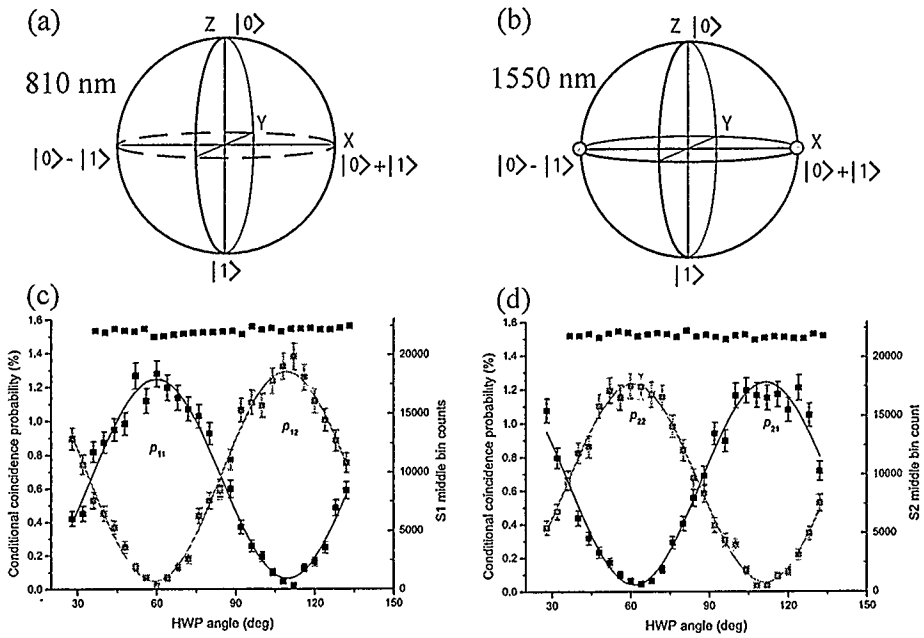

Figure 3.8: Entanglement visibility circle 1: (a) The projection of the 810 nm photons was rotated around the X-Y circle. (b) The 1550 nm photons were projected onto $\pm X$ (c),(d) Visibility curves showing an average visibility of $92.0 \pm 1.5\%$.

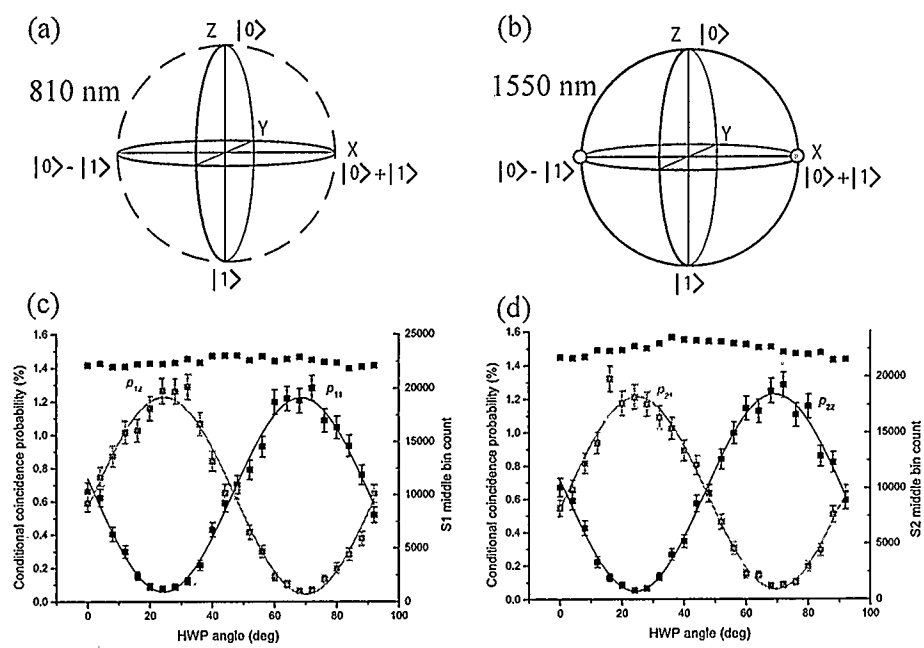

Figure 3.9: Entanglement visibility circle 2: (a) The projection of the 810 nm photons was rotated around the Z-X circle. (b) The 1550 nm photons were projected onto $\pm X$ (c),(d) Visibility curves showing an average visibility of $91.6 \pm 1.3\%$.

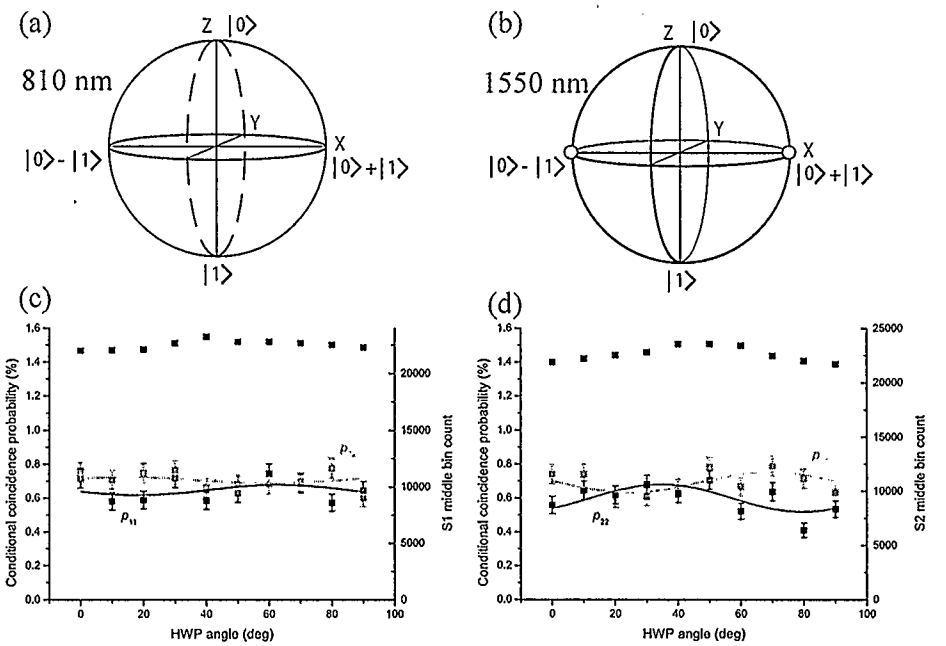

Figure 3.10: Entanglement visibility circle 3: (a) The projection of the 810 nm photons was rotated around the Z-Y circle. (b) The 1550 nm photons were projected onto $\pm X$ (c),(d) Visibility curves showing an average visibility of $7.4 \pm 4.2\%$.

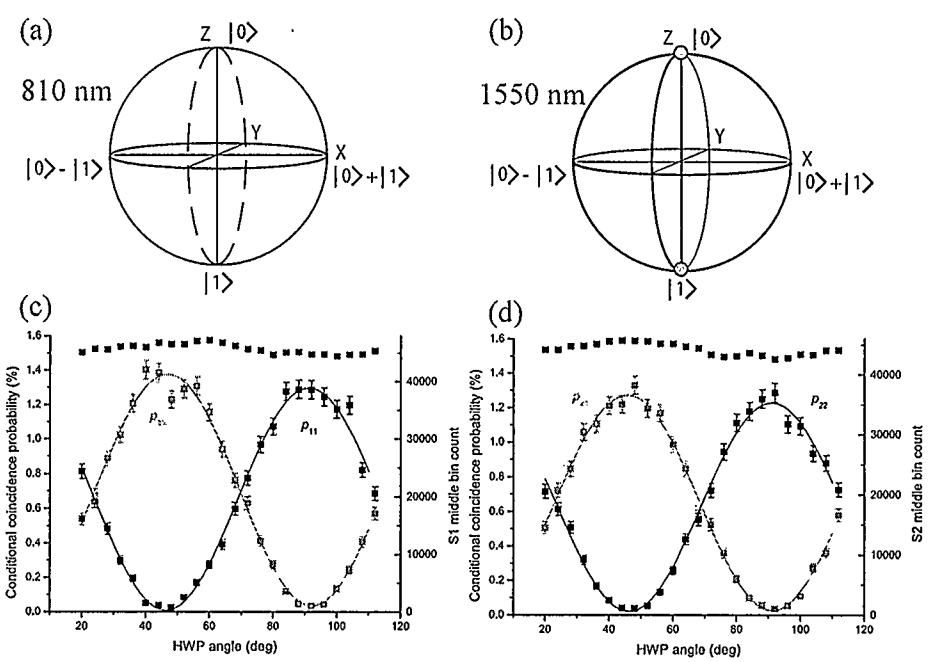

Figure 3.11: Entanglement visibility circle 4: (a) The projection of the 810 nm photons was rotated around the Z-Y circle. (b) The 1550 nm photons were projected onto $\pm Z$ (c),(d) Visibility curves showing an average visibility of $96.7 \pm 1.5\%$.

