Towards Real-World Adoption of Quantum Key Distribution using Entangled Photons

by

Catherine Holloway

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

Waterloo, Ontario, Canada, 2012

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

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

Abstract

In order for quantum key distribution (QKD) to move from the lab to widespread adoption, it will need to be compatible with existing infrastructure. To that end, I demonstrate an implementation of QKD with entangled photons on active, standard telecommunications fiber. By using a wavelength outside of the conventional band used by telecommunications traffic, I achieve minimal disruption to either the quantum or classical signals. In an attempt to extend the reach of QKD with entangled photons I studied the parameters of these systems. I developed a model for the number of measured two-fold coincidences that maximizes the secure key rate (SKR), for any combination of system parameters, using a symbolic regression algorithm based on simulated data. I validated this model against experimental data, and demonstrated its usefulness by applying it to simulations of QKD between the ground and a satellite and in optical fibers. Finally, I worked on a step towards a new entangled photon source that is a hybrid between visible and telecommunications wavelengths by building a hybrid single photon source.

Acknowledgements

I would like to acknowledge the support and education provided by other members of Dr. Jennewein's research group. Thanks to Rolf Horn for all of his advice both in and out of the lab. Thanks to Piotr Kolenderski for teaching me everything I know about optics. Thanks to Chris Erven for trusting me with his entangled photon source. Thanks to my fellow grad students, especially Evan Meyer-Scott and Jean-Phillipe Bourgoin, for putting up with my hijinxs. I also acknowledge the help provided by Zhizhong Yang, Brendon Higgins, Krister Shalm, and Deny Hamel. Thanks Judy McDonnell for her administrative assistance. Thanks to John Doucette for being my constant cheerleader.

I would also like to thank the various diversions that kept me sane during the past two years: A Song of Fire and Ice, The Economist, Read it and Weep, Rupaul's Drag Race, cookie time, Rio Grande Games, the Metropolitan Opera's production of the Ring Cycle, Let's Talk Science, and the Kitchener Musical Society Band.

Dedication

To Donna Huffman and Steven Holloway

Table of Contents

List of Tables **x**

List of Figures **xii**

1 Introduction **1**

2 Quantum Optics and its Applications **5**

2.1 Photons as Qubits 5

2.2 Quantum Physics Theories that enable Key Distribution 7

2.2.1 The No-Cloning theorem 7

2.2.2 Bell's Theorem 8

2.3 Nonlinear Quantum Optics Processes 10

2.3.1 Parametric Conversion 11

2.3.2 Second Harmonic Generation 12

2.3.3 Spontaneous Parametric Down Conversion 14

2.4 Polarization-Encoded Photonic Qubits 17

2.4.1 Making Entangled Photons 17

2.4.2 Measuring Qubits 18

2.4.3 Mathematical Models of Single Photon Detectors 21

2.5 Quantum Key Distribution Protocols 22

2.5.1 Quantum Key Distribution with single photons 22

2.5.2 Quantum Key Distribution with Entanglement 23
2.6 Practical QKD Considerations 24
2.6.1 Post-Processing 24
2.6.2 Key Rate Estimation 26
2.7 Conclusions 30

3 QKD over Active Telecommunication Channels 31
3.1 Fiber-Based QKD demonstrations 31
3.1.1 Optical Telecommunications Networks 36
3.2 Experimental Design 38
3.2.1 Generation and Measurement of Entangled Photons 38
3.2.2 Waveguide theory in Single Mode Fibers 41
3.2.3 Fiber Channel and Detection 46
3.2.4 Fiber Mixing processes 47
3.2.5 QKD Results 50
3.3 Conclusions 53

4 Optimal Parameters for Entanglement-Based QKD 54
4.1 Limiting factors in QKD implementation 55
4.1.1 Signal Attenuation and Interference 55
4.1.2 Detector Efficiencies 57
4.1.3 Higher-order photon emission 58
4.1.4 A model for the optimal Two-Fold coincidence rate 58
4.2 Simulation and Modelling of QKD with Entangled states and the optimal coincidence rate 60
4.2.1 Validation with Previous Theoretical Work 63
4.2.2 Validation with Experimental Data 63
4.2.3 Validation from Analysis 65

4.3 Application: Predictions of Maximal distance of QKD to the State of the Art in Photon Detection and Fiber Optics 67
4.3.1 Noise budgets 69
4.4 Application: Satellite Uplink 70
4.5 Discussion 72
4.6 Conclusions 74

5 Hybrid Heralded Single Photon Source 75
5.1 Uses of Heralded Single Photon Sources 76
5.2 Construction of a Heralded Single Photon Source 76
5.2.1 Pump wavelength tuning 76
5.2.2 Alignment 79
5.2.3 Beam separation 81
5.2.4 Mode-matching 82
5.2.5 Timing Adjustment 82
5.3 Comparison of HSPS 82
5.4 Conclusion 83

6 Conclusions 84

References 87

Appendices 99

A Contributions to the Spacelike-separated GHZ state measurement 99
A.1 Polarisation Stability Measurements 99

B Acronyms used in this thesis 103

C Additional proofs 105
C.1 Expectation values of a Bell state measurement with a CHSH formulation . 105
C.2 Error rates with symmetric attacks 106

D Code Written for this thesis **108**

D.1 Bucket Detector with Poissonian distribution of dark counts 108

D.2 Coincidence measurements with Squashing 109

D.3 Secure Key Rate Simulation 111

List of Tables

2.1 Sample polarizations and their qubit representation equivalents. 5

2.2 The Sellmeier equations for crystals used in this thesis. Partly adapted from [90]. 13

2.3 A sample key distribution with BB84. R means rectilinear basis, D means diagonal basis. Adapted from [10]. 22

3.1 Selected demonstrations of QKD with entangled photon sources. The secure key rates with stars indicate estimated rates from QBER and coincidence rates while the non-star values were the rates in a secure key exchange. . . 33

3.2 Selected previous experiments with BB84 over active telecommunications fibers. 33

3.3 Fiber optic ethernet standards (as defined by the IEEE). 34

4.1 Optimal values of two-fold coincidence rates corresponding to the experiments in figure 4.2.2, based on experiment, simulations, and the model (eq. 4.1). 63

4.2 Optimal coincidence rates, and the Loss Budget in order to get a key (50,000 secure key bits) in an hour or ten years for symmetric entanglement-based QKD for common single photon detectors for telecom frequency photons. Table adapted from Bulter and Collins [15]. 68

4.3 The additional key and total key generated by optimizing the two-fold coincidence rate compared with keeping the coincidence rate fixed. The first number is the amount of additional secure key bits shared per pass, the second number is the percentage increase. The conditions are: source and transmitter on a mountain, or at sea-level, source and transmitter 20 km away from a city, source and transmitter 45 km away from a city. There is no data for the median pass for a transmitter at sea-level and 20 km from Ottawa because it is not possible to exchange a key under these conditions. The median passes show the most improvement 71

5.1 Expected transmittivities (in percent) of the wavelengths used in this source to the fiber couplers 81

List of Figures

1.1 The predicted year of factoring prime numbers, based on the bit length of the prime number in the general number field sieve (GNFS) algorithm. . . 2

2.1 Polarization States of light. Adapted from images on Wikimedia Commons. 6

2.2 Poincaré sphere with certain polarization states from table 2.1 and figure 2.1. 7

2.3 Type-I non-collinear SPDC 12

2.4 Type-II non-collinear SPDC 12

2.5 Entangled photon states from a type-I SPDC source using a half-wave plate and a beam splitter. 16

2.6 Entangled photon states from a type-II SPDC source in a Sagnac Interferometer loop. 16

2.7 Entangled photon states created by stacking two nonlinear crystals at 90 degrees with type-I SPDC processes. 17

2.8 Polarization analysis module with a passive basis choice and with an active basis choice 19

2.9 Detector click probabilities considering a single photon incident on both detectors versus channel efficiency. The detector dark count probability is 0.1. Note that the probability of clicking in the simple model exceeds 1 for efficient channels, while the poissonian model is always less than one. When the dark count probability is zero, these models reduce to the same value. . 20

2.10 The error correction efficiency of Brassard and Salvail's [14] CASCADE algorithm for various rates of QBER. The data points are derived from equation 2.54 with 100 rounds of error correction, and a block length chosen such that the initial errors per block is $E_1 \leq -\frac{ln(\frac{1}{2})}{2}$. The values for error correction are discrete due to the rounding of integers in the calculation of the amount of information shared in error correction. The plotted line corresponds to the equation $f(\mathcal{D}) = 1.169 + \mathcal{D}$. 27

3.1 A comparison of the key rates at 1 km of telecommunications fiber between this and other experiments and the optical power of the classical traffic, (results from [17, 80, 30, 19]). 32

3.2 Demand and capacity for information in fiber optic channels. Graph courtesy of Neng Bai. 35

3.3 Experimental set-up for a demonstration of QKD on an active telecommunications network 39

3.4 Measured transmissions for the fiber splitter (Thorlabs 10202A-50-FC) used to combine classical and quantum signals and extract the quantum signal. In this image, orange lines represent 1550 nm light, and maroon represents 810 nm light. Quantum signals were injected into the fiber using the black-to-black ends, and then extracted from the fiber using the black-to-black end. Classical signals used the red-to-black ends to enter the fiber and the black-to-blue ends to exit the fiber. Transmission was measured with a power meter. 40

3.5 The first mode for 1550 nm and the first two spatial modes of 810 nm plotted with the profile of the difference (in percent) between the indices of refraction for the core and cladding for SMF28. 42

3.6 The first mode of 810 nm in SMF28, and the first mode of 810 nm in SMF 800. Core size is assumed to be 2.5 um. 43

3.7 Calculated coupling coefficient between two SMF28 cores in a symetric waveguide, dependent on the separation of the cores. The dashed line highlights the separation distance for a 50:50 splitter. Note that this coupling coefficient is a term in a differential equation describing the transfer between modes, and does not represent the transmission from one mode to another. 44

3.8 Wavelength-binned number of counts over 10 minutes of exposure for the case where polarization-entangled photons at 810 nm travelled in the same direction, in the opposite direction, and in the absense of photons at 1550 nm generated by a classical router. 48

3.9 Measured detector counts in the presence of quantum and classical signals. Detector dark counts (false positives) are represented by a dashed line. . . 49

3.10 Measured and theoretical predictions for QBER with and without the presence of classical traffic. Lines are the values from simulation fitting the experimental parameters. 50

3.11 Measured and theoretical predictions for SKR with and without the presence of classical traffic. Lines are the values from simulation fitting the experimental parameters. 51

3.12 The evolution of QBER in time, while the classical traffic is increased from 0 to 100 Mbps and back to 0 Mbps in factors of 10 every 50 s. 52

4.1 The attenuation of light signals for various wavelengths. The contributions that add to the attenuation - Rayleigh scattering, ultra-violet scattering (the Urbach edge), multi-phonon absorption and absorption due to impurities in the manufacturing process, are plotted. 55

4.2 Four scattering processes that add to the attenuation in fiber. From left to right, the processes depicted are Rayleigh Scattering, Raman (Stokes) scattering, Raman (anti-Stokes) scattering, and Brillouin Scattering. Purple dashed lines represent virtual states. ω_i is the input photon, ω_s is the scattered photon, and ω_{ph} is the photon resulting from Brillouin scattering 56

4.3 Comparison of the amount of key with a constant power rate compared to an optimized key rate. In this simulation, the coincidence window is 2×10^{-9} s, the detector efficiency is 50%, and the dark count rate is 5×10^{5} per second.This dark count rate is very large in order to emphasize the difference in optimization. 59

4.4 While the party A received and correctly measured a horizontally polarized photon, the party B received a mult-photon state and measured two orthogonal detectors clicking at the same time, leading to an error. 60

4.5 The model for the optimal coincidence rate as determined by Eureqa. The channel efficiencies for Alice and Bob are plotted along the x and y axes. The two-fold coincidence rate is plotted in log base 10 scale. The model also depends on the background counts in Alice and Bob, but only by a constant factor. 61

4.6 Comparison of the optimal squeezing rate between our simulation and Ma et. al 's ([70]) optimal squeezing rate. 64

4.7 Experimental configuration used to validate the model. The entangled photon source is based on a PPKTP crystal in a Sagnac configuration [35]. The pump power was varied in order to observe the resulting coincidence rates and QBER. Loss was introduced by adding neutral density filters, or by using a free-space channel. 65

4.8 Comparison of experimental data for three different channels. Three different experimental conditions were used: uncovered polarization analyzer without neutral density filters($d = 7 \times 10^{-5} \pm 1 \times 10^{-5}$, $\eta = 0.25 \pm 1 \times 10^{-2}$, graph A), covered polarization analyzers with neutral density filters ($d = 5.92 \times 10^{-6} \pm 1 \times 10^{-8}$, $\eta = 0.085 \pm 1 \times 10^{-3}$, graph B), and after a free space channel ($d = 5.92 \times 10^{-6} \pm 5 \times 10^{-8}$, $\eta = 0.12 \pm 1 \times 10^{-2}$, graph C) 66

4.9 Operating conditions of the satellite passes studied in this section. Passes were ordered by their minimum loss, and I picked out the best, 75 % percentile pass, and 50 % percentile pass. Ground stations are placed at 20 km and 45 km away from Ottawa, either at sea-level or on a mountain (2.4 km above sea-level). The transmission efficiency is for photons at 785 nm. The transmitting telescope has an area of 25 cm, and the receiving telescope on the satellite has an area of 20 km. The constant source rate used for comparison was 5.4×10^8 70

4.10 The predicted optimal source rate (directly at the source, assuming 50% detection efficiency detectors) and additional secure key bits for transmissions between the ground and a LEO satellite, with a ground station at sea-level, 45 km from Ottawa. 71

4.11 The probability of getting a secure key bit for a system with the corresponding two-fold coincidence probabilities for an ideal state (described in equation 4.4), a “pseudo-ideal” state (described in equation 4.3) and a state from SPDC sources (described in equation 2.28). The “pseudo-ideal” and SPDC source states both exhibit a maximum secure key probability, and both have multi-order terms. The ideal state has no maxima and increases linearly with increasing two-fold coincidences. 73

5.1 Experimental schematic for the HSPS described in this chapter. 77

5.2 Imaged second harmonic beam with a continuous wave pump. The beam appears elliptical due to the walk-off effects in the crystal, and appears doubled due to the dichroic mirror used to separate the pump from the second harmonic. 78

5.3 Imaged downconversion rings on a beam profiler CCD camera. From left to right, the images represent a tilt of 1 degree, 4 degrees, 10 degrees and 20 degrees. 79

5.4 Image of downconversion rings taken with an iPod camera. 80

A.1 Schematic of measurement device. In this diagram, the LED is a low-power thorlabs LED at 805 nm. LP= Linear polarizer, Col.= FC Collimator, FPC= fiber polarisation controller (bat-ears), FC-FC = FC-FC mating adaptor, HWP= half-wave-plate, PBS= Polarising beam splitter, and PMD= Thorlabs PM100D power meter with S120C series silicon detector. 99

Chapter 1

Introduction

Quantum Key Distribution (QKD) is on the cusp of being a disruptive technology. Several key engineering challenges must be resolved in order for it to make it into the market. In this thesis, I aim to tackle two of them.

Moore's law, the prediction that the number of transistors on an inexpensive and widely available integrated chip will double every two years, was first proposed in 1965 and has so far held true. With this power function has come an explosion of new technologies, practices and businesses. The way we communicate, shop, and work is markedly different from the way our parents did at our age. Massive amounts of data that used to be kept private, such as medical histories, state secrets, and credit card information, are now routinely shared online, on publicly accessible infrastructure.

We feel secure doing this because we have public-key-encryption. Without any prior communication with a website hosted on a server many thousands of kilometers away from us, can give us a private key with that we can use to encrypt our data when we share it with them. All public-key encryption protocols rely on computational complexity; that the operation we do in order to generate our key is easier to do than it is to undo.

Although this form of security might be sufficient on a short term basis, considering the accelerating returns of computing power, it can be said with some certainty that all currently used public-key security protocols will someday be broken. A common cryptographic hash function that is used to store passwords on many websites, MD5, could be broken by state-of-the-art research computers in 2004 [115], and can now be broken with collision attacks in a matter of minutes using a macbook from 2006 [57].

The RSA algorithm, the method that underpins all internet security, usually involves the factorization of numbers that are 1024-2048 bits long. In 2010, a research-grade com-

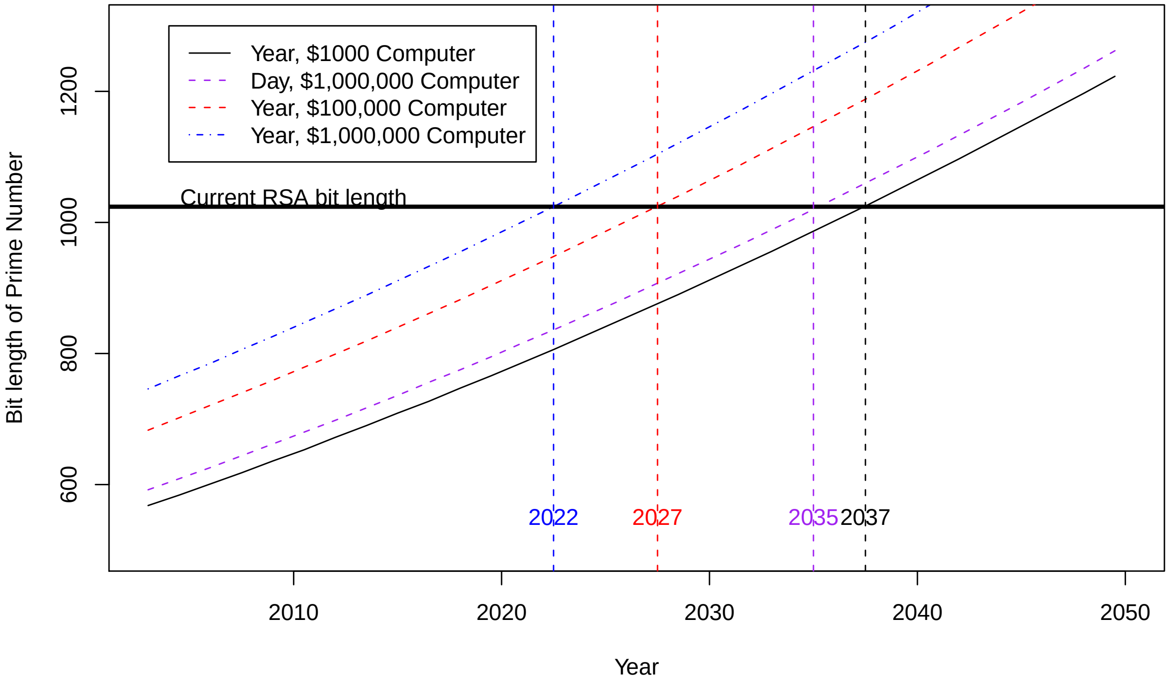


Figure 1.1: The predicted year of factoring prime numbers, based on the bit length of the prime number in the general number field sieve (GNFS) algorithm.

puter, using the equivalent of 400 hours computing time on the latest macbook pro, broke a 768 bit key [56]. The best known factoring algorithm on classical computers is the general number field sieve (GNFS)[67]. GNFS requires a roughly exponential number of operations to factor a number based on the bits needed to represent the number. Using previous record holders in the RSA factorization challenges, the complexity of the GNFS algorithm, and Moore's Law, it is possible to estimate when it will be possible to factor numbers of various lengths on commercially available computers (or what you can buy for $1000, $100,000, and $1,000,000) given a year of computational time. These curves, along with the intersection point with today's number lengths, are presented in figure 1. The GNFS algorithm is parallelizable, so it is reasonable to say that two computers can do in six months what one computer can do in 1 year, so on.

This does not even consider the existence of quantum computers, for which there is a sub-exponential algorithm for factoring prime numbers.

Considering these advances, it is clear that our current methods of key exchange are not "future-proof" and that, at some point in the not-to-distant future, they will be broken. This is a sobering prospect that much of our modern secrecy has less than a ten year expiration date. Humans with confidential financial and medical information will outlive the next ten years. State and institutional secrets will want to be kept secret for more than ten years. The only way to make information future proof to malicious eavesdroppers is to use a one time pad. The only methods of transferring a one-time pad are on foot or via quantum key distribution. And even on foot, the key could be surrepticiously copied without the knowledge of the bearer. QKD guarantees that within a small probability epsilon, the key shared has not been eavesdropped on.

QKD can be performed by distributing pairs of photons that are entangled in their polarization state. Photons are generated somewhere in the middle between two parties, Alice and Bob. One of the entangled photons is sent to Alice, the other to Bob. Alice and Bob can then do projective measurements on their photons. If their particle is entangled, they should get correlations with the measurement of their partner. By rotating their photons in a quarter wave plate, they can measure in a basis at 45 degrees and thus introduce an element of randomness into their measurements required for QKD protocols. If an eavesdropped has extracted any useful information from the exchange, it will appear in the measurement results as increased errors.

QKD with entangled photons has been demonstrated in the lab many times. In this thesis, I aim to cover some of the practical issues regarding the widespread adoption and integration of QKD with entangled photons into existing infrastructure. In chapter 2, I will cover the creation and measurement of entangled photon states, the protocol for QKD with entangled photons, and realistic estimates of secure key rate based on error correction and privacy amplification. In chapter 3 I present an implementation of QKD with entangled photons that is compatible with classical telecommunications traffic. In chapter 4 I study the optimal parameters for QKD with realistic entangled photon states. Finally, in chapter 5, I present the first steps towards a new entangled photon source that can bridge the gap between fiber optic and free-space QKD, providing the possibility of worldwide networks of entangled photon distribution.

The purpose of this thesis is not only to provide a record of my work, but as a document that, if I ever encounter a time machine or a tunnel to another dimension that is out of sync with this one, I can hand to a version of myself in 2010, with knowledge of undergraduate-level classical mechanics, optics, quantum mechanics and electro-magnetism but with no knowledge of nonlinear optics or quantum information, and hopefully have myself understand what I did.

Chapter 2

Quantum Optics and its Applications

2.1 Photons as Qubits

All wave phenomena where the direction of oscillation and propagation are perpendicular have a property called polarization, which describes the orientation of their oscillations with respect to their propagation. Electromagnetic waves (light) exhibits this phenomenon. When it propagates in only one dimension it is called linearly polarized, when it travels in a corkscrew around an axis it is called circularly polarized. Figure 2.1 shows a graphical representation of several polarization states with respect to their axes of propagation.

Qubits can be made out of polarized light if the H and V polarizations represent the $|0\rangle$ and $|1\rangle$ basis states. Using this notation, we can represent the polarizations in figure 2.1 in qubit notation. This is described in table 2.1, as well on the Poincaré sphere in figure 2.2.

Polarization description	Representation in figure 2.1	Qubit notation
Horizontally polarized	H	$\|0\rangle$
Vertically polarized	V	$\|1\rangle$
Polarized at +45 degrees	+	$\frac{\sqrt{2}}{2}(\|0\rangle + \|1\rangle)$
Polarized at -45 degrees	-	$\frac{\sqrt{2}}{2}(\|0\rangle - \|1\rangle)$
Right circularly polarized light	R	$\frac{\sqrt{2}}{2}(\|0\rangle - i\|1\rangle)$
Left circularly polarized light	L	$\frac{\sqrt{2}}{2}(\|0\rangle + i\|1\rangle)$

Table 2.1: Sample polarizations and their qubit representation equivalents.

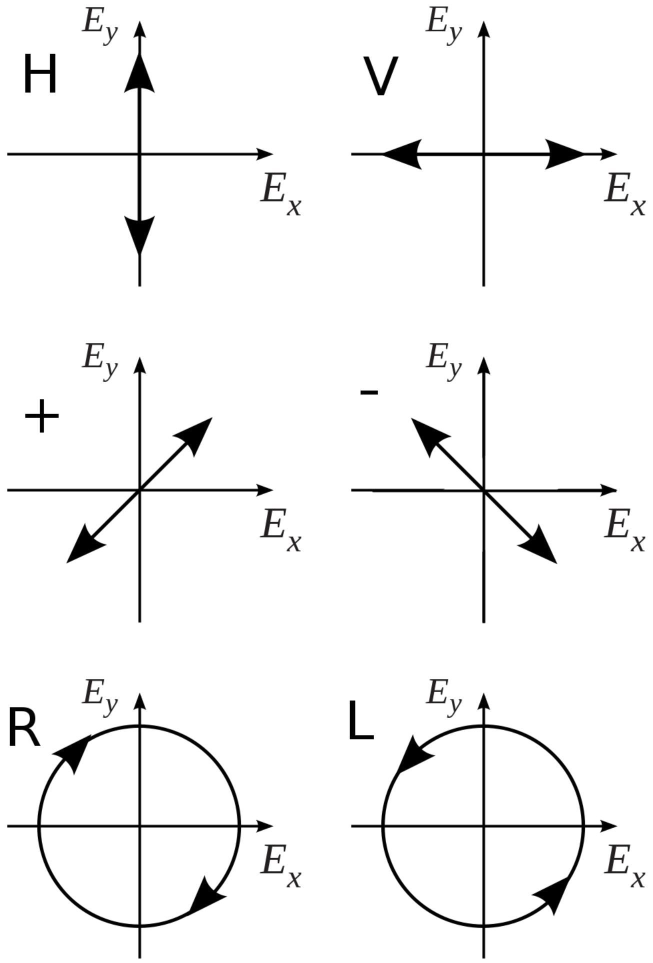


Figure 2.1: Polarization States of light. Adapted from images on Wikimedia Commons.

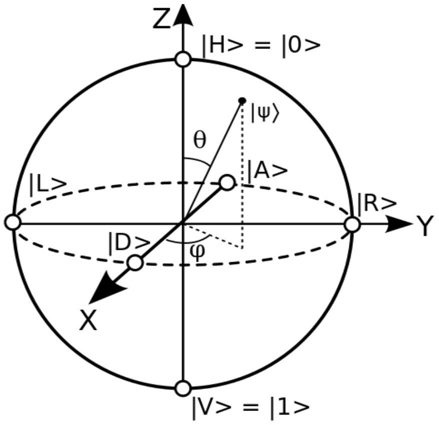


Figure 2.2: Poincaré sphere with certain polarization states from table 2.1 and figure 2.1.

Single qubit transformations are very simple. Any arbitrary rotation around the Poincaré sphere can be accomplished with birefringent materials that act as a phase retarder. A common polarization control is the use of a quarter-wave-plate (QWP) followed by a half-wave-plate (HWP) followed by another QWP. Two-qubit transformations, which would be needed for quantum computing applications, are difficult to realize because photons don't interact with each other.

2.2 Quantum Physics Theories that enable Key Distribution

Two theories are responsible for the phenomenon of being able to use entangled qubits to share secret keys, these are the No-Cloning theorem and Bell's theorem.

2.2.1 The No-Cloning theorem

The no-cloning theorem means that it is impossible for a copy of a quantum state to be made, as one would copy classical information like bits in a computer or text on a page. The first proof of the no-cloning theorem was published by Wooters and Zurek[118]. The proof of the no-cloning theorem on qubits is as follows. Suppose we have a unitary operator such that for a specific input qubit $|e\rangle$ and a qubit to be cloned, $|\psi\rangle = a|0\rangle + b|1\rangle$, the output after time Δt is:

$$\begin{aligned} U(\Delta t)|\psi\rangle|e\rangle &= |\psi\rangle|\psi\rangle && (2.1)\\ &= (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle) && (2.2)\\ &= a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle && (2.3)\end{aligned}$$

However, the cloner must also work on the basis states of the qubit, i.e. $U(\Delta t)|0\rangle|e\rangle = |00\rangle$ and $U(\Delta t)|1\rangle|e\rangle = |11\rangle$. For this to be valid, the cloner on state $|\psi\rangle$ must work on the superposition of both basis states:

$$\begin{aligned} U(\Delta t)|\psi\rangle|e\rangle &= aU(\Delta t)|0\rangle|e\rangle + bU(\Delta t)|1\rangle|e\rangle && (2.4)\\ &= a|00\rangle + b|11\rangle && (2.5)\end{aligned}$$

Equation 2.1 is not the same as equation 2.4, thus such a cloning operator is unphysical.

2.2.2 Bell's Theorem

Bell's theorem is like the no-cloning theorem in that it is a negative theorem. It states that no theory of local hidden variables can explain all of the predictions of quantum mechanics.

In order to understand how we arrived at Bell's theorem, and what the implications are to quantum optics and quantum communication, a brief history lesson is needed. In the 1930s, when quantum mechanics was in its infancy, Einstein co-authored a paper in which he described a thought experiment which he thought highlighted his biggest problem with the field, now commonly known as the EPR paradox[26].

Imagine a photon breaking apart into two photons with lower energy, and the photons travel in opposite directions [1]. In order for momentum to be conserved, if one of the two photons ends up with H polarization, the other must end up with V polarization, and vice versa. The same is true for the diagonal basis, if one photon ends up with + polarization, the other must end up with - polarization, and vice versa.

Suppose these two photons then travel a long distance and are then measured by two parties, Alice and Bob. If Alice and Bob measure only in the rectilinear basis (the H/V basis), then a description of quantum physics is not required to explain their measurements. If Alice measures her particle as being H, she knows that Bob must measure V. This can be

[1] A common description of the EPR paradox involves the decay of a spin-0 into two spin-1/2 particles[12]. A photon being downconverted in a sandwich source, described in the next section 2.4.1 is sort of analogous to the decay of a spin-0 particle.

explained using classical correlations - one of the photons was H since the decay, and one was V. However, in order to get a + or - polarizations, you need a superposition of H and V polarizations. If Alice and Bob measured a pair of photons that had classical correlations in the rectilinear basis in the diagonal basis (the +/- basis), their measurements must be random, but when they measure the quantum state described above, their measurements will always be anti-correlated.

My favourite quantum physics textbook describes the paradox as such [108]:

> Imagine that you hold in your hand two colored balls that are identical in feel but one is green and the other is red. You separate the balls without looking and put one in each hand. If you look at the ball in your left hand and find it is red, you have immediately determined that the ball in your right hand is green, even before you open your right hand. You would, of course, presume that the ball in your right hand was green all along, whether or not you had opened your left hand to check the color of the ball. This cannot, however, be an adequate explanation of what is going on...
>
> In our example of the colored balls, it would be similar to the balls having two other colors such as blue and yellow, as well as red and green. Finding one of the balls to be yellow demands that the other is blue, just as finding one of the balls to be red demands that the other ball be green. However, a single ball cannot simultaneously have two colors and be, for example, both red and yellow. So what color is the ball in your right hand before you look?

This paradox was deeply unsettling to Einstein, who believed there there must exist some larger classical theory that could explain quantum correlations, called the hidden-variable theory, and that there was no experimental test that could be performed to distinguish between the two theories.

In the 1960s, John Bell came up with an inequality that would allow for a direct experimental test of the two theories [7]. It involves measuring a spin-$\frac{1}{2}$ particle pair along three different basis measurements. In order to get the maximum quantum violation, these measurement bases need to be separated by $\frac{\pi}{2}$ radians. The three axes of the bloch sphere are an example of such measurements. With photons, this means that the three measurement bases are the rectilinear, diagonal, and circular bases.

