Daylight operation of a free space, entanglement-based quantum key distribution system

Matthew P. Peloso

(B.Sc.(Hons.), University of Waterloo)

A THESIS SUBMITTED FOR THE DEGREE OF

MASTER OF PHYSICS

DEPARTMENT OF PHYSICS

NATIONAL UNIVERSITY OF SINGAPORE

2009

0.1 Acknowledgments

I wish to thank the Center for Quantum Technologies and the National University of Singapore who provided resources and funding for the project. Thanks to my supervisors Christian Kurtsiefer and Antía Lamas-Linares for the help and for the hard work which went into the QKD system. Special thanks goes to Ilja Gerhardt who collaborated on the daylight experiment while it needed to be monitored 24/7 for an entire week rain or shine, and for helping to clean up (pick up, and reassemble) the QKD system in the middle of the night after a heavy tropical windstorm! Also, thanks to Gregor Weihs and Chris Erven who have both collaborated and shared ideas on practical QKD experiments in free space. Thanks to Lijian Mai who set up the spectrometer used to measure the source spectrum in this paper. As well, I appreciate the past discussions and enthusiasm from Alexander Ling, Caleb Ho, Gleb Maslennikov, Brenda Chng, Meng Khoon Tey, and the rest of the quantum optics group at the CQT.

Contents

0.1 Acknowledgments ii

1 Introduction **1**

1.1 Quantum Cryptography and Daylight Operation of Quantum Key Distribution Systems 1

1.1.1 How to communicate securely using quantum bits 1

1.1.2 A closer look at quantum security 5

2 Theory **11**

2.1 Entanglement 11

2.2 The No-Cloning Theorem 12

2.3 Basis of Security of QKD 14

2.4 Visibility as a Measure of Entanglement 16

2.5 The BBM92 protocol 17

2.6 The Quantum Bit Error Ratio in Daylight 19

2.7 Generation of Correlated Photon Pairs 24

2.7.1 Non-Collinear Phase Matching in a BBO crystal 27

2.7.2 Quasi-phase Matching in a PPKTP Crystal 28

2.8 Atmosphere Absorption and Turbulence 35

2.8.1 Beam spreading and wandering 37

3 The Experiment **39**

3.1 Set-up 39

3.2 Filtering Techniques 42

3.2.1 Temporal Filter . . . 43
3.2.2 Spectral Filter . . . 44
3.2.3 Spatial Filter . . . 46
3.3 Alignment Procedure . . . 50
3.3.1 Source . . . 51
3.3.2 Free Space Coupling . . . 52

4 Experimental Results 55
4.1 48 Hours of Key Exchange . . . 58
4.2 Synchronization . . . 63
4.3 Applying Random Number Tests to the Key . . . 66
4.3.1 Frequency Tests . . . 69
4.3.2 Runs Tests . . . 70
4.3.3 Binary Matrix Rank Test . . . 70
4.3.4 Approximate Entropy Test . . . 71
4.3.5 Compression Tests . . . 72
4.3.6 Excursions Tests . . . 73
4.3.7 Template Matching Tests . . . 76
4.3.8 Discussion of the random number tests . . . 78

5 Conclusion 80
5.1 Final Discussion . . . 80
5.2 Improvements . . . 82

A Appendix 83
A.1 CAD - Solid Models and Drafts for Optical Mechanics . . . 83
A.2 Template Matching Tests . . . 87
A.2.1 Non-Overlapping Template matching Tests . . . 87
A.2.2 Overlapping Template Matching Tests . . . 90

Summary

Quantum Key Distribution (QKD) is among the first established quantum information technologies (QIT) which are based on the laws of quantum mechanics. QKD allows the generation of identical random numbers at two remote locations. These numbers are used as keys to encrypt and decrypt communications between parties at those points. The cryptographic key is generated by distributing quantum states between the two parties. The quantum state is either sent through air in a free space channel, or through a fiber optic cable. This technology requires optical hardware including linear optic elements, a source of photons in a quantum state, and single photon detectors. This makes robust implementations of QKD possible given current optical communication technologies, and moreover, it is compatible with many current optical communications technologies.

The key generated via QKD satisfies a high level of cryptographic security, and under certain assumptions is considered to be *completely secure*. By *completely secure* it is meant that the two parties who wish to communicate in secret may infer that any eavesdropper will have no knowledge of the final binary sequence they share. The final key is the result of error correction and compression on the raw measurement results of the photons that are distributed. The final key may then be used to establish secure communication using a cryptographic communication protocol.

It has been shown that the security claims about QKD are stronger when a source of entangled photons is used to distribute the key [1, 2]. Previously, an implementation of such an entanglement-based QKD protocol distributed over a free space optical channel has only been successful at night, since the key information is extracted from single photons which are not easily distinguished from the large background of sunlight in the channel during daytime. This limitation on the effective use of QKD resulted from the difficulty of distinguishing daylight photon counts of the sun from the series of single photons distributed for key generation.

This thesis presents the experimental set up, procedure, and data, resulting in the first demonstration of an experimental quantum cryptographic protocol based on entangled photon sources which operates in daylight conditions over a free space channel. An efficient key exchange using a robust and portable entanglement-based QKD system, during both day and night for a continuous 48 hour cycle, is presented. An average of 385 bits of key per second are generated resulting in more than 65 Mbits of final key. We have thus overcome the previous limitation of entanglement-based QKD to night time use. Over the whole period the rate of detected pairs and background events varied by about 2 orders of magnitude. A summary of this thesis may be found in the New Journal of Physics, April 2009 special issue on Quantum Cryptography [3].

List of Tables

2.1 KTP Sellmeier Coefficients 32

2.2 KTP Temperature Coefficients 34

3.1 Pinhole Transmission Measurements 46

4.1 Tomography of the Four Detectors 58

4.2 Synchronization Tests 65

4.3 Random Number Test Summary 79

List of Figures

1.1 Layout of the Quantum Key Distribution Experiment 3
1.2 QKD based on a Bell test 10

2.1 Mutual Information: calculating the error threshold 15
2.2 The BBM92 Measurement Device 18
2.3 The QBER with Large Background Levels 22
2.4 The QBER with Large background Levels at both Detectors 24
2.5 Orientation of three waves mixing in a nonlinear medium 28
2.6 Image of the PPKTP crystal 29
2.7 Phase Mismatch in PPKTP 31
2.8 PPKTP Temperature and Pump Wavelength Dependence 33
2.9 PPKTP Temperature Tuning Curves 35

3.1 Bird's eye view of the Channel 40
3.2 Experimental setup for QKD 42
3.3 Time delay of the Detectors 44
3.4 Spectrum of the Entanglement Source 45
3.5 Telescope Baffles and Orientation 47
3.6 Spatial Filters Effect on Background 48
3.7 Ray Tracing of the Field of View 49
3.8 Field of View Dependence on Pinhole Size 50
3.9 Polarization Entanglement Source 52

4.1 Background levels during day 56

4.2 Key Generation Rate Plots 57

4.3 Tomography of detection events 60

4.4 Histogram of Key Generation Events with Background Levels 62

4.5 Monobit Frequency Test Results 69

4.6 Block Frequency Test Results 70

4.7 Runs Test Results 71

4.8 Binary Matrix Rank Test Results 71

4.9 Approximate Entropy Test Results 72

4.10 Maurer's Universal Statistical Test Results: large blocks 73

4.11 Maurer's Universal Statistical Test Results: small blocks 73

4.12 Random Excursions Test Results: 1^{st} state 74

4.13 Random Excursions Test Results: 2^{nd} State 75

4.14 Random Excursions Test Results: 6^{th} State 76

4.15 Random Excursions Test Results: 7^{th} State 76

4.16 Random Excursions Variant Test Results: 2^{nd} state 77

4.17 Random Excursions Variant Test Results: 6^{th} state 77

4.18 CUSUM Test Results 78

A.1 CAD Mechanical Draft: Baffles 91

A.2 CAD Mechanical Draft: Baffle Mount 92

A.3 CAD Mechanical Assembly: Baffles 93

A.4 Non-Overlapping Template Matching: pattern *001* 94

A.5 Non-Overlapping Template Matching: pattern *011* 94

A.6 Non-Overlapping Template Matching: pattern *100* 94

A.7 Non-Overlapping Template Matching: pattern *1000* 95

A.8 Non-Overlapping Template Matching: pattern *10101010* 95

A.9 Non-Overlapping Template Matching: pattern *00011001* 95

A.10 Non-Overlapping Template Matching: pattern *000000001* 95

A.11 Non-Overlapping Template Matching: pattern *100100100101* 96

A.12 Non-Overlapping Template Matching: pattern *10010010110100101* 96

A.13 Overlapping Template Matching: pattern *01* 97
A.14 Overlapping Template Matching: pattern *111* 97
A.15 Overlapping Template Matching: pattern *101* 97
A.16 Overlapping Template Matching: pattern *011* 98
A.17 Overlapping Template Matching: pattern *001* 98
A.18 Overlapping Template Matching: pattern *0011* 98
A.19 Overlapping Template Matching: pattern *0110* 98
A.20 Overlapping Template Matching: pattern *1001* 99
A.21 Overlapping Template Matching: pattern *1110* 99
A.22 Overlapping Template Matching: pattern *11011* 99
A.23 Overlapping Template Matching: pattern *01110* 99
A.24 Overlapping Template Matching: pattern *010101* 100
A.25 Overlapping Template Matching: pattern *1010101* 100
A.26 Overlapping Template Matching: pattern *1000000* 100

Chapter 1

Introduction

1.1 Quantum Cryptography and Daylight Operation of Quantum Key Distribution Systems

1.1.1 How to communicate securely using quantum bits

This section outlines quantum key distribution for cryptography, and its physical requirements. As well, we describe in simple terms why quantum key distribution is secure.