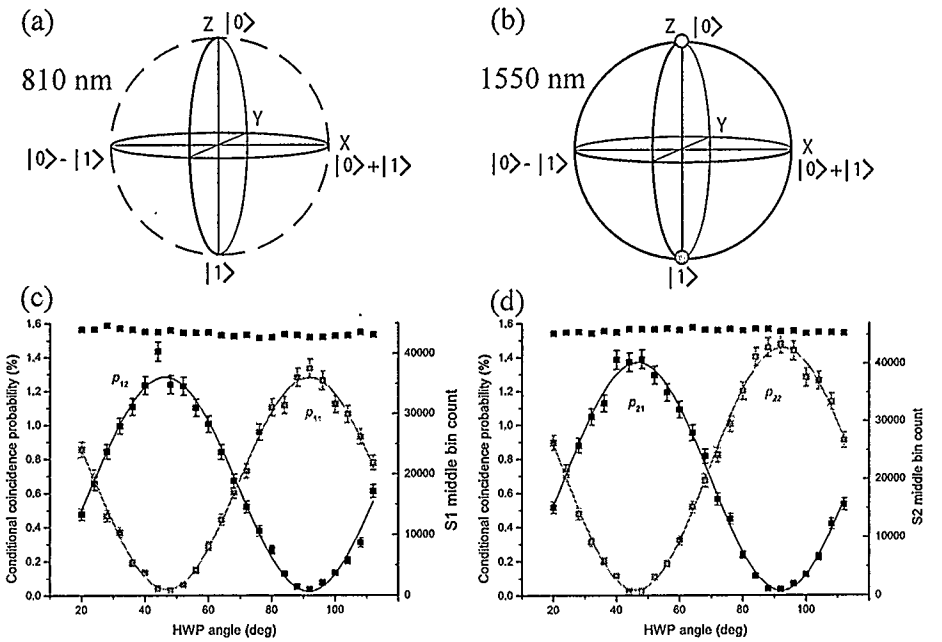

Figure 3.12: Entanglement visibility circle 5: (a) The projection of the 810 nm photons was rotated around the Z-X circle. (b) The 1550 nm photons were projected onto $\pm Z$. (c),(d) Visibility curves showing an average visibility of $95.6 \pm 1.9\%$.

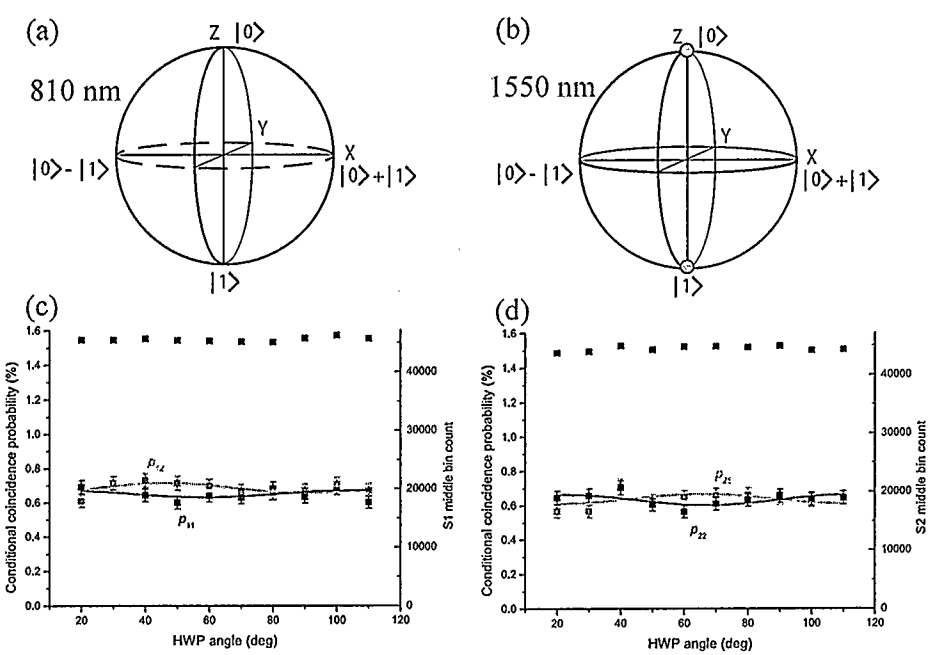

Figure 3.13: Entanglement visibility circle 6: (a) The projection of the 810 nm photons was rotated around the X-Y circle. (b) The 1550 nm photons were projected onto $\pm Z$ (c),(d) Visibility curves showing an average visibility of $4.1 \pm 2.6\%$.

Table 3.3: Visibility results summary

1550 nm projection	810 nm projection circle	Measured Visibility
$\pm X$ with 1550 time-bin interferometer	X-Y	$90.2 \pm 1.8\%$
$\pm X$ with 1550 conversion interferometer	X-Y	$92.5 \pm 1.5\%$
	Z-X	$91.6 \pm 1.3\%$
	Z-Y	$7.4 \pm 4.2\%$
$\pm Z$ with 1550 conversion interferometer	Z-Y	$96.7 \pm 1.5\%$
	Z-X	$95.6 \pm 1.9\%$
	X-Y	$4.1 \pm 2.6\%$

3.4 Discussion

The high visibility measurements, $91.6\% \pm 1.3\% \leq V \leq 96.7\% \pm 2.3\%$, and the violation of the CHSH form of Bell's inequality, $S = 2.61 \pm 0.14$ verify that our source does indeed produce hybrid entangled photons. These measurements make this the first source of hybrid entanglement needed to allow quantum repeaters to link free-space and optical fibre quantum communication channels. Although, further development (i.e. spectral filtering) is needed before teleportation experiments, required for quantum repeaters themselves, can be performed, albeit in the lab. Nevertheless, these results indicate that this source can be readily used in a number of quantum communication tasks. In particular, it is well suited for QKD, which requires that $V > 78\%$ (or $S > 2.21$) to guarantee security against coherent attacks [2].

Furthermore, when considering the conversion interferometers as part of the analysis (instead of part of the state preparation) these results demonstrate, for the first time, the ability to project a time-bin qubit anywhere on the Bloch sphere instead of just the poles

and equator, as in the standard time-bin analyzer. This added versatility makes this source well suited for quantum communication tasks that require projections onto non-orthogonal bases, such as quantum coin flipping. This new versatility in measurements of time-bin qubits, along with the high quality of this novel form of entanglement, makes these results particularly consequential for the field of quantum communication.

Chapter 4

Quantum Coin Flipping

4.1 Background

Coin flipping is a communication task that can be performed better in the quantum mechanical world. As discussed earlier, the task is for Alice and Bob to select a random bit (i.e. a coin flip), but it is beneficial for one or both parties to choose the bit rather than allow random chance to decide. If Alice and Bob are at the same place the task is straightforward. One of them can simply flip a coin and then both can see the result. However, if Alice and Bob are separated by some large distance, and neither trusts the other and they cannot agree on a third-party to flip the coin, it is unreasonable to let one player flip the coin. That player could simple declare himself or herself the winner while the other must trust the result. They are at a stalemate.

In principle, one solution is to have both players send the other a random bit (A and B) simultaneously and let the coin flip result be equal to $A \oplus B$. Unfortunately, protocols based on this idea, known as relativistic protocols [84], are extremely difficult to implement as their security is based on the simultaneity of the classical transmission and thus the physical distance between the players. If one player can lie about his or her location the protocol breaks down. A protocol where one player can cheat such that he or she always wins is described as completely broken. The only option at this point is to break the symmetry of the protocol and expect the first player to communicate information before the second. In this case, it turns out that there does not exist a classical coin flipping protocol that is not completely broken. The second player can always use the information sent by the first to his or her advantage and win the game.

Surprisingly, coin flipping performed via the exchange of quantum states, along with classical information, can perform better than coin tossing with classical information alone. This is usually assessed by determining the maximum winning probability one player can achieve for any possible cheating strategy. The first attempt at a quantum coin flipping protocol was presented 1984 by C. H. Bennett and G. Brassard [12], at the same time as QKD, although it turned out to be completely broken. In 1998 and 1999 two teams proved that a perfect quantum coin tossing protocol, that is a protocol with a maximum winning probability of 50%, could not exist [16, 17]. In 2000 D. Aharnov, A. Ta-Shma, U. Vazirani and A. C.-C. Yao [18] developed the ATVY protocol, which was the first quantum coin tossing protocol with a maximum winning probability under 100%. It surpassed the flaws of the original BB84 protocol and achieved a maximum winning probability of 92% for any cheating strategy Alice or Bob could employ. Later, in 2004, A. Kitaev proved that that best possible quantum coin tossing protocol could have a maximum winning probability of $\frac{1}{\sqrt{2}} \approx 70.7\%$ [19] and A. Ambainis proposed a new protocol with a maximum winning probability of 75% [85]. Unfortunately, these protocols have one practical vulnerability: they would be completely broken in any implementation that involves losses. It is possible for one player to exploit the communication asymmetry and the unavoidable losses in a quantum channel to ensure victory.

The above protocols, which are based on the idea of bit commitment, proceed as follows. Alice encodes her bit, A, in a quantum state and sends it to Bob. Alice is now committed to A even though Bob cannot measure the state to conclusively determine A because he does not know in which basis Alice encoded her bit. Bob then sends B, a classical bit, to Alice and finally, Alice reveals A, as well as how she encoded it into her quantum state so that Bob can verify that Alice is being honest. The coin flip itself is $A \oplus B$. While this base structure works in theory, any implementation needs to address what should happen if there are losses in the quantum channel i.e. Bob does not receive

the qubit. If the protocol is allowed to continue (see [18]) then Alice's best strategy to win is straightforward. She simple doesn't send a qubit and then she exploits the communication asymmetry by waiting until she knows B to pick an A such that she will win. Bob will have no way to verify that Alice is cheating and thus, she'll win 100% of the time. On the other hand, if the protocol is allowed to restart then Bob has the advantage. There may exist an Unambiguous State Discrimination (USD) measurement [86], which is a measurement that has a probability to conclusively identify between two states. If such a measurement is possible (see [85]) Bob can repeatedly tell Alice that he did not receive a photon until his USD conclusively tells him what state Alice sent. At which point he picks B such that he will win and thus he can win 100% of the time.