However, another inequality more suitable to measuring entangled particles on two channels, with two bases, is the CHSH inequality[21] (Clauser, Horne, Shimony, Holt). Clauser et al. propose a measurement apparatus nearly identical to that used in Bennett, Brassard and Mermin's 1992 quantum key distribution protocol (described in section 2.5.2

). In it, Alice and Bob share an entangled photon pair and measure it with a device that can separate orthogonally-polarized particles, such as a polarizing beam splitter. They also have a half-wave plate that can allow them to choose what bases the measure in. The bases that provide the most violation of this inequality are for Alice to measure in the rectilinear and diagonal bases (represented by a, a') and for Bob to measure in bases at 22.5 and 67.5 degrees to the rectilinear basis (represented by b, b'). They compare their coincidences, and report the value $E(a, b)$ as being 1 or -1, depending on whether they both measured the same detector click, or different detectors clicking. For purely classical correlations, the value of:

$$S = E(a, b) - E(a, b') + E(a', b) + E(a', b') \tag{2.6}$$

must be between:

$$-2 \leq S \leq 2 \tag{2.7}$$

For the case of quantum correlations, such as the Bell state $|\psi\rangle = \frac{\sqrt{2}}{2}(|01\rangle - |10\rangle)$, the expectation values are[2]:

$$E(a, b) = E(a', b) = E(a', b') = \frac{\sqrt{2}}{2} \tag{2.8}$$

and

$$E(a, b') = -\frac{\sqrt{2}}{2} \tag{2.9}$$

Putting these back into the inequality, we get that:

$$S = 2\sqrt{2} \geq 2 \tag{2.10}$$

thus, the inequality is violated.

Freedman and Clauser [36] were the first group to violate this inequality using polarization-entangled photons. Aspect et al. [6] later demonstrated it with entangled photons from nonlinear quantum optics.

2.3 Nonlinear Quantum Optics Processes

A common way to create entangled photons in large numbers is to use nonlinear optics.

[2] For a more detailed calculation of these expectation values, please see appendix C.1

Nonlinear optics is the study of the processes that occur due to the non-linear dielectric susceptibility of certain materials. For a good overview of the math of nonlinear optics, please see Fredrik Jonsson's lecture notes[54] which are available online.

Nonlinear phenomena are very common in science. Famous examples include the Lotka-Volterra equation describing predator-prey population models and the Black-Scholes equation for pricing stocks. These nonlinear phenomena are usually the result of an inhomogenous term being added to a differential equation. For example, the normal differential equation for an electromagnetic wave travelling in free space is:

$$\nabla^2 E - \frac{n^2}{c^2}\frac{\partial^2}{\partial t^2}E = 0 \tag{2.11}$$

When travelling through a dielectric material, the wave is going to encounters a large number of electric dipole moments, so the inhomogenous term based on the polarization density is added:

$$\nabla^2 E - \frac{n^2}{c^2}\frac{\partial^2}{\partial t^2}E = \frac{1}{c^2}\frac{\partial^2}{\partial t^2}P \tag{2.12}$$

where P is the polarization density, which is the dipole moment per unit volume.

A solution to the inhomogenous wave equation is a Taylor series expansion of the polarization density function:

$$P(t) \propto \chi^{(1)}E(t) + \chi^{(2)}E^2(t) + \chi^{(3)}E^3(t) + \cdots \tag{2.13}$$

where $\chi^{(n)}$ are the electric susceptibilities. The non-linear terms in this equation allow for conversions in energy, just like how a spring-mass system with a nonlinear driving force can be doubled in period.

2.3.1 Parametric Conversion

Parametric nonlinear processes are conversions that occur in nonlinear materials that are instantaneous and preserve both energy and momentum, while leaving the nonlinear material undisturbed. Because parametric processes conserve energy and momentum, the input and output waves involved must satisfy the following two conditions:

$$\sum \omega_{in} = \sum \omega_{out} \tag{2.14}$$

and

$$\sum \vec{k}_{in} = \sum \vec{k}_{out} \tag{2.15}$$

This means that the polarizations of the resulting waves will be correlated with the polarizations of the pump waves.

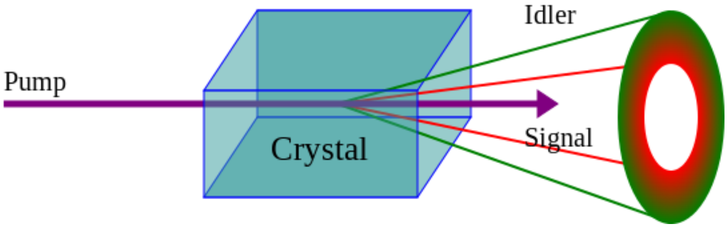


Figure 2.3: Type-I non-collinear SPDC

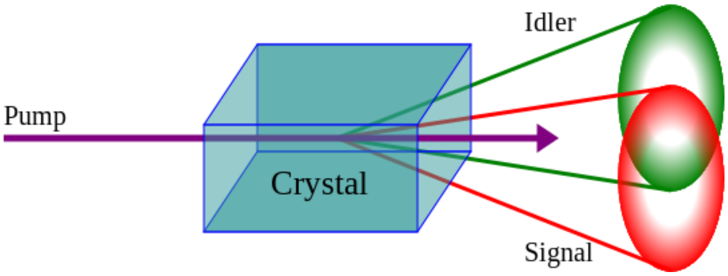


Figure 2.4: Type-II non-collinear SPDC

2.3.2 Second Harmonic Generation

Suppose we have a electromagentic wave with a single frequency $E(t) = E_0 e^{-i\omega t} + c.c.$ in a dielectric material. The first nonlinear reaction will be[3]:

$$P(t) \propto \chi^{(2)} E^2(t) = \chi^{(2)} |E_0|^2 (e^{-i2\omega t} + e^{(i\omega - i\omega)t} + e^{i2\omega t}) \tag{2.16}$$

This reaction allows for a process called Second Harmonic Generation (SHG), in which two photons with frequency ω to be converted to a single photon with frequency 2ω.

[3] The typesetting for many of the equations in this section were copied off of wikipedia because I am lazy.

Material	Sellmeier Equation (Wavelength λ in μm)	Wavelength Range (μm)
BBO	$n_o^2 = 2.7359 + \dfrac{0.01878}{\lambda^2 - 0.01822} - 0.01352\lambda^2$ $n_e^2 = 2.3753 + \dfrac{0.01224}{\lambda^2 - 0.01667} - 0.01516\lambda^2$	0.22-1.06
KDP	$n_o^2 = 1 + \dfrac{1.2566\lambda^2}{\lambda^2 - 0.008447} + \dfrac{33.8991\lambda^2}{\lambda^2 - 1113.9040}$ $n_e^2 = 1 + \dfrac{1.1311\lambda^2}{\lambda^2 - 0.008147} + \dfrac{5.7568\lambda^2}{\lambda^2 - 811.7542}$	0.4-1.06
KTP	$n_x^2 = 2.10468 + \dfrac{0.89342\lambda^2}{\lambda^2 - 0.04438} - 0.01036\lambda^2$ $n_y^2 = 2.14559 + \dfrac{0.87629\lambda^2}{\lambda^2 - 0.0485} - 0.01173\lambda^2$ $n_z^2 = 1.9446 + \dfrac{1.3617\lambda^2}{\lambda^2 - 0.047} - 0.01491\lambda^2$	0.5-3.3
BIBO	$n_x^2 = 3.6545 + \dfrac{0.0511\lambda^2}{\lambda^2 - 0.0371} - 0.0226\lambda^2$ $n_y^2 = 3.0740 + \dfrac{0.0323\lambda^2}{\lambda^2 - 0.0316} - 0.01337\lambda^2$ $n_z^2 = 3.1685 + \dfrac{0.0373\lambda^2}{\lambda^2 - 0.0346} - 0.01750\lambda^2$	0.5-3.5

Table 2.2: The Sellmeier equations for crystals used in this thesis. Partly adapted from [90].

2.3.3 Spontaneous Parametric Down Conversion

Now consider that an electromagnetic wave with two frequency components, $E(t) = E_1 e^{-i\omega_1 t} + E_2 e^{-i\omega_2 t} + c.c.$. The first-order nonlinear response will be:

$$\begin{aligned} P(t) \propto \chi^{(2)} E^2(t) = \chi^{(2)} [&|E_1|^2 e^{-i2\omega_1 t} + |E_2|^2 e^{-i2\omega_2 t} && (2.17)\\ &+ 2E_1 E_2 e^{-i(\omega_1+\omega_2)t} && (2.18)\\ &+ 2E_1 E_2^* e^{-i(\omega_1-\omega_2)t} && (2.19)\\ &+ 2\left(|E_1| + |E_2|\right) e^0], && (2.20) \end{aligned}$$

This means that in certain conditions, two photons with frequencies ω_1 and ω_2 can be used to generate a photon with frequency $\omega_1 + \omega_2$. This process is known as sum frequency generation, and the two input photons referred to as the signal and pump photons, and the output photon is referred to as the idler photon.

Because all optical processes are time reversable, this process can also go the other way, where one higher-energy photon breaks apart into two lower energy photons. This is called spontaneous parametric down-conversion (SPDC).

Due to the conservation of momentum, the wave vectors of the pump, signal and idler must add up such that:

$$k_p = k_i + k_s \tag{2.21}$$

Due to the conservation of energy, the frequencies of the pump, signal and idler must add up such that:

$$\omega_p = \omega_i + \omega_s \tag{2.22}$$

These are known as the phase-matching condition. The wave vectors of the waves involved in sum-frequency generation are referenced by their orientation to the crystal axis. The crystal axis is defined as the orientation for which vertically polarized light will experience no birefringence - meaning it will not experience any displacement due to the refractive indices. If a wave vector is parallel to this optical axis, it is called extraordinary, if it is perpendicular, it is referred to as ordinary. There are two commonly used phase matching conditions in quantum optics, Type I, where the signal and idler both have ordinary polarizations, and the pump has an extraordinary polarization, and Type II, where the pump and idler have extraordinary polarizations but the signal is ordinary.

In addition to the polarization requirements on the phase matching condition, the direction of travel of the waves must also be taken into account. In order to get the signal and idler travelling in the same direction as the pump beam, (referred to as the collinear case) the following additional condition must be achieved:

$$\omega_p n_p = \omega_s n_s + \omega_i n_i \tag{2.23}$$

where n_p, n_s, n_i are the refractive indexes of the three waves.

In uniaxial crystals, the medium for some of the SPDC processes in this thesis, the index of refraction experienced by waves is dependent on the orientation of their optical axis, the frequency of the wave, and its polarization. Ordinary waves will experience indices of refraction independent of the orientation of the crystal perpendicular to its optical axis, but the index of refraction of extraordinary waves will be dependent on the orientation of the crystal. The index of refraction of the extraordinary beam will be:

$$\frac{1}{n^2(\theta,\omega)} = \frac{\cos^2\theta}{n_o^2(\omega)} + \frac{\sin^2\theta}{n_e^2(\omega)} \tag{2.24}$$

Where θ is the orientation of the crystal's optical axis with respect to the angle of entry of the pump, and ω is the frequency of the ordinary ray.

In order to determine the tilt angle for a uniaxial crystal in SPDC, one must solve the equations of the walk-off, either for Type-I:

$$\omega_p n(\theta,\omega_p) = \omega_s n_o(\omega_s) + \omega_p n_o(\omega_p) \tag{2.25}$$

or for type-II

$$\omega_p n(\theta,\omega_p) = \omega_s n_o(\omega_s) + \omega_p n(\theta,\omega_p) \tag{2.26}$$

You can determine $n(\theta,\omega)$ from equation 2.24, and $n_o(\omega)$ and $n_e(\omega)$ from the Sellmeier equation. The Sellmeier equations for the crystals used in this thesis are presented in table 2.2.

Spontaneous Parametric Downconversion is important because it can produce photons that are correlated in polarization, which can be used to create polarization-entangled photons. In the next section I will explain the various methods of generating Bell states from SPDC sources.

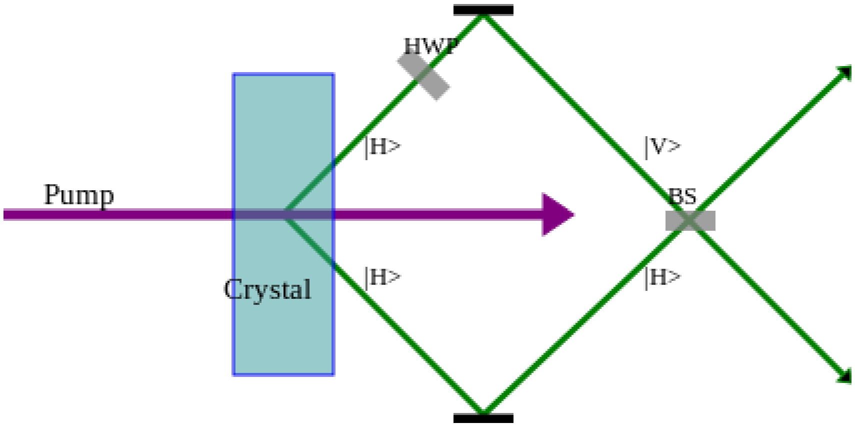


Figure 2.5: Entangled photon states from a type-I SPDC source using a half-wave plate and a beam splitter.

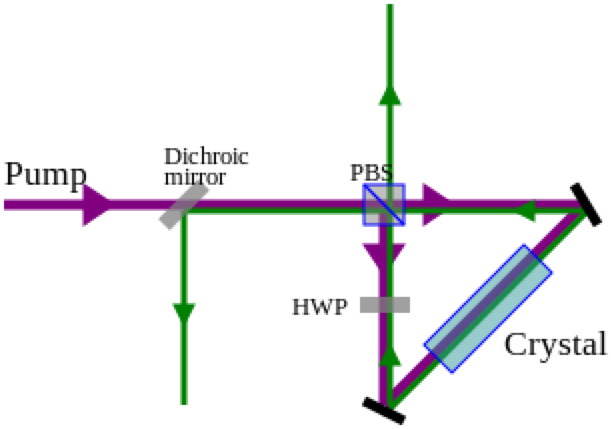


Figure 2.6: Entangled photon states from a type-II SPDC source in a Sagnac Interferometer loop.

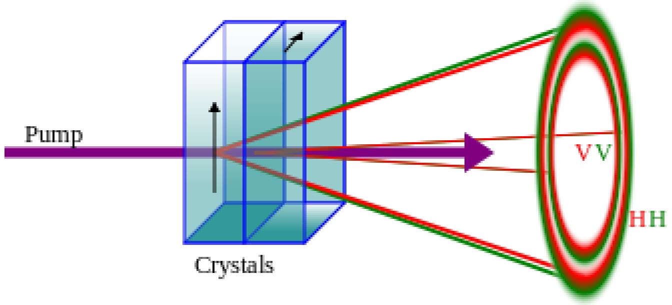


Figure 2.7: Entangled photon states created by stacking two nonlinear crystals at 90 degrees with type-I SPDC processes.

2.4 Polarization-Encoded Photonic Qubits

2.4.1 Making Entangled Photons

SPDC produces 'squeezed' states, represented by the hamiltonian [52]:

$$H = -i\epsilon(a_H^\dagger b_H^\dagger - a_H b_H + a_V^\dagger b_V^\dagger - a_V b_V) \tag{2.27}$$

where ϵ is the squeezing parameter. Here we assume that the process that creates the HH pairs is as efficient as the process that creates the HV pairs, as the same value of ϵ is used for both.

When this operator is applied to the vacuum state, it produces [70]:

$$U_{SPDC} \mid 0000\rangle = C_s \sum_{s=0}^{\infty} \sum_{t=0}^{s} (-1)^t |s-t, t, t, s-t\rangle \tag{2.28}$$

Where the representation of states here is:

$$\mid \psi\rangle = \mid n\rangle_{H,Alice} \otimes \mid n\rangle_{V,Alice} \otimes \mid n\rangle_{H,Bob} \otimes \mid n\rangle_{V,Bob} \tag{2.29}$$

and

$$C_s = \cosh{(\epsilon)}^{-2} \tanh{(\epsilon)}^s \tag{2.30}$$

Written out, the first terms of this are:

$$\mid \psi\rangle = 2C_0 \mid 0000\rangle + C_1 \mid 0110\rangle + C_1 \mid 1001\rangle + 2C_2 \mid 1111\rangle + ... \tag{2.31}$$

There are three common sources of entangled photons: sandwich sources, Sagnac interferometer loops and sources involving picking up the light cones emmitted by SPDC sources.

Due to the phase matching conditions of type-II SPDC (shown in figure 2.3) and the birefringence of the nonlinear crystal, signal and idler photons will exit the crystal in two cones, one on top of the other, with two points of intersection. The first method of generating entangled photons was two pick up these overlapping modes in a type-II SPDC source [61] (shown in figure 2.5). This type of source is difficult to build because it requires very precise coupling of the spatial modes, and most of the downconverted photons must be discarded.

The second source of entangled photons was also discovered by Kwiat et al. and is referred to as a sandwich source [63] (shown in figure 2.6). This is because it is made with two nonlinear crystals stacked on top of each other at orthogonal angles. The pump beam is then focused on the interface between these two crystals, where it has an equal probability of being downconverted in the first crystal (making a HV pair or an HH pair) or the second crystal (making a VH pair or a VV pair).

The source used in this thesis is a Sagnac source (shown in figure 2.6). The Sagnac source was originally designed by Shi and Tomita [98], and refined by Fedrizzi et al. [35] and Wong et al. [117]. Full details of the construction and alignment of the source used in this thesis can be found in Chris Erven's master's thesis[31]. A sagnac source uses a nonlinear crystal in a sagnac loop. The pump has two equally probable paths through the loop. In one path is a HWP that rotates the output photons. This means that one direction through the loop creates HV pairs, while the other direction creates VH pairs.

2.4.2 Measuring Qubits

Once you have your qubits, you must measure them. However, measuring quantum states is an art unto itself. Single photons have very little energy, which makes them hard to detect. They exist in states characterized by their polarization, spatial, frequency, and excitation modes, but quantum information processes tend to assume they are characterized only by their polarization modes and are degenerate in other characteristics. This is unrealistic. Measurements on the polarization state need to account for the fact that they are operating in a subspace of the quantum state of the photon. In addition, single photon detectors are imperfect devices with noise and inefficiencies.

The components involved in measuring photonic qubits are HWPs, polarizing beam splitters (PBS) and single photon detectors. As described before, half-wave plates are

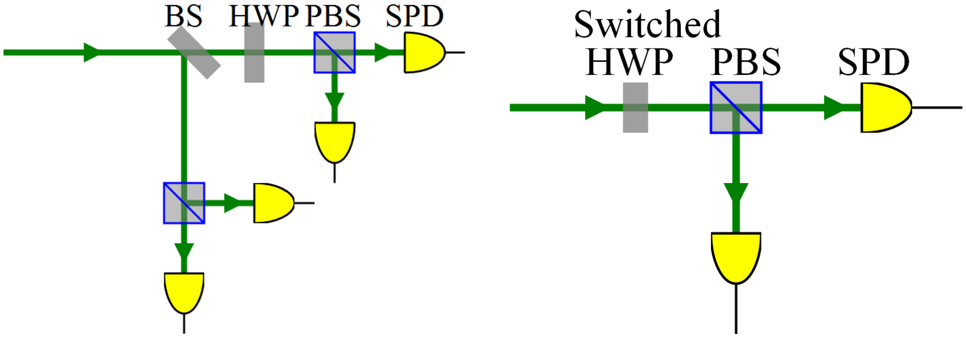


Figure 2.8: Polarization analysis module with a passive basis choice and with an active basis choice

made with phase retarders. If a HWP is used to actively switch the polarization state, this is called an active measurement, if instead the photons go through a 50:50 beam splitter where one path is rotated by 45 degrees and one isn't, this is called a passive measurement. The difference between active and passive measurements is illustrated in 2.8.

PBSs are made by stacking several layers of dielectric material together so that the Brewster angle is at 45 degrees to the incident light. This means that at each layer of the material, some of the unpolarized incident light is reflected and polarized in the V basis. This also means that if H polarized light is incident on the PBS it will be transmitted, while V polarized light will be reflected. Couplers are positioned to pick off the transmitted and reflected light and are then sent into single photon detectors.

If the single photon detector in the reflected path 'clicks' meaning it registered a detection event, and the single photon detector in the transmitted path does not, we have measured the qubit to be in the $|1\rangle$ state, and the oposite means the qubit is in the state $|0\rangle$ state. If we want to measure in the diagonal basis, we can put a HWP before the PBS, which will rotate the qubit into the rectilinear basis for measurement.

However, the single photon detectors used in these experiments are 'bucket' type detectors, meaning they are sensitive to single photons but will also click in the presence of multiple photons. Thus, in simulation of quantum optics systems, it is important to use mathematical models of bucket detectors when dealing with detections.

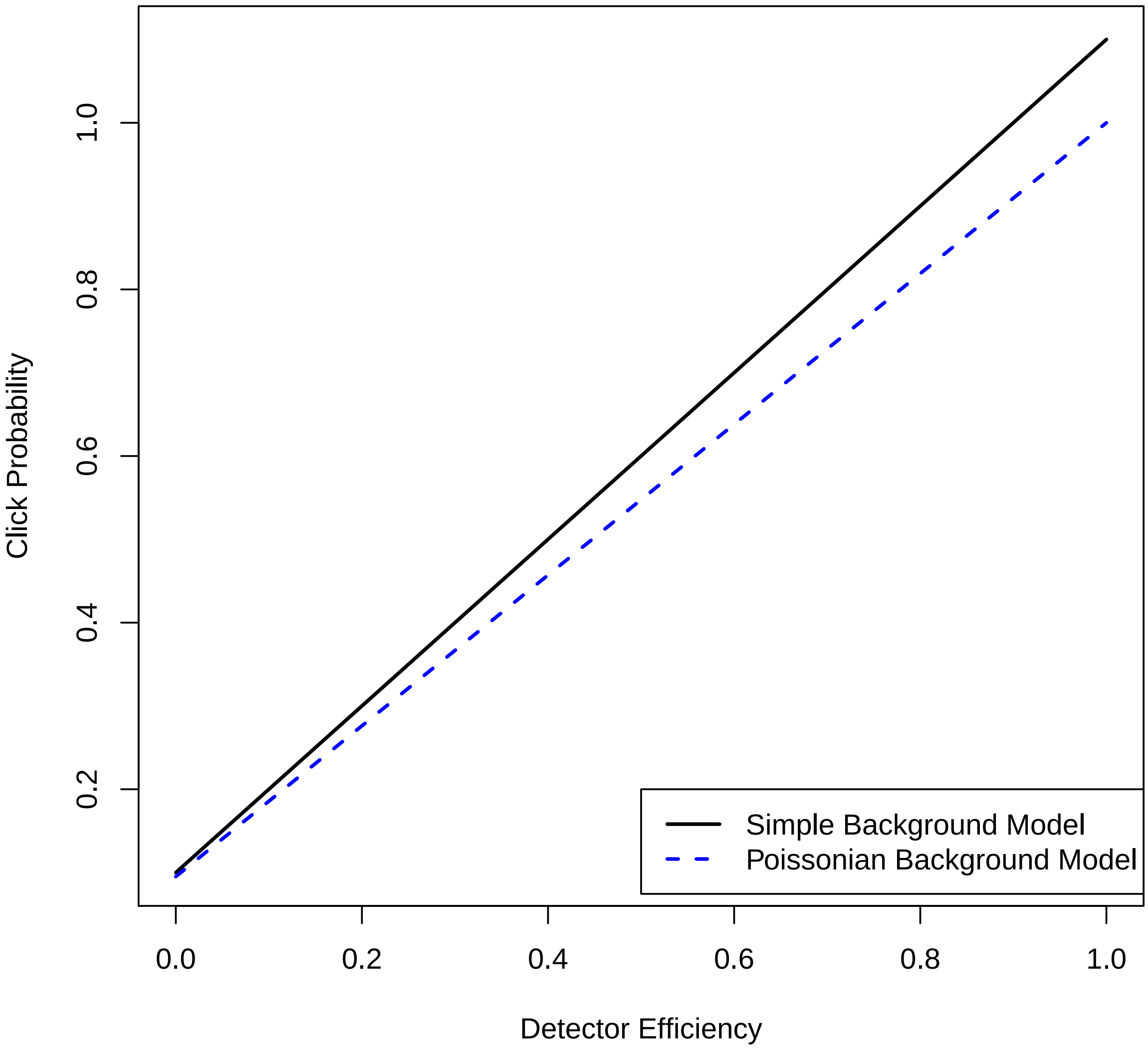


Figure 2.9: Detector click probabilities considering a single photon incident on both detectors versus channel efficiency. The detector dark count probability is 0.1. Note that the probability of clicking in the simple model exceeds 1 for efficient channels, while the poissonian model is always less than one. When the dark count probability is zero, these models reduce to the same value.

2.4.3 Mathematical Models of Single Photon Detectors

In Jennewein et al.'s paper [52] in which they model several components in linear optics quantum computing, they model 'bucket' detectors, meaning they 'click' if they observe any light at all, and do not 'click' otherwise, as:

$$P(c|i) = 1 - (1-\eta)^i + n \tag{2.32}$$

Where η is the detector efficiency, n is the dark count probability, and i is the number of incident photons within the time resolution of the detectors.

However, this model assumes a flat rate of detector dark counts. If we assume instead that detector dark counts follow a poissonian distribution, then we should use the following model, built from Lee et al.'s [66] model of photon-number discriminating detectors. A very simple model for a photon-number discriminating detector is:

$$P(k|i) = \binom{i}{k} \eta^k (1-\eta)^{i-k} \tag{2.33}$$

This is the probability of the detector reporting a detection of k photons given i incident photons, where η is the detection probability of each individual photon. This is a binomial distribution, as we are trying to sum over all the possible ways of getting k photons given i incident photons.

Suppose we have a distribution of dark counts, where $D(d)$ is the probability that there are d dark counts at once. This distribution sums to one. The above model is then modified to be:

$$P(k|i) = \sum_{d=0}^{\infty} D(d) \binom{i}{k-d} \eta^{k-d} (1-\eta)^{i-k+d} \tag{2.34}$$

To get this model, we sum over all of the cases of different number of dark counts. The previous equation must have its lower index modified from k to $k-d$, because now we want to know, given that we have d dark counts, how many additional photons i can be detected (and in how many permutations) and still add up to k photons over all.

We can turn this photon-number discriminating detector into a bucket detector by summing over all of the detection probabilities from 0 to infinity. The probability of clicking given an incident number of photons i is:

$$P(c|i) = \sum_{k=1}^{\infty} \sum_{d=0}^{k} D(n,d) \binom{i}{k-d} \eta^{k-d} (1-\eta)^{i-k+d} \tag{2.35}$$

Alice's sending bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Alice's sending basis	D	R	D	R	R	R	R	R	D	D	R	D	D	R	R
Alice sends	+	V	-	H	V	V	H	H	-	+	V	-	+	H	V
Bob's measurement basis	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bob's measured bits	1	0	1	0	1	0	0	0	1	1	1	1	1	0	1
Public Discussion															
Bits after basis reconciliation			1	0	1			0	1			1		0	1
Bits after sifting			1					0				1		0	

Table 2.3: A sample key distribution with BB84. R means rectilinear basis, D means diagonal basis. Adapted from [10].

In this model, η is the detector efficiency, n is the detector dark count probability within a detection window and $D(n, d) = exp(-n)\frac{n^d}{d!}$. These two models are compared in figure 2.4.3.

2.5 Quantum Key Distribution Protocols

The idea of using quantum physics for encryption was Stephen Wiesner's Conjugate Coding manuscript which proposed using quantum states to make un-counterfeitable money [116]. Based on this work, Bennett and Brassard were inspired to propose using quantum states for quantum key distribution [10]. This work is commonly referred to as 'BB84', and the security of this protocol is based on the no-cloning theorem. However, this protocol is very susceptible to attack, and in 1992 Ekert proposed a method of quantum key distribution with entangled photons where the security is based on both the no-cloning theorem and Bell's theorem.

2.5.1 Quantum Key Distribution with single photons

The BB84 key distribution protocol involves one party (commonly referred to as Alice) preparing and sending a quantum state along a public channel to another party (referred to as Bob) which has the possibility of being interrupted by a hostile party (referred to as Eve). BB84 proceeds as follows. Alice generates a string of random bits (perhaps from a Quantum Random Number Generator (QRNG)). She uses this string of random bits to determine what bit to send as well as what basis, either rectilinear or diagonal to send the bit in. If the basis is rectilinear, she sends photons in either the $|H\rangle$ or $|V\rangle$ polarization states, if the basis is diagonal, she sends either the $|+\rangle$ or $|-\rangle$ polarization states.

At the other end of the channel, Bob performs measurements on each individual qubit as they arrive in either the rectilinear and diagonal bases. His measurement bases are chosen at random. Bob then announces what bases were used to measure his qubits. Alice will then either confirm or gainsay Bob's measurements. The bits where Alice and Bob prepared and measured in the same basis are kept, and all others are discarded, as Bob's measurements will be random.

Next, Alice and Bob need to check for errors. Assuming that Alice prepares single photon states, if Eve intercepts the qubit measures it in the wrong basis, and then prepares the result of her measurement and sends it along the channel to Bob, her state will be essentially random noise. This will introduce errors into Alice and Bob's shared key.

If Alice and Bob's quantum bit error rate (QBER) is below a certain percentage, defined to be the maximum possible error rate that Eve could introduce into their shared key and acquire any useful information, they can conclude that their communication has not eavesdropped on, and thus they are the only people with knowledge of the key. Proofs of the lower bound on this percentage are presented in 2.6.1.

2.5.2 Quantum Key Distribution with Entanglement

In 1991, while working with David Deutsch, Artur Ekert discovered a second form of quantum key distribution independently from Bennett and Brassard. In his formulation, Alice and Bob each receive a half of an entangled photon source [27]. The source may be controlled by Eve, but they can assure themselves of the security of their system by performing a Bell test. Other than that, the protocol is very similar to BB84. In fact, Gisin et al. [38] have pointed out that E91 is the same as BB84, if the preparation operation is moved until after the state is created.

Bennett and Brassard published a letter criticizing this protocol soon after. They claimed that the Bell test was not necessary for security [11]. Since performing a Bell test requires three bases instead of 2, the probability that Alice and Bob have guessed the same basis is $\frac{2}{9}$, rather than $\frac{1}{2}$ in the 2-basis BB84 protocol. In their criticism, they published a modification of E91 which performs QKD with entangled photons in 2 bases. This protocol is refered to as BBM92.

2.6 Practical QKD Considerations

2.6.1 Post-Processing

It is important for security considerations to know the error rate, meaning the coincidences where two of the same photon are measured, or cases where orthogonal measurements in either of Alice or Bob's detection modules are measured.

We define the QBER as:

$$\mathcal{D} = \frac{N_{bad}}{N_{total}} \tag{2.36}$$

where N_{bad} is the number of bad events, and N_{total} is the total number of events.

When we measure the polarization state of the qubits using single photon detectors we are measuring only a subspace of the photon's total state. When we measure detector double clicks, when Alice or Bob's H/V or +/- detectors click simultaneously, we must assign them to random measurements, as imposed by [59]. Thus, our modified QBER given double clicks is:

$$\mathcal{D} = \frac{N_{bad}}{N_{total}} + \frac{0.5(N_{Alicedouble} + N_{Bobdouble})}{N_{total}} + \frac{0.25N_{bothdouble}}{N_{total}} \tag{2.37}$$

This holds for active measurements, where only measurements in a single basis at the same time. For passive measurements, correctly post-processing is more complicated, because there are four detectors working simultaneously. Two methods have been suggested for dealing with this. In the first option, cases where clicks in conflicting bases are measured are discarded. In the second, these cases are assigned to random bit values [39].

Knowing the QBER is important for two reasons - first, it is important in eavesdropper detection, and secondly, it is important in estimating the key rate of QKD systems.

Errors due to Eavesdroppers

Given the transmission and measurement of qubits over a public channel, what is the minimum possible error rate that an eavesdropper could introduce? A first intuitive estimate would be 25 %, as the eavesdropper has a 50% chance of measuring in the wrong basis, and then a 50% chance of sending on the wrong bit value. This assumes that Eve can only intercept and resend qubits and measure them in the same bases as Bob.