Quantum key distribution (QKD) has been demonstrated for practical use as a key distribution protocol for cryptography, and is one of the original developments of an information technology based on the laws of quantum physics. Quantum information technology (QIT) has matured from the earliest conception which supposed quantum principles, namely the *superposition and uncertainty principles*, would be a hindrance to technical development and limit the growth of computing power predicted by MOORE in 1965 [4, 5]. But quantum physics was later shown to be have some advantages when used for communication and computing through a variety of different implementations [6, 7, 8, 9]. Such developments originated in the early 1970's from STEPHEN WIESNER'S original idea; that quantum particles embedded into bank notes would allow their unique identification, thereby creating useful *quantum money*. The significance of the idea was not well understood, and the idea remained unpublished until much later [10].

In 1984 the use of quantum systems for a cryptographic key exchange protocol known as BB84 for the inventors Bennett and Brassard [11] attracted considerable interest from scientists, and now quantum cryptographic systems are available in the market[1]. QKD theoretically allows secure communication based on some principles of quantum physics. The most simple explanation is based on the no-cloning theorem. The no-cloning theorem is presented in greater detail in section 2.2. Here is the basic idea: Given a single quantum particle with two possible (orthogonal) states denoted 0 or 1, we can define a resource know as a Qubit written in the Dirac notation as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ where } \alpha, \beta \in [0,1] \tag{1.1}$$

and $\langle\psi|\psi\rangle = \alpha^2 + \beta^2 = 1$, for normalization.

This describes a quantum particle which is in a superposition of two states; $|0\rangle$ and $|1\rangle$ for a complex variable α and β. It was proved with the no-cloning theorem that this quantum state cannot be copied in a single measurement [12].

Measurement of a qubit does not yield a value for the α or β in equation 1.1.1. The measurement only reveals the result of the state; i.e either a $|0\rangle$ or $|1\rangle$ can be distinguished. Thus, it is not possible for an eavesdropper to recreated the state of the qubit in equation 1.1.1 based on a single measurement. In respect to a hacking attempt, there can be two cases when a single qubit is measured, either the measurement has destroyed the particle or an imperfect replacement may be sent in it's place by an eavesdropper. Thus, a measurement on the qubit will either *disturb or destroy* the final qubit which is distributed between the two parties for QKD. The result is that a hacking attempt based on a measurement of the distributed qubit can be observed as an increasing error ratio in the raw key bits that are distributed. Information leakage may be estimated by monitoring the fraction of errors in the results between the two communicating parties.

To place a bound on the information an eavesdropper has of the final key, an error threshold for the protocol must be maintained to conclude a third party has limited

[1] See MagiQ Technologies: www.magiqtech.com, and IDquantique: www.idquantique.com

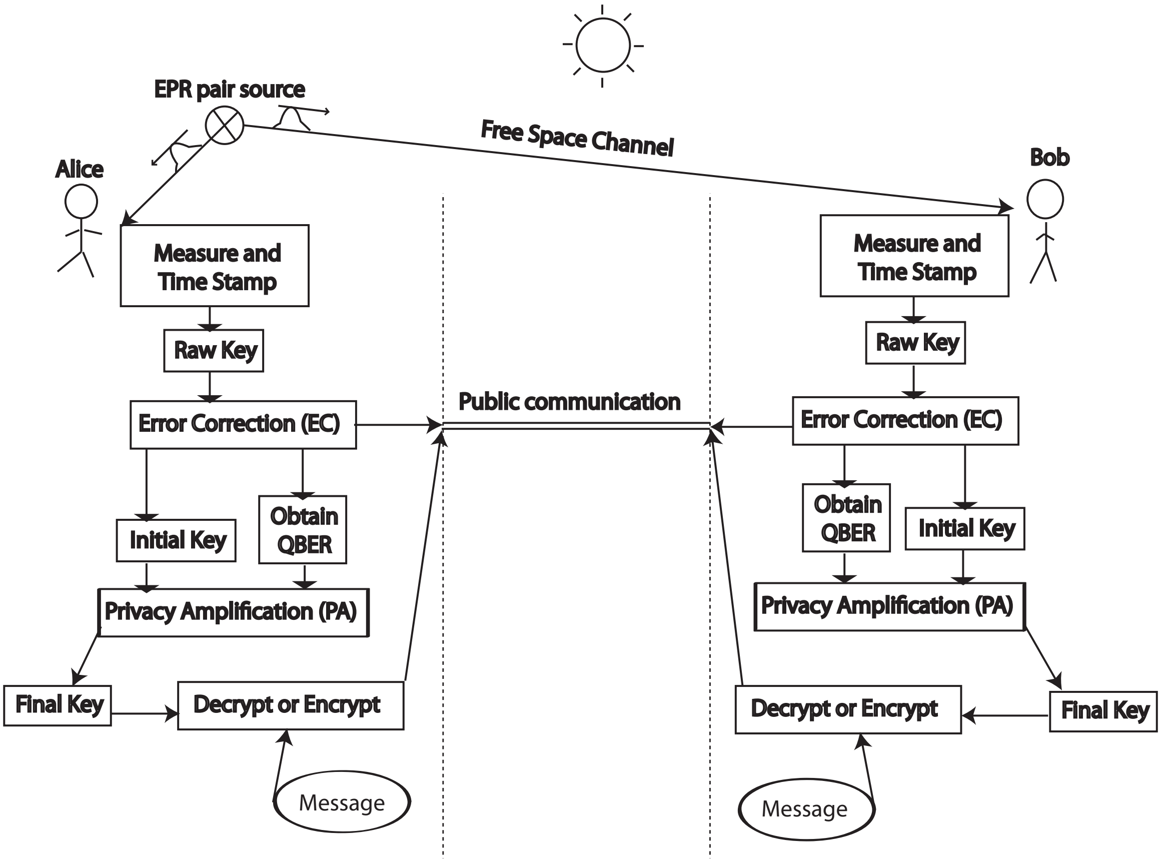


Figure 1.1: Layout of the Quantum Key Distribution Experiment: Photon pairs are obtained from an EPR source, and distributed to two parties. Those parties measure the polarization of each photon and attach to each result a time tag for processing. The resulting raw key information is input to the error correction algorithm, which yields the error ratio known as the Quantum Bit Error Ratio (QBER) and an initial key. This requires some public discussion leading to some leakage of information to an eavesdropper. The QBER is used to decide upon the amount of compression required in the Privacy Amplification stage which outputs a final key. The final key may be used to encrypt or decrypt public communications. Dual solid lines represent transmission of classical information, while the single solid line represents quantum information.

information of the key. This requires that the information shared between the two parties is compressed in a post processing procedure called privacy amplification (PA) by an amount depending on the error ratio. Note, this occurs after error correction (EC) is applied to the raw key generated from measurements on a series of qubits. The parties may then use their keys to encrypt and decrypt their *plaintext* and create a secret *cipher* which can be communicated publicly in a symmetric[2] key protocol over a classical channel between them. Only the key which they hold may be used to decrypt that cipher and reveal the plaintext. It should be pointed out that the most secure way to use the key is as a *one-time-pad*[3][13] where it is applied *once* with no repetition, and then disposed of. Otherwise an eavesdropper may compare segments of the cipher to decode the key itself, and access the plaintext.

In quantum cryptography, photons provide the physical basis for encoding the key bit since they may be transmitted over long distances without interacting strongly with the medium of the channel. The transmission is either sent through fiber optic cables, or simple sent through air in a collimated light beam[4] to be coupled into a detecting telescope. This later transmission method is known as free space optical communication and is applied in this experiment. It has the added advantage that the channel between two remote points may be established *ad hoc* with the only requirement that there is no obstruction in the channel.

The degrees of freedom of a photon including the polarization, detection time, spectrum, or spatial location may all be used to define the qubit, but the most natural choice for a free space based experiment is the *polarization* of the photon. We can then write our qubits in equation 1.1.1 from here on as

$$\alpha|H\rangle + \beta|V\rangle \tag{1.2}$$

where H and V are the horizontal and vertical polarization states respectively and normalization is ignored. This choice arises since air has negligible birefringence, and will therefore not cause uncertain rotations in the polarization based on the trajectory the photon travels.

Up to this point we have seen that quantum states used to distribute a cryptographic

[2] As opposed to *asymmetric* cryptography such as an RSA protocol where parties use *different* keys for key distribution.

[3] Also known as the Vernam cipher. This limits the plaintext to a block which is equivalent in size with the key.

[4] In the literature, a collimated beam is often referred to as a *tight light beam* in the context of atmospheric turbulence.

key between two remote locations provides a solution to the problem of secure key distribution. Succinctly, any measurement of the photons in the transmission channel will influence the result at the end of the channel. As well, we have introduced the physical means by which we intend to prepare and distribute a quantum state for QKD. Now we can look at a basic arrangement for the experiment. Referring to figure 1.1, observers at points A and B (typically observed by the two parties *Alice* and *Bob*, respectively) want to communicate a secret message. They have a quantum channel and a classical channel. The basic processing of the data is outlined in a flow diagram and finally the process by which they can perform cryptographic communication is shown. A good review of QKD is by GISIN in [13].