Not only are these protocols completely broken but, as explained in the following section, they are also un-fair. There is an asymmetry in the results of each protocol as the maximum winning probability for one player is higher than the maximum winning probability for the other.

Although the asymmetry in the classical communication means that perfect coin flipping is impossible (both classical and quantum mechanically) quantum protocols that are not completely broken exist. However, they must be designed such that one cannot exploit the communication asymmetry and implementation imperfections such as losses to guarantee victory. As well, an ideal protocol should be fair.

4.2 A Fair, Loss Tolerant Protocol

The following protocol, developed by G. Berlin, G. Brassard, F. Bussières and N. Godbout in 2008 [20] and referred to as the BBBG protocol hereafter, was the first proposed fair loss-tolerant protocol.

Alice and Bob agree on the following two sets of basis states (here, $|\psi_{(X,A)}\rangle$ indicates

basis X and bit value A):

$$\begin{aligned} |\psi_{(0,0)}\rangle &= |0\rangle \\ |\psi_{(0,1)}\rangle &= |1\rangle \\ |\psi_{(1,0)}\rangle &= |\phi+\rangle \\ |\psi_{(1,1)}\rangle &= |\phi-\rangle \end{aligned} \tag{4.1}$$

where,

$$\begin{aligned} |\phi+\rangle &= \cos(\phi)|0\rangle + \sin(\phi)|1\rangle \\ |\phi+\rangle &= \sin(\phi)|0\rangle - \cos(\phi)|1\rangle \end{aligned} \tag{4.2}$$

Then the protocol proceeds as follows:

1. Alice prepares a qubit in a randomly chosen state $|\psi_{X,A}\rangle$ and sends it to Bob.
2. Bob measures the received qubit in a randomly chosen basis, $\hat{X}$, and calls the result $\hat{x}$. If he does not detect a photon Alice and Bob restart the protocol.
3. Bob sends a randomly chosen classical bit, B, to Alice.
4. Alice reveals her original X and A to Bob.
5. If $X = \hat{X}$ but $A \neq \hat{x}$ the protocol is aborted. Either an error occurred or Alice lied to Bob. If $X \neq \hat{X}$ Bob has no way to verify A and the protocol continues.
6. The coin flip is $A \oplus B$

Regardlessly of the value of ϕ, if both players play the protocol honestly then the probability for each to win is 50%, as both are picking a random bit value that contributes to the outcome of the coin toss. If one of the players decides to cheat then the game is different. As explained in more detail below, the protocol cannot be completely broken by exploiting losses. Bob is allowed to declare that he did not receive a qubit and restart

the protocol, as opposed to the ATVY protocol [18], and there does not exist a USD measurement that Bob can employ to conclusively determine A, as opposed to [85]. Thus the protocol is loss-tolerant.

If Bob plans to cheat he needs to be able to determine A from one measurement of the quantum state Alice sent. This amounts to being able to distinguish between the density matrix for $A = 0$ and the density matrix for $A = 1$.

$$\begin{aligned}
\rho_0 &= \frac{1}{2}|\psi_{(0,0)}\rangle\langle\psi_{(0,0)}| + \frac{1}{2}|\psi_{(1,0)}\rangle\langle\psi_{(1,0)}| \\
&= \frac{1}{2}\begin{pmatrix} 1+\cos^2(\phi) & \cos(\phi)\sin(\phi) \\ \cos(\phi)\sin(\phi) & \sin^2(\phi) \end{pmatrix} \\
\rho_1 &= \frac{1}{2}|\psi_{(0,1)}\rangle\langle\psi_{(0,1)}| + \frac{1}{2}|\psi_{(1,1)}\rangle\langle\psi_{(1,1)}| \\
&= \frac{1}{2}\begin{pmatrix} \sin^2(\phi) & -\cos(\phi)\sin(\phi) \\ -\cos(\phi)\sin(\phi) & 1+\cos^2(\phi) \end{pmatrix}
\end{aligned} \tag{4.3}$$

Unfortunately for Bob, there does not exist a USD measurement to distinguish between these two density matrices. Thus, Bob can not gain from asking Alice to re-send her qubit. His best strategy is to perform a Helstrom measurement [87], which is a measurement designed to output A with minimum error. Here, the Helstrom measurement corresponds to measuring one of the basis vectors exactly half-way between $|\psi_{(0,0)}\rangle$ and $|\phi+\rangle$ (or $|\psi_{(0,1)}\rangle$ and $|\phi-\rangle$:

$$\begin{aligned}
|\mathcal{B}\rangle &= \cos(\phi/2)|0\rangle + \sin(\phi/2)|1\rangle \\
|\mathcal{B}^{\perp}\rangle &= \sin(\phi/2)|0\rangle - \cos(\phi/2)|1\rangle
\end{aligned} \tag{4.4}$$

This measurement correctly distinguishes between the two density matrices with the following probability [87]:

$$\frac{1}{2} + \frac{1}{4}\mathrm{Tr}|\rho_0 - \rho_1| = \frac{1}{2} + \frac{1}{2}\cos(\phi) \tag{4.5}$$

Bob can then pick a properly chosen 'random' bit for step three of the protocol and win with the same probability. With the remaining probability Bob loses the coin toss. Note

that after Alice declares her bit Bob can either accept the loss or declare that Alice is the cheater. In either case though, Bob loses his ability to confidently detect if Alice is cheating, as in step five of the protocol.

For Alice to cheat, she must send some quantum state to Bob before learning Bob's bit B. For Alice's optimal cheating strategy she must send some quantum state such that after she learns Bob's bit B, she can declare to Bob that she sent one of the four states in equation (4.1) that maximizes her probability to win. This problem turns out to be closely related to the bit commitment problem mentioned in Chapter 1 [22]. The optimal cheating strategy is to randomly send one of the following two states:

$$\begin{aligned} |\mathcal{A}\rangle &= \cos(-\phi/2)|0\rangle + \sin(-\phi/2)|1\rangle \\ |\mathcal{A}^{\perp}\rangle &= \sin(-\phi/2)|0\rangle - \cos(-\phi/2)|1\rangle \end{aligned} \tag{4.6}$$

Accounting for the 50% of coin flips where Bob cannot verify what Alice sent, he will believe Alice with the following probability:

$$\frac{1}{2} + \frac{1}{4}(1 + \mathrm{F}(\rho_0\rho_1)) = \frac{3 + \sin(\phi)}{4} \tag{4.7}$$

In the cases where Bob's measurement does not agree he will declare that Alice has lied to him and tried to cheat and he will abort the protocol.

Finally, if both players cheat the game will likely end in an abort. As Alice is cheating, she will always declare an A value, in step 4 of the protocol after she learns B, such that she wins the toss. As Bob is cheating, and likely refuses to lose, he will declare Alice a cheater regardless of his own measurement. Thus, the protocol will end in an abort.

As for the value of ϕ, it seems natural to choose $\phi = \frac{\pi}{4}$ as this gives four symmetrically distributed states around the Bloch sphere that are often used in other quantum communication tasks such as QKD. A graphical representation of all the states discussed here are presented in figure (4.1).

$$\begin{aligned} |\psi_{(0,0)}\rangle &= |0\rangle \\ |\psi_{(0,1)}\rangle &= |1\rangle \\ |\phi+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\phi+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{4.8}$$

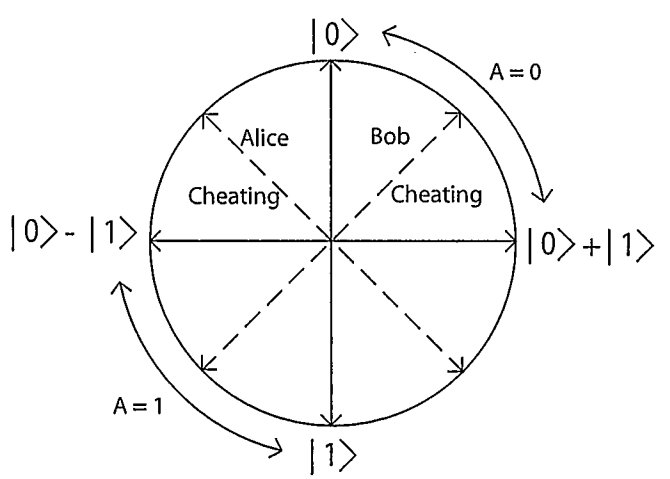

Figure 4.1: BB84 Quantum Coin Flipping States: On this slice of the Bloch sphere, Alice prepares one of the four states diagramed with solid lines (both states in the top right corner correspond to a bit value of $A = 0$ while bottom left corner corresponds to bit value of $A = 1$). The optimal cheating states for Alice and optimal cheating projection measurements for Bob are indicated by dashed lines.

The above cheating analysis applied to these states yields the following results presented in table (4.1).