If Eve can choose any measurement basis, meaning she can perform any unitary operation on Alice and Bob's qubits, then she can capture the same amount of mutual information to Bob as between Bob and Alice while causing fewer errors. The following is a synopsis of the proof first derived by Fuchs et al. ([37]) as described by Gisin et al. in [38]. Suppose Eve has a 'probe' that can interact with the qubit state being sent to Bob [4]. She can apply unitary operators to the combined qubit and probe operators with the effect:

$$U|0\rangle_{qubit} \otimes |0\rangle_{probe} = |0\rangle \otimes \phi_0 + |1\rangle \otimes \theta_0 \tag{2.38}$$

$$U|1\rangle_{qubit} \otimes |0\rangle_{probe} = |1\rangle \otimes \phi_1 + |0\rangle \otimes \theta_1 \tag{2.39}$$

Assuming a perfect channel, this means that the fidelity of Bob's measurements will be $|\phi_0|^2 = |\phi_1|^2 = \mathcal{F}$, and his QBER will be $|\theta_0|^2 = |\theta_1|^2 = \mathcal{D}$. The maximum probability for distinguishing two states with overlap $\langle\phi|\psi\rangle = cos(x)$ is $P = \frac{1+sin(x)}{2}$ (a proof of this can be found in [88]). If we set $\langle\phi_0|\phi_1\rangle = \mathcal{F}cos(x)$ and $\langle\theta_0|\theta_1\rangle = \mathcal{D}cos(y)$, that means that the mutual information between Alice and Eve is:

$$I(\alpha,\epsilon) = \mathcal{F}(1 - H(\frac{1+sin(x)}{2})) + \mathcal{D}(1 - H(\frac{1+sin(y)}{2})) \tag{2.40}$$

This equation is maximized when $x = y$. With a few assumptions, it can be shown that $\mathcal{D} = \frac{1-cos(x)}{2}$ (see appendix section C.2 for complete details). This means that the maximum mutual information between Alice and Eve is:

$$I_{max}(\alpha,\epsilon) = 1 - H(\frac{1+sin(x)}{2}) \tag{2.41}$$

where $H(x)$ is the Shannon information as described in the next section 2.50. This appears very similar to the equation for Alice and Bob's mutual information:

$$I(\alpha,\beta) = 1 - H(\mathcal{D}) \tag{2.42}$$

In order to have a system where secrets can be shared, the mutual information between Alice and Bob must be larger than the mutual information between Alice and Eve. With a

[4] For the purposes of this explanation, BB84 will be used, but it can be extended to BB92 by assuming that Alice's state is the basis used to send Bob's state, and that in this case fidelity $\mathcal{F}$ is the inner product between Alice and Bob's qubits, rather than between the state Alice sends and Bob measures.

little re-arranging, we can see that equations 2.42 and 2.41 will intersect when $tan(x) = -1$. Thus,

$$\mathcal{D} = \frac{1 - cos(\frac{\pi}{4})}{2} = \frac{2 + \sqrt{2}}{4} \approx 15\% \tag{2.43}$$

However, this is not the final, largest amount of error that Eve can introduce, as we have assumed that Eve probes each qubit individually. What if Eve can perform attacks on an ensemble of qubits?

An 'ultimate' proof of the security proposed by Gisin et al. [38] relies on two intuitive theorems. First, as used above, that Alice and Bob can share secrets only if the mutual information between them is larger than the mutual information of either Eve and Alice or Eve and Bob:

$$\begin{aligned} I(\alpha, \beta) &\geq I(\alpha, \epsilon) && (2.44) \\ &\geq I(\beta, \epsilon) && (2.45) \end{aligned}$$

The second assumption is that the sum of the mutual information between Alice and Bob and Alice and Eve must be equal to the number of bits, meaning that Eve and Bob can't get any more information than what Alice generates:

$$I(\alpha, \beta) + I(\alpha, \epsilon) = n \tag{2.46}$$

Combining these two theorems, we get that the mutual information between Alice and Bob must be greater than half of the number of bits sent:

$$I(\alpha, \beta) \geq \frac{n}{2} \tag{2.47}$$

Using the Shannon mutual information, $I(\alpha, \beta) = n(\mathcal{D}\log_2(\mathcal{D}) + (1 - \mathcal{D})\log_2(1 - \mathcal{D}))$, this means that the largest error that can be introduced by Eve within a secure system occurs when:

$$\mathcal{D}\log_2(\mathcal{D}) + (1 - \mathcal{D})\log_2(1 - \mathcal{D}) = \frac{1}{2} \tag{2.48}$$

Solving this numerically, we get $\mathcal{D} \approx 11\%$.

2.6.2 Key Rate Estimation

After Alice and Bob compare bases, and check the error rate during the sifting step, two final processes bound the limit of their key rate: error correction and privacy amplication.

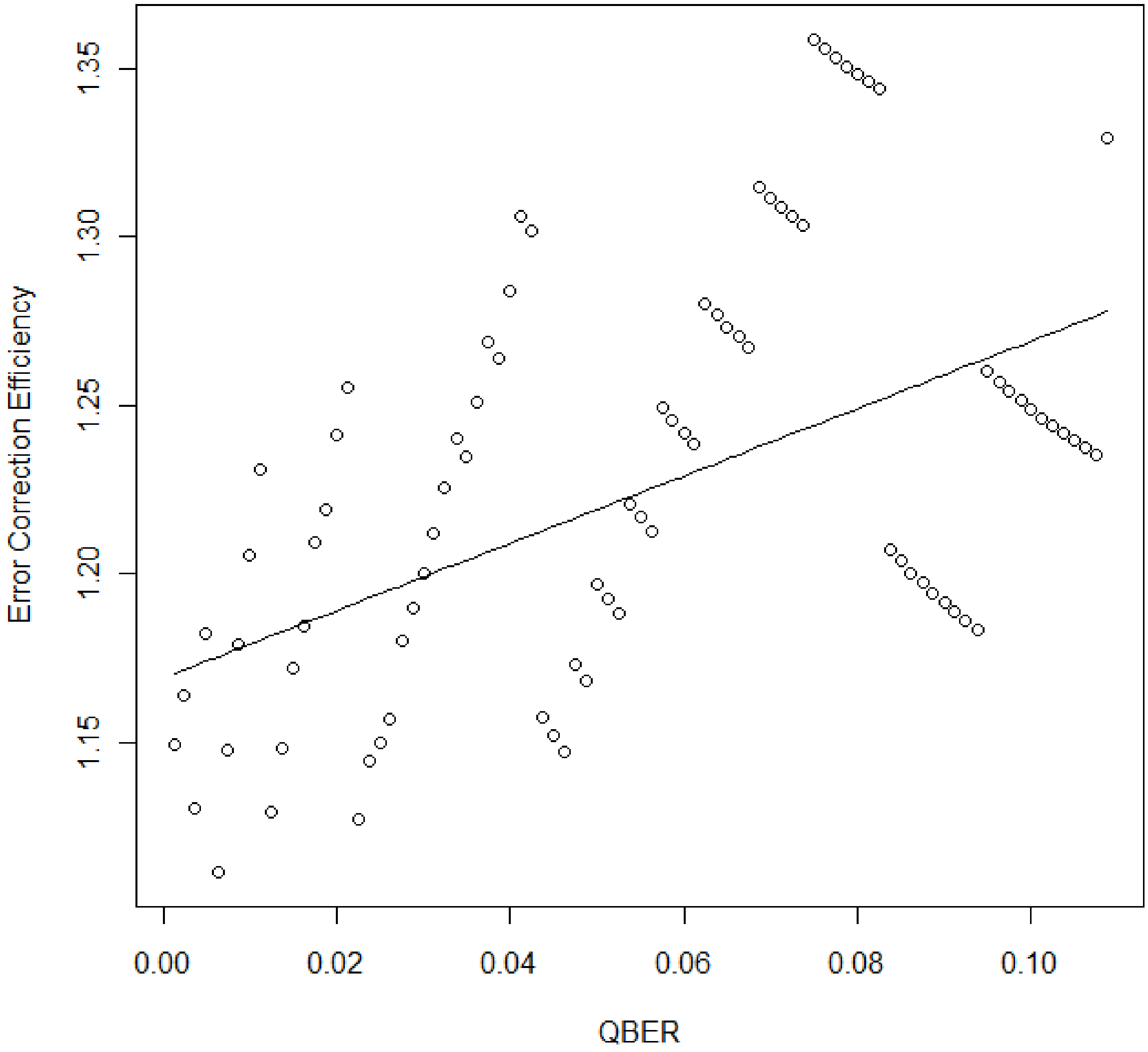


Figure 2.10: The error correction efficiency of Brassard and Salvail's [14] CASCADE algorithm for various rates of QBER. The data points are derived from equation 2.54 with 100 rounds of error correction, and a block length chosen such that the initial errors per block is $E_1 \leq -\frac{ln(\frac{1}{2})}{2}$. The values for error correction are discrete due to the rounding of integers in the calculation of the amount of information shared in error correction. The plotted line corresponds to the equation $f(\mathcal{D}) = 1.169 + \mathcal{D}$.

Error Correction

Some errors will occur in the sifted key after Alice and Bob compare bases. Alice and Bob will have to use error correction to ensure that their final key is identical. They can do this by using a parity check matrix, where they use part of their sifted key to become reasonably sure that the remainder of their sifted key contains no errors.

In the limit of a large number of bits, Shannon discovered a function for the minimum amount of information needed to correct two identical strings of bits [97]. Subtracting this from the sifted key rate, we find a total key rate of:

$$N_{corrected} = N_{sifted}(1 - f(\mathcal{D})H(\mathcal{D})) \tag{2.49}$$

where

$$H(\mathcal{D}) = -\mathcal{D}\log_2 \mathcal{D} - (1-\mathcal{D})\log_2(1-\mathcal{D}) \tag{2.50}$$

is the Shannon binary entropy function, and $f(\mathcal{D})$ is the error correction efficiency. The Shannon limit for the best possible error correction is $f(\mathcal{D}) \geq 1$. In the QKD experiments in this thesis, Brassard and Salvail's CASCADE algorithm for error correction [14] was used.

CASCADE consist of several rounds of parity checking followed by a binary search to determine the source of error. After the sifting step, Alice and Bob divide their key into sections of length k_1. The report the parity of each of their sections, meaning they add up the number of ones in their string and report whether their number is odd or even. If they report different results, they know that they have at least one error.

For each of the sections of their strings that differ in parity, Alice and Bob then perform a binary search method of comparing their parities. This means that they split the section of interest in half, and then compare the parity of the half. If their parities are the same, they know there must still be at least one error in the other half, if their parities are different they know their must be an error in the half examined. They continue this procedure until they have isolated the bit that must be an error and correct it.

After the binary search method, Alice and Bob repeat the procedure of checking sections. For each of the next rounds of error correction, they use a $k_n \geq k_1$ based on a previously determined function.

Assuming the errors are distributed according to a binomial distribution, this means that probability that there is an error in an initial block of length j is:

$$\delta(j) = prob(X = 2j) + prob(X = 2j + 1) \tag{2.51}$$

where $X = \binom{k_1}{\mathcal{D}}$. The expected number of errors per block before error correction is then [5]:

$$E_1 = 2 \sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor} \delta(j) = k_1 \mathcal{D} - \frac{1-(1-\mathcal{D})^{k_1}}{2} \tag{2.52}$$

Brassard and Salvail suggest that the initial k_1 be chosen so that on average the starting number of errors in a block is $E_1 \leq -\frac{ln(\frac{1}{2})}{2}$. With a bit more work, Brassard and Salvail can put the upper bound on the amount of information shared in error correction for ω rounds of error correction as:

$$I(\omega) \leq 2 + \frac{1-(1-\mathcal{D})^{k_1}}{2} \lceil \log k_1 \rceil + 2 \sum_{l=2}^{\omega} \sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor} \frac{j\delta(j)}{2^{l-1}} \lceil \log k_1 \rceil \tag{2.53}$$

From this bound, we can estimate the error correction efficiency by dividing this information by the entropy of the original block:

$$f(\mathcal{D}) = \frac{I(\infty)}{k_1 H(\mathcal{D})} \tag{2.54}$$

Due to the rounding of integers in choosing the initial block size, $f(\mathcal{D})$ is not a continuous function. It can be roughly interpolated as a linear function [83]. A plot of the various values for $f(\mathcal{D})$ compared to a linear function are presented in fig. 2.6.2. Error correction efficiencies were calculated using 100 rounds of error correction, however, the amount of information leaked reached an asymptotic limit around 5 passes.

The CASCADE algorithm is not really the fastest or more efficient error correction method, as it requires a lot of classical communication. Recently, there has been some promising work in the use of low density parity check (LDPC) matrices[28, 29] which has been used in a real-world implementation of QKD [92]. However, most implementations still use CASCADE, including those in this thesis.

Privacy Amplification

In addition, Alice and Bob will need to perform privacy amplification to reduce the fraction of the key that any eavesdropper may have aquired to a exponentially small amount. Using

[5] In this thesis, the notation $\lfloor x \rfloor$ means x rounded down to the nearest integer, and $\lceil x \rceil$ means x rounded up to the nearest integer.

the key estimation provided in Ma et al.'s theoretical analysis of an polarization-entangled photon source from SPDC sources [70], the fraction of the key that must be given up to privacy amplication is equal to the Shannon binary entropy function of the QBER. Thus, the final key in the limit of many keys shared is:

$$N_{final} \geq N_{sifted}(1 - f(\mathcal{D})H(\mathcal{D}) - H(\mathcal{D})) \tag{2.55}$$

However, this assumes that Eve's information is purely classical. If we consider that Eve may have a quantum state, then we must return to the Holevo bound [85]:

$$N_{final} \geq S([Z \otimes \rho]) - S([\rho]) \tag{2.56}$$

2.7 Conclusions

In this chapter I have attempted to demonstrate the possibility of using polarization state of light as a qubit state. I have also described the process for creating bell states from optical processes, as well as the method of measuring optical qubits. I have described a QKD protocol with entangled photon states, the security estimates on this protocol, and a realistic estimation of how much of the pair measurements are given up in the process of generating a key.

Chapter 3

QKD over Active Telecommunication Channels

The growth of e-commerce and internet communications has led to a plethora of investment in large inter-continental fiber optic links, including the $300 million dollar Emerald Express project, a 60Tbits/s link between Ireland and the USA set to begin operation in 2013, and the billion dollar WASACE network which should connect Brazil to North America, Europe and Africa in time for the 2014 FIFA world cup.

Given the growth in fiber optics infrastructure, the construction of a system which can perform key growth via quantum key distribution protocols on an active telecommunications network, with minimal effort or disruption to classical traffic, would be a disruptive technology.

3.1 Fiber-Based QKD demonstrations

QKD has been demonstrated several times in dark optical fibers, that is, fibers with no other light than the quantum signal. It has also been demonstrated on active telecommunications networks, occupying part of the DWDM spectrum [17, 80, 30, 64, 19]. Chapuran et al. [17] used 1310 nm light for the quantum signal, and had to reduce the power level of the classical communication from 2 dBm to -8 dBm. Choi et al. [19] placed their quantum signals at 1290 nm, and had to reduce the power of the classical signals so that it would be at 20% of the minimum threshold data. This reduced the visibility of the classical data and resulted in a slower classical data rate. Lancho et al. [64] occupied the 1550 nm part

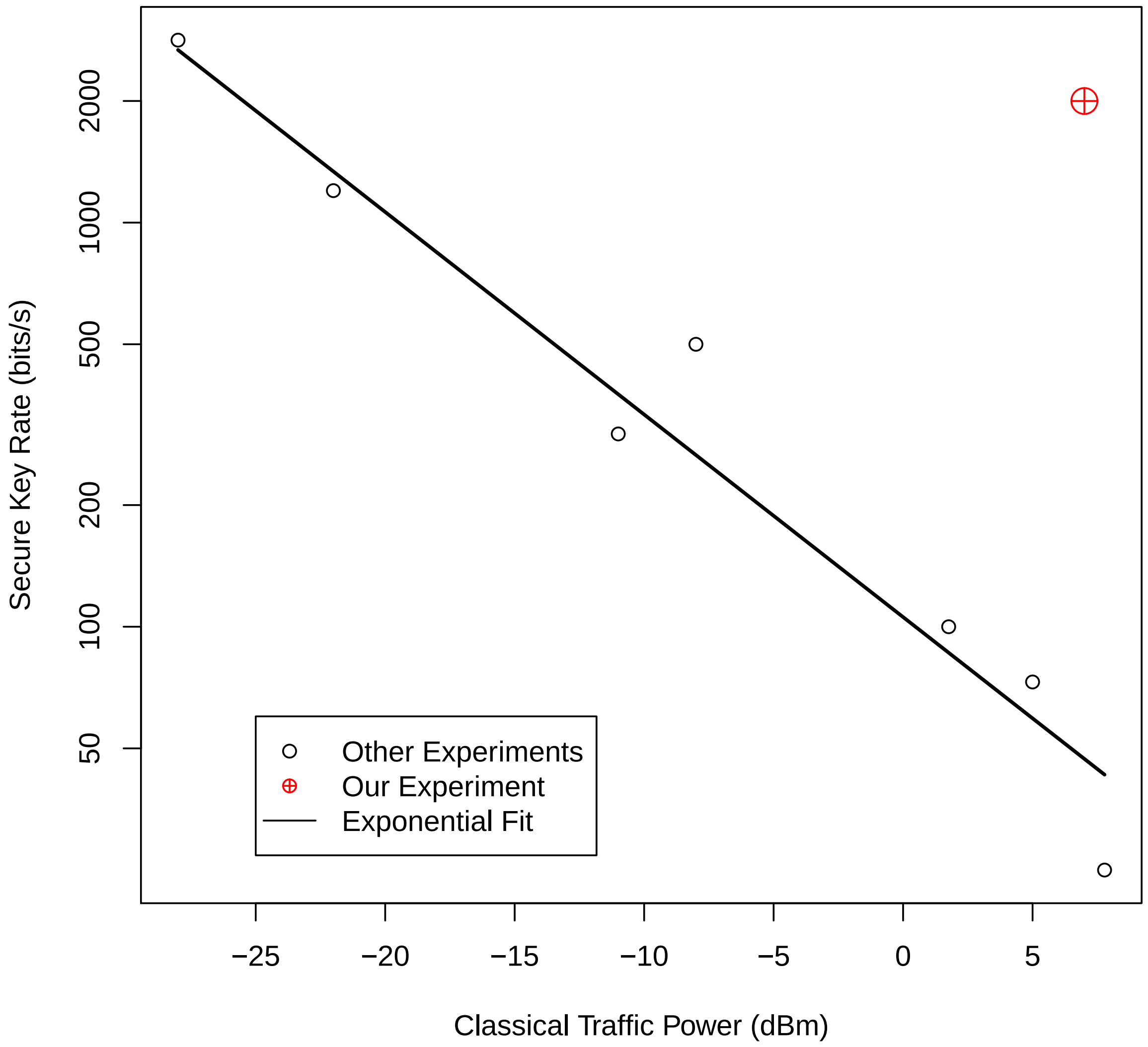


Figure 3.1: A comparison of the key rates at 1 km of telecommunications fiber between this and other experiments and the optical power of the classical traffic, (results from [17, 80, 30, 19]).

Experiment	Channel	Distance	Coincidence Rate	Secure Key Rate
Jennewein et al., 2000 [50]	dark fiber	1 km	1700 c/s	400 bits/s
Poppe et al., 2004 [82]	dark fiber	1.45 km	1200 c/s	76 bits/s
Hubel et al., 2007 [46]	dark telecom fiber	101 km	105 c/s	35 bits/s*
Erven et al., 2008 [33]	free-space	1.6 km	1200 c/s	85 bits/s
Dynes et al., 2009 [25]	dark fiber	200 km		0.1 bits/s
Scheidl et al., 2009 [94]	free-space	288 km	26000 c/s	24 bits/s*
Meyer-Scott et al., 2010 [73]	dark telecom fiber	4 km	3600 c/s	850 bits/s*
Holloway et al., 2011 [44]	active telecom fiber	6 km	1000 c/s	14 bits/s*

Table 3.1: Selected demonstrations of QKD with entangled photon sources. The secure key rates with stars indicate estimated rates from QBER and coincidence rates while the non-star values were the rates in a secure key exchange.

Experiment	Distance	Key Rate at 1 km (bits/s)	Classical Power rate at 1 km (dBm)
Chapuran et al., [17]	10 km	500	-8
		25	6
Peters et al., [80]	25 km	300	-11
		100	1.76
		73	5
Eraerds et al., [30]	50 km	2829	-28
Lancho et al., [64]	10 km	500	Unspecified
Choi et al., [19]	10 km	1200	-22

Table 3.2: Selected previous experiments with BB84 over active telecommunications fibers.

Standard Name	Wavelength (nm)	SM/MMF	Fiber Length	Speed
10GBASE-SR	850	MM	26 m	10.3125 Gbit/s
10GBASE-LR	1310	SM	10 km	10.3125 Gbit/s
10GBASE-LRM	1310	MM	220 m	10.3125 Gbit/s
10GBASE-ER	1550	SM	40 km	10.3125 Gbit/s
10GBASE-ZR	1550	SM	80 km	10.3125 Gbit/s
10GBASE-LX4	1310	SM/MM	10 km/300 m	10.3125 Gbit/s
40GBASE-SR4	1310	MM	125 m	41.25 Gbit/s
40GBASE-LR4	1310	SM	10 km	41.25 Gbit/s
100GBASE-SR10	1310	MM	125 m	103.125 Gbit/s
100GBASE-LR4	1310	SM	10 km	103.125 Gbit/s
100GBASE-ER4	1550	SM	40 km	103.125 Gbit/s

Table 3.3: Fiber optic ethernet standards (as defined by the IEEE).

of a classical communication protocol, which has been set aside for video broadcast but is currently underused. However, given the current interest in the 1550 nm band for fiber optic communication, it is unlikely that this band will be underused for long. Eraerds et al. [30] demonstrated QKD using a wavelength in the O band of a DWDM system, however, in order to keep the Raman scattering low, they had to restrict the power of their classical signals to -28 dBm, and this reduced the data rate to 1 Gbps. Peters et al. [80] did the same, but instead of reducing the classical power, attempted to filter out the noise in their quantum channel. Unfortunately, this meant that their key rates were very low (20 bit/s at 1 km at 1.75 dBm of classical power). A comparison between the secure key rate and the classical traffic power for all of these experiments is presented in figure 3.1.

In this chapter, I will show that, by putting the quantum signal at 810 nm, we can take advantage of low mixing rates to show higher rates of secure key generation, over longer distances, at higher data rates, and at higher classical powers (1 kb/s of key, 2 km of fiber, 7 dBm classical laser power, and 100 MBps.) using a very simple method of combining signals. Unlike the other attempts to combine quantum and classical signals, we do nothing to alter the classical signals or the operation of the transceiver or receiver. Our method of performing QKD is thus compatible with all of the commercially available fiber optics protocols.

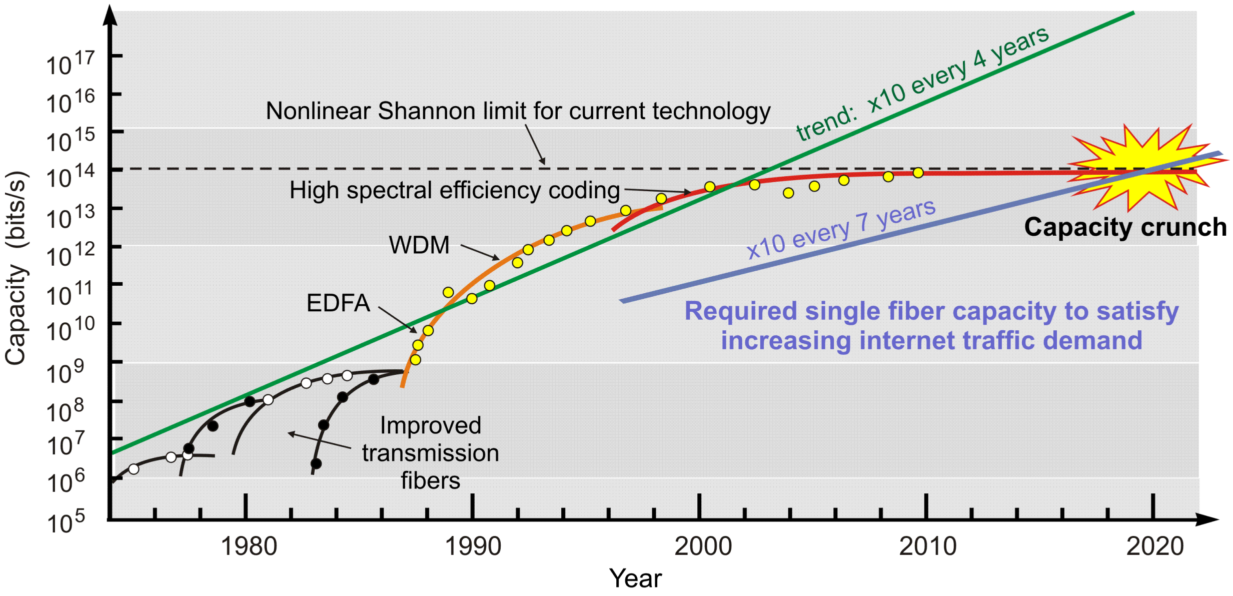


Figure 3.2: Demand and capacity for information in fiber optic channels. Graph courtesy of Neng Bai.

3.1.1 Optical Telecommunications Networks

Two factors are the primary limitations to optical telecommunications networks: attenuation and chromatic dispersion. Attenuation is the decline in the power of the optical signal due to absorption or scattering. For a more in-depth discussion of the effects that lead to attenuation, see section 4.1.1 and figure (4.1). Attenuation is typically measured in decibles of signal per kilometer of fiber (dB/km). Chromatic dispersion is the phenomena of different input wavelengths having different travel times through materials, which leads to pulse broadening which can introduce noise. Chromatic dispersion is typically measured in picoseconds of delay in arrival times per nanometer wavelength of the signal per kilometer of fiber (ps/km-nm).

Most fiber optic communications networks operate in the C-Band (conventional-band), defined as 1.53-1.57 μm. At this range, the attenuation of optical power in fiber is minimized (currently around 0.16 dB/km), but the chromatic dispersion is not (+80 dB/km-nm). The O-Band (original-band), defined as 1.26-1.36 μm and is used because the chromatic dispersion for silica passes through zero at 1.31 μm (with an attenuation of 0.3 dB/km).

Although telecommunications networks use single-mode fibers at 1.55 μm, the fibers are not truely single mode and allow for wavelengths throughout the C band. Modern telecommunications networks use this fact to implement wavelength-division multiplexing (WDM), where channels at different wavelengths are used to carry multiple signals in the same fiber. Multiplexing and demultiplexing of wavelengths can be accomplished in many ways: diffraction gratings, thin-film filters, fiber bragg gratings, microring resonators, and arrayed waveguides. Arrayed waveguides are now the standard method of multiplexing/demultiplexing optical signals in optical networks.

Two categories of WDM are often used in fiber optics communications: Coarse-WDM (CWDM) and Dense-WDM (DWDM). In CWDM, few wavelengths are used, wavelengths in the O band are used in conjunction with the C band, and data is sent in both directions. The downstream data, for example from a hub to a customer, is transmitted at 1.55 μm, and the upstream data, from the customer to the hub, is transmitted at 1.31 μm. In DWDM, only the O-band is used and the wavelengths spacings are much shorter. A common standard of DWDM uses 40 channels, however researchers are constantly trying to improve the number of channels that can be used by reducing the spacing between wavelengths. The current record is 432 channels at 171 Gb/s [91].

For DWDM, the C-Band is preferred to the O-Band because the higher the chromatic dispersion, the less cross-phase-modulation (the interaction between two wavelength channels), since as the wavelengths travel further away from each other in time, they are less likely to collide [99]. Larger chromatic dispersions can also help to reduce four-wave -mixing processes [107].

In order to achieve smaller and smaller gaps between channels, low-bandwidth, extremely stable lasers must be used. An active area of research into better lasers for DWDM is in optical frequency combs [24]. In addition, many mixing processes begin to occur when the channels are so close in wavelength. A common solution is simply to use more power in order to improve the signal-to-noise ratio and apply a threshold to signal. Optical fiber networks have also been increased in channel capacity by using differential phase shift keying (DPSK) and exploiting spatial modes. DPSK is a fancy way of saying they encode two to eight channels into the polarization states of light [55]. By packing several cores together, it is possible to encode information into the spatial modes of light accross the cores and separate them at output [119].

The demand for telecommunications capacity has been increasing exponentially since the sixties and currently grows by 50 % every year. Figure 3.1.1 shows the demand for capacity, and the methods for providing this capacity. The current methods of dealing with this increased demand is in laying extra fibers under the ocean every few years, and adopting new forms of WDM that allow for more channels, encoded with higher precision wavelength or in the spatial and polarization mode of the light. However, considering the accelerating returns of information technology, these peace-meal measures will not be enough. Although this issue is not of primary concern to experimental quantum physicists, it does mean that the solutions implemented will leave less and less space for quantum key distribution if we want to take advantage of the growing fiber optic network.

Table 3.1.1 shows many of the standards set by the IEEE communications society. These standards are used for small networks, such as server rooms on a campus, or that connect a city or neighborhood. The large backbone links under the ocean are managed internally and have their own standards. The standards that involve multi-mode fibers are typically intended for very short distances - such as between to racks in a data center. Multimode fibers are used because there are fewer constraints on the stability of the spatial and spectral modes of the fibers and so cost less. Similarly, lasers at 1310 nm have been around for longer and can be made out of common semiconductor material, whereas lasers at 1550 nm require either stimulated emmission from a source of erbium or a raman source. Because of this, lasers at 1310 nm have historically been cheaper than 1550 nm lasers.

Although optical fiber communications are primarily used at the moment for very long distances (transatlantic links) and very short distances (between servers), several companies are investing in technologies categorized as fiber-to-the-x, where x is either the node (greater than 300 m away from the end user), the cabinet (less than 300 m away from the end user), to the home, and to the device (meaning the end user's computer). In Canada, a company called Intercontinental Atlantic, has put down over 600 km of optical fiber which extends from the transatlantic link hubs that touch down on the coast of Nova Scotia to downtown Halifax and all over the most populated areas of Nova Scotia and Newfoundland. Bell-Aliant, a telecommunications company in the Maritime provinces, has purchased operation time on this network, and is able to offer fiber-to-the-home to customers in Nova Scotia and Newfoundland. Large fiber bundles travel under the major arteries of Nova Scotia and Halifax, and smaller fiber bundles branch off of these travelling along the power lines. Customers on Bell-Aliant's fiber-to-the-home service can expect 250/30 Mbit/s download/upload. Fiber-to-the-home is likely to become more common in the future, but will require a large investment in order to make it out to Ontario due to the fact that the cables must be buried underground, compared to being dropped underwater as they are with transatlantic links.

As the demand for HD video and high-speed increases, the investment cost in these networks will be overcome and it will make commercial sense for fiber-to-the-home to be offered all over Canada. At the moment many fiber-to-the-x networks require active systems where the WDM signals are split up at a central hub and then re-amplified and sent to their respective end-point users. Passive systems, where there is one continuous optical mode between two end users, are available. These systems rely on end-point security. Passive networks will be cheaper overall to operate. Passive networks also have the advantage that the bulk of the information being sent is HD video, which does not require routing [16].

Given that these passive optical networks, with single-mode-fiber and fiber-to-the-home or fiber-to-the-device are becoming quite popular and commercially profitable, there is an opportunity for fiber-based networks to be operated between any two end users. In the experiment that follows, I demonstrate that QKD with entangled photons can be readily and cheaply integrated into existing telecommunications networks and protocols, while those networks are active and in use.