1.1.2 A closer look at quantum security

We have a basic outline of the QKD experiment. Now we outline some different protocols for QKD and discuss the security in more detail, which leads us to understand why an entanglement source is used for this experiment.

There are a number of different quantum cryptographic protocols, and we will discuss three protocols: the BB84, BBM92, and E91 protocols. The **BB84** protocol [11] of BENNETT and BRASSARD is the first design, relying on the preparation of a qubit in a single photon. The single photon is actively prepared in one of two possible bases. An eavesdropper cannot find a simple measurement technique to distinguish $|H\rangle$ or $|V\rangle$ single photon states from diagonal ones. Although the orthogonal states $|H\rangle$ and $|V\rangle$ are defined in reference to a measurement basis, the measurement results in one basis, chosen for example with respect to the gravitational field, will be different from measurement results in a basis rotated by 45° to that *vertical* measurement basis. Alice uses a random number to select the basis, and Alice and Bob will keep the measurement results in which Bob happens to choose the correct basis by comparing the basis results publically. Doing this does not disclose their measurement results to Eve and is thus secure.

Another protocol named **BBM92** developed by BENNETT, BRASSARD and MERMIN

[14] replaces the choice of basis at the prepare portion of the BB84 protocol with a passive measurement apparatus which measures in two different basis randomly, while the qubit is now replaced with an entangled photon pair. The basis choice can be done by including a passive optical element in the detection unit which splits the photon into two paths. The measurement basis is chosen randomly by including a polarization rotation in one path so that for example, the photon traveling in one path is measured with respect to the gravitational field, and the photon in the other path is measured in a basis again rotated by 45° to be orthogonal to the first. The use of EPR pairs ensures that correlations among the detection events will result, so that a key can be generated

The BBM92 protocol comments on another paper by Ekert published in 1991 [15] which describes another protocol for QKD, called E91. This **E91** protocol obtains it's security based on a measurement of entanglement. The development of the role of entanglement in these protocols is important to understand the motivation of this experiment. The E91 version of the experiment was based on Bell states which serve to replace the channel of BB84 with an EPR pair [16]. Alice and Bob would observe correlations from this EPR pair to extract their key. With the two qubits in a maximally entangled singlet state of the polarization

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|HV\rangle - |VH\rangle\right), \tag{1.3}$$

the two can test the correlation of the state to rule out the eavesdropper. This is because the correlations in the state could not be predicted by a hypothetical *Eve*, unless you are to accept that some *hidden variable* exists allowing the hacker to control the EPR correlations. That is to say, if an eavesdropper has *a-priori* knowledge of the EPR correlations, then this would mean there exists a hidden variable. This hidden variable was originally ruled out by the violation of Bell's inequalities [17, 18] experimentally by Aspect in the early 1980's [19, 20]. In the E91 protocol, it is this violation that must be measured to gain cryptographic security.

However, it was argued in the formulation of the BBM92 protocol that the E91 security claim was equivalent to this newly proposed protocol, as well as BB84. This was argued by considering the two particles of the EPR pair traveling in different trajectories, both to and from the EPR source so that the EPR pairs were deemed unnecessary [15]. The choice of photon source for some time was ignored, and an approximation to a single photon source was employed for QKD. Using an attenuated laser[5] with a mean photon number $\mu \approx 0.1$, a single photon state can be obtained, albeit imperfectly. High repetition pulses, when comparing the emission rate of entanglement based sources, can be prepared from an attenuated laser; hence the popularity of this light source. Thus, prepare-and-send (PnS) methods based on the BB84 protocol use coherent pulses, whereby Alice generates an *imperfect* single photon and prepares it in a particular state, then uses a random number generator to actively prepare the state in a basis.

However, the question remained if quantum cryptography was really secure by encoding qubits in highly attenuated laser pulses. Alice can not know how many photons are within each pulse she encodes, due to the nature of the coherent photon state. Such states obey a Poissonian probability statistic

$$P\left(\mu, n\right) = \frac{\mu^n}{n!} e^{-\mu}$$

in the photon number state $|n\rangle$[6] for a mean photon number μ. There is always some probability $P_2 \approx \mu^2/2$ of a two photon emission occurring. Alice may unknowingly send a pulse containing two photons in a key bit to Bob. Even when Bob receives one photon, Eve may have gained information of their qubit using the Photon Number Splitting Attack[7] (PNS) leaving no evidence of her presence. Further discussion of realistic photon sources in QKD revealed flaws in the security assumptions [22]. However, it was eventually discovered that secure exchange using the coherent state as an approximation to a single photon is possible by using *decoy pulses* [23].

[5] Which gives a *faint* coherent pulse: a superposition of photon number states

[6] Also known as a Fock state.

[7] This attack simply describes the case where Eve measures one of the two photons, which will be in an identical state to the other. The second photon is still distributed for key generation, leaving no trace of an error.

While the security proofs on the coherent state protocols were developed, others raised the issue of the equivalence of the E91 and BB84 type protocols. In particular it was noticed that the assumptions in previous security proofs about the size of the Hilbert space of the photon are not always justified. This is because two polarizations may be distinguished by another variable, the spectrum of the photons for example, or possibly by the timing of the two polarizations. This higher dimension of the Hilbert space meant that a hacker could use the second degree of freedom as a *side-channel* [24, 25] to distinguish the outcome of a key bit without disturbing the quantum state.

Considering a higher dimensional Hilbert space, security in a scenario where practical devices cannot be trusted [1, 26] suggests the E91 entanglement based protocol obtains greater security than protocols relying on a measurement of the error ratio. Moreover, using a measure of entanglement to test security offers simplicity as it uses a single parameter; the Bell violation, while the other protocols may actually need to monitor a large number of side-channels for errors. Such flaws in the basic assumptions of the *unconditional* security proofs for QKD point out the advantage of using entangled photon sources in quantum cryptographic protocols. The first experimental version of an E91 protocol, where a violation of a Bell inequality was used as a measure of secrecy, was performed by Alexander Ling and others in our lab in 2008 [2]. The key generated in this experiment is presented in figure 1.2 where it can be seen that a measurement monitors the Bell inequality for violation, and verifies the security of the key exchange.

All of the experimental free-space protocols which use entangled photon pairs to distribute the key have so far been implemented at night [27, 28, 29, 2, 30], because daytime atmospheric light coupled in the measurement devices contributes too much background light to allow secure key generation. The background would either saturate the detectors into an unsafe operating regime, or contribute strongly to errors in the key. This problem can be seen in our Bell measurement experiment in figure 1.2 and places an obvious limitation on free space QKD's practical use. Yet this problem may not be impossible to overcome. Daylight versions of QKD using faint coherent pulses have been successful [31, 32], but here the bandwidth of the signal photons may be tightly controlled so that interference filters may be matched spectrally at the receiver. Yet, the advantages of using entanglement based QKD systems is apparent. Thus, further techniques for filtering background light coupled in the free space channel during daytime must be explored for entanglement based quantum key distribution protocols. This is the motivation of the following experiment.

As a final point on security, it should always be assumed that the eavesdropper has no access to the remote locations A and B. Otherwise, she can simply observe the development of a cipher and would not be detected as an increasing error ratio. As a more sophisticated point, any compromising emanations of the hardware can be considered as access to the lab. For example, a distinguishing electrical signal radiating from the detectors and escaping the lab would be information available revealing which detection event occurred. Other forms of leakage include a flash from the breakdown of an avalanche photo detector, electrical waves correlated to the QKD device through a room power outlet, acoustic noise, radio frequency emanations, and more. Studies of such information leakage are attempted, for example, in the TEMPEST project[8]. As well, we must assume the system should behave as an unbiased random number generator, otherwise an eavesdropper can use knowledge about the generator and obtain a larger probability of extracting the key. This assumption must be tested empirically, and is discussed further with the results of the random number tests performed on the raw key.