Table 4.1: The maximum winning probability and abort probability for the BBBG coin tossing protocol when $\phi = \pi/4$

	Alice Wins	Bob Wins	Bob Aborts
No Cheater	50%	50%	0%
Alice Cheats	92.7%	0%	7.3%
Bob Cheats	14.6%	85.4%	0%

If one intends to cheat there is clearly an advantage to play as Alice. However, one can make the protocol fair by finding a set of 'fair-cheating' states that ensures that the maximum winning probability for each player is equal. By equating equation (4.5) to (4.7) and solving for ϕ, one finds:

$$\begin{aligned} &\frac{1}{2} + \frac{1}{2}\cos(\phi) = \frac{3 + \sin(\phi)}{4} \\ &\rightarrow \phi = 36.8^\circ \end{aligned} \tag{4.9}$$

By using these specific non-symmetrically distributed states the protocol becomes symmetric in the maximum winning probability. A graphical representation of these states is presented in figure (4.2) and the cheating analysis applied to these states is presented below. Note that in the case where Bob is cheating, if Alice is about to win, Bob may refuse to lose the coin toss and declare that Alice is cheating and abort the protocol. The 10% in the 'Bob Cheats' row of table (4.2) could be moved to the abort column depending on how Bob chooses to play the game (i.e. if he absolutely refuses to lose).

Table 4.2: The maximum winning probability and abort probability for the BBBG coin tossing protocol with fair cheating: $\phi = 36.8^\circ$

	Alice Wins	Bob Wins	Bob Aborts
No Cheater	50%	50%	0%
Alice Cheats	90.0%	0%	10.0%
Bob Cheats	10.0%	90.0%	0%

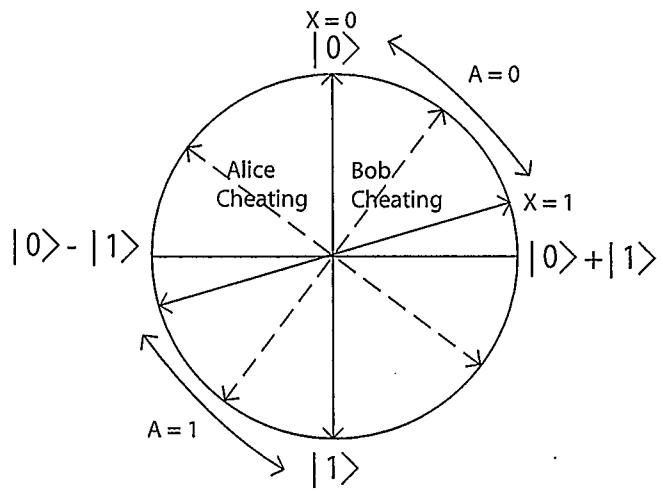

Figure 4.2: Fair Quantum Coin Flipping States: On this slice of the Bloch sphere, Alice prepares one of the four states diagramed with solid lines (Both states in the top right corner correspond to a bit value of $A = 0$ while bottom left corner corresponds to bit value of $A = 1$). The optimal cheating states for Alice and optimal cheating projection measurement for Bob are indicated by dashed lines.

4.3 Experimental Setup

For practical reasons Alice requires a source of entanglement or a perfect single photon source. If Alice's source sometimes accidentally prepares multiple qubits with the same value of X and A (as is the case with laser pulses attenuated to the single photon level and photon pair implementations based on HSPSs) Bob could tell Alice that he did not receive anything until he receives many qubits at once. Then he could measure each qubit and compile the results to determine A with high confidence. On the other hand, if a source produces a pair of entangled qubits, then projecting one qubit at Alice's side prepares a state on the second qubit being sent to Bob. As the projection of each qubit is random, should the source produce multiple entangled pairs then Alice's projection of one qubit from each pair will not encode the same A on all the qubits she sends to Bob. If either player detects multiple photons they need to restart the protocol immediately as detections will no longer be correlated.

Another benefit of using a source of entanglement is that it allows for random selections of X, A and $\hat{X}$ (Alice's basis, Alice's bit and Bob's basis respectively). With our hybrid entanglement setup described in section 3.2 the random arrival time of the photon at the detector allows for random state selection, as required by step one of the protocol: the first and third arrival time corresponds to projections onto $|t_0\rangle$ and $|t_1\rangle$ respectively (basis $X = 0$) and the second arrival time corresponds to projections onto a superposition of the two time-bin states ($X = 1$). With the standard time-bin analyzer only the un-fair BB84 states, see equation (4.8), can be implemented in this fashion as only equal superpositions are accessible in the middle arrival time. With our novel interferometers any projection is possible and thus it is possible to implement the BBBG protocol with both the fair and un-fair states, as well as the optimal cheating strategies, with random basis selection.

For these experiments, Alice is considered to be the source of entanglement along with the 810-conversion interferometer and associated polarization optics and detectors. The projection of her photon prepares the identical state onto the photon being sent to Bob. Bob possesses the 1550-conversion interferometer and detectors. Data were collected as in section 3.2.2 and analyzed using in-house developed software. A single computer played the roles of both Alice and Bob.

4.4 Results

Before beginning coin tossing Alice and Bob must verify that they share entanglement and must establish a phase reference. This was done by measuring a entire visibility curve, by scanning the phase of the 810-conversion interferometer, and then adjusting the phase to a maximum in the coincidence detection probability.

As explained earlier, changing the measurement bases of the middle arrival time is

straightforward: Alice can adjust the HWP after the 810-conversion interferometer while Bob can adjust the fibre polarization controller after the 1550-conversion interferometer.

First, the game was played with the BB84 states, as described in equation (4.8), first with no-cheater and then with Alice cheating and finally with Bob cheating. Alice and Bob used the optimal cheating strategies as described above. Second, coin flipping was repeated with the fair-cheating basis states. The results are presented below in table (4.3) and match very well with theoretical predictions.

Table 4.3: BBBG coin tossing results. The first column and second column correspond to the BB84 and Fair states respectively. Over 40,000 coin flips were collected for each setting so that the statistical error on each experimental point is under 0.2%

Cheater		BB84 Alice Wins	Basis Bob Wins	States Abort	Fair Alice Wins	Basis Bob Wins	States Abort
None	Theory	50.0%	50.0%	0%	50.0%	50.0%	0%
	Experimental	49.1%	49.3%	1.6%	49.0%	49.0%	2.0%
Alice	Theory	92.7%	0%	7.3%	90.0%	0%	10.0%
	Experimental	91.1%	0%	8.9%	86.5%	0%	13.5%
Bob	Theory	14.6%	85.4%	0%	10.0%	90.0%	0%
	Experimental	17.8%	82.2%	0%	13.3%	86.7%	0%

4.5 Discussion

We present the first demonstration of the BBBG quantum coin flipping protocol. All experimental values agree very well with theoretical predictions. In particular, the results in table (4.3) clearly demonstrate the difference between using the BB84 basis states and the fair-cheating basis states: There is a statistically significant increase (decrease) in Bob's (Alice's) maximum probability to win when using the fair cheating basis states. Also, in the fair basis the maximum probability to win for each player is equal to within error.

All winning probabilities are slightly lower than theoretical values because of detector noise, imperfect entanglement visibility and imperfect phase alignment. These errors open up an avenue of attack for Bob. Whenever Alice would win, a cheating Bob could abort the protocol by declaring that he measured a different result than what Alice declared. If errors are present in an implementation then Bob can always claim an error occurred, whether or not Alice actually cheated, until he wins the coin flip. Unfortunately, to date, there is no protocol that is tolerant to errors. In our experiments, these errors decrease the winning probability (increase in abort probability) by between 1.6% and 3.5%.

These results successfully demonstrate the first loss-tolerant quantum coin flipping protocol. On top of this, it is a demonstration that would not be possible without the hybrid entanglement and novel analyzing interferometers developed here. Overall, it is clear evidence that in some cases communication tasks can be performed better with quantum mechanics.

Chapter 5

Summary and Outlook

Quantum communication can, in certain cases, provide improvements over the best capabilities of classical communication. In particular, QKD for communication security and quantum coin flipping for distant bit agreement between two adversarial parties both, in theory, provide improvements over their classical counterparts.

At the heart of all developing technologies for quantum communication are sources of entangled photon pairs. These highly non-classical sources exhibit the weirdness of the quantum world by showing stronger statistical correlations than anything in the classical (i.e. local realistic) world while at the same time being resistant to perfect copying or cloning. And it is these very properties that make them required not just for the specific gains that quantum communication protocols offer but also for the construction of future quantum networks complete with quantum repeaters based on quantum teleportation.

This thesis demonstrates several new photon pair technologies of interest to the field of quantum communication. First, a source of photon pairs was constructed and then characterized using a novel theoretical model based on statistical matrices. We demonstrated the ability to characterize the brightness, or mean number of photon pairs emitted per laser pulse, from our source considerably faster than previous methods. As a verification, the model was used to predict measured detection probabilities and statistical correlations over a wide range of brightness. The ability to assess the brightness quickly has tremendous importance to quantum communication where QKD security and quantum repeater success rate depends crucially on the brightness.

Second, using our photon pair source we developed the first source of hybrid entanglement between two photons: one photon was suitable for transmission through optical

fibre channels and one photon was suitable for transmission through free-space channels. Such sources of entanglement are required for quantum repeaters to link together fibre and free-space quantum networks into one coherent network. This source of entanglement was verified through standard time-bin visibility curves and a CHSH violation as well as through the use of novel analyzers with the ability to access the entire Bloch sphere. We demonstrated entanglement visibility curves around Bloch sphere circles never before accessed with time-bin entanglement.