3.2 Experimental Design

3.2.1 Generation and Measurement of Entangled Photons

The entangled photons used in this work were produced from a Sagnac-loop through PP-KTP [35] built by Chris Erven for the free-space QKD demonstration [33].

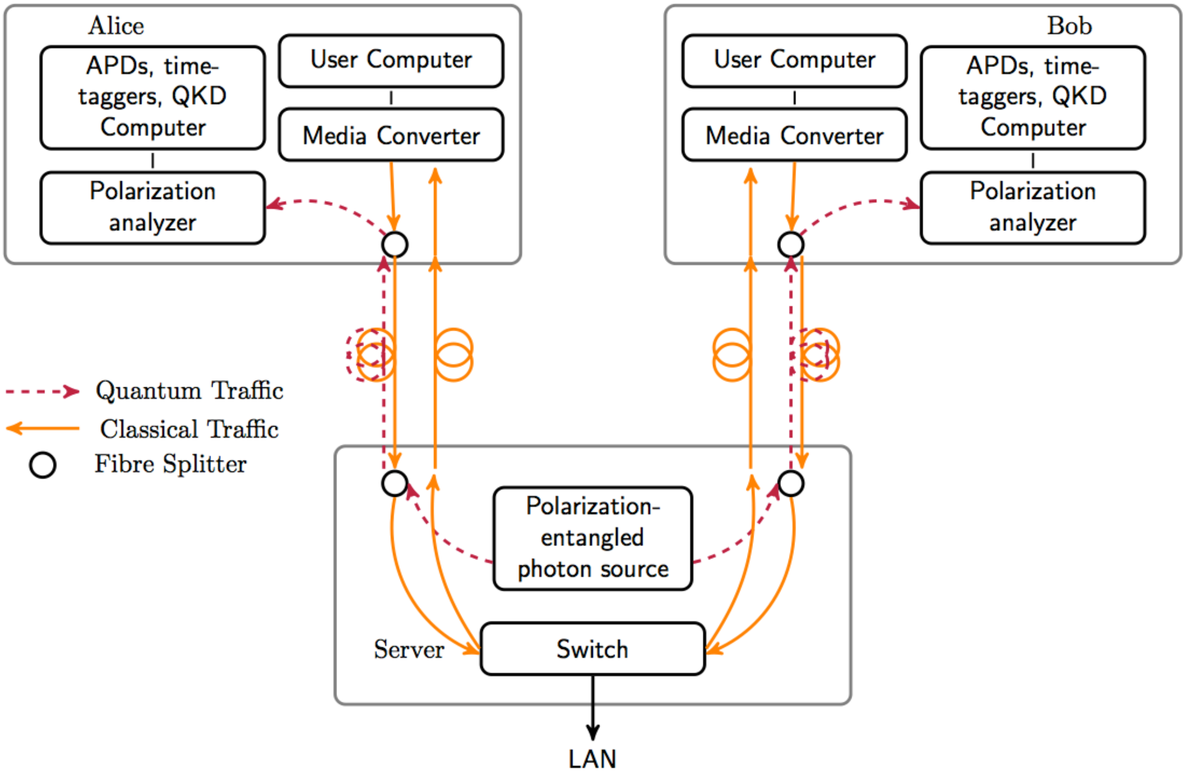


Figure 3.3: Experimental set-up for a demonstration of QKD on an active telecommunications network

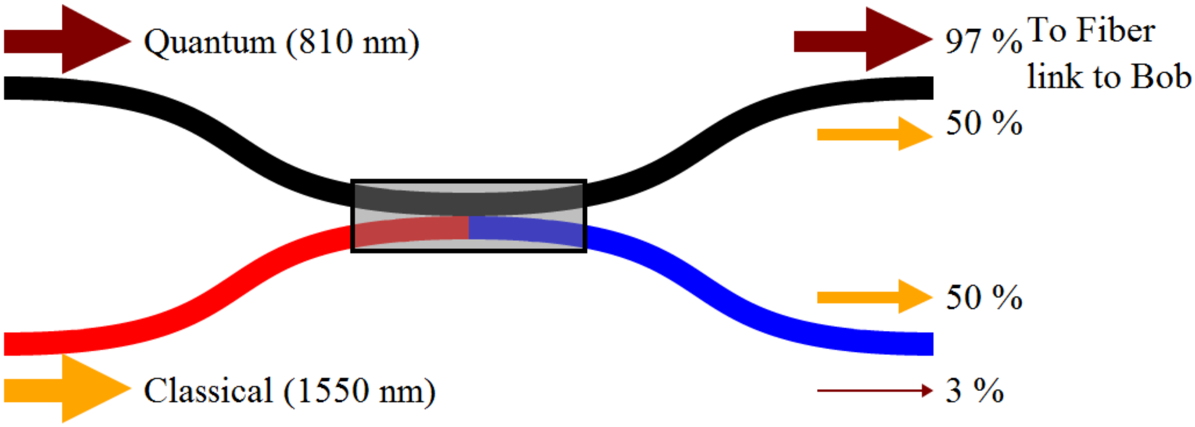


Figure 3.4: Measured transmissions for the fiber splitter (Thorlabs 10202A-50-FC) used to combine classical and quantum signals and extract the quantum signal. In this image, orange lines represent 1550 nm light, and maroon represents 810 nm light. Quantum signals were injected into the fiber using the black-to-black ends, and then extracted from the fiber using the black-to-black end. Classical signals used the red-to-black ends to enter the fiber and the black-to-blue ends to exit the fiber. Transmission was measured with a power meter.

As described in fig 3.2, the two outputs of the sagnac source were fed into two fused biconical taper fiber beamsplitters for 1550 nm light. The output of the Sagnac source will be henceforth be referred to as the 'quantum signal'. These beamsplitters evenly distribute input signals at 1550 nm amoung both outputs, but 810 nm light couples only weakly to one of the outputs and strongly to the other [90]. This concept is illustrated with the transmissions in figure 3.2, and is a very simple, elegant and cost-effective method of multiplexing and demultiplexing the quantum and classical signals.

3.2.2 Waveguide theory in Single Mode Fibers

Jackson's Classical Electrodynamics contains a brief overview of electromagnetic fields in Waveguides. A single mode fiber can be approximated as a cylindrical waveguide within a larger cylindrical waveguide. Due to the cylindrical geometry, it is possible to assume travelling waves along the axis of the cylinder. Using this assumption, it is possible to combine Maxwell's equations into the Helmholtz wave equation:

$$\nabla^2 E + (\frac{n(r)\omega}{c})^2 E = 0 \tag{3.1}$$

In single mode fibers, $n(r)$ is a step function, with a higher index of refraction at the centre than at the edges. This means that the solution will have two different regions, where a is the radius of the core:

$$\begin{aligned} u(\rho,\phi) &\propto J_m(\gamma\rho)e^{im\phi}, & \rho < a \qquad (3.2)\\ &\propto K_m(\beta\rho)e^{im\phi}, & \rho > a \qquad (3.3)\end{aligned}$$

Where $\gamma^2 = n_1^2\omega^2/c^2 - k_z^2$, and $\beta^2 = k_z^2 - n_2^2\omega^2/c^2$. SMF28 has a core radius of 4.1 μm. The core index of refraction can be found using the Sellemeier equation for fused silica [1]. In order to find k_z, the equation:

$$\gamma\rho\frac{J_1(\gamma\rho)}{J_1(\gamma\rho)} = \beta\rho\frac{J_1(\gamma\rho)}{J_1(\gamma\rho)} \tag{3.4}$$

Note that in order to achieve the graphs in figure 3.2.2, the equation 3.2 must be normalized.

Fibers are defined by their "mode parameter", which is $V = \sqrt{n_1^2 - n_2^2}2\pi a/\lambda$. If $V < 2.405$, the fiber has one mode for that wavelength. The V parameter for SMF28 is

[1] http://refractiveindex.info/?group=GLASSES&material=F_SILICA

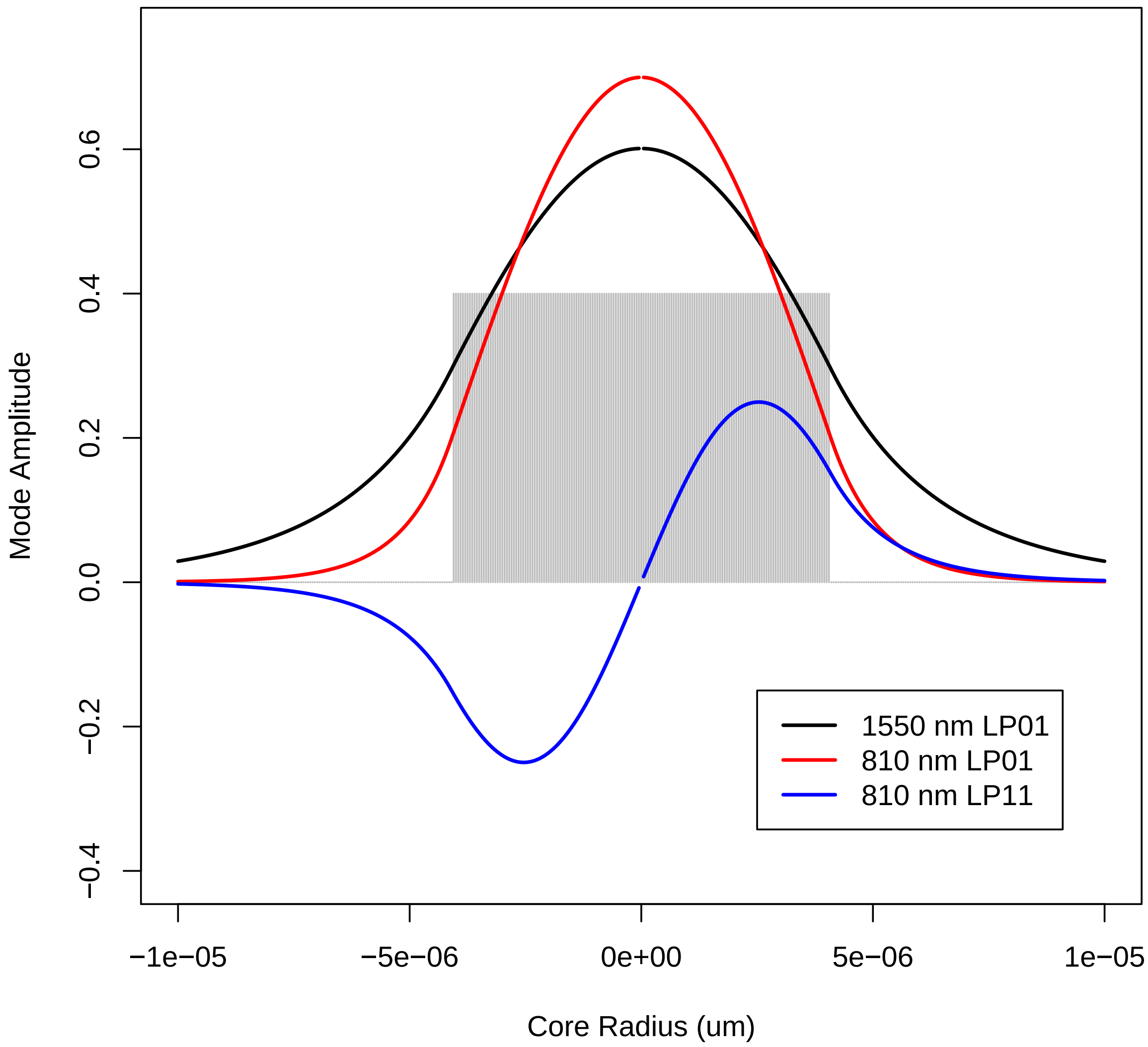


Figure 3.5: The first mode for 1550 nm and the first two spatial modes of 810 nm plotted with the profile of the difference (in percent) between the indices of refraction for the core and cladding for SMF28.

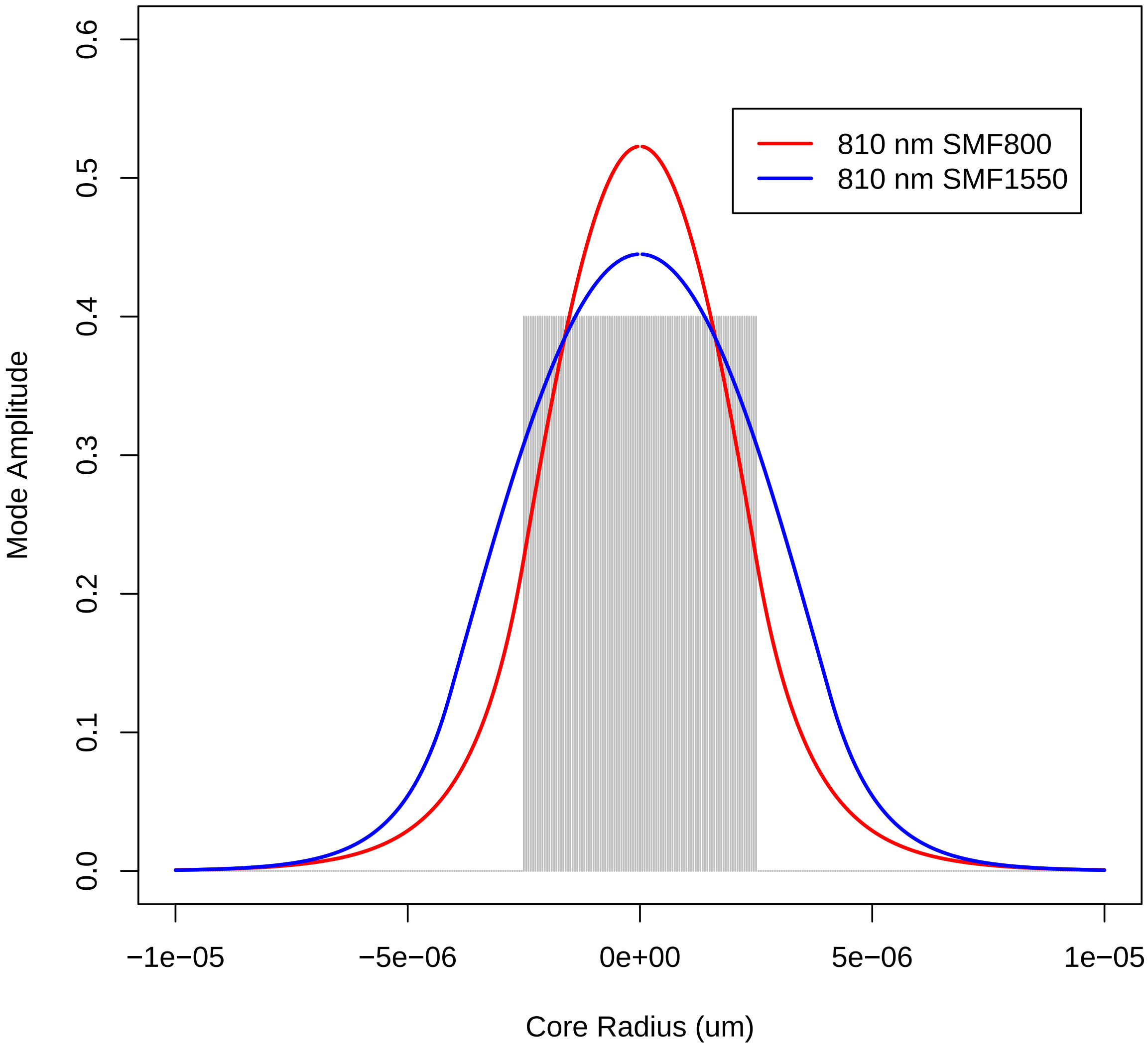


Figure 3.6: The first mode of 810 nm in SMF28, and the first mode of 810 nm in SMF 800. Core size is assumed to be 2.5 um.

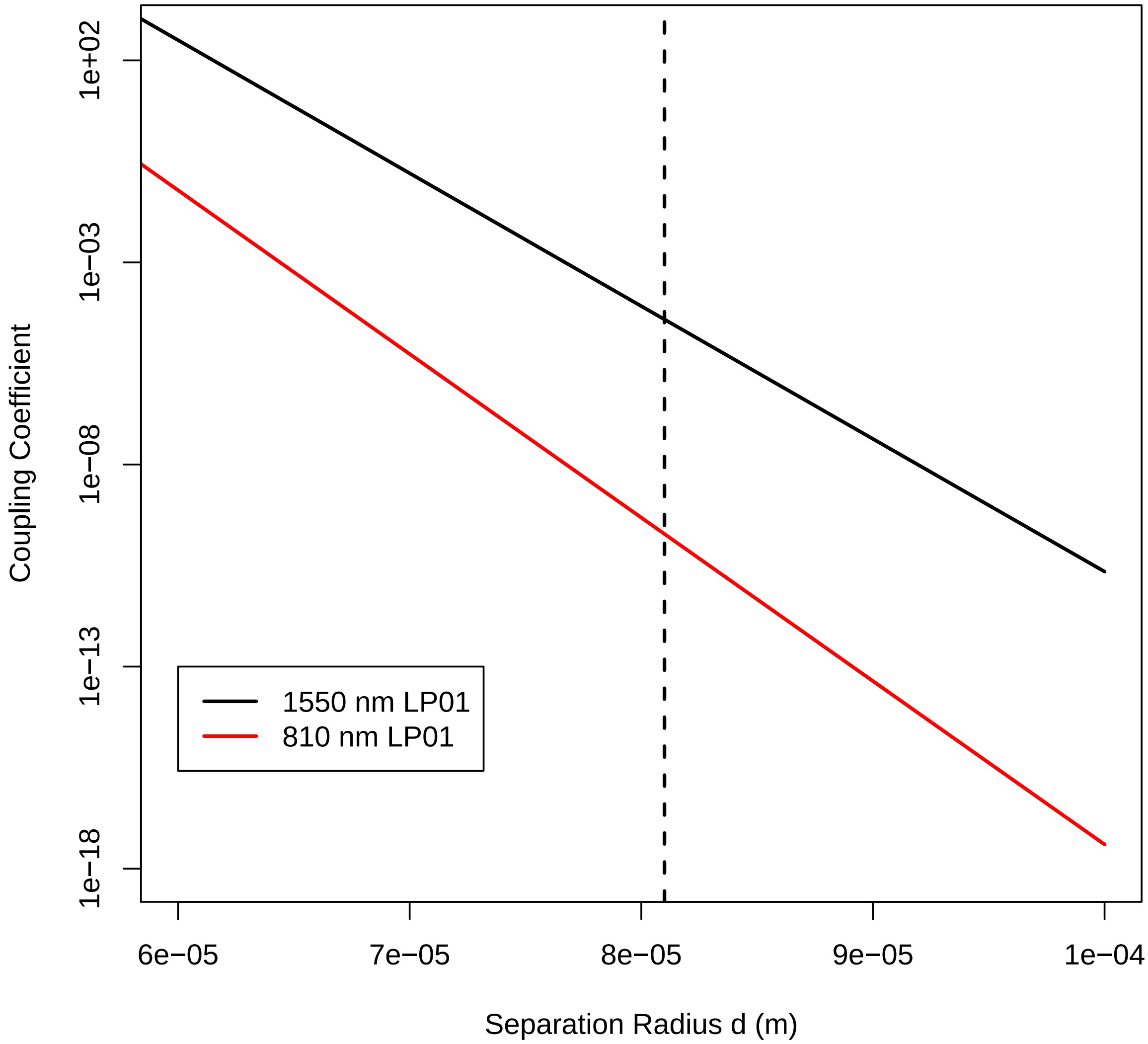


Figure 3.7: Calculated coupling coefficient between two SMF28 cores in a symetric waveguide, dependent on the separation of the cores. The dashed line highlights the separation distance for a 50:50 splitter. Note that this coupling coefficient is a term in a differential equation describing the transfer between modes, and does not represent the transmission from one mode to another.

2.03 for 1550 nm, and 3.91 for 810 nm. This means that SMF28 is single-mode for 1550 nm, but multi-mode for 810 nm. These spatial modes along the the cross-section of the percent change of the index of refraction of the fiber are plotted in 3.2.2.

Allison MacDonald and Evan Meyer-Scott studied the propagation of these modes in theory and experiment, and found that for 810 nm in SMF28, the LP_{11} tails the LP_{01} mode by 2.2 ns per km [109]. This means that with symmetric 2 km long links, there will be peaks in the coincidence counts between the LP_{01} mode of Alice and the LP_{11} mode of Bob, and vice versa, at the ± 5 ns. Evan Meyer-Scott found that this second mode could be filtered out in post-processing by optimizing the coincidence window for visibility[73]. Inserting a 2 m single mode fiber at 800 nm between the fiber splitter and the polarization analyzer box acted as a spatial filter. The first mode in SMF 800 mostly overlaps with the first mode in SMF28 (see figure 3.2.2), but does not overlap with the second order mode for 810 nm and does not allow the propagation of the first mode for 1550 nm, keeping it out of the polarization analysis box.

The mode overlap can be calculated using:

$$\eta = \frac{|\int U_1(\rho,\phi) * U_2(\rho,\phi) dA|^2}{\int |U_1(\rho,\phi)|^2 dA \int |U_2(\rho,\phi)|^2 dA} \tag{3.5}$$

This equation comes from [23], equation 5.4.1. η is 92% between the first order modes for 810 nm in both SMF800 and SMF28, and 3% between the first order mode in 810 nm in SMF800, and the second order mode for 810 nm for 1550 nm.

Waveguide theory also explains why a fused fiber splitter which has 50:50 coupling for 1550 nm couples only to one mode for 810 nm. Samuel Varghese's PhD Thesis contains a chapter with a good introduction to the theory and practice of fused fiber splitters [113]. Fused fiber splitters are made by taking two single mode fibers, twisting them around each other, heating them to 80 degrees celcius, and then slowly stretchting them out. In the process, the fibers fuse together, deforming them, but also reducing the distance between the two. Fused fiber splitters can be approximated as two parallel cylindrical waveguides. If the separation of the waveguides is small enough, there will be some coupling between the waveguides. The coupling ratio of the fused fibers depends on two factors: the separation between the cores, and the interaction length between the two fibers (the length that they've been fused together).

The coupling coefficient between the two cores depends on the overlab between the two spatial modes of the fibers [90]:

$$C = 0.5NA\frac{k_0^2}{\beta}\int_{d}^{d+2a} u(\rho + d)u(\rho - d)d\rho \tag{3.6}$$

where NA is the numerical apeture of the fiber (0.14 for SMF28), d is the separation of the cores, and $u(\rho)$ is the equation defined in 3.2, and a is the core radius. When the interaction length equals:

$$L = \frac{\pi}{4C} \tag{3.7}$$

the fiber coupler acts as a 50:50 splitter. For a 1550 nm coupler, this occurs at an interaction length of 3.45 mm. The coupling coefficient is highly dependent on the separation of the modes. Note that this coupling coefficient is a factor in the differential equation describing the change in amplitude between the two modes, and does not represent the efficiency of transmission. Figure 3.2.2 shows the relationship between coupling coefficient and separation between the first modes of both 1550 nm and 810 nm light in SMF28. The coupling coefficient drops off exponentially as the distance between the cores increases. At the separation distance which would result in a 50:50 splitter for 1550 nm, the coupling coefficient for the 810 nm modes is $1{\times}10^{-9}$, meaning the power in the second mode, which is $P = P(0)sin(1 \times 10^{-9}3.45 \times 10^{-3})$, is effectively zero [2].

3.2.3 Fiber Channel and Detection

The quantum signals sent through various lengths of SMF-28 fiber[47], a commonly used single mode fiber for 1550 nm fibers. These fibers were symmetric in length to both Alice and Bob's detectors, with lengths of 0.25, 0.5, 1, 2, and 3 km. The output of this fiber was attached to a fiber beamsplitter, and the output of the beamsplitter that the quantum signal couples to was directed to a detector module. The classical communication standard used in this experiment was 10GBASE-ZR.

The detector module used in this experiment was built by Chris Erven. A 50:50 beamsplitter was used to make the measurement basis choice, and a polarizing beam splitter was used to differentiate between orthogonal states. A Perkin-Elmer SiAPD SPCM Quad-Array [104] was used for photon detection. The photon detection signals were attached to a timetagger and then sent to a computer for analysis, with a C# program written by Chris Erven.

[2] Due to the imperfections in our real device we nevertheless observe a coupling ratio for the 810 nm photons of about 1%.

A single 5 nm wide band-pass filter at 810 nm was used to filter the telecommunications signal out of the detection module.

3.2.4 Fiber Mixing processes

Mixing processes in fiber are a nuisance in classical telecommunications. In quantum key distribution systems on active telecommunications with DWDM, they can be an obstacle, as the quantum signal is much more sensitive to background noise than classical telecommunications traffic [17]. Since the quantum signal is at a wavelength far from telecommunications wavelengths, the noise due to mixing processes will not be as pronounced.

The optical transceiver used in this experiment operates at 5 mW, because the 1000BASE-ZX's receiver's minimum threshold power is -23 dBm (0.005 mW), and it's loss budget is 21 dB [20]. 1000BASE-ZX is currently the longest reaching fiber optic protocol that is commercially available, and as such is also the protocol which operates at the highest optical power. It can be thus expected that this protocol is the one that suffers from the most non-linear mixing effects. Thus, if mixing effects are negligible in this experiment, they can be expected to me negligible on all other commercially available fiber optic protocols. According to the Nonlinear Optics textbook [2], nonlinear effects start to present problems in terms of nonlinear effects at around 1.2 mW.

Some nonlinear mixing still occurs between classical and quantum signals. In order to quantify this effect, the spectrum around 810 nm was observed on a 2 km fiber with no classical signal, with classical signal propagating parallel to (meaning in the same direction as) the quantum signal, and with the classical signal travelling opposite to the quantum signal 3.2.4. The opposite propagation produced fewer extra counts than the parallel propagation, so this propagation was used in the experiment.

The dark counts were measured with different lengths of fiber with classical and quantum signals on their own and together and compared against the average detector counts 3.2.4. The dark counts with the quantum signal remained roughly the same with the length of the fiber in the arm, while the classical traffic introduced many extra counts that decreased with increasing fiber length. From this, we can conclude that the extra dark counts seen in this experiment are likely due to classical traffic and not from both combined. What is surprising is that the counts decrease rather than increase with increasing fiber length, which is not what would be expected if the extra counts were a result of a mixing process.

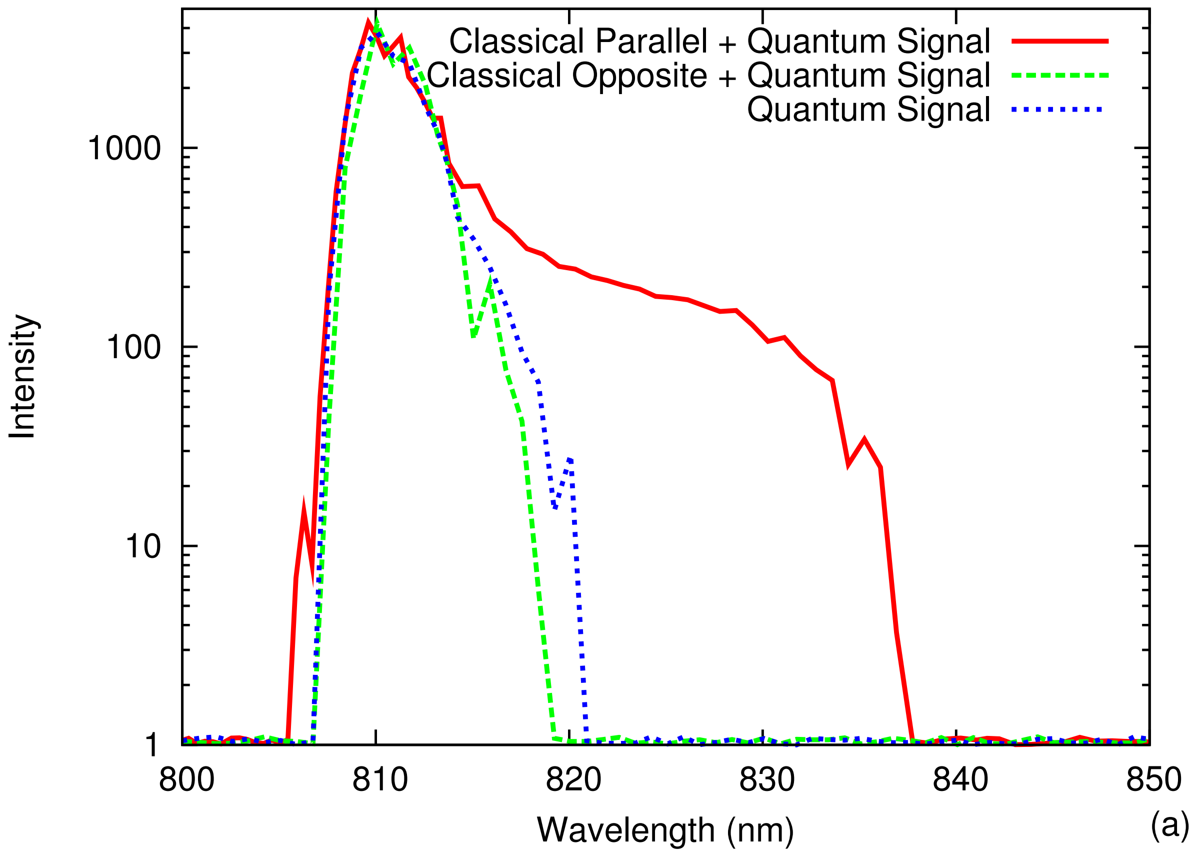


Figure 3.8: Wavelength-binned number of counts over 10 minutes of exposure for the case where polarization-entangled photons at 810 nm travelled in the same direction, in the opposite direction, and in the absense of photons at 1550 nm generated by a classical router.

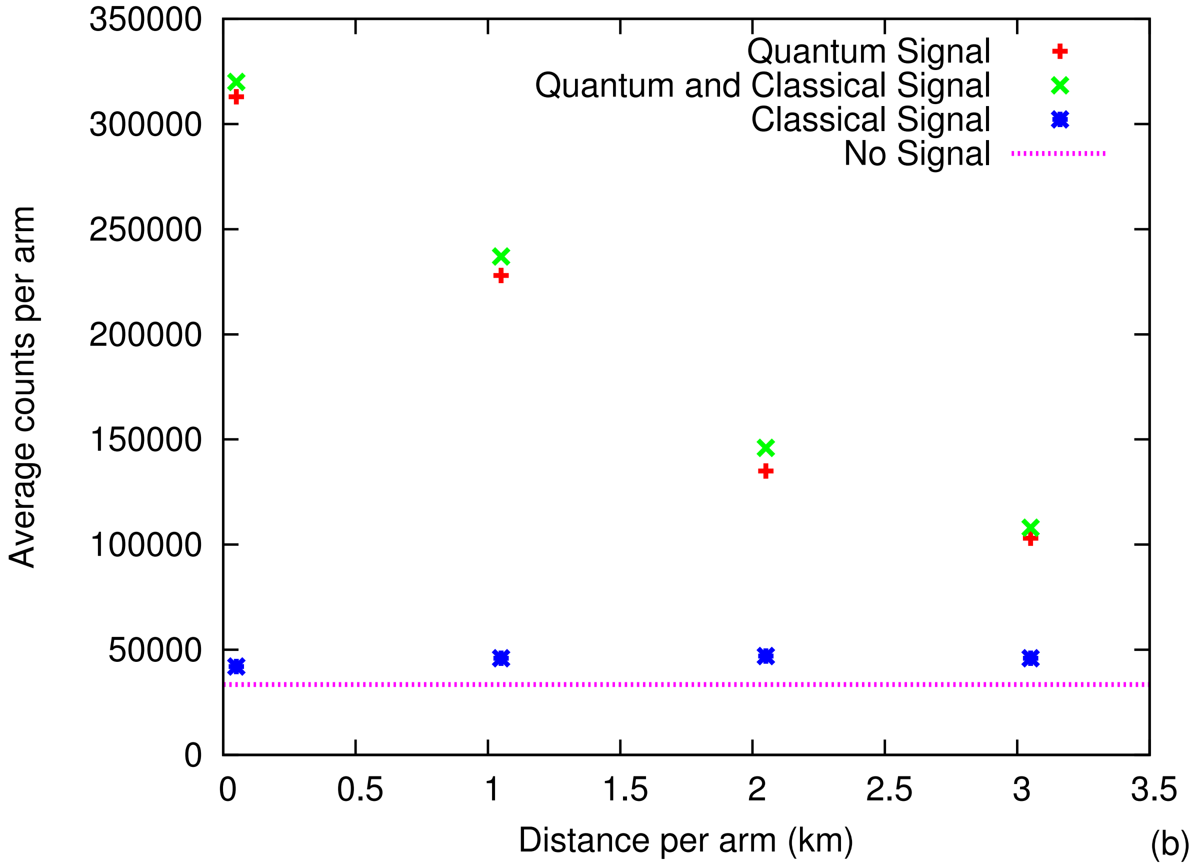


Figure 3.9: Measured detector counts in the presence of quantum and classical signals. Detector dark counts (false positives) are represented by a dashed line.