[8] See www.eskimo.com/ joelm/tempest.html

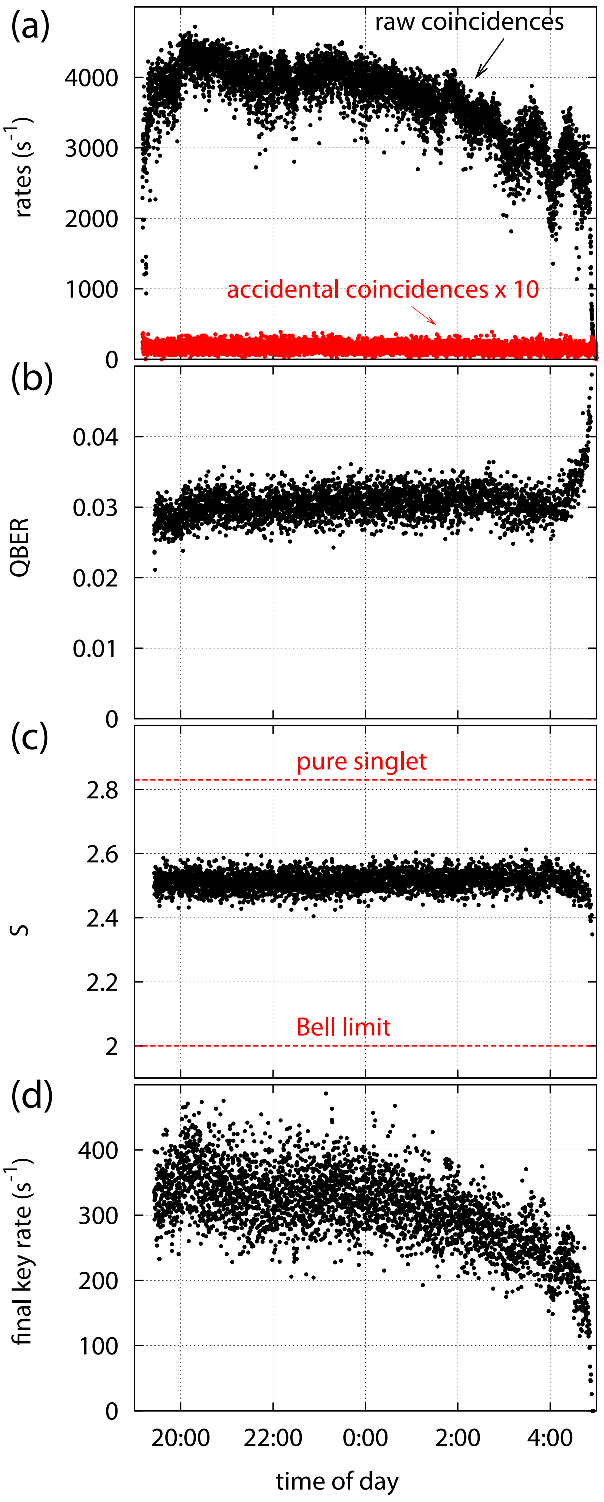


Figure 1.2: QKD based on a Bell test: A Bell violation (panel c) is monitored while key (panel d) is generated. Note that the key exchange breaks down at sunrise, as we see the error (panel b) jump and the key rate (panel d) drop dramatically at the right of the graph during sunrise. At this time no more key may be distributed. See reference [2] for further details of this experiment.

Chapter 2

Theory

2.1 Entanglement

A brief description of entanglement.

Entanglement is arguably one of the most interesting properties of physics today. An example of an entangled state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B + e^{\imath\theta}|V\rangle_A|H\rangle_B\right) \equiv \frac{1}{\sqrt{2}}\left(|HV\rangle_{AB} + e^{\imath\theta}|VH\rangle_{AB}\right) \tag{2.1}$$

with θ the phase difference between the $|HV\rangle$ and $|VH\rangle$ states. The subscripts mean that measurement is performed at two distinguishable systems A or B, usually a spatial variable. Here, ignoring the phase term θ, either at location A, H is measured, and at location B, V is measured, or vice-versa. Loosly speaking, entangled systems are correlated in this way, with the measurements at the points A and B resulting in opposite results, for example. More formally, an entangled system is defined as one in which the state cannot be written as a product of states, or $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$. More information may be found through reference [33] at the section *8.1.2 Seperability and Entanglement.*

The Bell states, which are maximally entangled states of two particles, are

$$\Phi^{\pm} = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \text{ and} \tag{2.2}$$

$$\Psi^{\pm} = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), \tag{2.3}$$

where Ψ^- is the singlet state which is used for our polarization entanglement source in this experiment. This state is antisymmetric with respect to exchanging the two systems A and B. An entangled state cannot be separated into two distinct parts, but is intuitively a single state of its own, albeit describing two particles which may be distinguished by their locations in space (i.e. *at* A or B). The entangled state exhibits quantum (i.e. *non-classical*) correlations upon measurement, also known as EPR correlations.

Correlations of an appropriately prepared system arise from quantum entanglement, which predicts that an entangled particle cannot be described without reference to its counterpart particle. To form a pair of quantum entangled bits usually the two bits must originate from the same source, or interact somehow. The correlations resulting from entanglement provide a resource for key distribution, since an appropriate measurement of an entangled state will yield the same result, opposite result, or otherwise predictable result between the entangled particles. Thus, a shared key will be obtained by both parties measuring the state. A good introduction to entanglement is in [33, 34].

2.2 The No-Cloning Theorem

The no-cloning theorem is discussed and the proof is shown.

The no-cloning theorem [12] is a simple example illustrating some of the profound differences between quantum and classical physics. It states that, given a general quantum state such as that of equation 1.1.1, that state cannot be copied unless the basis to measure the state in is known. This results from the superposition principle where the quantum state probabilistically collapses into a possible measurement result, but it is debatable if they exist as a superposition of those states prior to actual detection. This idea has opened the door for quantum communication. A review of the subject can be found in the paper by Valerio Scarani, Antonio Acin et al, in reference [35].

Here we outline the proof of the no-cloning theorem: Consider two general states, ϕ and ψ, and an ancilla state S which is used to store the copy. Performing a generalized unitary operation U on the two states we obtain a set of two equations:

$$|\phi\rangle_A \otimes |S\rangle_B \xrightarrow{U} |\phi\rangle_A \otimes |\phi\rangle_B,$$

and

$$|\psi\rangle_A \otimes |S\rangle_B \xrightarrow{U} |\psi\rangle_A \otimes |\psi\rangle_B.$$

Now taking the inner product of these two equations we have $LHS = \langle s|s\rangle \otimes \langle\psi|\phi\rangle = 1 \otimes \langle\psi|\phi\rangle = RHS = \langle\psi|\phi\rangle^2$, and writing $x = \langle\psi|\phi\rangle$ we have

$$x = x^2 \to x = \{0, 1\}\,. \tag{2.4}$$

The two solutions for the cloning equation imply that either the states ψ and ϕ are in fact equal (i.e. $\langle\psi|\phi\rangle = 1$) or are orthogonal (i.e. $\langle\psi|\phi\rangle = 0$) to each other, which means that a quantum state can be copied if the measurement basis is known, but in general the resulting equation is a contradiction. Thus, it is not possible to copy an unknown quantum state using the generalized unitary operator.

Another way to illustrate the inability to obtaining a copy of a qubit, is by considering the expansion of two qubits in a superposition of states $|0\rangle$ and $|1\rangle$[1] You may imagine one is the real state, while the other bit should be the resulting copy.

$$\begin{aligned}
(|0\rangle + |1\rangle)_A \otimes (|0\rangle + |1\rangle)_B &= |00\rangle_{AB} + |01\rangle_{AB} + |10\rangle_{AB} + |11\rangle_{AB} && (2.5)\\
&= |0\rangle_A (|0\rangle + |1\rangle)_B + |1\rangle_A (|0\rangle + |1\rangle)_B && (2.6)\\
&\neq |00\rangle_{AB} + |11\rangle_{AB} && (2.7)
\end{aligned}$$

The final inequality is the case required for identical bits of the superposition of states to result upon measurement. In the second line of the equation we can see that a measurement applied to the first bit in attempt to gather information about the second bit will obtain an uncertain result $(|0\rangle + |1\rangle)_B$ for either case $|0\rangle_A$ or $|1\rangle_A$. In fact, we see in the second line that the measurement of the second bit is just the original superposition and has no relation to the result of the first bit in a product of superpositions. The state that would be required in the last inequality 2.7 is in fact an entangled state [18] or Einstein-Podolsky-Rosen (EPR) pair.

[1] Normalization terms are ignored here.

2.3 Basis of Security of QKD

Previously it was shown that the security of QKD requires monitoring of a error ratio in the distributed key. Here a illustration of the security proofs is presented to yield a threshold value for the QBER.

The security of a QKD scheme is based on an evaluation of the information shared between Alice and Bob, and that accessible to an eavesdropper, to form a bound on the information leakage to an eavesdropper. The information between both parties can be represented by the Shannon information $I(A, B)$ between the two parties Alice (A) and Bob (B) [36, 37]. We will denote Alice and Bob as usual here, and let Eve be denoted by (E) so her mutual information with Alice is $I(A, E)$. For secure communication Alice and Bob should observe a low mutual information entropy, while Eve's goal is to decrease her mutual information entropy between either Alice or Bob. If Eve decreases her information entropy between Alice or Bob, then Alice and Bob will observe an increase in the entropy of their sequences, showing up as an increasing error ratio in the correlated key. This is because Eve's gain will disturb or destroy the state, and she cannot recreate the state of the original quantum bit to hide her hacking attempt, as suggested by the discussion of the no-cloning theorem above.

The secrecy $S(A, B|E)$ obtained by Alice and Bob against Eve is represented by the inequality

$$S(A, B|E) \geq \max \{I(A, B) - I(A, E), I(A, B) - I(B, E)\} \tag{2.8}$$

which requires intuitively that Alice and Bob share more information than the increase in information that Eve may obtain by eavesdropping on their communications. That error ratio represents the amount of errors added into the key by a hypothetical eavesdropping attempt and can be taken directly from the error correction (EC) algorithm.