Finally, as an application for these novel photon pair technologies we successfully implemented a quantum coin flipping protocol that requires entanglement to prevent completely successful cheating. We implemented the situation where both parties played fair as well as each parties used optimal cheating strategy. The latter was only possible with our novel interferometer design. All results agreed very well with theoretical predictions.

This table top quantum coin tossing experiment is only the first quantum communication task that can be implemented with this new entanglement source and novel technologies. As further experimental control is developed full quantum state tomography (i.e. the reconstruction of the full density matrix associated with the state of the phonts [88]), which has never been done with time-bin qubits, could be performed on this source. Long-distance quantum coin flipping along with long-distance QKD, entanglement visibility measurements, CHSH violations and more will all be possible with further developments using an installed optical fibre link between our QC2 labs at the University of Calgary and lab space at the Southern Alberta Institute for Technology (SAIT). Further into the future, even longer distance experiments could be performed with this entanglement source between three locations, with one connected via free-space and one connected via optical fibre.

Moreover, with work on spectral filtering it will be possible to begin quantum tele-

portation experiments as required for future quantum repeater experiments. These could be the first quantum repeater experiments linking together different media into a single quantum network.

With the experiments performed here, several new photon pair technologies for quantum communication have demonstrated their usefulness for the field of quantum communication in general. The world of quantum mechanics may be a strange one, but it is destined to become an ever increasing part of our communication infrastructure.

Bibliography

[1] www.wikipedia.org.

[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. *Rev. Mod. Phys.* **74**, 145 (2002).

[3] S. Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography.* Fourth Estate, New York NY, (1999).

[4] M. Blum. *Advances in Cryptology: A Report on CRYPTO'81* **74**, 11 (1981).

[5] C. Cohen-Tannoudji, B. Diu, F. Laloë. *Quantum Mechanics: Volume One.* Hermann, USA, (1977).

[6] B. H. Bransden, C. J. Joachain. *Quantum Mechanics: Second Edition.* Pearson Education Limited, Edinburgh Gate UK, (2000).

[7] M. Nielsen, I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge, Cambridge UK, (2000).

[8] A. Einstein, B. Podolsky, N. Rosen. *Phys. Rev.* **47**, 777 (1935).

[9] J. S. Bell. *Physics* **1**, 195 (1964).

[10] W. K. Wootters, W. H. Zurek. *Nature* **299**, 802 (1982).

[11] A. K. Ekert. *Phys. Rev. Lett.* **67**, 661 (1991).

[12] C. H. Bennett, G. Brassard. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* , 175 (1984).

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

[14] D. Pearson. *Quantum Communication, Measurement and Computing. AIP Conference Proceedings* **734**, 299 (2004).

[15] C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer. *IEEE Transactions on Information Theory* **41**, 6 (1995).

[16] H.-K. Lo, H. F. Chau. *Physica D* **120**, 177 (1998).

[17] D. Mayers, L. Salvail, Y. Chiba-Kohno. *arXiv:quant-ph/9904078v1* .

[18] D. Aharonov, A. Ta-Shma, U. Vazirani, A.C.-C. Yao. *Proceedings of* 32nd *Annual ACM Symposium on Theory of Computing* , 705 (2000).

[19] A. Kitaev. *Lecture delivered at QIP 2003, MSRI, Berkeley, CA (unpublished)* .

[20] G. Berlin, G. Brassard, F. Bussières, N. Godbout. *Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM08)* , Sainte Luce, Martinique (2008).

[21] P. W. Shor. *Proceedings of the* 35th *Annual Symposium on Foundations of Computer Science* (1994).

[22] R. Spekkens, T. Rudolph. *Phys. Rev. A* **65**, 012310 (2002).

[23] L. K. Grover. *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (1996).

[24] W. Tittel, G. Weihs. *Quantum Information and Computation* **1**, 3 (2001).

[25] J. Brendel, N. Gisin, W. Tittel, H. Zbinden. *Phys. Rev. Lett.* **82**, 2594 (1999).

[26] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden. *New J. Phys.* **4**, 41 (2002).

[27] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, Y. Yamamoto. *New J. Phys.* **7**, 232 (2005).

[28] www.idQuantique.com.

[29] G. P. Agrawal. *Fiber-Optic Communication Systems.* John Wiley & Sons, New York NY, (1997).

[30] J. G. Rarity, P. M. Gorman, P. R. Tapster. *J. Mod. Opt.* **48**, 1887 (2001).

[31] R. J. Hughes, J. E. Nordholt, D. Derkacs, C. G. Peterson. *New J. Phys.* **4**, 43 (2002).

[32] R. Ursin, F. Tiefenbacher, T. Shmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trokek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger. *Nature Physics* **3**, 481 (2007).

[33] C. Erven, C. Couteau, R. Laflamme, G. Weihs. *Opt. Exp.* **16**, 16840 (2008).

[34] R. Hughes, W. Buttler, P. Kwiat, S. Lamoreaux, G. Morgan, J. Nordhold, G. Peterson. *J. Mod. Opt.* **47**, 549562 (2000).

[35] W. Tittel, M. Afzelius, R. L. Cone, T. Chanelire, S. Kröll, S. A. Moiseev, M. Sellars. *arXiv:quant-ph/0810.0172v1* (2008).

[36] K. Hammerer, A. S. Sorensen, E. S. Polzik. *arXiv:quant-ph/0807.3358v2* (2008).

[37] M. Fleischhauer, A. Imamoglu, J. P. Marangos. *Rev. Mod. Phys.* **77**, 633 (2005).

[38] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters. *Phys. Rev. Lett.* **70**, 1895 (1993).

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

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

[41] R. Munroe. *http://xkcd.com* **433** (2008).

[42] S. J. Freedman, J. F. Clauser. *Phys. Rev. Lett.* **28**, 938 (1972).

[43] A. Aspect, P. Grangier, G. Roger. *Phys. Rev. Lett.* **47**, 460 (1981).

[44] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, Y. Shih. *Phys. Rev. Lett.* **75**, 4337 (1995).

[45] D. C. Burnham, D. L. Weinberg. *Phys. Rev. Lett.* **25**, 84 (1970).

[46] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, P. H. Eberhard. *Phys. Rev. A* **60**, R773 (1999).

[47] K. Sanaka, K. Kawahara, T. Kuga. *Phys. Rev. Lett.* **86**, 5620 (2001).

[48] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, N. Gisin. *Eur. Phys. J. D* **18**, 155 (2002).

[49] R. W. Boyd. *Nonlinear Optics, Second Edition.* Academic Press, San Diego CA, (2002).

[50] M. Fiorentino, P. L. Voss, J. E. Sharping, P. Kumar. *IEEE Photon. Technol. Lett.* **14**, 983 (2002).

[51] X. Li, P. L. Voss, J. E. Sharping, P. Kumar. *Phys. Rev. Lett.* **94**, 53201 (2005).

[52] J. Rarity, J. Fulconis, J. Duligall, W. Wadsworth, P. Russell. *Opt. Exp.* **13**, 534 (2005).

[53] O. Alibart, J. Fulconis, G. K. L. Wong, S. G. Murdoch, W. J. Wadsworth, J. G. Rarity. *New J. Phys.* **8**, 67 (2006).

[54] T. Chanelière, D. N. Matsukevich, S. D. Jenkins, T. A. B. Kennedy, M. S. Chapman, A. Kuzmich. *Phys. Rev. Lett.* **96**, 93604 (2006).

[55] C. C. Gerry, P. L. Knight. *Introductory Quantum Optics.* Cambridge University Press, Cambridge UK, (2005).

[56] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, H. Zbinden. *New J. Phys.* **6**, 163 (2004).

[57] R. Hanbury Brown, R. Q. Twiss. *Nature* **178**, 1046 (1956).

[58] E. Waks, C. Santori, Y. Yamamoto. *Phys. Rev. A* **66**, 042315 (2002).

[59] Q. W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, A. Karlsson. *Phys. Rev. Lett.* **100**, 090501 (2008).

[60] Y. Adachi, T. Yamamoto, M. Koashi, N. Imoto. *Phys. Rev. Lett.* **99**, 0180503 (2007).

[61] W. Mauerer, C. Silberhorn. *Phys. Rev. A* **75**, 050305(R) (2007).

[62] X. Ma, C.-H. Fred Fung, H.-K. Lo. *Phys. Rev. A* **76**, 012307 (2007).

[63] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, N. Gisin. *Phys. Rev. A* **67**, 022301 (2003).

[64] H. C. Lim, A. Yoshizawa, H. Tsuchida, K. Kikuchi. *Opt. Exp.* **16**, 14512 (2008).

[65] S. Takeuchi, R. Okamoto, K. Sasaki. *Applied Optics* **43**, 5708 (2004).

[66] R. Okamoto, S. Takeuchi, K. Sasaki. *J. Opt. Soc. Am. B* **22**, 2393 (2005).

[67] M. Tengner, D. Ljunggren. *arXiv:quant-ph/0706.2985v1* (2007).

[68] L. Mandel, E. Wolf. *Optical coherence and quantum optics.* Cambridge University Press, Cambridge UK.

[69] J. Simon, H. Tanji, J. K. Thompson, V. Vuletic. *Phys. Rev. Lett.* **98**, 183601 (2007).

[70] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, N. Gisin. *Phys. Rev. A* **66**, 062308 (2002).

[71] F. Bussières, J. Slater, N. Godbout, W. Tittel. *Opt. Exp.* **16**, 17060 (2008).

[72] H. de Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, N. Gisin. *J. Mod. Opt.* **98**, 183601 (2007).