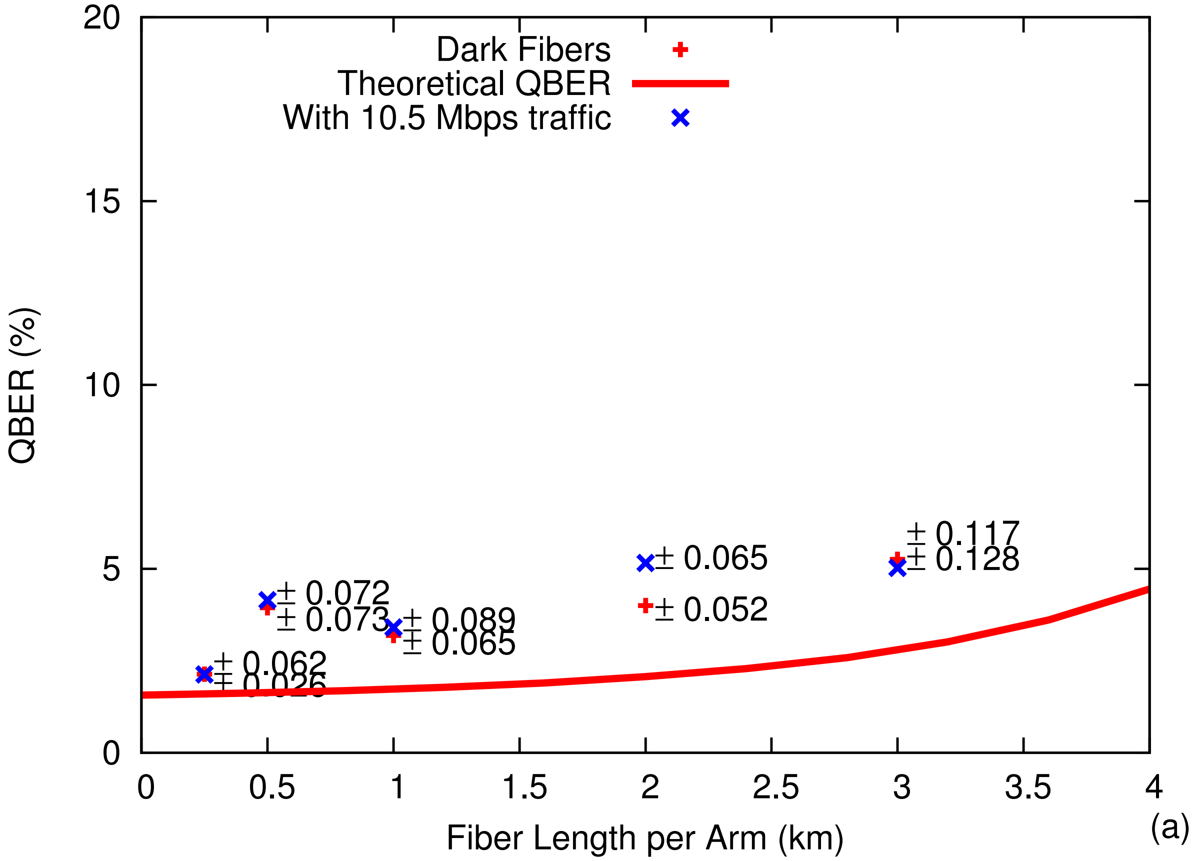


Figure 3.10: Measured and theoretical predictions for QBER with and without the presence of classical traffic. Lines are the values from simulation fitting the experimental parameters.

3.2.5 QKD Results

For all lengths of fiber studied, the QBER did not increase when the classical traffic was turned on, and the coincidence rate also remained the same (see figures 3.2.5 and 3.2.5). This means that the predicted SKR will not increase in the presence of classical traffic.

The QBER was observed while the classical traffic was increased in powers of 10 from 0 to 100 Mbps and decreased back down again. The QBER drifts upwards over time, but this is likely due to the polarization drift in the mechanical relaxation of the fibers, and not due to the presence of classical traffic. There is no increase in QBER corresponding to the beginning of the classical signal, and the QBER continues to monotonically increase when the classical signal is turned off again. This measurement is presented in figure 3.2.5.

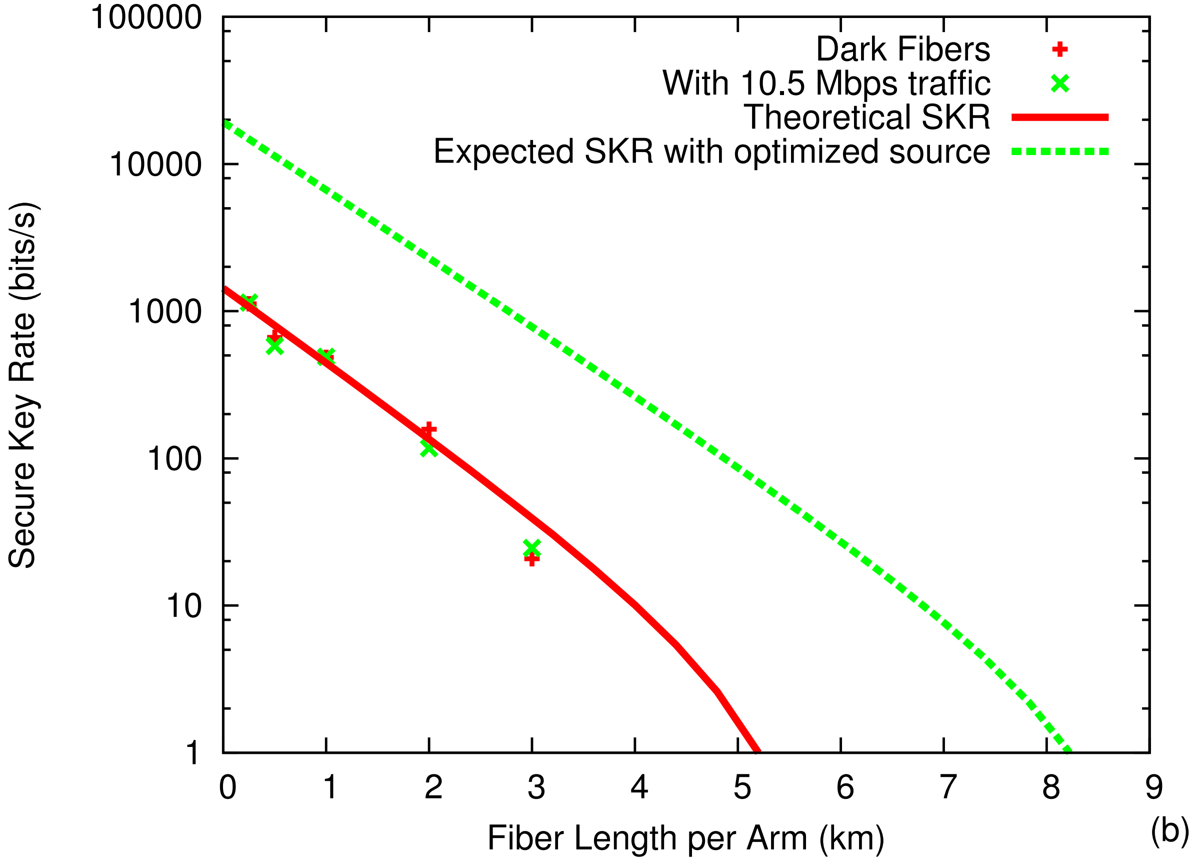


Figure 3.11: Measured and theoretical predictions for SKR with and without the presence of classical traffic. Lines are the values from simulation fitting the experimental parameters.

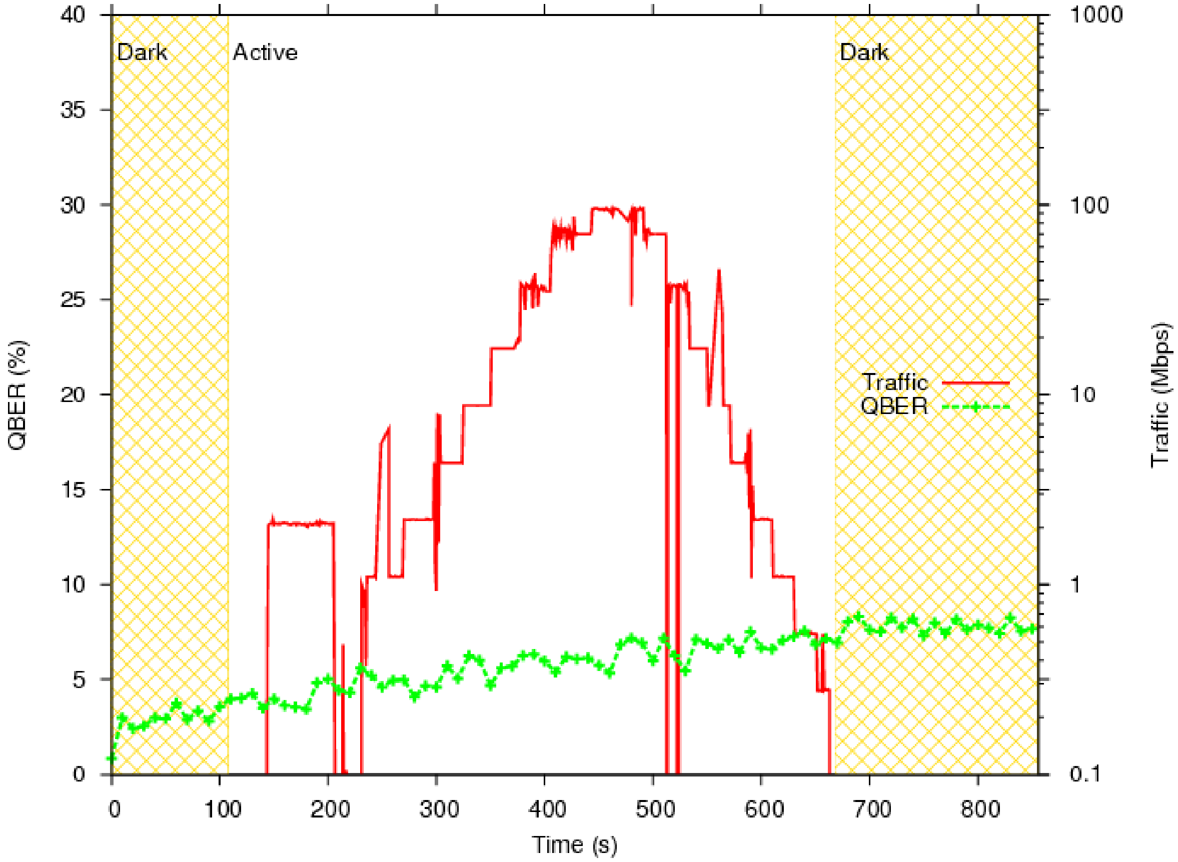


Figure 3.12: The evolution of QBER in time, while the classical traffic is increased from 0 to 100 Mbps and back to 0 Mbps in factors of 10 every 50 s.

Finally, as a demonstration, a key was exchanged for a fiber length of 2 km. By simulating our system (Matlab, QOToolbox[106]), we found that the maximum distance of our system with our source rate was 10 km. With an optimized source rate, this distance can be extended to 16 km. In the next chapter, I built a model for automatically determining the optimal source rate.

3.3 Conclusions

In this chapter I have motivated the utility of demonstrating the compatibility of QKD with classical optical networks by discussing the future likelihood of device-to-device passive optical networks. This would allow for QKD between any two devices. I have experimentally demonstrated the compatibility of QKD with entanglement over short, active, standard classical telecommunications lengths with low-cross talk using 810 nm photons.

In addition, it should be noted that the incorporation of QKD into the classical fibers was very simple. Due to the non-symmetric nature of the coupling of bi-conical fused fibers, all that was required to multiplex and de-multiplex the quantum signals and classical signals was a 50:50 fiber beamsplitter, ($136 each from Thorlabs).

Using this method, with current detectors, we believe that QKD between devices could span optical networks of 16 km, enough to cover a university or business campus, or the downtown area of a city. With perfect detectors (0 dark counts, 100% detection efficiency), this distance could extend to 20 km.

Chapter 4

Optimal Parameters for Entanglement-Based QKD

Quantum key distribution has come a long way from Bennett and Brassard's first implementation of QKD accross a tube of length 32 cm [9] using a polarizer in a electronically controlled rotation mount and a pockels cell. A few companies have been established with the goal of developing commercially-available QKD systems, including ID Quantique in Geneva and MagiQ in Boston.

QKD protocols based on the distribution of entangled photons are an important area of research because they can lead to future technologies involving teleportation. However, the most common way of generating entangled photons, the combination of two SPDC photon pair sources, does not produce ideal entangled quantum states. Realistic sources of entangled photons contain higher order terms, meaning more than two photons may be detected in certain states. This occurs because more than one photon may be downconverted simultaneously, and because sources of entangled photons involve combining two correlated pair sources in a way that makes them indistinguishable. Assuming these pair sources are independent, there will be some instances where both pair sources generate photons during the same coincidence window.

When these multi-photon states are detected, they can lead to errors. In order to account for measuring on a subset of the Hilbert space, a squashing scheme must be implemented, as described in chapter 1. If multiple photons are detected simultaneously, the squashing scheme means that these events will increase the QBER.

Many experimentalists demonstrating QKD restrict the power in their QKD systems in order to achieve the highest visibilities. However, in order to match the distance and

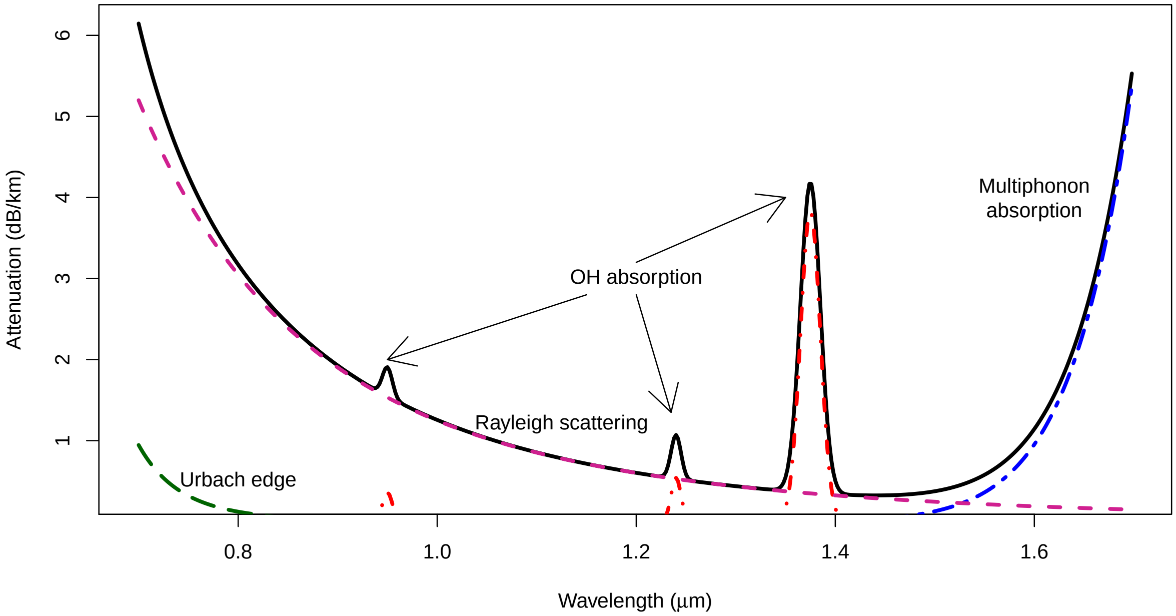


Figure 4.1: The attenuation of light signals for various wavelengths. The contributions that add to the attenuation - Rayleigh scattering, ultra-violet scattering (the Urbach edge), multi-phonon absorption and absorption due to impurities in the manufacturing process, are plotted.

key rate generation demands of commercial implementations, designers of QKD systems will have to trade off higher raw key rates for lower secure key rates.

In this chapter, I report on my work investigating the limitations to QKD with entangled photons, as well as my work developing a useful model for the optimal coincidence rate.

4.1 Limiting factors in QKD implementation

4.1.1 Signal Attenuation and Interference

As described in the previous chapter (3.1.1), attenuation and chromatic dispersion are the two main factors that are of concern to classical fiber optics. Attenuation can be attributed

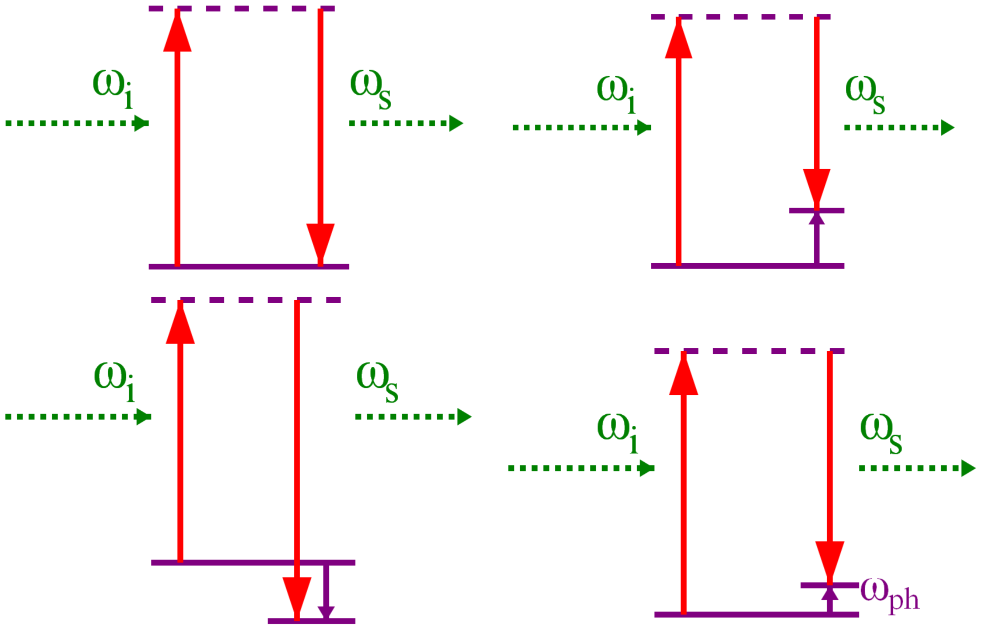


Figure 4.2: Four scattering processes that add to the attenuation in fiber. From left to right, the processes depicted are Rayleigh Scattering, Raman (Stokes) scattering, Raman (anti-Stokes) scattering, and Brillouin Scattering. Purple dashed lines represent virtual states. ω_i is the input photon, ω_s is the scattered photon, and ω_{ph} is the photon resulting from Brillouin scattering

to four scattering processes that lead to four separate increases in attenuation at different wavelengths.

The four scattering processes are described in 4.2. They are: Rayleigh scattering, where light bounces off of molecules like a billiard ball, Raman (also called Stokes) scattering, where light bounces off of molecules but looses energy in the process, Raman (anti-Stokes) scattering, where light bounces off of molecules and gains energy in the process, and Brillouin Scattering, where phonons in the material absorb the energy of the photons. Some of these processes lead to the contributions of different absoption and attenuation processes that sum to the curve described in fig. 4.1. Rayleigh scattering effects mostly visible light. Brillouin scattering is responsible for the steep curve in attenuation after 1550 nm. OH impurities in the fiber due to the fiber manufacturing process account for some absorption bumps in the attenuation curves.

Raman scattering processes, along with some non-linear effects, lead to cross talk in fibers that can limit the performance in WDM systems.

In free-space transmission, the amount of loss depends on two large factors - the geometric expansion of the beam, and Rayleigh scattering of the beam off of the atmosphere. When looking straight up, the effective length of the atmosphere is 13 km, meaning that beams that travel 13 km through the air from two points on the ground will experience the same amount of scattering that a beam going off of the earth would experience. This does not account for the loss of beam due to diffraction and the expansion of the beam. In the course of the uplink (meaning ground to satellite) transmission to a low earth-orbit (LEO) satellite, the loss can be at best 33 dB, and worst 60 dB. [1]

4.1.2 Detector Efficiencies

The two most common single photon detector materials are made of Silicon or InGaAs. Silicon detectors have detection efficiencies between 30 % - 70 % for visible light. InGaAs detectors have detection efficiencies between 20 % - 50 %. InGaAs detectors typically have several orders of magnitude more dark counts (false positives). In general, the higher the detection efficiency, the higher the number of dark counts.

Lesser known, more experimental types of detectors are based on quantum dots, upconversion processes, and superconducting devices.

In this analysis, we incorporate the detection efficiency into the total channel efficiency for our analysis.

[1] These numbers come from Jean-Phillipe Bourgoin's simulations, as yet unpublished.

4.1.3 Higher-order photon emission

An ideal entangled photon source would have some small probability of creating the vacuum state or a bellstate within each timing resolution of our detectors. However, it is difficult to create such a device. In practice, bell states are generated by combining two squeezed photon states, such as with non-linear processes in birefringeant crystals. In this case, there will be a large probability of getting the vacuum state, a small probability of getting a unique bell state, a smaller probability of getting two simultaneous, orthogonal bell states, and then multi-order photon states with vanishing probabilities. See the quantum state described in equation 2.31.

When two orthogonal detection events occur, as in figure 4.4, the detection result must be assigned to a random measurement due to security concerns [59]. This is called 'Squashing' [41, 75] In cases where background noise and channel losses are low, and the source rate is low, these multi-photon states don't add to the quantum bit error rate.

4.1.4 A model for the optimal Two-Fold coincidence rate

As the power to the input SPDC source of entangled photons increases, the number of twofolds increases, but so does the number of multi-photon states. Multi-photon states contribute to the QBER [58]. The higher the QBER, the larger the percentage of the key that needs to be shared during error correction and privacy amplification (see equation 2.55). Thus, there is an optimization trade-off that needs to occur in order to maximize the SKR.

The problem of an optimal source rate for decoy state protocols has been examined and results in an inequality that must be numerically solved [71]. Typical values for μ are between 0.5 and 0.6. For QKD with entanglement, this problem is more challenging as the multiphoton effects also distort the measurement of μ.

Different approaches have been tried to optimize this situation. Some experiments try a few different power levels before settling on the one that gives the lowest QBER [33, 18, 110, 78]. Some run numerical simulations of the loss and background counts in their systems before running the experiment [68, 87, 96]. In some experiments the limiting factor is computing power or the size of memory, and so the pumping rate is reduced to the number of counts that Alice and Bob's computers can process [3, 86].

In the real world, these methods will be obsolete. In realistic fiber-optic QKD systems or in free-space channels, the loss will vary greatly with the presence of other traffic, vibration from the traffic above the fiber optic channel, and weather conditions. It will

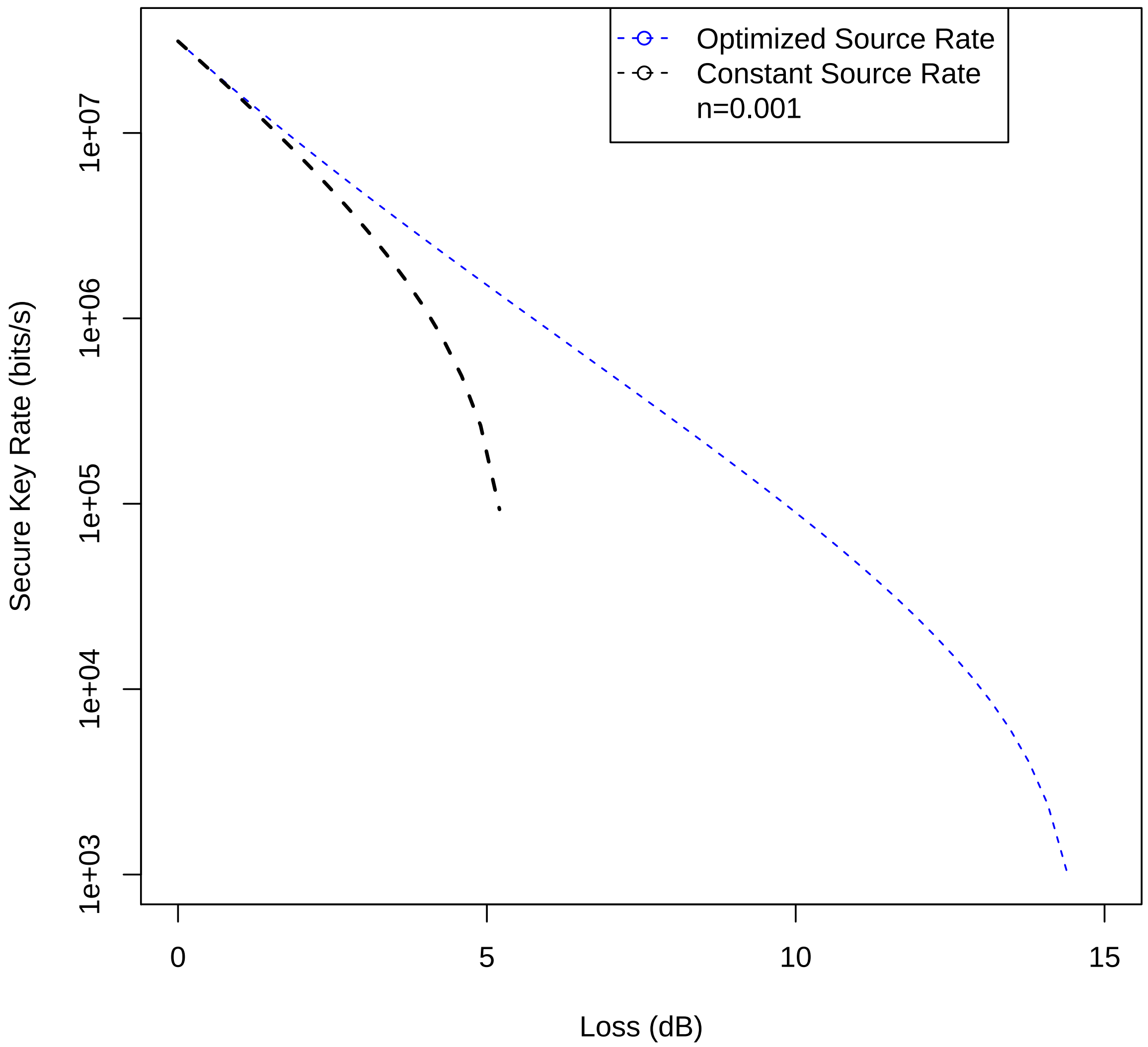


Figure 4.3: Comparison of the amount of key with a constant power rate compared to an optimized key rate. In this simulation, the coincidence window is 2×10^{-9} s, the detector efficiency is 50%, and the dark count rate is 5×10^{5} per second.This dark count rate is very large in order to emphasize the difference in optimization.

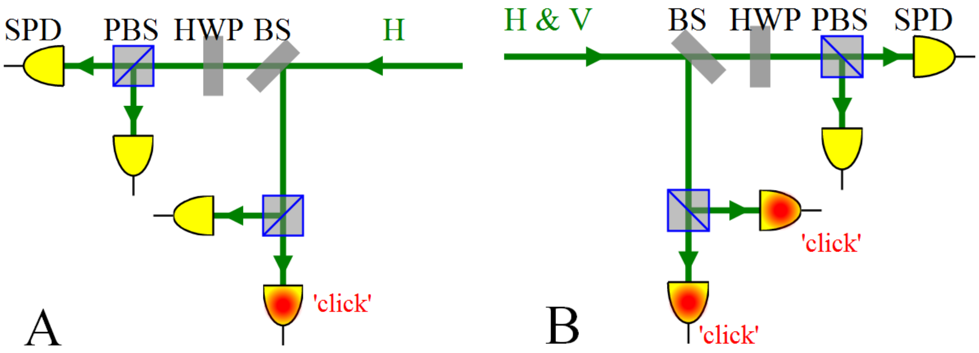


Figure 4.4: While the party A received and correctly measured a horizontally polarized photon, the party B received a mult-photon state and measured two orthogonal detectors clicking at the same time, leading to an error.

not be possible to run simulations of the experiment, or to guess at the power level and measure the resulting SKR, and one would expect that these experiments would happen between powerful computers where processing speed is not an issue.

In this chapter, I first developed a highly-predictive simulation for twofold coincidence probabilities, SKR and QBER for any combination of channel efficiencies, background noises, squeezing factor and coincidence window. I numerically found a value for the two-fold coincidence rate for every combination of channel efficiencies, background noises and coincidence window within a range of realistic values. These values of optimal two-fold coincidence rate were fed into a symbolic regression program called Eureqa Formulize ([95]), which produced a simple equation relating the variables.

4.2 Simulation and Modelling of QKD with Entangled states and the optimal coincidence rate

The simulation of QBER, SKR and two-fold coincidence rate for any channel efficiencies, background noise, squeezing factor and coincidence window was initially written using Matlab and the quantum optics toolbox (QOToolbox[106]). The simulations were later re-written in Python and the QuTIP library [53] in order to be easily parallelized.

Simulation starts by exponentiating the hamiltonian described in 2.27 and applying it to the vacuum state. In order to create a entangled state, this state is repeated for the V

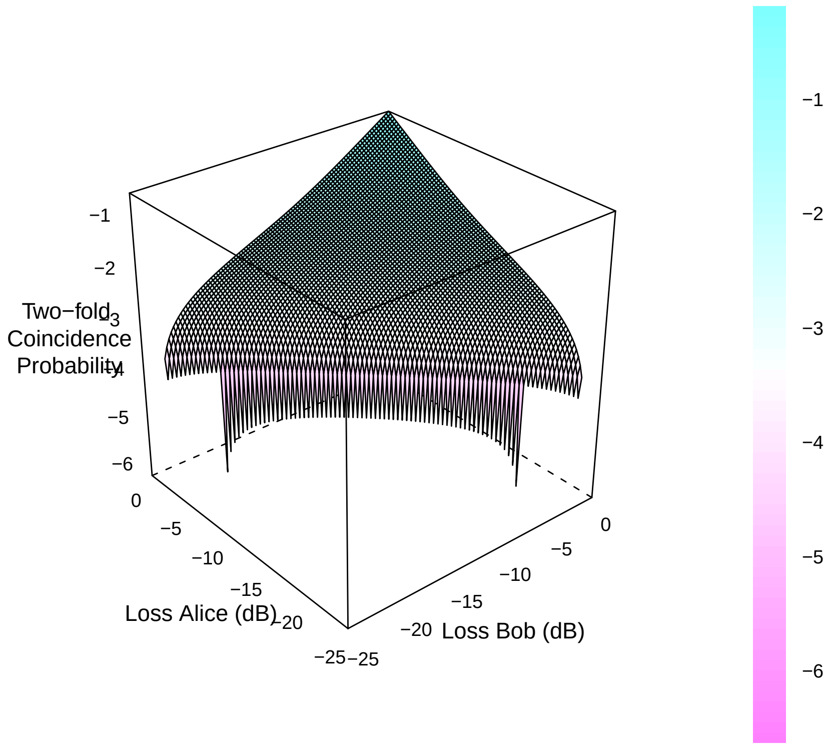


Figure 4.5: The model for the optimal coincidence rate as determined by Eureqa. The channel efficiencies for Alice and Bob are plotted along the x and y axes. The two-fold coincidence rate is plotted in log base 10 scale. The model also depends on the background counts in Alice and Bob, but only by a constant factor.

polarization. These states are tensored together and permuted so that Alice and Bob each get one of the photons in each pair.