Security proofs for QKD form an extremely active field of research. We will not go into the details of the proofs which usually make assumptions so as to prove *unconditional security*. The bounds found are as follows: Gisin *et al* calculate the maximum information

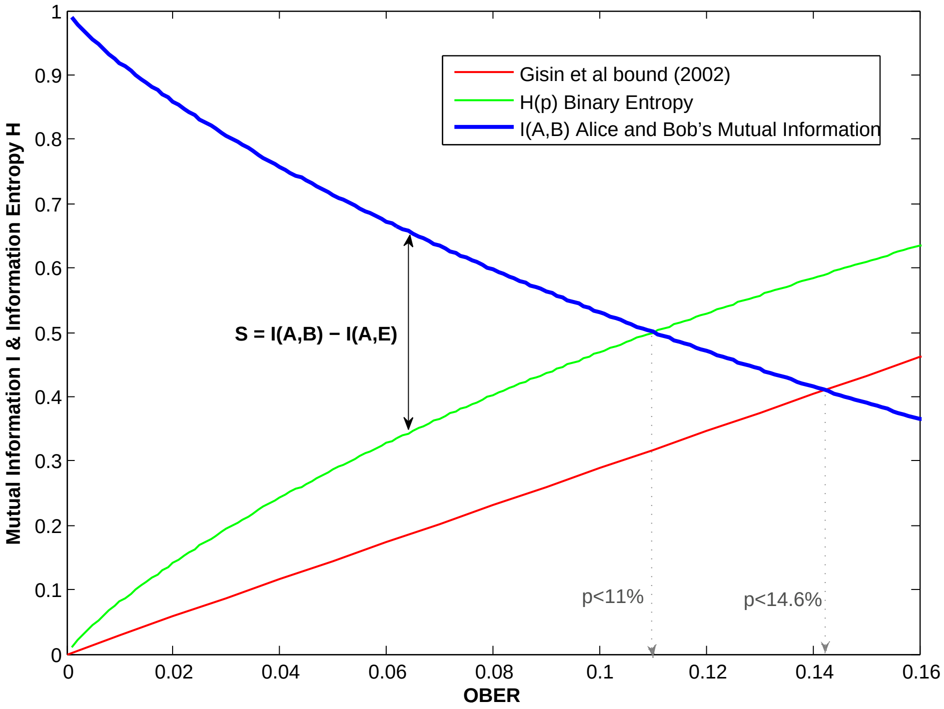


Figure 2.1: Mutual Information and the Information Entropy Function with Respect to the Quantum Bit Error Ratio. The blue trace represents the mutual information shared by Alice and Bob, while the orange trace is the threshold for I(A,B) from the Shor Preskill security proof. The red trace is the standard bound by Gisin[14]. Where these lines cross the secrecy obtained by the two parties goes to zero. The green trace is the Shannon information entropy function.

Eve obtains in relation to the errors as $I(A,E) \approx \frac{2}{2ln(p)}p$, to first order. This curve is plotted in figure 2.1. The maximum error tolerable in this scenario is the crossing point at $p = \frac{1-\frac{1}{\sqrt{2}}}{2} \approx 14.6\%$. In this scenario it was assumed Eve individually measures a photon and hacks the channel one bit at a time. In a *coherent* attack Eve collects a large number of photons and can manipulate them to hack the communication. This case was explored in a number of papers [38, 39] and has been improved on by Shor and Preskill [40], who's security bound is the one accepted in our experimental protocol. They find the bound at $plog_2(p) + (1-p)\,log_2(1-p) \leq 1/2$. This bound is also plotted in figure 2.1.

The information leakage is quantified by the binary entropy function to the error rate as

$$H(p) = -p\log_2(p) - (1-p)\log_2(1-p) \tag{2.9}$$

where p is the error ratio which is observed, or $p = QBER$. In figure 2.1 we can see that the secrecy goes to zero near $QBER = 11\%$ at the point where Eve's information becomes greater than Alice and Bob's information. Eve's information here is presented assuming $I(A, E)$ is the maximal information Eve gained. The information she has accounts for both the public information discussed by Alice and Bob, as well as the information she has gained by eavesdropping which added errors to the key, while Alice and Bob share the mutual information $1 - H(p)$. For further information on the security proofs for quantum key distribution an excellent article would be the summary by Valerio Scarani [41], or the Ph.D. thesis of Rennato Renner on the security of quantum information [42]. For a more sophistocated version of a security proof for QKD refer to the *Shor-Preskill* proof for the BB84 protocol [40].

2.4 Visibility as a Measure of Entanglement

To measure entanglement quality the visibility is used. This measurement is described here.

The quality of an entanglement source is typically measured by what is known of as the *visibility* or *visibility of quantum entanglement.* This quantity is computed by the function

$$V = (r_{max} - r_{min}) / (r_{max} + r_{min}) \tag{2.10}$$

where r_{max} and r_{min} are the maximum and minimum number of correlation counts in the sinusoidal fringe resulting from the following measurement:

1. entangled photon pairs are measured where one photon is coupled into a detector through a polarization analyzer, thus measuring it in a particular polarization state.

2. In the detection on the corresponding photon, the state is measured through a number of different polarization states.

3. A sinusoidal curve resulting from quantum interference of the outcomes is recorded from which the Visibility may be calculated from the count rates.

Note, the basis in which this measurement is relevant is formed by the setting of the first polarization analyzer that is fixed in respect to the crystal axis. We test two bases, the HV basis and ±45° basis, to find the corresponding visibilities V_{HV} and $V_{\pm 45^\circ}$, respectively. Ideally, the minimum of the fringe r_{min} will be zero, but in practice there is usually some noise in the detector and errors in the generation of the entangled pairs. The resulting interference gives a measure of the quantum correlation present in the source of entanglement with the actual detectors used, and thus can be used as one measure of entanglement quality.

2.5 The BBM92 protocol

The protocol known as BBM92 is used in this experiment. This protocol uses the entangled photon source, and it is described in detail in this section. The measurement apparatus for the protocol is also presented.

In the BBM92 protocol, the measurement is performed in two bases randomly. The basis is selected probabilistically by a simple linear optic 50/50 beam splitter at the input port of the analyzer, and means that an eavesdropper will not be able to know the correct basis in which to measure a particular bit. One basis would be $|0\rangle$ and $|1\rangle$ and the other rotated by 45° to this basis. The layout of a BBM92 detector is in figure 2.2. The two parties use an entangled state, but do not monitor a Bell violation. They compare the independent measurement basis and remove all the bits which correspond to measurements done in two different bases, known as *sifting*. Half the time their measurements should be in the same basis so they get roughly $r_{initial} \approx \frac{1}{2} r_c$ from the rate r_c of correlations observed.

They now remove as well any events where no detection occurred. The remaining bits should be perfectly correlated due to the source used, although will have some error due

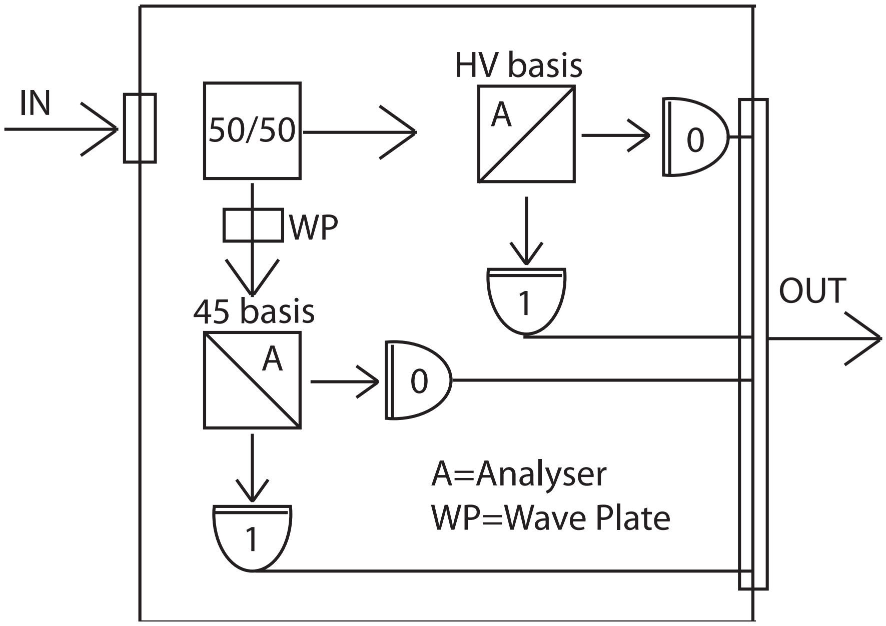


Figure 2.2: The detector layout for measuring the polarization state of the qubit at both A and B. The information enters in a quantum state which is a superposition of the possible states, and the measurement result cannot be determined. It is measured in one of the bases with a 50/50 percent probability, and is analyzed at the optical element labeled A. This is a polarizing beam splitter. Note, the detector includes a wave plate which rotates the quantum bits into the ±45° basis in the lower measurement mode labeled *45 basis*. Upon detection the quantum state collapses at both Alice and Bob and the bits become classical information. When the measurement basis at both sides is the same, the bits will be the same value. In our case the *singlet* state which is anti-correlated, is used, so the bit is anti-symmetric upon measurement before it is processed to a final key.

to imperfections, or eavesdropping attempts. They perform error correction on the keys and find the error ratio. Then, the key is compressed by a ratio to satisfy the security conditions. The BBM92 protocol allows more key to be exchanged in comparison to the E91 version which requires measurement of an inequality. It however will not have the same repetition rates of a BB84 protocol which can use a weak single photon source. BBM92 does require the EPR pair as a source of light so will be an ideal protocol for our daylight test. The BBM92 detection apparatus can be used to monitor the Bell inequality with a simple modification of the detectors [2].

2.6 The Quantum Bit Error Ratio in Daylight

Given that we want to run this experiment during day, we must consider the errors which will be contributed to the key by the background light. We present the theory here to calculate the quantum bit error ratio (QBER) accounting for daylight background counts.

Measurement of the Quantum Bit Error Ratio (QBER) is of primary importance for QKD. The QBER is the ratio of erroneous bits to total bits left in the sifted key, and gives a value which places a bound on the information which could be due to eavesdropping attempts. The increase in background levels means that correlated events due to detection of sunlight coinciding with a real detection of the source will begin to contribute to the generation of key bits. Since these correlations will increase the QBER these increasing errors must be maintained below certain levels imposed by the security threshold.