[73] D. H. Jundt. *Optics Letters* **22**, 1553 (1997).

[74] A. Rubenok, W. Tittel. *Manuscript of final research project, University of Calgary* (2007).

[75] T. Stuart, F. Bussières, J. A. Slater, W. Tittel. *Manuscript of final research project, University of Calgary* (2008).

[76] A. Peres. *Phys. Rev. Lett.* **77**, 1413 (1996).

[77] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt. *Phys. Rev. Lett.* **23**, 880 (1969).

[78] C. E. Kuklewicz, M. Fiorentino, G. Messin, F. N. C. Wong, J. H. Shapiro. *Phys. Rev. A* **69**, 013807 (2004).

[79] H. de Riedmatten, J. Laurat, C. W. Chou, E. W. Schomburg, D. Felinto, H. J. Kimble. *Phys. Rev. Lett.* **97**, 113603 (2006).

[80] J. G. Rarity, P. R. Tapster. *Phys. Rev. A* **41**, 5139 (1990).

[81] J. D. Franson. *Phys. Rev. Lett.* **62**, 2205 (1989).

[82] J. Brendel, E. Mohler, W. Martienssen. *Europhs. Lett.* **20**, 575 (1992).

[83] M. Fiorentino, P. L. Voss, J. E. Sharping, P. Kumar. *Phys. Rev. A* **47**, R2472 (1993).

[84] A. Kent. *Phys. Rev. Lett.* **83**, 5382 (1999).

[85] A. Ambainis. *Journal of Computer and System Sciences* **68**, 398 (2004).

[86] I. D. Ivanovic. *Physics Letters A* **123**, 257 (1987).

[87] C. Helstrom. *Quantum Detection and Estimation Theory.* Academic Press, (1976).

[88] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat. *Advances in Atomic, Molecular, and Optical Physics: Photonic State Tomography* , 2005 – available at http://research.physics.uiuc.edu/QI/Photonics/Tomography/index.html.

[89] G. P. Agrawal. *Nonlinear Fiber Optics: Fourth Edition.* Academic Press, .

[90] D. Marcuse. *J. Opt. Soc. Am.* **68**, 103 (1978).

[91] X. Daxhelet. *private communication.* (2007).

[92] G. K. L. Wong, A. Y. H. Chen, S. W. Ha, R. J. Kruhlak, S. G. Murdoch, R. Leonhardt, J. D. Harvey, N. Y. Joly. *Opt. Exp.* **13**, 8662 (2005).

[93] I. H. Malitson. *J. Opt. Soc. Am.* **55**, 1205 (1965).

Appendix A

Details on Four-Wave Mixing Phase Matching in Optical Fibre

A.1 Phase-Matching Theory

Optical fibre, which is made of silica oxide, does not have a $\chi^{(2)}$ non-linearity but does have a third-order $\chi^{(3)}$ non-linearity. As a result, second-order non-linear processes, like parametric down-conversion, are typically non-existent in optical fiber. Instead, third-order non-linear effects known as four-wave mixing (FWM) are dominant. In a FWM process of particular interest two pump photons can interact to produce a photon pair if the appropriate conservation laws are satisfied [89]:

$$2\omega_p = \omega_s + \omega_i \tag{A.1a}$$

$$2n_p\omega_p = n_s\omega_s + n_i\omega_i + 2\gamma \mathrm{P}_p \tag{A.1b}$$

In this process a pump laser, at wavelength λ_p with power P_p, is required. The effect of the third-order non-linearity is to modify the phase matching condition by a power dependent term proportional to the nonlinear parameter $\gamma = \frac{n_{nl}\omega}{c\mathrm{A}_{eff}}$, where n_{nl} is nonlinear-index coefficient, ω is the frequency of the pump field and A_{eff} is the effective area of the field (details to follow). Only the collinear case (all wavevectors are parallel) is examined here as all fields are guided by the optical fibre.

Several experiments using various fibre types and a single pump beam have produced photon pairs [50, 51, 52, 53]. What has been received little consideration in the past is FWM to produce photon pairs at widely separated wavelengths (i.e. 1550 nm and 810 nm) and the use of two pump beams at widely separated wavelengths.

To examine this case, equation (A.1) can be re-derived without the assumption that both pump photons are at the same wavelength. Here, the notation is changed such that

fields 1 and 2 represent the two pump fields, 3 represents the signal field and 4 represents the idler field.

$$\omega_1 + \omega_2 = \omega_3 + \omega_4 \tag{A.2a}$$

$$n_1\omega_1 + n_2\omega_2 = n_3\omega_3 + n_4\omega_4 + \hat{\gamma}_1 \mathrm{P}_1 + \hat{\gamma}_2 \mathrm{P}_2 \tag{A.2b}$$

Here,

$$\hat{\gamma}_i = 2(\gamma_{3i} + \gamma_{4i} - \gamma_{1i} - \gamma_{2i} - \frac{1}{2}\gamma_{ii}) \tag{A.3}$$

Where,

$$\gamma_{ji} = \frac{n_{nl}\omega_j F_{ji}}{c} \tag{A.4}$$

Again, n_{nl} is the nonlinear index coefficient, which has a typical value of 2×10^{-20} m^2/W [29], ω_j is the frequency of the jth field, and F_{ji} is the overlap of the two fields. If only the fundamental mode of the fibre is considered then all fields propagate with a Gaussian distribution, $e^{-x^2/w_i^2}e^{-y^2/w_i^2}$, where w_j is the field radius, and then:

$$F_{ji} = \frac{2}{\pi(w_j^2 + w_i^2)} \tag{A.5}$$

In general, the field radius is well approximated by the following analytic approximation [90]

$$w_j \approx a(0.65 + 1.619V_j^{-2/3} + 2.879V_j^{-6}) \tag{A.6}$$

where a is the radius of the fibre core and V is the known as the normalized frequency:

$$V = \frac{2\pi a}{\lambda_j}\sqrt{n_{\text{cladding}}^2 - n_{\text{core}}^2} \tag{A.7}$$

If one assumes that the pump fields have identical frequencies, and thus overlaps, and that the signal and idler fields are generated close to the pump frequency, equation (A.5) reduces to:

$$F_{ji} = \frac{1}{\pi w^2} \equiv \frac{1}{\mathrm{A}_{\text{eff}}} \tag{A.8}$$

and equation (A.2) reduces to equation (A.1).

A.2 Phase-Matching in Standard Optical Fiber

Standard telecommunication dispersion shifted fibre (DSF) has been used, with a single pump beam, to produce photon pairs, with small wavelength separations from the single pump beam, around telecommunication wavelengths (1550 nm) [50, 51].

Using a refractive index profile for SMF28 from [91] along with the theory outlined above, it is possible to calculate phase-matching curves for FWM in standard fiber. The results of these calculations are presented in figure (A.1). These figures demonstrate that with a single pump, FWM in SMF28 will not allowing phase-matching to produce a signal field at 1550 nm and an idler field at 810 nm, which are the desired wavelengths described in the main text. As the refractive index profile is fixed nothing can be changed to allow for the desired phase-matching. With dual pumping schemes the wavelength separation between signal (or idler) photons and pump beams is around 1 nm. The technical challenges associated with separating these two beams makes FWM with standard telecommunication fibre an undesirable option for the goals outlined in the main text.

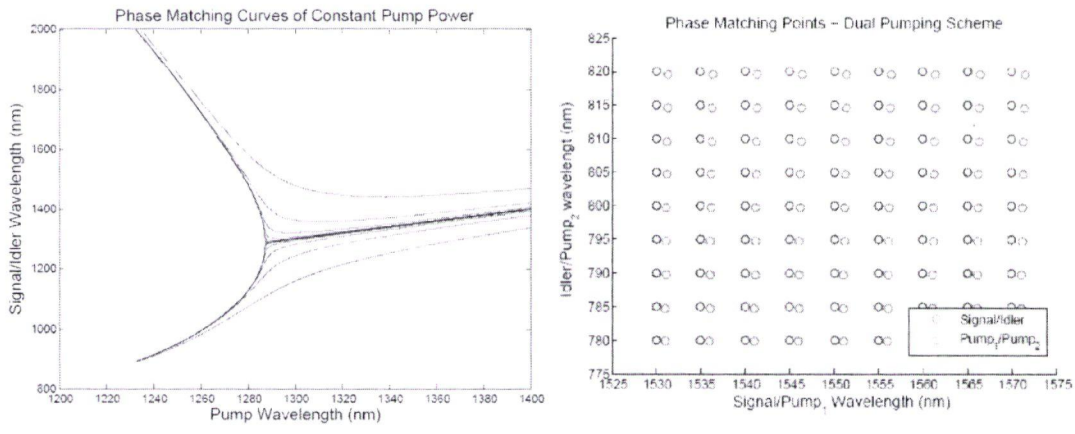

Figure A.1: (a) Phase matching curves for FWM in SMF28 with a single pump. Top (bottom) curves are the phase-matched signal (idler) wavelength. Pairs of curves with larger separations correspond to larger pump powers inside the fibre. (b) Phase matching curves for FWM in SMF28 with two pumps. Each red circle corresponds to two specific pump wavelengths. The nearest blue circle corresponds to the phase-matched signal and idler wavelength. All red-blue circle pairs are separated by less than 1 nm.