Next, the bucket detector operators are created according to eq. 2.35. The detector efficiency is combined with the channel efficiency. Expectation values of the bucket detector operators are applied to the entangled SPDC state, and these are then used in squashing models such as eq. 2.37 to determine QBER and twofold-coincidence rates. Finally, the SKR can be estimated using eq. 2.55.

This simulation correlates very strongly with experimental data and has been used previously to great effect in [44, 73].

For over half a million different combinations of channel efficiencies and background noises, the squeezing factor that optimized the SKR was determined using Scipy's optimization function[2]. Using this optimal squeezing factor, we determined the resulting SKR, QBER and two-fold coincidence probability. In order to distill some meaning from these half-million data points, they were fed into the program Eureqa formulize, with the instructions to develop a model that optimize the R^2 correlation coefficient. The mathematical operations that Formulize was allowed to search over included addition, subtraction, multiplication, division, basic trigonometric functions, exponentiation, natural logarithms, and power laws. From these data points, and the allowed operations, formulize built the model for the optimal two-fold coincidence probability as:

$$P_{tf} = A\sqrt{\eta_a \eta_b} + B(\sqrt{\eta_a \eta_b}^3 \sin{(C - D\sqrt{\eta_a \eta_b} - \eta_a - \eta_b)} - d_a - d_b) + E \tag{4.1}$$

Where η_a, η_b, d_a, d_b are the channel efficiencies and the background noises to Alice and Bob, respectively, and $A = 0.03579$,$B = 0.23$,$C = 1.162$, $D = 2.496$, and $E = -0.002444$. P_{tf} is the probability of measuring a two-fold coincidence within a coincidence window that optimizes the secure key rate. In order to determine the two-fold coincidence rate that this corresponds to, this number must be divided by the coincidence window. This model is plotted in fig 4.2.

As the channel efficiency improves, the optimal two fold probability increases. This is because as the two-fold probability increases, so does the errors caused by multi-photon detection. Higher channel efficiencies have more room for error. Increasing the background noise decreases the optimal two-fold probability, by the same argument. Dark counts increase the amount of error, which leaves the system less tolerant to errors caused by multi-photon detection.

[2] http://docs.scipy.org/doc/scipy/reference/generated/scipy.optimize.fmin_cg.html

Channel	Optimal from Experimental Data		Optimal from Simulated data		Optimal from Model
	Value	Uncertainty Margin	Value	Uncertainty Margin	Value
Noisy channel (A)	2.79×10^5	5×10^4	3.13×10^5	1×10^4	3.1×10^5
Lossy channel (B)	3.46×10^6	1×10^6	3.01×10^6	1×10^5	3.0×10^6
Free-Space Channel (C)			6.29×10^5	2×10^4	6.25×10^5

Table 4.1: Optimal values of two-fold coincidence rates corresponding to the experiments in figure 4.2.2, based on experiment, simulations, and the model (eq. 4.1).

4.2.1 Validation with Previous Theoretical Work

Xiongfeng Ma et al. produced a model for SKR [70]. In the appendix, they take the derivative of this model with respect to SKR and find the root numerically with respect to the squeezing parameter and an induced error rate e_d in two extreme cases: when the channel efficiency is perfect ($\eta = 1$) and when it is very bad ($\eta << 1$).

Although this is a useful exercise, there are several issues with this. First, it is very difficult to experimentally measure the squeezing factor, but it is very easy to measure the two-fold coincidence probability. Secondly, the rate at which quantum channels induce flip errors is minimal compared to the signal attenuation, the dark count rate, and the errors due to multi-photon detection.

In developing this model, I did not study the effects of bit flips or find the optimal value in terms of squeezing factor. However, it does provide a useful sanity check. I induced bit-flip errors by simulating the effect of a half-wave plate in front of one channel.

There are a few differences between our methods, in that Ma et. al approach the problem from a theoretical standpoint and I approach the problem from an empirical standpoint. Ma et. al model detectors and measurements differently than I do. However, given the figure 4.2.1, these differences in simulation lead to small differences in the value of the optimal squeezing factor.

4.2.2 Validation with Experimental Data

The model was also validated against experimental data. The polarization analysis boxes were exposed to light in order to increase the background noise. The channel efficiency was

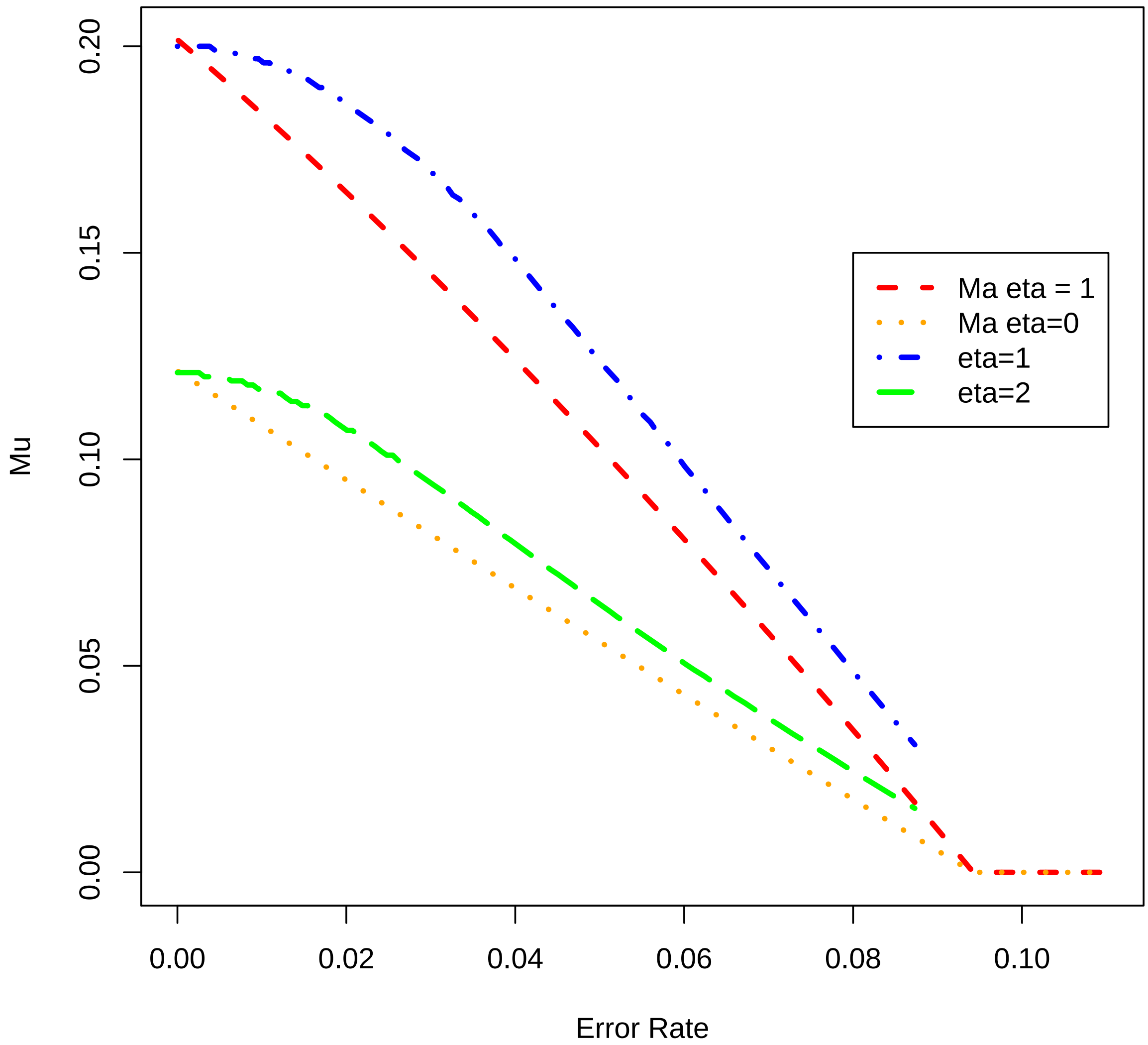


Figure 4.6: Comparison of the optimal squeezing rate between our simulation and Ma et. al 's ([70]) optimal squeezing rate.

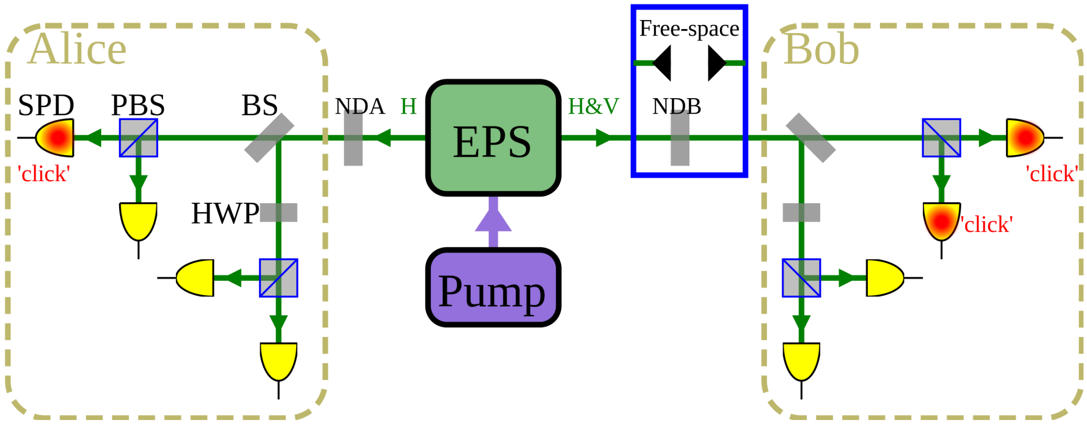


Figure 4.7: Experimental configuration used to validate the model. The entangled photon source is based on a PPKTP crystal in a Sagnac configuration [35]. The pump power was varied in order to observe the resulting coincidence rates and QBER. Loss was introduced by adding neutral density filters, or by using a free-space channel.

reduced by placing neutral density filters in the paths from the entangled photon source before the polarization analysis boxes. Finally, data was collected under normal operation from normal usage of entangled photon source in a free-space channel [3].

The pump power of the crystal was increased from 0 to 60 mW in increments of 5 mW. The resulting two-fold coincidences and QBER was measured, and using these two numbers in eq. 2.55. The experimental data, the simulation matching the measured values of background counts and channel efficiency, and predicted maximum from the model are plotted in figure 4.2.2.

For the two channels from which an experimentally determined maximum can be estimated, the optimal from the simulated data and the model are within the margin of error of the experimental data. For all three chanels, the predicted optimal from the model matches the simulation data.

4.2.3 Validation from Analysis

Eureqa Formulize was run 7 times on the data until the maturity reached ≥ 90 %. Maturity refers to what fractions of the total possible reasonable permutations of the current

[3] collected by Chris Erven as a part of his PhD thesis [32])

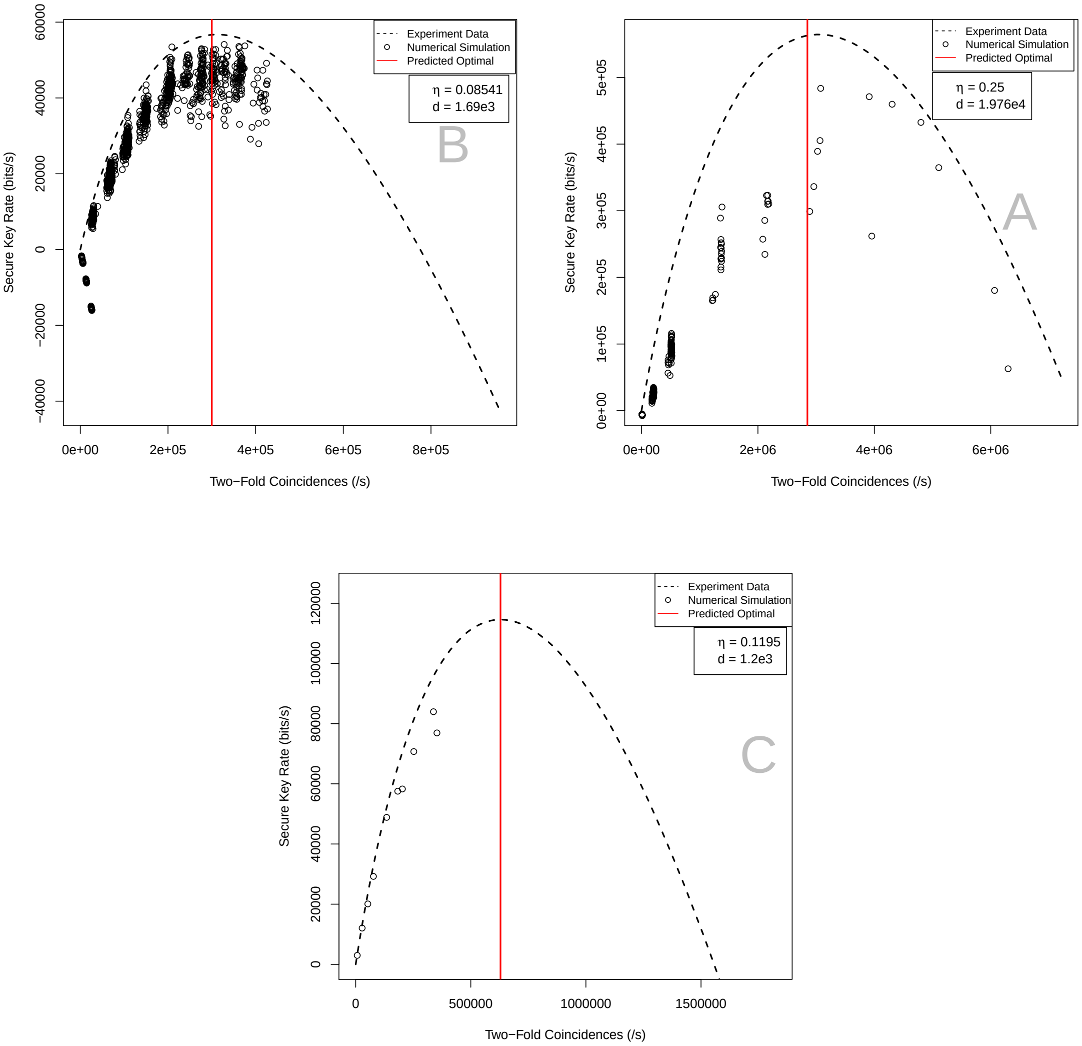


Figure 4.8: Comparison of experimental data for three different channels. Three different experimental conditions were used: uncovered polarization analyzer without neutral density filters($d = 7 \times 10^{-5} \pm 1 \times 10^{-5}$, $\eta = 0.25 \pm 1 \times 10^{-2}$, graph A), covered polarization analyzers with neutral density filters ($d = 5.92 \times 10^{-6} \pm 1 \times 10^{-8}$, $\eta = 0.085 \pm 1 \times 10^{-3}$, graph B), and after a free space channel ($d = 5.92 \times 10^{-6} \pm 5 \times 10^{-8}$, $\eta = 0.12 \pm 1 \times 10^{-2}$, graph C)

solutions are tested. This took about four hours using 4 cores of a core i7 cpu.

The set of operations allowed in building models included addition, division, multiplication, exponentiation, logarithms, sine, cosine, and power laws. Although the parameters of the best models changed slightly between runs, certain features were the same - the appearance of the square root of the product of the two channel efficiencies, the sine function, the negative linear dependence on background noises, and the cube power of the square root of the product of the efficiencies.

4.3 Application: Predictions of Maximal distance of QKD to the State of the Art in Photon Detection and Fiber Optics

In the previous chapter I argued for the widespread adoption of QKD from device-to-device over large, active telecommunications networks in passive fiber optic networks. In such networks, QKD engineers will have to work to integrate quantum signals alongside classical communications. Classical communication is much more resistant to attenuation, nonlinear effects and dispersion compared to quantum signals. Fiber optic cables are often installed under streets or along power lines, which can change unpredictably in the amount of loss and background counts experienced by the quantum signal.

Loss in optical fibers is also mostly exponential with respect to the length of the cable, which gives us another aspect to study with the optimal coincidence model. Given the best detectors available today, and an optimal source rate, how long can the fiber in each arm be before it is impossible to get a key (50k secure bits according to Scarani and Renner [93]) in an hour and in ten years (our stand in for infinity). We assume symmetric amounts of loss in each arm in order to maximize the distance [94].

Buller and Collins [15] provide a good overview of the state of the art in single photon detection. I used these values to construct table 4.3. I calculate the loss budget by determining the largest loss per arm, and subtract off the loss due to the imperfect efficiency of the detector. This loss budget can then be divided by the loss in decibels (dB) per kilometer in order to estimate the maximum possible distance of fiber-based QKD systems with entanglement.

Assuming little insertion loss, compensation for dispersion effects, and symmetric, dark, fiber links, the maximum distance that can be achieved with fiber-based implementations is 204 km (0.22 dB/km for 1550 nm in standard telecommunications fibers) or 303 km with

Type	Wavelength (nm)	Time Resolution (ps)	Efficiency (%)	Dark Counts (per s)	Key in an Hour		Key in ten years	
					Optimal Coincidence Rate (pairs/s)	Loss Budget (dB)	Optimal Coincidence Rate (pairs/s)	Loss Budget (dB)
Si-SPAD (thin junction)	550	35	52	300	857	30.6	17.9	39.0
Quantum Dot	550	150,000	13	0	768	6.54	0.0112	30.7
Si-SPAD (thin junction)	850	35	12	300	857	24.2	17.9	32.6
Si-SPAD (thick junction)	830	500	45	25	853	24.2	1.25	38.3
InGaAs SPAD	1550	500	3	40,000	8660	6.01	7160	6.30
InGaAs SPAD	1550	55	11	2,925	1010	22.4	7.70	32.2
Tungsten transition edge sensor	1550	90,000	88	10	778	16.1	0.124	34.1
NbN nanowire	1557	60	1	10	958	10.5	10.7	20.3
Up-conversion assisted hybrid photodetector	1550	200	4	30,000	3000	12.1	1650	13.0
Up-Conversion	1560	50	5	50,000	2540	16.5	1190	17.8

Table 4.2: Optimal coincidence rates, and the Loss Budget in order to get a key (50,000 secure key bits) in an hour or ten years for symmetric entanglement-based QKD for common single photon detectors for telecom frequency photons. Table adapted from Bulter and Collins [15].

ultra-low-loss fibers (0.148 dB/km [76]) with an InGaAs SPAD. If we restrict the case to having only a positive key (or a key in ten years), then this distance extends to 310 km with standard fibers and 461 km with ultra-low-loss fibers with a tungsten-transition edge detector. The difference between these two detectors is that the InGaAs SPAD has a very low detection efficiency and also low detector dark counts, while the transition edge sensor has a large number of dark counts and a high detection efficiency. This suggests, perhaps counter-intuitively, that in the limit of long detection times and high loss, dark counts don't matter as much as detector efficiency.

4.3.1 Noise budgets

The above predictions apply only to dark fibers. In a real hybrid quantum-classical fiber, the dark counts will be much higher. It is difficult to estimate how much background noise will be introduced in the presence of multiplexed classical channels. The nonlinear effects which are detrimental to classical WDM signals begin to occur when the optical power is above 1.2 mW.

Extra background counts due to the cross-talk between channels in DWDM is more likely to effect the quantum signal when it is in the telecommunication band compared to at the edge of the visible band, such as with implementations of the previous chapter. Assuming mininimal extra noise, this means that the maximum possible distance for visible-light systems is 16 km for a key in an hour, (3 dB/km of loss at 810 nm [73]) or 25.5 km for a key in ten years (both with a thick-junction Si-SPAD). Given these numbers, long-distance QKD is likely to be reserved to telecommunications wavelengths or free-space implementations.

Using the simulation and symbolic regression, it is possible to make a model for the 'noise budget' of a QKD system that describes the maximum possible background noise for given values of the channel efficiencies, for which it is still possible to share a positive amount of key. This relationship is:

$$d \leq \frac{0.0732\eta_a\eta_b}{\eta_a + \eta_b} \tag{4.2}$$

Note that this d is dark count probability per coincidence window, per detector. In order to find the DCR, you must divide this number by the coincidence window.

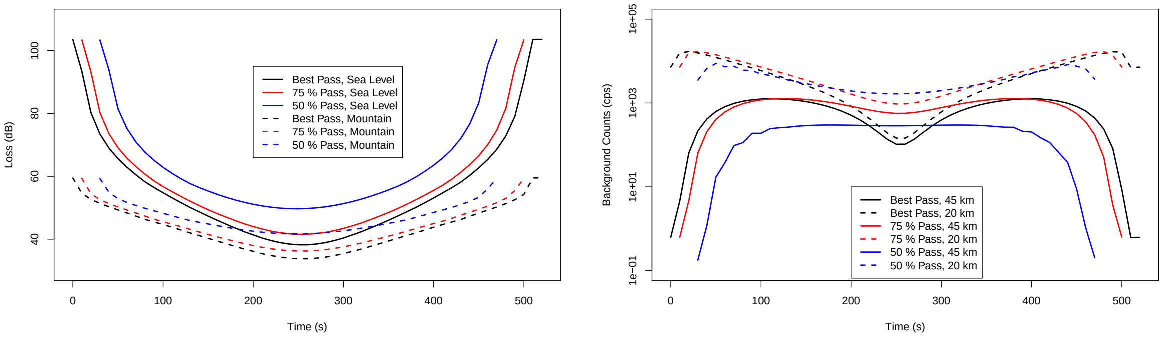


Figure 4.9: Operating conditions of the satellite passes studied in this section. Passes were ordered by their minimum loss, and I picked out the best, 75 % percentile pass, and 50 % percentile pass. Ground stations are placed at 20 km and 45 km away from Ottawa, either at sea-level or on a mountain (2.4 km above sea-level). The transmission efficiency is for photons at 785 nm. The transmitting telescope has an area of 25 cm, and the receiving telescope on the satellite has an area of 20 km. The constant source rate used for comparison was 5.4×10^8

4.4 Application: Satellite Uplink

Satellite implementations of entanglement-based QKD provide another useful application of the model for optimal two-fold coincidences. Consider a entanglement based QKD system where one photon is measured locally at a ground station, while the other photon is sent upwards through the atmosphere to a LEO satellite. The Jennewein lab has invested a lot of research effort into the concept of uplink to a LEO satellite [74, 42, 49], so simulated loss and background count information was easily obtained.

I looked at data for a year of satellite passes between a transmitting telescope of 25 cm on the ground and a receiving telescope of 20 cm on a LEO satellite. The passes were organized by the minimum loss, and in this section I examine the best, 75th and 50th percentile passes. Loss and background count conditions are presented in figure 4.9. Four locations were studied for the transmitting telescope: either at sea-level or on a mountain (2.4 km above sea-level), either 20 km from Ottawa or 45 km from Ottawa.

Using these loss and background count conditions, I simulate QKD and estimate the SKR given an optimized two-fold coincidence rate from the model, and a constant two-fold coincidence rate that optimized SKR over all passes. I assume red-shifted Si-APDs for

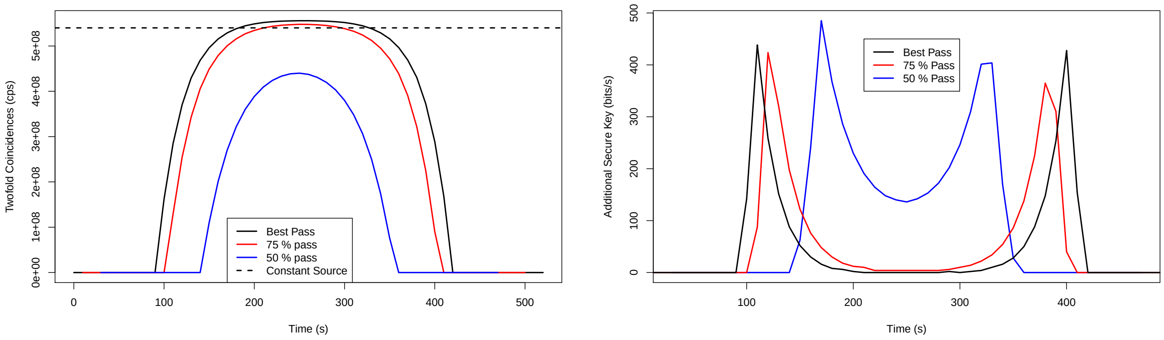


Figure 4.10: The predicted optimal source rate (directly at the source, assuming 50% detection efficiency detectors) and additional secure key bits for transmissions between the ground and a LEO satellite, with a ground station at sea-level, 45 km from Ottawa.

Additional Key	Best Pass	75% Pass	Median Pass
Mountain (45 km)	2383 (0.74%)	4089 (2.65%)	4681 (21.90%)
Mountain (20 km)	3651 (1.22%)	2676 (1.48%)	6341 (623.40%)
Sea-Level (45 km)	444 (0.46%)	507 (1.15%)	810 (45.75%)
Sea-Level (20 km)	1106 (1.27%)	1460 (4.63%)	-

Total Key	Best Pass	75% Pass	Median Pass
Mountain (45 km)	322692	183523	26058
Mountain (20 km)	301849	158257	7358
Sea-Level (45 km)	88216	44492	2581
Sea-Level (20 km)	97812	33010	-

Table 4.3: The additional key and total key generated by optimizing the two-fold coincidence rate compared with keeping the coincidence rate fixed. The first number is the amount of additional secure key bits shared per pass, the second number is the percentage increase. The conditions are: source and transmitter on a mountain, or at sea-level, source and transmitter 20 km away from a city, source and transmitter 45 km away from a city. There is no data for the median pass for a transmitter at sea-level and 20 km from Ottawa because it is not possible to exchange a key under these conditions. The median passes show the most improvement

SPDs with a detection efficiency of 50 % and DCR of 100 cps. In table 4.3 I present the additional key generated for each set of conditions, as well as what percentage increase over the non-optimized SKR this presents. Optimization helps the best in extreme conditions, when the loss or background counts are high. Optimization gives the greatest percentage increase for the medium passes over the upper quartile and best passes, for passes that are closer to Ottawa than further away, and for stations at sea-level over at the height of mountains.

The additional key and source rate are graphed in figure 4.4. During a satellite pass, the loss goes from a higher value to a minimum and then back up again as the angle towards the satellite changes such that the beam goes through more of the atmosphere. This means that optimizing gives the most extra key over the fringes of the pass, and can tranform previously unusable parts of the pass into usable parts. In some cases the amount of usable time more than doubles. Increasing the amount of time that QKD can be performed makes the transmission more robust against unpredictable changes in weather or turbulence. The source rate on the ground is reasonable considering today's entangled photon sources.

In an implementation of this model, experimentalists could measure the loss using a classical light source, and the DCR by turning off the source for a millisecond. They could then plug these numbers into the model, and compare this number against the measured two-fold coincidence rate in real-time. This would allow them to use the most of their satellite link, and adapt rapidly to changing conditions.

4.5 Discussion

In this chapter we have discussed how multi-photon squeezed states affect the upper bounds on SKR in QKD. However, suppose that instead of a set of polarization-correlated pair sources are combined on a beamsplitter, such as using quantum dots. The resulting quantum state would look like:

$$U_{pseudo-ideal} \mid 0000\rangle = (1-\epsilon^2) \mid 0000\rangle + \epsilon\sqrt{1-\epsilon^2}(\mid 1010\rangle + \mid 0101\rangle) + \epsilon^2 \mid 1111\rangle \quad (4.3)$$

We can also compare this to the 'optimal' source of entangled photons, which would produce quantum states such as:

$$U_{ideal} \mid 0000\rangle = \sqrt{1-\epsilon^2} \mid 0000\rangle + \frac{\epsilon}{\sqrt{2}}(\mid 1010\rangle + e^{i\theta} \mid 0101\rangle) \quad (4.4)$$

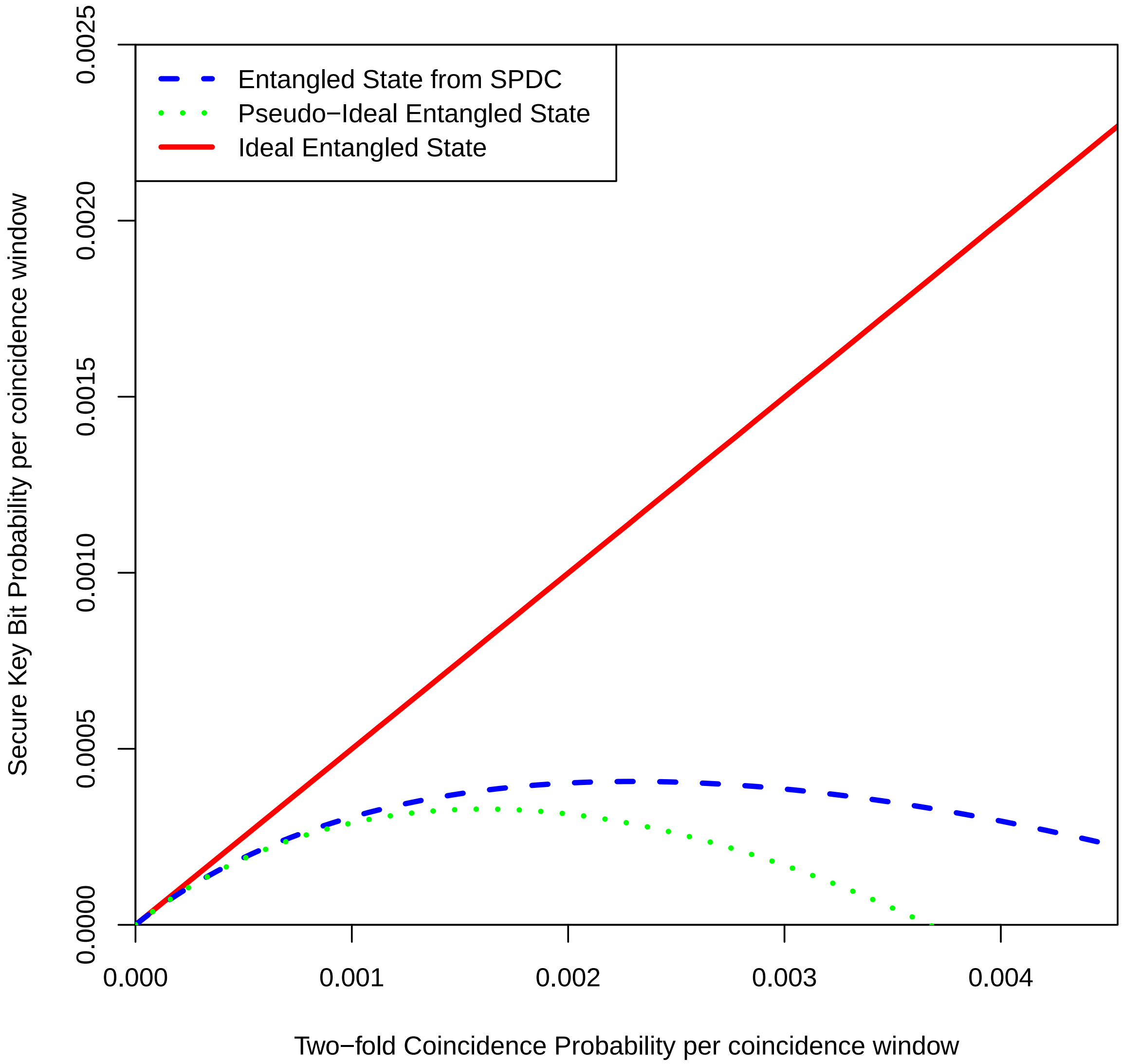


Figure 4.11: The probability of getting a secure key bit for a system with the corresponding two-fold coincidence probabilities for an ideal state (described in equation 4.4), a “pseudo-ideal” state (described in equation 4.3) and a state from SPDC sources (described in equation 2.28). The “pseudo-ideal” and SPDC source states both exhibit a maximum secure key probability, and both have multi-order terms. The ideal state has no maxima and increases linearly with increasing two-fold coincidences.