Assume that the detector at Bob's side is exposed to sunlight, while Alice's detector is embedded directly on the source, so does not detect the background light from the sun. The high background level will lead to detection events which are mistaken with the detection of a photon pair. These are uncorrelated to the single photon source in their polarization and lead to an increase in the QBER, which is used to establish a bound for the knowledge of an eavesdropper. The QBER will tend to 50% as the background level rises, because an event at Alice's detector recorded along with an unpolarized photon from the sun on Bob's detector will match in polarization only half the time.

In the following, we estimate the operational limit for generating a useful key under such conditions, assuming the implementation of a symmetrical BBM92 protocol, where both complementary measurement bases are chosen with an equal probability at the beam splitter. The rate of correlations for two random signals is

$$r = S_1 \times S_2 \times \tau_c, \tag{2.11}$$

where S_1 and S_2 are uncorrelated detection rates and τ_c is the time window of observation. Since the source includes actual correlated events, we must remove those rates from the uncorrelated rate for estimating the effect of the added background. Assuming that all quoted rates already include detector efficiencies, we can characterize a pair source by its single event rates, r_1, r_2, and its coincidence rate r_c. We denote the transmission of the entire optical channel[2] as η_t.

Letting S_1 be at Alice's side and directly connected to the source, while S_2 is at Bob's detector and exposed to the background in the free-space channel we have

$$S_1 = r_1 - \eta_t r_\mathrm{c} + r_\mathrm{dc1},$$

and

$$S_2 = r_\mathrm{bg} + \eta_t (r_2 - r_\mathrm{c}) + r_\mathrm{dc2}$$

where r_{dci} is the dark count rate at $i = \{1, 2\}$. An imbalance in counts over the four detectors, which may arise due to unequal quantum efficiencies of the detector diode or imperfections in the optical elements, would give rise to effects potentially exploitable for hacking the key, in the form of bit patterns in the key. This will be tested in the section 4.3. We use the average to approximate $r_\mathrm{dc1} = r_\mathrm{dc2} = r_\mathrm{dc} \cong 2000 - 3000/s$ for our detector. In what follows, the averaged effect of dark counts may be simply added to the total QBER so that the minimum QBER does not quite reach the intrinsic QBER from the source.

The signal or raw key rate for a symmetric BBM92 protocol is given by half of the detected coincidence rate, and accounting for sifted bits we get

$$r_\mathrm{sig} = \frac{1}{2} r_\mathrm{c} \eta_t \,. \tag{2.12}$$

Let r_bg be an external background event rate depending on the inclination of the sun, orientation of the optical channel, and spectral bandwidth being measured. Assuming there are no correlations between the source and background events, the accidental coincidence rate with matching bases by substitution into equation 2.11 is then given by

[2] This includes absorptive losses in optical components (including a large loss of about 50% from the interference filter) and air, geometrical losses due to imperfect mode transfer from an optical fiber, and losses due to atmospheric turbulence effects such as beam wandering, as well as losses in spatial filters.

$$r_a = \frac{1}{2}(r_1 - \eta_t r_\mathrm{c} + r_\mathrm{dc})\left(r_\mathrm{bg} + \eta_t(r_2 - r_\mathrm{c}) + r_\mathrm{dc}\right)\tau_\mathrm{c}\,, \tag{2.13}$$

where only one of the detectors, here with index 2, is exposed to the background events.

Imperfections in practical entangled photon pair sources, and detector projection errors, are often characterized by visibilities of polarization correlations V_{HV} and $V_{\pm 45^\circ}$. This gives rise to the intrinsic QBER q_i of the QKD source[3]. With a symmetric usage of both bases this is given by

$$q_\mathrm{i} = \frac{1}{2}\left(1 - \frac{V_{HV} + V_{\pm 45^\circ}}{2}\right)\,. \tag{2.14}$$

The total QBER q_t of the complete ensemble is given by the weighted average over both the accidental and real signal components

$$\begin{aligned} q_\mathrm{t} &= \frac{1}{r_\mathrm{sig} + r_a}\left(q_\mathrm{i} r_\mathrm{sig} + \frac{1}{2} r_a\right) \\ &= \frac{q_\mathrm{i} r_\mathrm{c}\eta_t + (r_1 - \eta_t r_\mathrm{c} + r_\mathrm{dc})\left(r_\mathrm{bg} + \eta_t(r_2 - r_\mathrm{c}) + r_\mathrm{dc}\right)\tau_\mathrm{c}/2}{r_\mathrm{c}\eta_t + (r_1 - \eta_t r_\mathrm{c} + r_\mathrm{dc})\left(r_\mathrm{bg} + \eta_t(r_2 - r_\mathrm{c}) + r_\mathrm{dc}\right)\tau_\mathrm{c}}\,. \end{aligned} \tag{2.15}$$

Note that as $\eta_t \to 0$, $q_\mathrm{t} \to \frac{1}{2}$, and likewise, as $r_\mathrm{bg} >> \eta_t r_\mathrm{c}$, again $q_\mathrm{t} \to \frac{1}{2}$ as expected. In figure 2.3, note that for large values of η_t, a nearly flat plateau lies inside the secure region of $q_\mathrm{t} < 11\%$. This emphasizes that a strong signal coupling, along with a linear reduction of the background rate are the main requirements for secure key generation, and may allow daylight operation in intense light. In practice, if $r_\mathrm{bg} >> \eta_t r_\mathrm{c}$ detector saturation and damage would become an issue much before the asymptotic limit of q_t.

Below the regime of detector damage, saturation of detectors still leads to a reduced probability of detecting photons at high light levels. This effect can usually be modeled by a dead time τ_d or recovery time for the device due to the finite time required to recharge the capacitance of the APD. For passively quenched APDs', this time is about $1\,\mu$s, and may be over an order of magnitude smaller for actively quenched devices. This gives a useful estimation of the fraction of time a detector can register photo events. Given an

[3] This was measured in the lab to be 4.3% prior to running the experiment. Since the experiment ran for some time, this was periodically tested during source maintenance, and usually fell in a range of 4.3 – 4.8%. See experimental section.

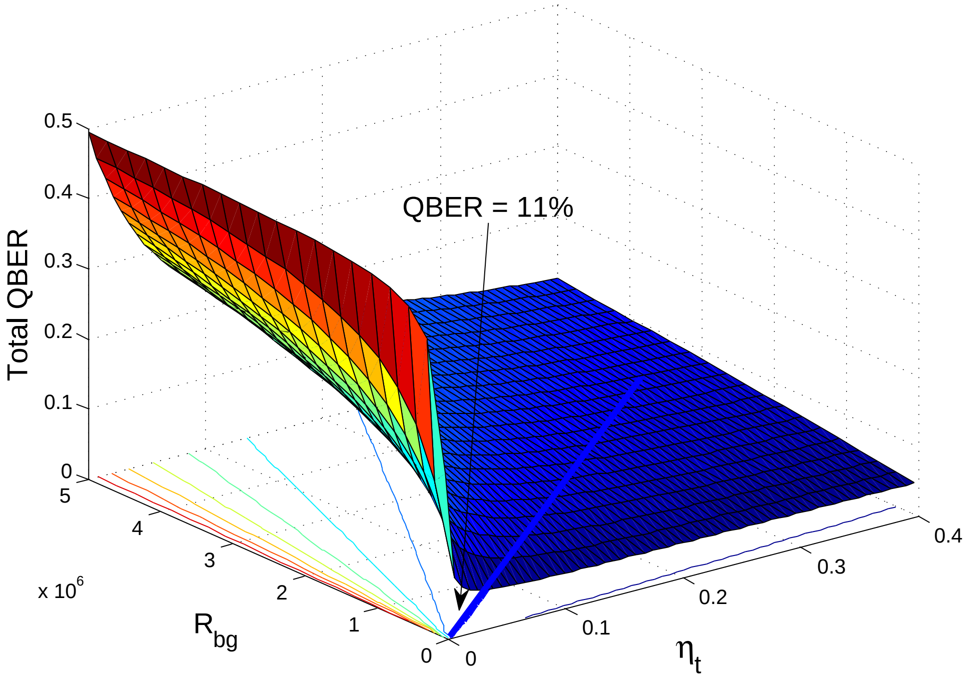


Figure 2.3: Total QBER Dependence on Background Levels and Signal Transmission. The contours (lower lines) show a linear dependence between the background rate and signal transmission for a given QBER. Notice that in the condition of a large background rate and small signal transmission, the error ratio goes toward the expected value of 1/2. The contour at the security threshold is marked with the thick line. Some typical parameters in our experiment used here are (r'_1=78 kcps, r'_2=71 kcps, r'_c=11 kcps, $\tau_\mathrm{d} = 1\,\mu$s, T=15%, q_i=4.3%, τ_c=2 ns).

initial photo event rate r (i.e., the rate a detector with no recovery time would report), a detector with dead time τ_d will register a rate of

$$r' = r(1 - r'\tau_\mathrm{d}) \quad \text{or} \quad r' = r\frac{1}{1 + r\tau_\mathrm{d}}. \tag{2.16}$$

The detector saturation modifies both signal and accidental rates similarly to equation 2.16 by the same dead time correction factor α, where we assume an equal distribution of photo events over all four detectors, resulting in a dead time constant of $\tau_\mathrm{d}/4$:

$$\alpha = \frac{1}{1 + (r_\mathrm{bg} + r_2\eta_t)\tau_\mathrm{d}/4}\,. \tag{2.17}$$

Therefore, the resulting QBER q_t in equation (2.15) does not get affected. However, the signal rate does, leading to the modified expression

$$r'_\mathrm{sig} = \alpha r_\mathrm{sig} = \frac{r_\mathrm{c}\eta_t/2}{1 + (r_\mathrm{bg} + r_2\eta_t)\tau_\mathrm{d}/4}. \tag{2.18}$$

Above a certain background rate, q_t exceeds the limit of 11% for which a secret key can be established for individual attack schemes. If both detectors are exposed to the large background of the sun it can be seen that the QBER of the key will be to large for secure transmission at much lower background levels since correlations of sunlight counts contribute much more strongly over both detectors. The case where both detectors may see background rates, as in the dual link set up [29] is plotted in figure 2.4 for comparison. Thus for such an experimental setup, stronger filtering should be applied.