A.3 Phase-Matching in Microstructured Fiber

Novel microstructured fibre (MSF) designs have also been examined for the generation of photon pairs. These fibres are constructed with a pure silica core and a honey-comb structure of silica and air-pockets for a cladding. Through different core sizes and cladding designs MSFs with custom refractive index profiles can be fabricated (see figure (A.2)). Also, by shrinking the core size MSFs create larger non-linear effects than standard fibre. To date, MSFs have been used to produce photon pairs at wider separation in visible and NIR wavelengths (600 nm to 900 nm) [52, 53]. No one has reported a photon pair source using MSF that produces photon pairs with one photon in the NIR (800 nm) and one photon at telecommunication wavelengths (1550 nm). To examine this possibility the refractive index profile of MSFs must be determined.

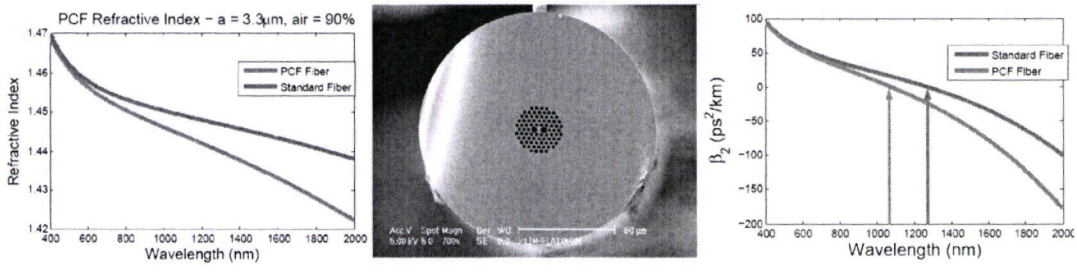

Figure A.2: (a) the refractive index profile of MSF can be customized by adjusting the design of the fiber. (b) MSF contain a pure silica core and a cladding composed of a honey-comb structure of air and silica (photo from [92]). (c) the dispersion profile of MSF steepens and the zero-dispersion wavelength (arrows) shifts to shorter wavelengths.

We use the model presented in [92] to determine the index profile of an MSF. This model uses two parameters: the core size, a, and the fraction of air in the cladding, S. With these parameters, and using the Sellmeier equation silica coefficients from [93] the

index of the core and cladding are modeled as:

$$n_{\text{core}} = n_{\text{pure silica}} \tag{A.9a}$$

$$n_{\text{cladding}} = (1 - S)n_{\text{pure silica}} + Sn_{\text{air}} \tag{A.9b}$$

and then the index profile of the MSF can be found by solving the standard propagation constant eigenvalue equation [89]. We only consider the fundamental mode of the fibre.

$$h\frac{J_1[ha]}{J_0[ha]} = (V^2 - h^2)\frac{K_1[(V^2 - h^2)a]}{K_0[(V^2 - h^2)a]} \tag{A.10}$$

Where $h = \frac{a\omega}{c}\sqrt{n_{\text{core}}^2 - n_{eff}^2}$, V is the normalized frequency, a is the core radius, and J and K are Bessel functions. By solving this equation for h it is possible to determine n_{eff} for a specific fibre design (a and S) at a specific wavelength.

With a modeled MSF refractive index profile and the theory outlined earlier, it is possible to calculate phase-matching curves for FWM. Some result are presented in figure (A.3). These results demonstrate that a properly designed MSF can phase-match to produce signal at 1550 nm and idler at 810 nm with a single pumping scheme or with a duel pumping scheme. This makes MSF a more appealing option than SMF28.

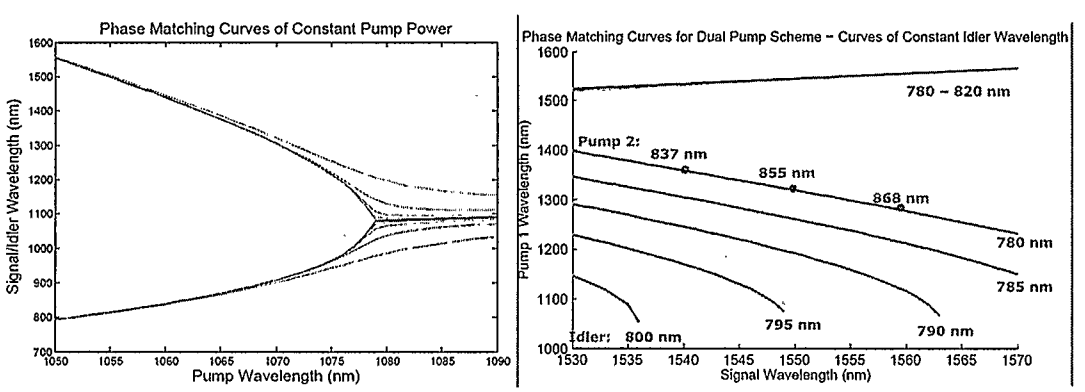

Figure A.3: FWM in MSF: With a (a) single pump or with (b) two pumps a properly designed MSF can phase-match near the desired wavelengths.

A.4 Experimental Work

To further this work we have begun collaborations with a group at the École Polytechnique in Montréal and a group at the Université de Limoges in France who have experience fabricating MSFs with a wide variety of designs. They have fabricated an MSF that produces signal and idler light at the desired wavelengths, see figure (A.4), and we have measured the spectrum at the single photon level, see figure (A.5).

Work is continuing to verify the production of FWM at the single photon level through measurements of the $g^{(2)}(0)$. The experimental setup in figure (A.6) is in the middle of construction.

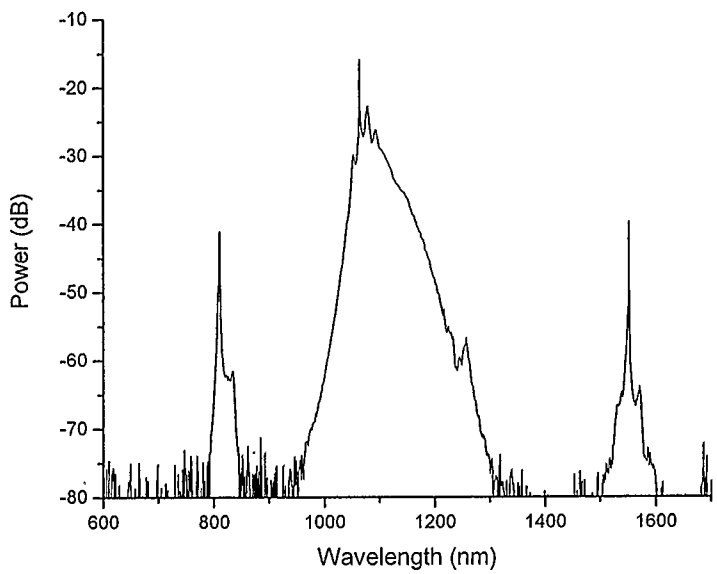

Figure A.4: The classical FWM production spectrum of an MSF fabricated at XLIM. A single pump at 1064 nm produces light at 810 nm and 1545 nm.

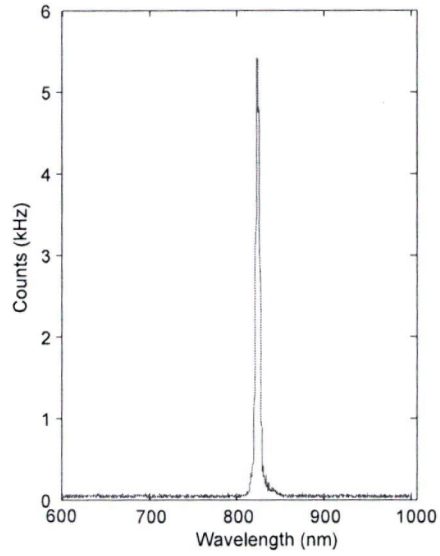

Figure A.5: The FWM production spectrum at the single photon level of an MSF fabricated at XLIM.

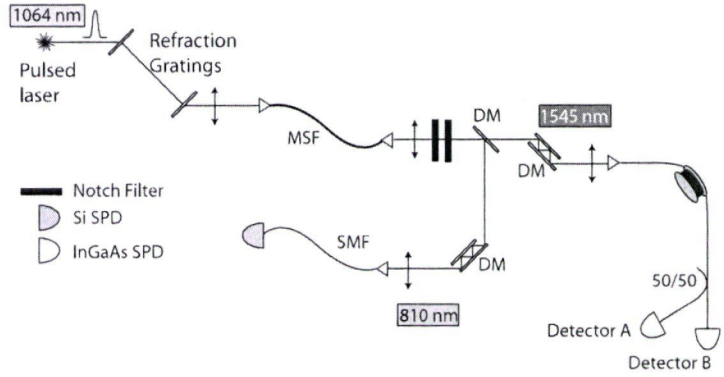

Figure A.6: Setup for experiments to verify the production of photon pairs through $g^{(2)}(0)$ measurements with a novel MSF design.

Appendix B

Details on Interferometer Design and Alignment

B.1 Interferometer Design

To create and analyze time-bin entanglement three interferometers are required: one interferometer to create the time-bin state in the pump beam and one interferometer to analyze each time-bin qubit. For the 810 nm light we built an interferometer that converts the time-bin qubit to a polarization qubit instead of the standard time-bin analyzing interferometer. For the 1550 nm light we built both the standard analyzer and a conversion interferometer. We also built an interferometer for the 530.6 nm pump light. These interferometers are hereafter referred to as the 810-conversion interferometer, the 1550 time-bin interferometer, the 1550-conversion interferometer and the pump interferometer respectively.