The relationship between two-fold coincidences and SKR are graphed in figure 4.11. The pseudo-ideal state exhibits a maxima, like the states from a SPDC source. Although the pseudo-ideal state does not have multi-photon terms like a squeezed state, there are cases when both pair sources emit a photon at the same time. This leads to double-clicks in detection, which increases the error rate as the two-fold coincidences. The pseudo-ideal state therefore has an optimal number of two-fold coincidences, just as an SPDC source does. The optimal does not occur at the same location as the SPDC source. What is interesting is that the squeezed states have an advantage over the directed pair sources in the pseudo-ideal state.

Of course, this analysis is not at the moment very practical as quantum dot sources of correlated photons can't match the production rate of SPDC processes, but it is an interesting point of inquiry.

4.6 Conclusions

I have developed a realistic simulation of QKD with entangled states from SPDC sources. I have implemented a new consistent model for bucket detectors, as well as dealing with detector double clicks. I have run an optimization algorithm on half a million different combinations of channel efficiencies and background noises. From this mountain of data I have distilled a useful and predictive model using symbolic regression.

I hope that in finding this relation, I have provided future experimentalists with a useful tool. At the moment many demonstrations of QKD with entangled photon pairs rely on low numbers of coincidences where the visibility is high[33, 44]. However, as detectors and sources improve and experimentalists compete for the new distance record, the issue of the tradeoffs between coincidence rate and visibility will have to be adressed. My model provides a simple method for maximizing the throughput of QKD systems, which relies only on presently measurable variables. I believe this model will allow for near real-time optimisation in pump power in real-world implementations such as on active telecommunications networks and satellite transmission, where background and losses change quickly and unpredictably. It could also provide a starting point for future theoretical exploration of this phenomenon.

Chapter 5

Hybrid Heralded Single Photon Source

In order to travel long distances around the world, QKD with entanglement will have to make use of LEO satellites, using the satellite as a trusted node. An entangled source suited for this application would be a hybrid of free-space and fiber transmission, where one of the entangled photons is optimized for transmission through the atmosphere, and one of the photons is optimized for transmission through optical fibers. Such an entangled photon source would be very useful from the perspective of relativistic quantum information, as one could study the effects of relativistic distances, and changing gravity fields on an entangled photon state.

As in chapter 3, current fiber optic channels experience the least amount of loss and dispersion at 1550 nm[47]. Infrared single photon detectors have highest efficiencies at around 1550 nm [89]. As discussed in chapter 2, 532 nm light is optimal for some visible light single photon detectors [84], and has low attenuation through the atmosphere [5].

In this chapter, I describe my efforts to construct the stepping stone to this entangled photon source: a heralded single photon source. Heralded single photon sources are in themselves very useful to science. This heralded single photon source can be changed into a sandwich source (described in section 2.4.1) by adding another identical crystal to the first at 90 degrees. Prisms can be used to compensate the polarization components in order to get the right phase on the bell state.

5.1 Uses of Heralded Single Photon Sources

Ou and Mandel were the first to propose using SPDC as a source of a single photon quantum state [45]. In their 1986 paper, they pumped a 8-cm-long potassium dihydrogen phostphate (KDP) crystal with 351.1 nm light to produce signal and idler photon paris at 746 nm and 659 nm. They use the signal photon to herald the detection of the idler. They report a pair detection rate of 14000 pairs per second.

In the 2000s, with the interest in quantum communication technologies, futher HSPSs were developed [4, 34, 81, 112].

One example where the use of an HSPS improved the measured quantum bound was in Kolenderski et. al.'s triple slit experiment [60]. The game being played is based on a qutrit state with two players, Alice and Bob, where the goal is for Alice to correctly guess the outcome of Bob's measurement, where Bob can access two of the three states. Played with classical states, Alice can do no better than chance - 50%. In the theoretical limit for the game with quantum states, Alice should always be able to guess correctly. Kolenderski et. al. devised an experimental set-up to test the game. When an attenuated diode laser was used, Alice won 82% of the time, when the experiment was repeated with photons from a heralded single photon source, Alice won 87% of the time.

5.2 Construction of a Heralded Single Photon Source

The HSPS constructed in this experiment used a bi-axial KTP crystal 5.2. A mode-locked Ti:Sapph laser was tuned to emit 792 nm light, which was then upconverted to 396 nm light in using Second Harmonic Generation in BBO crystal. This allowed use to pump the KTP crystal with pulsed 396 nm light, atmosphere [5].

5.2.1 Pump wavelength tuning

Energy conservation requires the production of photon pairs at 1550 nm and 532 nm to be pumped by photons at 396 nm. In order to produce pulses at 396 nm, second harmonic generation was used in a BBO 2 mm crystal. This is a common optical process, including in the construction of a sagnac source where the pump wavelength was doubled from 810 nm to 405 nm [101].

Due to the fact that BBO is a bi-axial crystal, previous experimenters have noticed walk-off effects which need to be compensated [101, 51]. We also encountered this effect in

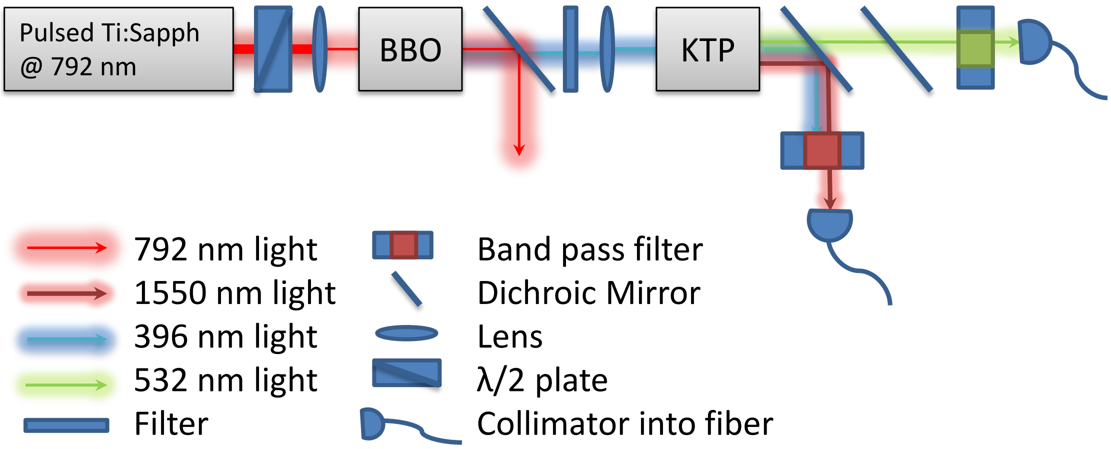


Figure 5.1: Experimental schematic for the HSPS described in this chapter.

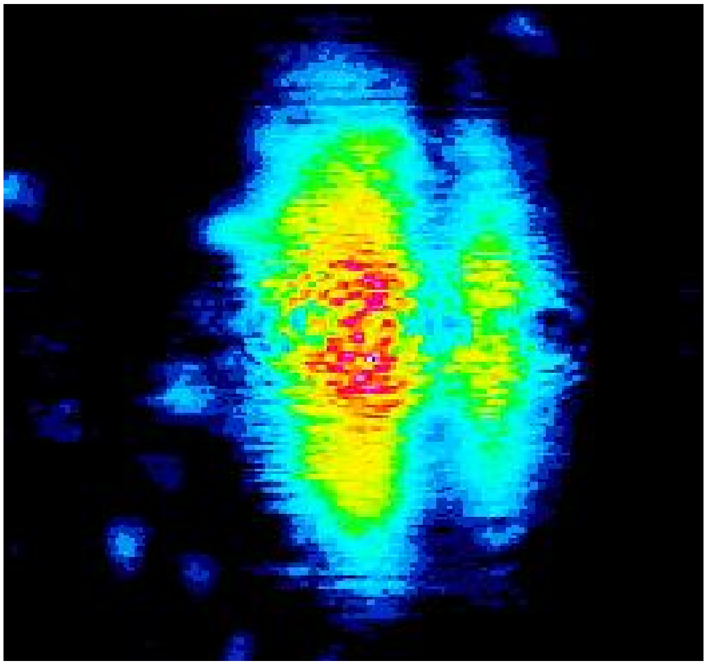


Figure 5.2: Imaged second harmonic beam with a continuous wave pump. The beam appears elliptical due to the walk-off effects in the crystal, and appears doubled due to the dichroic mirror used to separate the pump from the second harmonic.

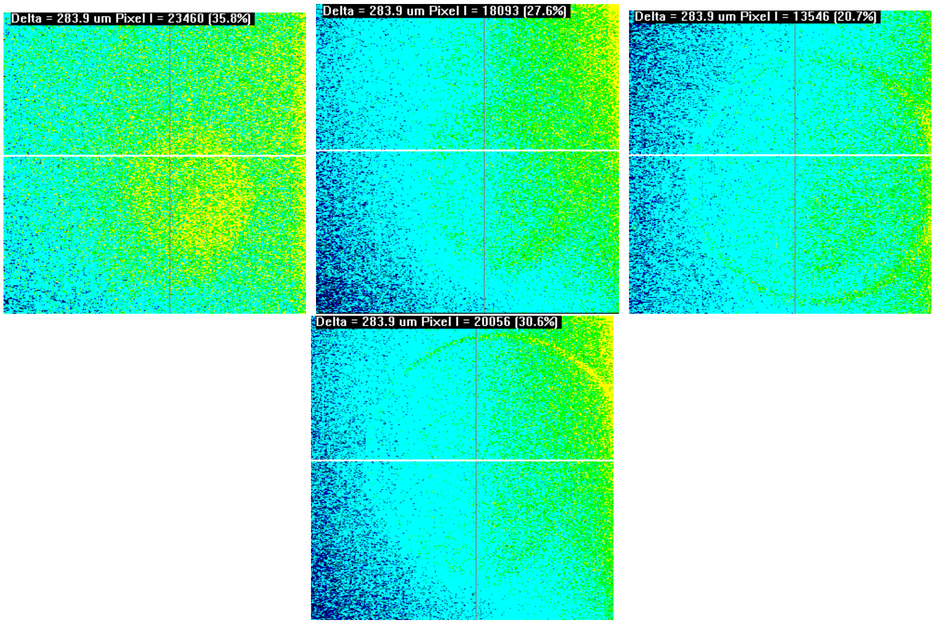


Figure 5.3: Imaged downconversion rings on a beam profiler CCD camera. From left to right, the images represent a tilt of 1 degree, 4 degrees, 10 degrees and 20 degrees.

our beam 5.2.1, which greatly decreased coupling efficiency. However, the beam appears much rounder when the pump was pulsed. In pulsed mode, we see 10% efficiency in conversion and 5% efficiency in coupling in pulsed mode, which means that 500 mW of pump power for the BBO crystal is converted into 2.5 mW pump power for the KTP crystal.

5.2.2 Alignment

In order to align the crystal for downconversion, the optical axis was measuredby placing a beam profiler after the crystal, and changing the pump polarization with a half-wave plate. Due to the large amount of beam walk-off, it was possible to see two beams on the profiler when the pump polarization was set to 45 degrees with respect to the crystal. By comparing the locations of the beams to an axis on the beam profiler perpendicular to the optical breadboard, we were able to precisely align the crystal's optical axis. Once this is done, the pump polarization could precisely be optimized fordownconversion by observing the amount of walkoff. Because, in a Type-I process, we expect a pump should be extraordinary and converted to an ordinary signal and an ordinary pump, and an

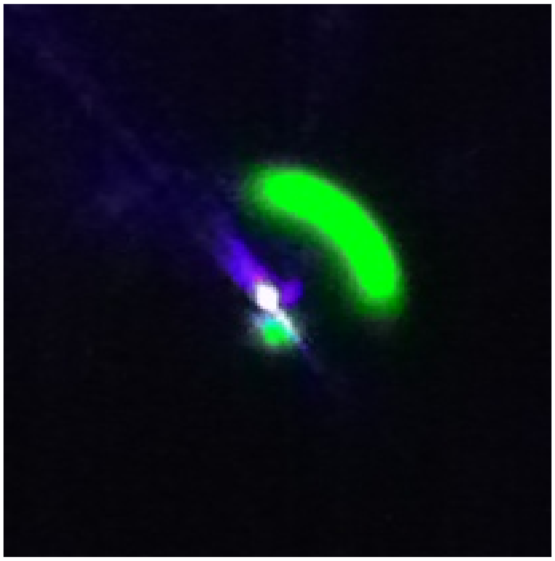


Figure 5.4: Image of downconversion rings taken with an iPod camera.

extraordinary polarization experiences the most walk-off in a crystal, in order to set the pump polarization we need to maximize the beam displacement.

A beam profiler was also used to assure that the pump was travelling parallel to the breadboard. This was done by a rough initial alignment was done with two mirrors in tilt stages and three pinholes. A beam profiler was then used to make sure that this beam was travelling at the same height with respect to the breadboard with an accuracy of $\pm 10 \mu m$. In order to attain a tight focus in the crystal, the beam was first expanded to a size of 12.5 mm using an aspheric lens with a focal length of 10 cm placed at the aperture of the single-mode optical fiber for 405 (thorlabs S405H). This beam was then focused by a uv-coated lens with a focal length of 10 cm. The beam profiler was then used to determine the location of the beam waist, and position the crystal in the beam waist. Using these lenses, we achieved a beam waist of $60 \mu m$.

Aligning the tilt of the crystal should be an easy process, as the crystal was ordered for this process and so was cut for the correct tilt angle, so it should be possible to align the crystal tilt by observing the back reflection. In practice, we found that the crystal needed to be tilted by 20 degrees compared to the manufacturing company's specifications. However, due to the high efficiency of the crystal for this downconversion process, assuming that the beam is tightly focused into the crystal, and the beam is travelling parallel to the breadboard, it should be possible to see the green rings of downconversion through a

	396 nm	532 nm	1550 nm
532 nm Coupler	4.78e-3	93.6	4.02
1550 nm Coupler	0.253	3.14e-4	92.1

Table 5.1: Expected transmittivities (in percent) of the wavelengths used in this source to the fiber couplers

532 nm band-pass filter with a minimal amount of pump power 1-3 mW, as evidenced by the resolution of the green rings on even an iPod camera - 5.2.2. These rings were imaged on a beam profiler using a 3 cm focal length lens. Images of the rings were captured at four different tilt angles in 5.2.2. The tilt of the crystal can be roughly set by eye by minimizing the size of the downconversion rings.

5.2.3 Beam separation

Several technical obstacles were overcome in building this source. The first was that due to the wavelengths chosen, finding appropriate optical elements was difficult. 532 nm and 396 nm are close in wavelength compared to 1550 nm, and few common applications involve both wavelengths simultaneously, thus few dichroics were available to separate these two beams. We used a 800 nm short-pass filter from thorlabs which had good reflectivity to 1550 nm and good transmittivity for 532 nm. The 396 nm was both transmitted and reflected, but the remaining 396 nm light was filtered out by more precise band-pass and long-pass filters at the entrance to each coupler. Below is a table with the estimated values of the transmittivity to each arm.

However, even with the dichroic mirror and the band pass filters in place, some 396 nm light coupled into the 532 nm fiber. This light appears to behave like signal, as when the counts in fiber are observed with SiAPDs. The counts increase and decrease sinosoidally with linear changes in the pump polarization, as the signal is expected to. This is due to the changing beam walk-off from the crystal. The counts in fiber also appear and disappear by tilting the crystal, but again this occurs due to beam walk-off. In addition, if a lot of 396 nm light is coupled to fiber, it can propagate in modes in the spectrometer that project into the grating range of 532 nm light, giving the appearance of having 532 nm light in the fiber. In order to couple to fiber, a third interference filter was used. Once some counts were seen in the SiAPDs, the light was observed in the spectrometer. If some counts were observed in the 532 nm range, but none in the 396 nm range, then it is likely that the signal was coupled into fiber. Once this coupling is optimized, it is possible to remove the third filter without too many additional 396 nm counts.

5.2.4 Mode-matching

Another technical challenge was making sure that the spatial modes of the signal and idler matched the back-propagating modes of the 1550 nm and 532 nm couplers. Originally, we planned on using collimmated beams in our source, for ease of coupling. However, our crystal is very short (3 mm), and PDC processes are more efficient with tight focus, so collimated beams were avoided in favor of achieving a very tight focus on the crystal. This made it more difficult to couple light into fiber, as the distance of the fiber tip to the coupling lens and the crystal then became important. The mode was estimated by minimizing the beam waist of the backpropagated beam at various different distances of the beam profiler to the crystal. The coupler was then moved to a distance where the optimized beam waist was 120 μm (twice the beam waist of the pump in the crystal)

Since the detectors being used (idQuantique 201) have multi-mode fiber inputs, we chose to use multi-mode fiber in the coupler in order to maximize counts. this also allowed for the use of red light in alignment for the 1550 nm arm since we expect it to have a similar beam size coming out of multi-mode fiber as 1550 nm light. Using visible light instead of infrared light alows for easier alignment, and for the same beam profiler to be used for both 1550 nm and 532 nm arms to compare beam waist with back-propagation.

5.2.5 Timing Adjustment

Once single photons were coupled into both telecom and green couplers and measured in the detectors, detector signals were fed into a Becker-Hickl single photon counting card. A peak of 3000 cps was observered in the histogram of coincidences. This allowed us to determine the delay between photon measurements in both arms. 20 m of multi-mode fiber was added between the telecom coupler and detector in order to create an artificial delay between detectors.

5.3 Comparison of HSPS

Our source is either more efficient or cheaper than the state of the art. Soujaeff et. al. pumped a BBO crystal with 390 nm pulses generated off of SHG from a Ti:Sapph laser to produce photon pairs at 520 nm and 1550 nm [103]. They report the production of 2.16×10^5 singles in green for 230 mW of pump power. We achieve 4.50×10^4 with a pump power of 2.2 mW of pump power.

Söller et al. [102] use four-wave-mixing (FWM) in specially designed and manufactured photonic crystal fiber (PCF) to create photon pairs at 1542 nm and 514 nm. With a pump power of 100 μW they measured a coincidence rate of 1.3×10^3 counts/s with signal and idler count rates of 16.5×10^3 and 6.0×10^3.

5.4 Conclusion

Based on the initial measurements of the signal photons in this SPDC process, this photon source has the potential to be very efficient compared to previous heralded single photon source. Do to time constraints, and difficulty in using the doubler, I have yet to efficiently collect the infrared photons in single-mode-fiber, but I am optimistic that I will see them in the future.

Chapter 6

Conclusions

In chapter 1, I motivated the need for QKD by estimating the date at which, assuming accelerating returns on computational power, the current length of RSA keys will be cracked assuming computers that cost $\$1\times10^6$, and $\$1\times10^3$. From these estimates, we can see that all current computational security is not *future-proof*, that is, that any eavesdropped 'secure' traffic has a secrecy lifespan of approximately 10 years.

In chapter 2, I introduced the concept of using the polarization states of photons to represent quantum bits of information. I also introduced the concept of entanglement and explained the process of generating entangled states from nonlinear processes in birefringeant crystals. I described the method of measuring these qubit states. I described the mathematical models for entangled photon states and bucket-detectors. I explained the protocols used for sharing a one-time-pad over a public channel using entangled photons and how the minimum amount of error an eavesdropper can introduce and gain useful secret information. Finally, I covered the calculation for the amount of secure key left over after error correction and privacy amplification.

In chapter 3, I experimentally demonstrated the compatibility of quantum key distribution using entangled photons at 810 nm on a standard single mode telecommunications fiber carrying signals from a gigabit internet transceiver at 1550 nm. This method of integrating QKD on active telecommunications networks involves very little cost as fused biconical fiber splitters were used to separate the quantum signal from the classical signal. Given the widespread adoption of passive optical fiber networks, and the efforts to get fiber from device to device, it is feasible that this method of hybrid systems will someday be used to share secrets between two computers. The distribution of entangled photons also has future applications in quantum repeater networks, blind quantum computing, and quantum teleportation. The mixing processes between quantum and classical signals were studied and found to be minimal in the quantum band. This experiment was conducted using the current longest-range optical gigabit internet protocol that is commercially available. It is also the highest-optical power protocol due to being the longest-ranged protocol, so we would expect the mixing processes to be reduced on other standards. We demonstrated that this system could reach 8 km, and could theoretically reach 16 km using an optimized source. With improvement in detector efficiencies, timing resolution and lower dark counts, this could reach even further.

After conducting the experiment in chapter 3, I wondered about the problem of optimal source rates, and whether it was possible to develop an equation useful to experimentalists that would describe the optimal measured source rate for any combination of detector dark counts and channel losses. In chapter 4, I wrote a simulation of QKD with entanglement using python based on the math described in chapter 2, used an optimization algorithm to determine the optimal squeezing rate, and simulated two-fold coincidence and secure key rates for half a million different combinations of channel efficiency and dark counts. These data points were fed into Eureqa Formulize in order to distill a meaningful equation from this mountain of data. The simulation and optimization method were compared against previous analytical work for validation. The simulation and optimal were compared against experimental data for validation. Two applications of the model were suggested: in estimating the maximum possible distance of fiber-based implementations with the state-of-the-art in single photon detection, and in optimizing the amount of key possible with a LEO satellite pass. The model has significant improvement in extending the range of QKD systems, where the loss is extreme.

If QKD with entanglement is to have a global reach, satellites will have to be used in this optical network. It would be very useful to have a hybrid source of entangled photons, which can bridge the gap between satellite and fiber transmission. However, many entangled photon sources in use today have both photons at the same wavelength. The best band of wavelengths for transmission through the atmosphere is very far from the best band of wavelengths for transmission in optical fiber. In chapter 5, I worked on a hybrid heralded single photon source, a stepping-stone in building a hybrid entangled photon source, where one photon is at a wavelength suitable for transmission through the atmosphere and one photon is at a wavelength suitable for transmission through an optical fiber. Preliminary results suggest that this photon source has a very high conversion efficiency.

After reading this thesis, my goal is that I have convinced you of three things:

1. That QKD is necessary

2. That QKD can be integrated into existing infrastructure
3. That QKD can be optimized beyond the lab setting

References

[1] Fibre channel low-cost 10-km optical 1063-mbaud interface (100-sm-lc-l).

[2] G.P. Agrawal. *Nonlinear Fiber Optics*. Optics and Photonics. Academic Press, 2006.

[3] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98:060503, Feb 2007.

[4] O. Alibart, D.B. Ostrowsky, P. Baldi, and S. Tanzilli. High-performance guided-wave asynchronous heralded single-photon source. *Optics letters*, 30(12):1539–1541, 2005. hsps.

[5] G.P. Anderson, A. Berk, P.K. Acharya, M.W. Matthew, L.S. Bernstein, J.H. Chetwynd Jr, H. Dothe, S.M. Adler-Golden, A.J. Ratkowski, G.W. Felde, et al. Modtran4: radiative transfer modeling for remote sensing. In *Proceedings of SPIE*, volume 3866, page 2, 1999.

[6] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via bell's theorem. *Physical Review Letters*, 47(7):460–463, 1981.

[7] J S Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1(3):195–200, 1964.

[8] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[9] C.H. Bennett and G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *ACM Sigact News*, 20(4):78–80, 1989.

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

[11] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without bells theorem. *Physical Review Letters*, 68(5):557–559, 1992.

[12] D. Bohm. *Quantum theory*. Dover Pubns, 1951.

[13] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[14] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in CryptologyEUROCRYPT93*, pages 410–423. Springer, 1994.

[15] GS Buller and RJ Collins. Single-photon generation and detection. *Measurement Science and Technology*, 21:012002, 2010.

[16] L. Cai, Z. Liu, S. Xiao, M. Zhu, R. Li, and W. Hu. Video-service-overlaid wavelength-division-multiplexed passive optical network. *Photonics Technology Letters, IEEE*, 21(14):990–992, 2009.

[17] TE Chapuran, P. Toliver, NA Peters, J. Jackel, MS Goodman, RJ Runser, SR McNown, N. Dallmann, RJ Hughes, KP McCabe, et al. Optical networking for quantum key distribution and quantum communications. *New Journal of Physics*, 11:105001, 2009.

[18] J Chen, G Wu, L Xu, X Gu, E Wu, and H Zeng. Stable quantum key distribution with active polarization control based on time-division multiplexing. *New Journal of Physics*, 11(6):065004, 2009.

[19] I. Choi, R.J. Young, and P.D. Townsend. Quantum information to the home. *New Journal of Physics*, 13:063039, 2011.

[20] Cisco. Cisco small form-factor pluggable modules for gigabit ethernet applications data sheet. online: http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecd8033f885.pdf, 2012.

[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23:880–884, October 1969.

[22] RJ Collins, PJ Clarke, V. Fernandez, KJ Gordon, MN Makhonin, JA Timpson, A. Tahraoui, M. Hopkinson, AM Fox, MS Skolnick, et al. Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source. *Journal of Applied Physics*, 107(7):073102–073102, 2010.

[23] J.N. Damask. *Polarization optics in telecommunications*, volume 101. Springer Verlag, 2005.

[24] P.J. Delfyett, S. Gee, M.T. Choi, H. Izadpanah, W. Lee, S. Ozharar, F. Quinlan, and T. Yilmaz. Optical frequency combs from semiconductor lasers and applications in ultrawideband signal processing and communications. *Lightwave Technology, Journal of*, 24(7):2701–2719, 2006.

[25] JF Dynes, H. Takesue, ZL Yuan, AW Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, et al. Efficient entanglement distribution over 200 kilometers. *Optics Express*, 17(14):11440–11449, 2009.

[26] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[27] A.K. Ekert. Quantum cryptography based on bells theorem. *Physical review letters*, 67(6):661–663, 1991.

[28] David Elkouss, Anthony Leverrier, Romain Alleaume, and Joseph Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. *CoRR*, abs/0901.2140, 2009.

[29] David Elkouss, Jesús Martínez-Mateo, Daniel Lancho, and Vicente Martin. Rate compatible protocol for information reconciliation: An application to qkd. *CoRR*, abs/1006.2660, 2010.

[30] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12:063027, 2010.

[31] C. Erven. On free space quantum key distribution and its implementation with a polarization-entangled parametric down conversion source. 2007.

[32] C. Erven. *On Experimental Quantum Communication and Cryptography*. PhD thesis, University of Waterloo, 2012.

[33] C. Erven, C. Couteau, R. Laflamme, and G. Weihs. Entangled quantum key distribution over two free-space optical links. *Opt. Express*, 16(21):16840–16853, Oct 2008.

[34] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden. High-quality asynchronous heralded single-photon source at telecom wavelength. *New Journal of Physics*, 6:163, 2004. hsps.

[35] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Optics Express*, 15(23):15377–15386, 2007.

[36] S.J. Freedman and J.F. Clauser. Experimental test of local hidden-variable theories. *Physical Review Letters*, 28(14):938–941, 1972.

[37] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Physical Review A*, 56(2):1163, 1997.

[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145–195, 2002.

[39] Oleg Gittsovich. personal communication, 2012.

[40] E. A. Goldschmidt, M. D. Eisaman, J. Fan, S. V. Polyakov, and A. Migdall. Spectrally bright and broad fiber-based heralded single-photon source. *Phys. Rev. A*, 78:013844, Jul 2008. HSPS.

[41] D. Gottesman, H.K. Lo, N. Lutkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, 2004.

[42] B.L. Higgins, J.P. Bourgoin, N. Gigov, E. Meyer-Scott, Z. Yan, and T. Jennewein. Detailed performance analysis of the proposed qeyssat quantum receiver satellite. In *CLEO: Applications and Technology*. Optical Society of America, 2012.

[43] PA Hiskett, D. Rosenberg, CG Peterson, RJ Hughes, S. Nam, AE Lita, AJ Miller, and JE Nordholt. Long-distance quantum key distribution in optical fibre. *New Journal of Physics*, 8:193, 2006.

[44] Catherine Holloway, Evan Meyer-Scott, Chris Erven, and Thomas Jennewein. Quantum entanglement distribution with 810 nm photons through active telecommunication fibers. *Opt. Express*, 19(21):20597–20603, Oct 2011.

[45] C. K. Hong and L. Mandel. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58–60, Jan 1986.

[46] H. Hübel, M.R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger. High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber. *Optics Express*, 15(12):7853–7862, 2007.

[47] Corning Incorporated. Corning smf-28tm optical fiber product information. Technical report, Corning Incorporated, 2002.

[48] John David Jackson. *Classical Electrodynamics, Third Edition.* John Wiley & Sons New York, 1999.

[49] Bassam Helou Jean-Philippe Bourgoin, Evan Meyer-Scott and Thomas Jennewein. Detailed link analysis of satellite quantum communication. In *QCRYPT 2011*, 2011.

[50] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters*, 84(20):4729–4732, 2000.

[51] Thomas Jennewein. *Quantum Communication and Teleportation Experiments using Entangled Photon Pairs.* PhD thesis, University of Vienna, 2002.

[52] Thomas Jennewein, Marco Barbieri, and Andrew G. White. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. *Journal of Modern Optics*, 58:276 – 287, 2011.

[53] JR Johansson, PD Nation, and F. Nori. Qutip: An open-source python framework for the dynamics of open quantum systems. *Arxiv preprint arXiv:1110.0573*, 2011.

[54] Fredrik Jonsson. *Lecture Notes On Nonlinear Optics.* Transactions of the Royal Institute of Technology, Stockholm, Sweden, 2003.

[55] C. Kim and G. Li. Direct-detection optical differential 8-level phase-shift keying (od8psk) for spectrally efficient transmission. *Opt. Express*, 12(15):3415–3421, 2004.

[56] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik, et al. Factorization of a 768-bit rsa modulus. *Advances in Cryptology–CRYPTO 2010*, pages 333–350, 2010.

[57] V. Klima. Tunnels in hash functions: Md5 collisions within a minute. 2006.

[58] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto. Security of entanglement-based quantum key distribution with practical detectors. *ArXiv e-prints*, April 2008.

[59] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.*, 90:057902, Feb 2003.

[60] P. Kolenderski, U. Sinha, L. Youning, T. Zhao, M. Volpini, A. Cabello, R. Laflamme, and T. Jennewein. Playing the aharon-vaidman quantum game with a young type photonic qutrit. *Arxiv preprint arXiv:1107.5828*, 2011.

[61] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters*, 75(24):4337–4341, 1995.

[62] P.G. Kwiat, A.M. Steinberg, and R.Y. Chiao. Observation of a quantum eraser: A revival of coherence in a two-photon interference experiment. *Physical Review A*, 45(11):7729, 1992.