It is instructive to consider the excess QBER due to background events:

$$\Delta q = q_\mathrm{t} - q_\mathrm{i} = (r_1 - \eta_t r_\mathrm{c})\, r_\mathrm{bg}\tau_\mathrm{c}\, \frac{1/2 - q_\mathrm{i}}{r_\mathrm{c}\eta_t + r_1 r_\mathrm{bg}\tau_\mathrm{c}}\,. \tag{2.19}$$

In a parameter regime useful for key generation, $q_\mathrm{i} \ll 1/2$, $r_\mathrm{sig} \gg r_a$, and for simplicity assuming $r_1 \gg T r_\mathrm{c}$, this quantity can be approximated by

$$\Delta q \approx \frac{r_\mathrm{bg}\tau_\mathrm{c}}{2\eta_t(r_\mathrm{c}/r_1)}\,. \tag{2.20}$$

The source property r_c/r_1 is the efficiency of the source. Optimization of this parameter is active research and it is set at it's maximum value of $r_\mathrm{c}/r_1 \approx 0.16$. As well, the channel transmission η_t, though requiring stabilization throughout the period of data acquisition, was quite good, and maximized as much as possible. The only way to reduce the excess error Δq is to reduce the background rate r_bg and the coincidence time window τ_c, while increasing the signal transmission η_t. The limitation on reducing τ_c is the timing jitter of all detectors, which in our case is on the order of a nanosecond. Emphasis thus has to be drawn to reduce the background rate r_bg and is discussed in the experimental section which introduces the filtering methods at section 3.2.

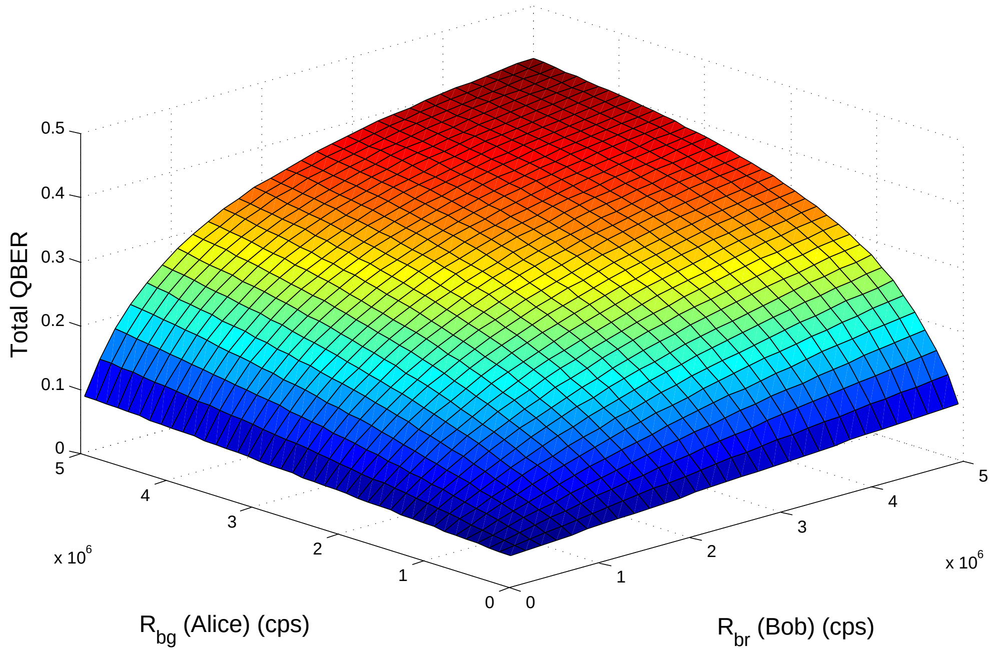


Figure 2.4: The total QBER dependent on background counts at either detector, using $\eta_t = 15\%$, an average value for the experiment. As compared to the case of an embedded detector in figure 2.3, having both detectors exposed to the background counts of the sun will require further filtering to maintain an appropriate bit ratio. Here the QBER rises approxiately with the square of the background level as the coincide at two detectors.

2.7 Generation of Correlated Photon Pairs

The generation of an entangled pair requires the creation of photon pairs, and is usually performed through a process called Spontaneous Parametric Down Conversion (SPDC). We outline the theory of the most common method of obtaining these states here; by using nonlinear optical crystals, which require optical wave mixing in a nonlinear medium.

In the discussion this far it has been assumed that it is possible to obtain entangled photons without going into details about the physical preparation of such states. It is possible to obtain bright sources of entangled photons coupled into single mode fibers for ease of use.

Specifically the process known as parametric down-conversion is used to create two photons in a spatial mode which may be collected into single mode fibers. To describe it simply, a pump photon in the nonlinear crystal may spontaneously split into two daughter photons, and the photon pairs may be used to create entangled pairs. In what follows, the two daughter photons are know as the signal and idler waves, or modes, which correspond to two axes of the crystal. The pump is simply referred to as the pump wavelength or mode, and the nonlinear medium is the optical crystal.

To generate photons using a continuous wave (cw) laser pumping the non-linear medium we rely on vacuum fluctuations, and thus the photon pair is output randomly in time, so that the resulting daughter photons emerge in a Poissonian temporal distribution. Down-conversion is the $\chi^{(2)}$ three wave mixing process by interaction in a nonlinear medium, where the nonlinear medium is left unchanged. This process can be described by the interaction Hamiltonian [38, 39], integrated over the volume of the crystal.

$$\widehat{H}_I = \int_V \chi^{(2)} \widehat{E}_p^{(+)}\left(\vec{r},t\right) \widehat{E}_s^{(-)}\left(\vec{r},t\right) \widehat{E}_i^{(-)}\left(\vec{r},t\right) dV + H.c. \tag{2.21}$$

Each of the three interacting waves $\widehat{E}_j\left(\vec{r},t\right) = \widehat{E}_j^{(+)}\left(\vec{r},t\right) + \widehat{E}_j^{(-)}\left(\vec{r},t\right)$ for $j = p, s, i$ include creation and annihilation components which represents difference frequency generation, and in the spacial case that $\omega_s = \omega_i$ we get frequency degenerate down-conversion. The inverse process is up-conversion (sum frequency generation) represented by the Hermitian conjugate $H.c.$, which we will ignore since we are sending pump light into the crystal for creation of lower energy pairs.

The time dependence of the state can be considered to first order by Taylor expansion. Reduction of the general time dependent Hamiltonian to the first order form gives

$$|\psi\left(t\right)\rangle = exp\left[\frac{1}{\imath\hbar}\int_{t_o}^{t} \widehat{H}_I\left(t^{'}\right) dt^{'}\right] |\psi\left(0\right)\rangle \longrightarrow \frac{1}{\imath\hbar}\int_{t_o}^{t} \widehat{H}_I\left(t^{'}\right) dt^{'} |\psi_o\rangle \tag{2.22}$$

where $|\psi\left(0\right)\rangle = |\psi_o\rangle$, is the vacuum state, assuming on the right hand side of the equation that there are no daughter photons before the pump is switched on. Higher order terms represent higher energy processes, for example the 2^{nd} order term is the interaction of two pump photons splitting into four daughter photons, etc. These higher order terms would result from further expansion of the left hand side of equation 2.22 due to the exponential function, but are ignored since the cw pump we used is not of sufficient intensity to generate many four photon events. Since the generation rate of signal and idler photons is small compared to the pump, it may be assumed that they do not re-enter the crystal at any time t and stimulate the inverse process, up-conversion.