We built the pump interferometer using a 50/50 beamsplitter (Thorlabs BS013) that separated the pump light into the two arms of the folded Mach-Zehnder interferometer. Each arm was terminated with a retroreflector (Edmund Optics NT45-202) designed to reverse the direction of the beam without a vertical translation. For alignment purposes the retroreflector on each arm was mounted on a translation stage (Thorlabs PT1/M). One stage moved perpendicular to the beam direction to overlap the output beam from each arm while the second stage moved parallel to the beam direction so that the path length difference could be adjusted. The second stage was fitted with a piezo-electric actuator from Piezomechanik to allow for fine adjustments of the phase difference. To provide increased phase-stability, all optics were mounted on a plate of Zerodur glass from Schott AD, which has a particularly small thermal expansion coefficient of 1×10^{-7} K^{-1}.

This was placed inside an PVC insulting box and temperature stabilized with a PID temperature controller (Thorlabs TED200C and AD590) to $28.0 \pm 0.1°C$.

The 810-conversion interferometer was built with the same retroreflectors, translation stages, Zerodur, piezo-electric actuator and temperature control system (stabilized to $27.9 \pm 0.4°C$) as the pump interferometer. However, instead of a BS this interferometer was built with a PBS (Edmund optics NT47-048) preceded by a HWP (Thorlabs WPH05M-808). Each arm of the interferometer also contained a QWP (Edmund Optics NT46-554). The HWP was aligned such that the horizontally polarized 810 nm photons were rotated to $\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. The rest of the interferometer operation follows the description in the main text.

The 1550 time-bin interferometer was entirely built with fibre optic components. A fibre 50/50 beamsplitter separated the 1550 nm light into the two arms of the Michelson interferometer. Each arm was terminated with a fibre Faraday mirror to remove any birefrengence effects in the fibre optic arms. The long arm was coiled around a round piezo-electric actuator (Piezomechanik) to allow for phase adjustments by stretching the fibre and thus increasing the path length. This interferometer was also placed inside an insulting PVC box and stabilized with a similar PID temperature controller to $26.36 \pm 0.05°C$.

The 1550-conversion interferometer was also built entirely with fibre optic components. A fibre PBS (General Photonics PBS-001-P-03-PM-NC) separated the 1550 nm light into the two arms of the Mach-Zehnder interferometer. The input and both outputs of this PBS were equipped with polarization maintaining fibre. The input PM fibre was aligned at 45° with respect to the PBS. The output arms of the first PBS were fused to two other PM fibres serving as inputs to a second PBS (General Photonics PBS-001-P-03-SM-NC). The output of the second PBS was SFM28 optical fibre. The net effect of this interferometer is the same as described by equation (3.15). This interferometer was

also place inside an insulting box that was stabilized with a similar PID temperature controller to $28.0 \pm 0.1°C$.

B.2 Interferometer Alignment

As described earlier, for high quality entanglement measurements the time difference introduced by all interferometers must be equal. The 1550 time-bin interferometer was constructed to have a 29.4 cm path length difference, which corresponds to a time difference of 1.44 ns (given that the index of SFM28 optical fibre is 1.4682).

To align the other interferometers to the same time difference a broadband amplified spontaneous emission (ASE) source was used. Light from the ASE source was sent through the 1550 time-bin interferometer and then through the pump interferometer. The path length difference of the pump interferometer was adjusted until maximum interference visibility was observed. The coherence length of this ASE was measured to be 36 μm. As this is much smaller than the coherence length of our down-converted light (see section 2.4.1), we were confident that we would see high visibility with the 1550 nm down-converted photons. The same procedure was followed to align the path length difference of the 810-conversion interferometer.

To set the path length difference of the 1550-conversion interferometer which was another fibre interferometer, the effective refractive index, n_{eff} of the fibre was needed. To determine the effective index, the following procedure was developed. The 1550-conversion interferometer was built with a small path length difference ($\sim$ 1 cm). The ASE was sent through this interferometer and then through the balanced free-space Michelson interferometer used in section 2.4.1. The translation stage of the free-space interferometer was adjusted until maximum visibility was achieved. Then, $\Delta l_{\text{cut}} = 1.000$ cm was precisely cut from the longer arm of the 1550-conversion interferometer and the ASE

was again sent through both interferometers. The translation stage was again adjusted until maximum visibility was again achieved. The effective index was calculated using Δl_{stage}, the difference in the two positions of the translation stage.

$$n_{\text{eff}} = \frac{2\Delta l_{\text{stage}}}{\Delta l_{\text{cut}}} \tag{B.1}$$

This procedure was repeated four times and produced a value of $n_{\text{eff}} = 1.4722 \pm 0.0062$.

For the final construction of the 1550-conversion interferometer, the two fibre arms were cut such that the path length difference was ~ 1 cm longer than required:

$$c \times \frac{1.44\text{nm}}{n_{\text{eff}}} + 1 \text{ cm} = 30.3 \text{ cm}. \tag{B.2}$$

Next, the ASE was sent through the 1550 time-bin interferometer, which is the reference interferometer for these experiments, and the free-space Michelson interferometer and the path length difference of the latter was adjusted until maximum visibility was achieved. Then, the ASE was sent through the 1550-conversion interferometer and the free-space Michelson interferometer and again the path length of the latter was adjusted until maximum visibility was achieved. The difference in the path length differences of the free-space interferometer, along with the measured effective index of the PM fibre, was used to determine precisely how much fibre to cut from the 1550-conversion interferometer such that its path length would be aligned on the reference interferometer. The final alignment was made by sending the ASE through the 1550-conversion interferometer and the 1550 time-bin interferometer and adjusting the temperature of each box until maximum visibility was achieved.

Appendix C

Details on Visibility Measurements

As described in the main text, the 810 nm photons were sent through the 810-conversion interferometer and the 1550 nm photons were sent through the 1550-conversion interferometer. As discussed in section 3.1.3, the following visibility measurements can be thought of as analyzing time-bin qubits by projecting onto circles around the Bloch sphere not always accessible with the standard time-bin analyzing interferometer. Here, we use the Z,Y,X notation as described in figure (3.1). For circles 1 through 3 the 1550-conversion interferometer was set to project the 1550 nm photons somewhere onto the X-Y circle (i.e. equal superpositions of $|t_0\rangle$ and $|t_1\rangle$) with an unknown phase. For each curve, the QWP was set such that rotating the HWP projected the 810 nm photon onto one of three orthogonal circles on the Bloch sphere, as described in figures (3.8) through (3.10) again with an unknown phase. For each set of visibility curves the phase of the 810-conversion interferometer was adjusted, as described below, to compensate for this ambiguity.

For the first visibility curves the QWP after the 810-conversion interferometer was set such that rotating the following HWP also projected the 810 nm photon onto the X-Y circle (i.e. equal superpositions between the two polarization states $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi_{810}}|V\rangle)$ or, equivalently, between the two time-bin states: $\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi_{810}}|t_1\rangle)$) on one Si detector and the orthogonal state on the other Si detector. These measurements are equivalent to the standard time-bin visibility curves, but performed with the novel interferometer, even though the phase of each interferometer was unknown. Figure (3.8) showed an average visibility of 92.0% $\pm$ 1.5%.

For the second visibility curves it was stated that the QWP was set such rotating the

HWP projected the 810 nm photons onto the Z-X circle. However, as the phase of each interferometer was unknown, the projection may not have passed through the X-axis. Nevertheless, it is known that the 810 nm photons were projected onto a circle that encompassed two points from the equator of equal superpositions and both poles. To ensure maximal visibility the HWP was initially set to project onto the equator of equal superpositions and then the phase of the 810-conversion interferometer was adjusted until a maximum coincidence detection probability was found. This non-local phase alignment between the two interferometers ensured that initially the two photons were projected onto the same state. Afterwards the HWP was rotated to produce figure (3.9), which showed an average visibility of $91.6\% \pm 1.3\%$.

For the third visibility curves it was stated that rotating the HWP projected the 810 nm photons onto the Z-Y circle. In fact, the same QWP and HWP settings as in the second set of curves were used. However, the HWP was initially set to project onto the equator of equal superpositions and then the phase of the 810-conversion interferometer was re-adjusted until a coincidence detection probability mid-way between the maximum and minimum was found. This corresponded to adjusting the phase by $\pi/2$ so that scanning the HWP setting was equivalent to scanning a circle perpendicular to the previous two measurements. This produced figure (3.10), which showed an average visibility of $7.4\% \pm 4.7\%$.

For circles 4 through 6 the 1550-conversion interferometer was set to project the 1550 nm photons onto Z (i.e. $|t_0\rangle$ and $|t_1\rangle$) and then measurements were taken with the same three QWP settings as before, as described in figures (3.11) through (3.13). Since the phase of the 1550-conversion interferometer does not affect these measurements it was not necessary to compensate for the phase ambiguity with a non-local phase alignment.

For the fourth and fifth visibility curves the QWP was set such that rotating the HWP projected the 810 nm photon onto circles that encompassed two points from the equator

of equal superpositions and both poles. The QWP was adjusted so that the phase of these projections differed by $\pi/2$. figures (3.11) and (3.12) showed average visibilities of $96.7\% \pm 2.3\%$ and $95.6\% \pm 1.9\%$ for these measurements.

Finally, for the sixth visibility curves the QWP set such that rotating the HWP projected the 810 nm photons onto the equator of equal superposition, although with an unknown phase at each measurement. Figure (3.13) showed and average visibility of $96.7\% \pm 2.3\%$.