[63] PG Kwiat, E. Waks, AG White, I. Appelbaum, and PH Eberhard. Ultrabright source of polarization-entangled photons. *Physical Review A*, 60(2), 1999.

[64] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin. Qkd in standard optical telecommunications networks. *Quantum Communication and Quantum Networking*, pages 142–149, 2010.

[65] J. Lavoie, R. Kaltenbaek, and K.J. Resch. Experimental violation of svetlichny's inequality. *New Journal of Physics*, 11:073051, 2009.

[66] Hwang Lee, Ulvi Yurtsever, Pieter Kok, George Hockney, Christoph Adami, Samuel Braunstein, and Jonathan Dowling. Towards photostatistics from photon-number discriminating detectors. *Journal of Modern Optics*, 51:15171528, 2004.

[67] A. Lenstra, H. Lenstra, M. Manasse, and J. Pollard. The number field sieve. *The development of the number field sieve*, pages 11–42, 1993.

[68] Han Chuen Lim, Akio Yoshizawa, Hidemi Tsuchida, and Kazuro Kikuchi. Distribution of polarization-entangled photon pairs produced via spontaneous parametricdown-conversion within a local-area fibernetwork: Theoretical model and experiment. *Opt. Express*, 16(19):14512–14523, Sep 2008.

[69] Norbert Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59:3301–3319, May 1999.

[70] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76(1):012307, Jul 2007.

[71] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[72] D. Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, 48(3):351–406, 2001.

[73] E. Meyer-Scott, H. Hubel, A. Fedrizzi, C. Erven, G. Weihs, and T. Jennewein. Quantum entanglement distribution with 810 nm photons through telecom fibers. *Applied Physics Letters*, 97(3):031117, 2010.

[74] E. Meyer-Scott, Z. Yan, A. MacDonald, J.P. Bourgoin, H. Hübel, and T. Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss. *Physical Review A*, 84(6):062326, 2011.

[75] Tobias Moroder, Otfried Gühne, Normand Beaudry, Marco Piani, and Norbert Lütkenhaus. Entanglement verification with realistic measurement devices via squashing operations. *Phys. Rev. A*, 81:052342, May 2010.

[76] K. Nagayama, M. Kakui, M. Matsui, I. Saitoh, and Y. Chigusa. Ultra-low-loss (0.1484 db/km) pure silica core fibre and extension of transmission distance. *Electronics Letters*, 38(20):1168–1169, 2002.

[77] ZY Ou and L. Mandel. Violation of bell's inequality and classical probability in a two-photon correlation experiment. *Physical review letters*, 61(1):50–53, 1988.

[78] Cheng-Zhi Peng, Tao Yang, Xiao-Hui Bao, Jun Zhang, Xian-Min Jin, Fa-Yong Feng, Bin Yang, Jian Yang, Juan Yin, Qiang Zhang, Nan Li, Bao-Li Tian, and Jian-Wei Pan. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94(15):150501, Apr 2005.

[79] A. Peres. *Quantum theory: concepts and methods*, volume 57. Springer, 1993.

[80] NA Peters, P. Toliver, TE Chapuran, RJ Runser, SR McNown, CG Peterson, D. Rosenberg, N. Dallmann, RJ Hughes, KP McCabe, et al. Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of Physics*, 11:045012, 2009.

[81] TB Pittman, BC Jacobs, and JD Franson. Heralding single photons from pulsed parametric down-conversion. *Optics communications*, 246(4-6):545–550, 2005. hsps.

[82] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, et al. Practical quantum key distribution with polarization entangled photons. *Optics Express*, 12(16):3865–3871, 2004.

[83] B. Qi, L.L. Huang, L. Qian, and H.K. Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Physical Review A*, 76(5):052323, 2007.

[84] I. Rech, G. Luo, M. Ghioni, H. Yang, X.S. Xie, and S. Cova. Photon-timing detector module for single-molecule spectroscopy with 60-ps resolution. *Selected Topics in Quantum Electronics, IEEE Journal of*, 10(4):788–795, 2004.

[85] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. *Theory of Cryptography*, pages 407–425, 2005.

[86] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Optics Express*, 13:202–+, January 2005.

[87] P. Rice and I. J. Owens. Comparison between continuous wave and pulsed laser eqkd systems. *ArXiv e-prints*, September 2008.

[88] T. Rudolph. Introduction to quantum information - lecture 8: Maximum likelihood classical probability distribution discrimination. online, October 2011.

[89] ID Quantique SA. id201 series single-photon detector for the near infrared. Datasheet, ID Quantique SA, 2010.

[90] B.E.A. Saleh and M.C. Teich. *Fundamentals of photonics*. John Wiley & Sons New York, 2007.

[91] A. Sano, H. Masuda, T. Kobayashi, M. Fujiwara, K. Horikoshi, E. Yoshida, Y. Miyamoto, M. Matsui, M. Mizoguchi, H. Yamazaki, et al. 69.1-tb/s (432 x 171-gb/s) c-and extended l-band transmission over 240 km using pdm-16-qam modulation and digital coherent detection. In *Optical Fiber Communication Conference*. Optical Society of America, 2010.

[92] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

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

[94] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, et al. Feasibility of 300 km quantum key distribution with entangled states. *New Journal of Physics*, 11:085002, 2009.

[95] Michael Schmidt and Hod Lipson. Distilling free-form natural laws from experimental data. *Science*, 324(5923):81–85, 2009.

[96] A. A. Semenov and W. Vogel. Entanglement transfer through the turbulent atmosphere. *Phys. Rev. A*, 81:023835, Feb 2010.

[97] C.E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28(4):656–715, 1949.

[98] B.S. Shi and A. Tomita. Generation of a pulsed polarization entangled photon pair using a sagnac interferometer. *Physical Review A*, 69(1):11, 2004.

[99] M. Shtaif, M. Eiselt, and L.D. Garrett. Cross-phase modulation distortion measurements in multispan wdm systems. *Photonics Technology Letters, IEEE*, 12(1):88–90, 2000.

[100] U. Sinha, C. Couteau, Z. Medendorp, I. Söllner, R. Laflamme, R. Sorkin, and G. Weihs. Testing born's rule in quantum mechanics with a triple slit experiment. *Arxiv preprint arXiv:0811.2068*, 2008.

[101] Devin Smith. An ultrafast source of polarization entangled photon pairs based on a sagnac interferometer. Master's thesis, University of Waterloo, 2009.

[102] C. Söller, B. Brecht, PJ Mosley, LY Zang, A. Podlipensky, NY Joly, P.S.J. Russell, and C. Silberhorn. Bridging visible and telecom wavelengths with a single-mode broadband photon pair source. *Physical Review A*, 81(3):31801, 2010.

[103] A. Soujaeff, S. Takeuchi, K. Sasaki, T. Hasegawa, and M. Matsui. Heralded single photon source at 1550 nm from pulsed parametric down conversion. *Journal of Modern Optics*, 54(2-3):467–471, 2007. hsps very similar to mine.

[104] S.P.C.M. SPCM and A.Q.R.S.D. Sheet. Perkinelmer optoelectronics, 2001.

[105] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4:41, 2002.

[106] S.M. Tan. A computational toolbox for quantum and atomic optics. *Journal of Optics B: Quantum and Semiclassical Optics*, 1:424, 1999.

[107] RW Tkach, AR Chraplyvy, F. Forghieri, AH Gnauck, and RM Derosier. Four-photon mixing and high-speed wdm systems. *Lightwave Technology, Journal of*, 13(5):841–849, 1995.

[108] J.S. Townsend. *A modern approach to quantum mechanics.* Univ Science Books, 2000.

[109] P.D. Townsend. Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems. *Photonics Technology Letters, IEEE*, 10(7):1048–1050, 1998.

[110] Alexander Treiber, Andreas Poppe, Michael Hentschel, Daniele Ferrini, Thomas Lornser, Edwin Querasser, Thomas Matyus, Hannes Hbel, and Anton Zeilinger. A fully automated entanglement-based quantum cryptography system for telecom fiber networks. *New Journal of Physics*, 11(4):045013, 2009.

[111] A. Trifonov and A. Zavriyev. Secure communication with a heralded single-photon source. *Journal of Optics B: Quantum and Semiclassical Optics*, 7:S772, 2005. hsps use.

[112] A.B. URen, C. Silberhorn, K. Banaszek, and I.A. Walmsley. Efficient conditional preparation of high-fidelity single photon states for fiber-optic quantum networks. *Physical review letters*, 93(9):93601, 2004. hsps.

[113] Samuel Varghese. *Fabrication and Characterization of All-Fiber Components for Optical Access Networks*. PhD thesis, International School of Photonics Cochin University of Science and Technology, 2008.

[114] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, 2005.

[115] X. Wang, D. Feng, X. Lai, and H. Yu. Collisions for hash functions md4, md5, haval-128 and ripemd. Technical report, Cryptology ePrint Archive, Report 2004/199, 2004.

[116] S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[117] F.N.C. Wong, JH Shapiro, and T. Kim. Efficient generation of polarization-entangled photons in a nonlinear crystal. *Laser physics*, 16(11):1517–1524, 2006.

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

[119] F. Yaman, N. Bai, YK Huang, MF Huang, B. Zhu, T. Wang, and G. Li. 10 x 112gb/s pdm-qpsk transmission over 5032 km in few-mode fibers. *Opt. Express*, 18(20):21342–21349, 2010.

Appendices

Appendix A

Contributions to the Spacelike-separated GHZ state measurement

A.1 Polarisation Stability Measurements

In order to preform the GHZ measurement, it is essential that the fibers being used do not introduce an arbitrary, changing unitary on the qubit states being transmitted from the lab on the first floor of RAC1 to the Crow's Nest where the transmitting telescopes are.

These transformations occur in fiber either due to nonlinear effects at high-power [2] or due to the birefringence induced by mechanical relaxation. The negative effect of these

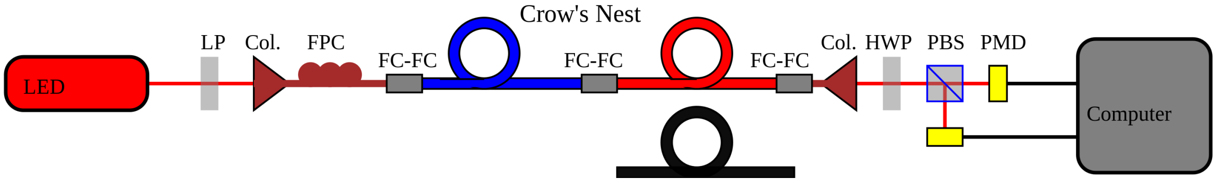
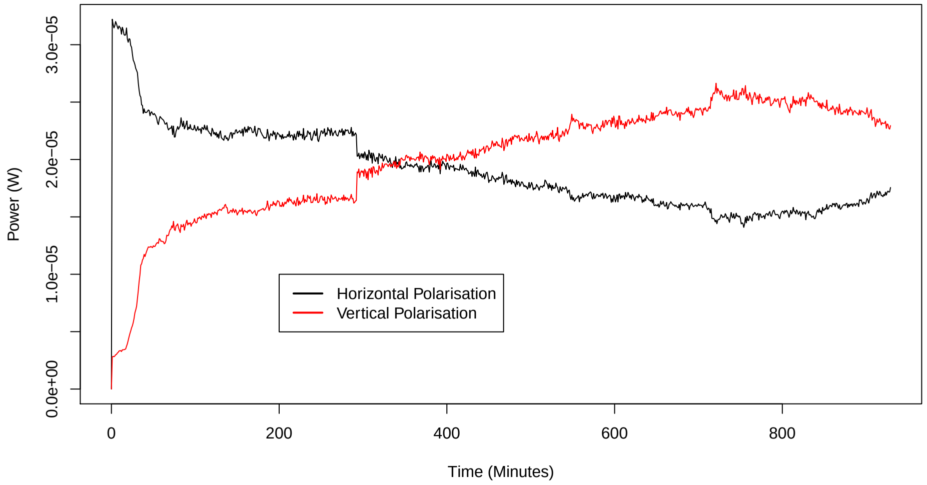
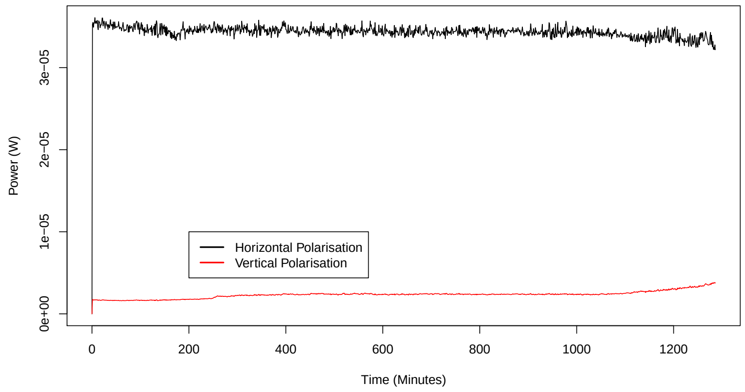
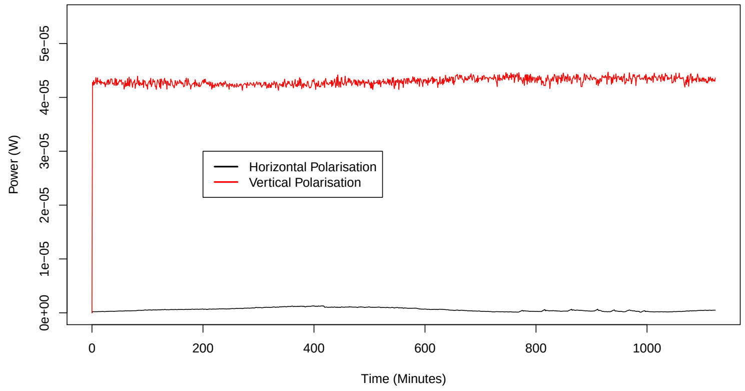


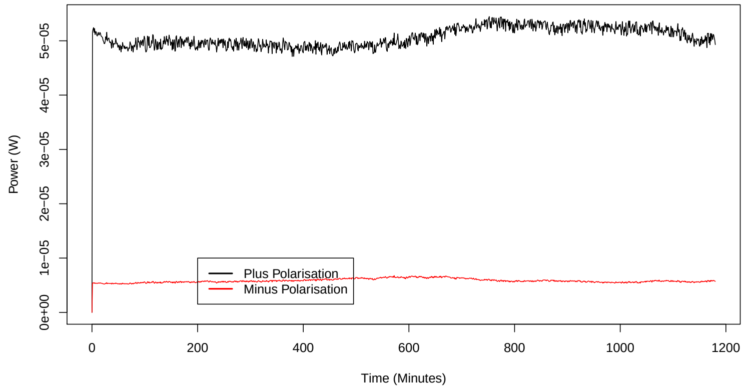
Figure A.1: Schematic of measurement device. In this diagram, the LED is a low-power thorlabs LED at 805 nm. LP= Linear polarizer, Col.= FC Collimator, FPC= fiber polarisation controller (bat-ears), FC-FC = FC-FC mating adaptor, HWP= half-wave-plate, PBS= Polarising beam splitter, and PMD= Thorlabs PM100D power meter with S120C series silicon detector.

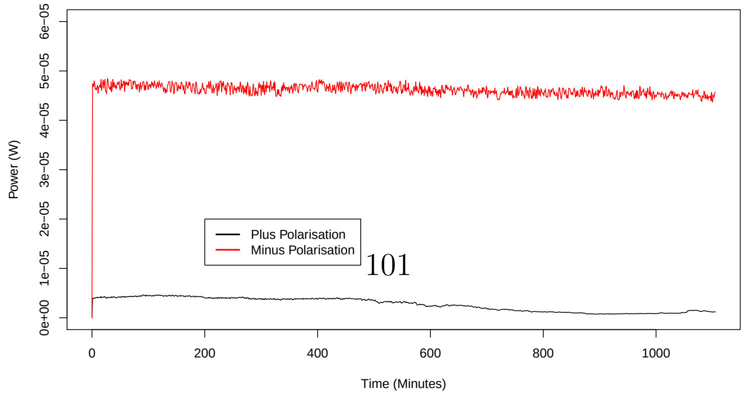


Fiber	State	Mean	Standard Deviation	Fidelity	Fidelity Variance
Red-Blue	H	3.436866e-05	7.849665e-13	0.9676887	3.338525e-05
Red-Blue	V	4.300512e-05	1.176338e-12	0.9931433	4.324852e-05
Red-Blue	D	5.068855e-05	3.630523e-12	0.9468985	1.071008e-05
Red-Blue	A	4.613969e-05	1.447756e-12	0.9721938	0.0001752664
Red-Black	D	4.755868e-05	2.240796e-12	0.9305715	2.134126e-05
Red-Black	A	5.120781e-05	1.697286e-12	0.958844	4.601961e-05


Power (W)
0e+00
1e−05
2e−05
3e−05
0
200
400
600
800
1000
1200
Time (Minutes)
Horizontal Polarisation
Vertical Polarisation


Power (W)
0e+00
1e−05
2e−05
3e−05
4e−05
5e−05
0
200
400
600
800
1000
Time (Minutes)
Horizontal Polarisation
Vertical Polarisation


Power (W)
0e+00
1e−05
2e−05
3e−05
4e−05
5e−05
0
200
400
600
800
1000
1200
Time (Minutes)
Plus Polarisation
Minus Polarisation


Power (W)
0e+00
1e−05
2e−05
3e−05
4e−05
5e−05
6e−05
0
200
400
600
800
1000
Time (Minutes)
Plus Polarisation
Minus Polarisation

transformations can be measured in a drift of the polarisation states sent through the fibers. This drift will cause an increase in QBER over time, which can limit the useful time of a GHZ state measurement. Given that a successful GHZ state measurement requires the near-simultaneous detection of four photons simultaneously [65] several times in order to build up a bayesian estimate of probability, a GHZ state measurement has to occur over a long time.

In order to measure the polarisation drift over time due to the fibers, the light of a Thorlabs low-power LED was polarised and coupled into fiber. The polarisation state was then transformed into a canonical state using a fiber polarisation controller (also colloquially known as fiber bat-ears). This light was then sent up to the roof through one of the three fibers and then sent back down to lab using another three fibers. The light is transferred between fibers using an FC-FC mating sleeve. The three fibers are labeled blue, red, and black. Back in the lab, the light is sent through a half-wave-plate and a polarising beam splitter. Collimators are used to couple the light into fibers and these fibers are attached to silicon visible-light power meters (Thorlabs S120C-series) which are then attached to meters (Thorlabs PM100D).

A program was written in C# that read the power off of the meters via USB and NI-VISA. Measurements were averaged over a time period of two seconds.

Appendix B

Acronyms used in this thesis

APD - Avalanche Photo-Diode

BB84 - Bennett and Brassard's 1984 QKD protocol

BBM92 - Bennet, Brassard and Mermin's 1992 QKD protocol

BBO - Beta barium borate ($\beta - BaB_2O_4$)

CEIT - Center for Environment and Information Technology

CCD - charge-coupled device

CSA - Canadian Space Agency

CWDM - Coarse Wavelength Division Multiplexing

DWDM - Dense Wavelength Division Multiplexing

E91 - Ekert's 1991 QKD protocol

Gbps - Giga-bits per second

GHZ - Greenberger-Horne-Zeilinger state

GNFS - General number field sieve

HSPS - Heralded Single Photon State

HWP - Half-Wave Plate

IQC - Institute for Quantum Computing

KDP - Potassium dihydrogen phosphate

KTP - Potassium titanyl phosphate

MMF - Multi-Mode Fiber

PBS - Polarizing Beam Splitter

PDC - Parametric down conversion

PI - Perimeter Institute

QBER - Quantum Bit Error Rate

QKD - Quantum Key Distribution

QRNG - Quantum Random Number Generator

QWP - Quarter-Wave Plate

SHG - Second Harmonic Generation

Si-APD - Silicon Avalanche Photo-Diode

SKR - Secure Key Rate

SMF - Single-Mode Fiber

SPDC - Spontaneous parametric down-conversion

WCP - Weak Coherent Pulses

WDM - Wavelength Division Multiplexing

UV - Ultra-Violet

Appendix C

Additional proofs

C.1 Expectation values of a Bell state measurement with a CHSH formulation

See Peres' quantum physics book [79] for a more general example of the following.

The Bell state being measured is:

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{C.1}$$

Alice and Bob's measurements are rotations, where $A(a) = rot(0), A(a') = rot(\frac{\pi}{4}), B(b) = rot(\frac{\pi}{8}), B(b') = rot(\frac{3\pi}{8})$. We can use the fact that for any two qubits, their expectation value is equal to:

$$\langle \sigma_a \otimes \sigma_b \rangle = cos2(\alpha - \beta) \tag{C.2}$$

Where α and β are the angles that represent the orientation of the qubit when projected into a two-dimensional space, for example, $\mid \psi\rangle_a = sin(\alpha) \mid 0\rangle + cos(\alpha) \mid 1\rangle$, and $\mid \psi\rangle_b =$

$sin(\beta) \mid 0\rangle + cos(\beta) \mid 1\rangle$. Using this equation, we can calculate:

$$\langle\phi \mid A(a) \otimes B(b) \mid \phi\rangle = cos2(\frac{-\pi}{4} - \frac{7\pi}{8}) \qquad = cos(\frac{-\pi}{4}) = \frac{\sqrt{2}}{2} \tag{C.3}$$

$$\langle\phi \mid A(a) \otimes B(b') \mid \phi\rangle = cos2(\frac{-\pi}{4} - \frac{9\pi}{8}) \qquad = cos(\frac{-3\pi}{4}) = -\frac{\sqrt{2}}{2} \tag{C.4}$$

$$\langle\phi \mid A(a') \otimes B(b) \mid \phi\rangle = cos2(0 - \frac{7\pi}{8}) \qquad = cos(\frac{-\pi}{4}) = \frac{\sqrt{2}}{2} \tag{C.5}$$

$$\langle\phi \mid A(a') \otimes B(b') \mid \phi\rangle = cos2(0 - \frac{9\pi}{8}) \qquad = cos(\frac{-\pi}{4}) = \frac{\sqrt{2}}{2} \tag{C.6}$$

As we needed to find in equations 2.8 and 2.9.

C.2 Error rates with symmetric attacks

The following is a proof of the claim that for symmetric attacks on a perfect channel, the error rate due to Eve is $\mathcal{D} = \frac{1-cos(x)}{2}$, where $cos(x)$ is the overlap between Eve's probe states, ϕ_0 and ϕ_1.

Eve's probe has the following effect on the H and V states:

$$U|0\rangle_{qubit} \otimes |0\rangle_{probe} = |0\rangle \otimes \phi_0 + |1\rangle \otimes \theta_0 \tag{C.7}$$

$$U|1\rangle_{qubit} \otimes |0\rangle_{probe} = |1\rangle \otimes \phi_1 + |0\rangle \otimes \theta_1 \tag{C.8}$$

On the + state, this means it has the following effect:

$$U|+\rangle_{qubit} \otimes |0\rangle_{probe} = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\phi_0\rangle + |1\rangle \otimes |\theta_0\rangle + |0\rangle \otimes |\theta_1\rangle + |1\rangle \otimes |\phi_1\rangle) \tag{C.9}$$

$$= |+\rangle \otimes |\phi_+\rangle + |-\rangle \otimes |\theta_+\rangle \tag{C.10}$$

With this new re-arrangement, this means that:

$$\phi_+ = \frac{1}{2}(\phi_0 + \phi_1 + \theta_0 + \theta_1) \tag{C.11}$$

In order to be physical, Eve's measurements must be orthogonal, $\phi_0 \perp \theta_0$, and $\phi_1 \perp \theta_1$. The effect of Bob's measurements after Eve's probe mean that $|\phi_0|^2 = |\phi_1|^2 \equiv \mathcal{F}$ and $|\theta_0|^2 = |\theta_1|^2 \equiv \mathcal{D}$. From unitarity, $\mathcal{F} + \mathcal{D} = 1$, and $\langle \phi_0 | \theta_1 \rangle + \langle \theta_0 | \phi_1 \rangle = 0$.

Assuming Eve attacks both bases equally, $|\phi_+|^2 = \mathcal{F}$. Squaring C.11, and removing the orthogonal terms, we get:

$$\mathcal{F} = \frac{1}{4}(2\mathcal{F} + 2\mathcal{D} + 2\mathcal{D}cos(x) + 2\mathcal{F}cos(y)) \tag{C.12}$$

Using $\mathcal{D} = 1 - \mathcal{F}$ and the fact that Eve will choose her states such that $x = y$ in order to maximize her mutual information, C.12, this becomes:

$$\mathcal{F} = \frac{1}{2}(1 + cos(x)) \tag{C.13}$$

Which means that the error rate is:

$$\mathcal{D} = \frac{1}{2}(1 - cos(x)) \tag{C.14}$$

Appendix D

Code Written for this thesis

The functions in this appendix were written using Python and the QuTIP library for python (qutip.googlecode.com). The QKD with entanglement code is based on Thomas Jennewein's matlab code.

D.1 Bucket Detector with Poissonian distribution of dark counts

```
def BucketDetector_realistic_detector(N,efficiency ,n_factor):
        """
        Bucket detector model based on H. Lee, U. Yurtsever, P. Kok,
        G. Hockney, C. Adami, S. Braunstein, and J. Dowling,
        "Towards photostatistics from photon-number discriminating
        detectors,"
        Journal of Modern Optics, vol. 51, p. 15171528, 2004.

        Parameters
        ----------
        N : int
            The Fock Space dimension.
        efficiency : float
            The channel efficiency.
        n_factor : float
            The average number of dark counts per detection window
            APD (Bucket Detector).

        Returns
        -------
        [proj, un_proj] : list
            The projection and unprojection operators.

        """
        proj=zeros((N,N));
        #APD (Bucket Detector) un_detector (=gives probability for
        # 0-detection)
        un_proj=identity(N);
        #n_factor = 0;
        for i in range(N-1):
            probs = 0;
            for k in range (1,100):
                for d in range(k):
                    if k-d<=i:
                        probs= probs+ (exp(-n_factor)*(n_factor)**(d))
                        /factorial(d)*choose(i,k-d)*efficiency**(k-d)*
                        (1-efficiency)**(i-k+d);

            proj[i,i]=probs;


        un_proj = un_proj-proj;
        un_proj = Qobj(un_proj);
        proj = Qobj(proj);
        return [proj,un_proj]
```

D.2 Coincidence measurements with Squashing

```
def measure_2folds_4modes_squashing(N,psi,proj,proj2):
    """
    Determines the 2-fold count rate on the joint state outputs
    for an array of double count probabilities.
```

```
Parameters
----------
N : int
    The Fock Space dimension.
psi: qobj
    The entangled state to analyze
proj1: qobj
    1st projection operator for the Channel between Alice and
the Channel between Bob.
proj2: qobj
    2nd projection operator for the Channel between Alice and
    the Channel between Bob.

Returns
-------
[HH,HV,VH,VV] : list
    Two-fold probabilities.

Notes
-----
The squashing (assigning double pairs to random bases) comes
 from two papers:

    T. Moroder, O. Guhne, N. Beaudry, M. Piani, and
    N. Lutkenhaus,
    "Entanglement verification with realistic measurement
    devices via squashing operations,"
    Phys. Rev. A, vol. 81, p. 052342, May 2010.

    N. Lutkenhaus, "Estimates for practical quantum
    cryptography," Phys. Rev.A,
    vol. 59, pp. 3301-3319, May 1999.

"""
ida=qeye(N);
final_state=psi;
det_exp = zeros((2,2,2,2));
```

```
    #i,j,k,l means Ha,Va,Hb,Vb, 0 means detector clicked,
    1 means detector did not click
    for i in range(2):
        for j in range(2):
            for k in range(2):
                for l in range(2):
                    #expectation values for different
                    # detector configurations
                    det_exp[i][j][k][l] =
                     abs(expect(tensor(proj[i],
                     proj[j],proj2[k],proj[l]),
                     final_state));
    #two fold probabilities
    HH = det_exp[0][1][0][1]+0.5*(det_exp[0][0][0][1]
    +det_exp[0][1][0][0])+0.25*det_exp[0][0][0][0];
    VV = det_exp[1][0][1][0]+0.5*(det_exp[0][0][1][0]
    +det_exp[1][0][0][0])+0.25*det_exp[0][0][0][0];
    HV = det_exp[0][1][1][0]+0.5*(det_exp[0][0][1][0]
    +det_exp[0][1][0][0])+0.25*det_exp[0][0][0][0];
    VH = det_exp[1][0][0][1]+0.5*(det_exp[0][0][0][1]
    +det_exp[1][0][0][0])+0.25*det_exp[0][0][0][0];

    return [HH,HV,VH,VV];
```

D.3 Secure Key Rate Simulation

```
def sim_qkd_entanglement(eps,loss_a,loss_b,n_factor_a,n_factor_b,N):
    """
    Simulate skr with an SPDC state.

    Parameters
    ----------
    eps : float
        The squeezing factor, sort of analogous to the amount of
        pumping power to the spdc source, but not really.
    loss_a : float
```

```
        Efficiency of the quantum channel going to Alice.
    loss_b : float
        Efficiency of the quantum channel going to Bob.
    n_factor_a : float
        Background noise in Alice's detection.
    n_factor_b : float
        Background noise in Bob's detection.
    N : int
        Size of the fock space that we allow for the states

    Returns
    -------
    qber : float
        The Quantum Bit Error Rate
    twofolds : float
        Probability of Alice and Bob getting a simultaneous
        detection of a photon pair
        (also referred to as coincidences) within a timing window.
    skr : float
        Probability of getting a secure key bit within a
        timing window, assuming error correction
        and privacy amplification, in the limit of many coincidences.

”””
    #make vaccuum state
    vacc = basis(N,0);

    #make squeezing operator for SPDC
    H_sq = 1j*eps*(tensor(create(N),create(N))+
    tensor(destroy(N),destroy(N)));

    #exponentiate hamiltonian and apply it to vaccuum state
     to make an SPDC state
    U_sq = H_sq.expm();
    spdc = U_sq*tensor(vacc,vacc);
    psi = tensor(spdc,spdc);
    #since qutip doesn't have a permute function, we have to
     do a couple of steps in between
```

```
#1. turn psi from a sparse matrix to a full matrix
out = psi.full();
#2. reshape psi into a 4-D matrix
out = reshape(out, (N,N,N,-1))
#3. permute the dimensions of our 4-D matrix
out = transpose(out,(0,3,2,1));
#4. turn the matrix back into a 1-D array
out = reshape(out,(N*N*N*N,-1));
#5. convert the matrix back into a quantum object
psi = Qobj(out,dims = [[N, N, N, N], [1, 1, 1, 1]]);

# model detectors
a_det = BucketDetector_realistic_detector(N,loss_a,n_factor_a);
b_det = BucketDetector_realistic_detector(N,loss_b,n_factor_b);

#measure detection probabilities
probs2f=measure_2folds_4modes_squashing(N,psi,a_det,b_det);

#Rates returned are 'per pulse', so multiply by source rate
twofolds=probs2f[0]+probs2f[1]+probs2f[2]+probs2f[3];
#Determine QBER from returned detection probabilities
qber = (probs2f[0]+probs2f[3])/twofolds;

#calculate the entropy of the qber
if qber>0:
        H2=-qber*log2(qber) - (1-qber)*log2(1-qber);
else:
        H2 = 0;
# estimate error correction efficiency from the CASCADE algorithm
f_e = 1.16904371810274 + qber;
#security analysis - calculate skr in infinite key limit
#See Chris Erven's PhD thesis or Xiongfeng Ma's paper to
understand where this equation comes from
skr=real(twofolds*0.5*(1-(1+f_e)*H2));
return [qber, skr, twofolds];
```