Ignoring the quantum state of the pump since the loss of a photon within a large electro-magnetic field is negligible, the annihilation operator in 2.21 is replaced with a classical field $E_p(\vec{r},t) = \widetilde{E}_p(t)\, e^{\imath \vec{k}_p z}$. Assume that we are considering an infinitely narrow bandwidth pump (i.e $\Delta\omega = 0$) and so the Fourier transform $\widetilde{E}_p(t) = \int E_p(\omega)\, d\omega e^{(\imath\omega_p t)}$ is a single frequency component. This is only approximate, however, in what follows we seek to find the mean wavelengths, while the broadband spectral characteristics of the signal and idler are suppressed, and thus any spread in the signal and idler wavelength due to the pump is not accounted for in this analysis. Substituting the electric field operator

$$\widehat{E}_j^{(-)}(\vec{r},t) = A \times \hat{a}_j^{\dagger} e^{-\imath\left(\vec{k}_j z - \omega_j t\right)}, j = s, i, \tag{2.23}$$

which represents the creation of a photon in phase with the pump photon, into 2.21 we can solve for the interaction by extending the time limit to ∞ and pulling the normalization terms $A_j = \imath\sqrt{\frac{\hbar\omega_j}{2\epsilon_0 n^2}}$ and the $\chi^{(2)}$ term which, will be constant for a given wavelength, from the integral. Integrating time leads to an expected constraint, the conservation of energy, since this integral over the exponential function gives a delta function $2\pi\delta(\omega_s + \omega_s - \omega_p)$, from which follows the equation

$$\omega_p = \omega_s + \omega_i, \tag{2.24}$$

The remaining integral from equation 2.21, and equation 2.22 is

$$\frac{2\pi A'}{\imath\hbar}\int_{-l/2}^{l/2} \hat{a}_s^{\dagger}\hat{a}_i^{\dagger} e^{-\imath\left[\left(\vec{k}_s+\vec{k}_i-\vec{k}_p\right)z\right]} dV|\psi_o\rangle = A''\Phi(\Delta_k l)\,|H_s\rangle|V_i\rangle \tag{2.25}$$

where the signal and idler give rise to a horizontally (H) and vertically (V) polarized single photon in the output mode of the crystal. A'' includes the slowly varying terms in 2.23 as well as E_p and $\chi^{(2)}$. The finite integral evaluates to a momentum conservation equation as

$$\Phi(\Delta_k l) = \frac{\sin(\Delta_k l)}{\Delta_k l}, \tag{2.26}$$

which is maximal in the conservation of momentum

$$\Delta_k = \vec{k}_s + \vec{k}_i - \vec{k}_p = 0. \tag{2.27}$$

Equation 2.27 is known as the phase matching condition. In the limit of the crystal length $l \to \infty$ the bandwidth goes to zero, as the sinc function goes to a delta function. This is of interest because a narrow bandwidth signal will allow stronger filtering, and can be obtained with a longer crystal. As well, in the larger volume where the waves interact the conversion rate will rise with a longer crystal. Thus it seems increasing the crystal length will only improve things. In practice however, there is a limit to the length of the crystal, since the pump and signal/idler waves will disperse differently due to the material properties at their respective wavelengths. At some point, the waves will become out of phase and there is no longer strong down-conversion. We see in the later section on quasi-phase matching that engineering the crystal to be periodically poled allows the crystal to be long while overcoming this effect, giving higher conversion and narrower bandwidths. The quantum mechanics of nonlinear optical processes is discussed in detail in the book by David Klyshko [38].

2.7.1 Non-Collinear Phase Matching in a BBO crystal

The source of entanglement for this experiment used a BBO down conversion crystal for the generation of photon pairs, which are collected into single mode fibers.

The source used for the experiment is based on birefringence phase matching in a Beta barium borate (BBO - β BaB_2O_4) crystal. This source has been well developed and it's parameters are reported on in the experimental section below. Physically, the generation of Type II entanglement is the same as described for SPDC in equations 2.27, 2.24 and 2.21. The output photons are collected at the cross-over point of two phase matched rings which are orthogonal in polarization. Thus, the source is termed to be in a non-collinear arrangement because of the angular properties of the output signal and idler photons. This source developed by Kwiat [40] can be referred to in our past paper [2].

2.7.2 Quasi-phase Matching in a PPKTP Crystal

There are limitations in the number of correlated photon pairs created in the BBO source, as well, a large spectral bandwidth for the daughter photons. These problems may be improved upon using a quasi-phased matched down conversion source with PPTKP as the conversion medium. The temperature tuning curves are calculated for this advanced pair source to be used in a second generation experiment.

Quasi-phase matching is a technique to engineer the phase matching conditions for nonlinear conversions that are not possible in a bulk crystal that relies on birefringence for phase matching. It is done by inverting the ferroelectric poles of the crystal periodically, allowing the introduction of a flexible term, the poling period Λ, for selection of a conversion mechanism. This allows many wavelengths to be generated by selecting the proper poling period to maximize the effective nonlinearity for a given polarization and direction of propagation in the crystal. In the following, a good reference which lists material properties is the book by Dmitriev [41] which has a good introduction to nonlinear optical physics, as well as information on other relevant optical materials.

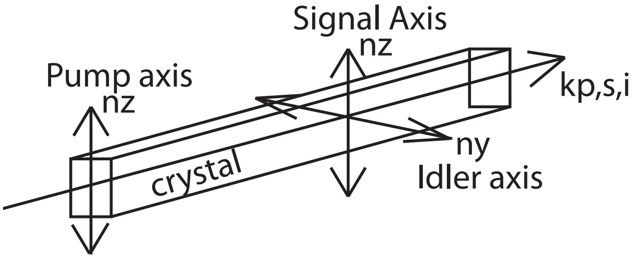


Figure 2.5: The orientation of polarizations for the particular case of Type II *collinear* wave mixing, for three waves; the pump, signal and idler, propagating in a nonlinear medium. Note, this case is used for the tuning curves of Periodically Poled Potassium Titanyl Phosphate (PPKTP) difference frequency generation.

The poling period is on the order m of the phase overlap between the pump and daughter photons. This poling period allows for correction of the phase mismatch between

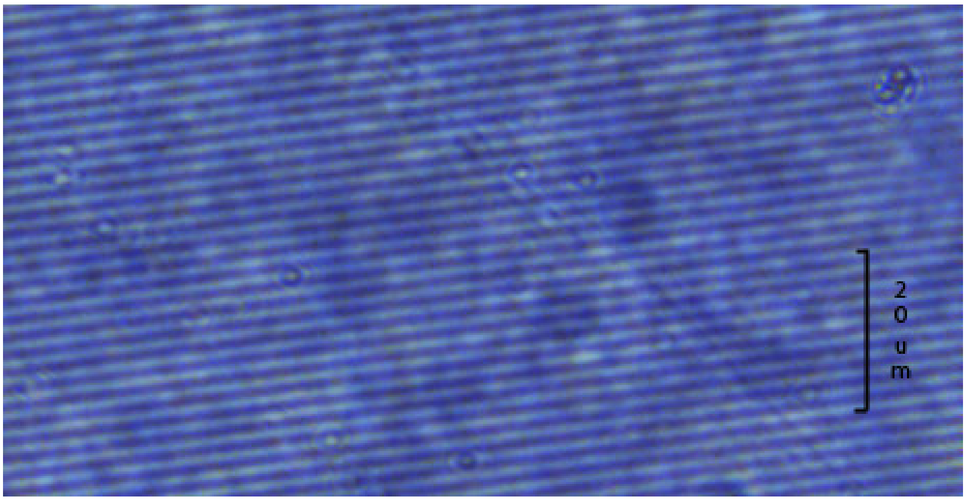


Figure 2.6: Image of the PPKTP showing periodic poling regions. The scale marked is approximate with lines ±1.

the signal or idler waves and the pump wave due to the various wavelengths traveling at different speeds in the conversion medium. Periodic poling can be used to allow conversion while extending the length of the crystal. Physically, only certain axes of the crystal may be used for this method, because poling of the crystal favors some directions along the crystal lattice. There are a number of methods to grow such a material, but succinctly, the material is typically heated to a large temperature ($> 800^\circ$ C) whereby a periodic voltage is applied across the crystal using a small patterned electrode. The crystal is then cooled to a temperature where the poling will become stable, and the electric field is removed. Figure 2.6 is a photograph showing the poling periods of a PPKTP crystal along the z axis.

A modified phase matching term from 2.27 includes the periodicity of the poling:

$$\Delta_k = \vec{k}_s + \vec{k}_i - \vec{k}_p - \frac{2\pi m}{\Lambda} \tag{2.28}$$

where m is the poling order.

Periodic Poling has been done usually in Lithium Tantalate (LT - $LiTaO_3$), Lithium Niobate (LN - $LiNbO_3$), and Potassium Titanyl Phosphate (KTP - $KTiOPO_4$) for useful generation of select frequencies. In particular, KTP is useful because of it's strong $\chi^{(2)}$ interaction and ability to generate Type II conversion for photon pairs in the collinear propagation direction which allows more signal to be collected. It is advantageously non-hydrophilic, and only slightly biaxial[4]. This means the crystal properties in these two axes will be roughly the same, namely we can use $n_x \approx n_y$.

For signal generation near 800 nm in KTP, the poling period $\Lambda = 10\,\mu$m, as may be calculated from equation 2.7.2 based on the material parameters for KTP. This crystal can be obtained at lengths from 5 mm to 25 mm currently. The longer crystal length makes the alignment harder but gives a narrower bandwidth, as can be determined from the sinc term of equation 2.7. This is advantageous for filtering. As well, a longer crystal means a larger signal rate since the volume of integration in equation 2.25 is larger. The increase in signal rate will lead directly to an increase in the rate of key generation as the QBER remains constant, assuming the quality of signal generated is constant with the crystal length.

We aim to calculate the temperature dependence of the phase matching for tuning of the wavelengths. The refractive index is sensitive to the temperature of the crystal, and so the temperature should be held stable for generation of the polarization entangled pairs. Additionally, degenerate frequency operation of the crystal is possible over a large spectral range of output wavelengths by temperature tuning. An operating temperature may also be chosen by a one to one correspondence with temperature to optimize signal wavelength, in respect to atmospheric transmission, background reduction in a free space link and detector sensitivity. To calculate the temperature tuning curves a number of factors must be considered; thermal expansion, refractive index gradients due to temperature changes, and the phase matching conditions. An experimental investigation [42] found the thermal expansion of the material to depend on temperature as

$$l^{'}(T)/l\left(25°C\right) = 1 + \alpha^{'}\left(T - 25°C\right) + \beta^{'}\left(T - 25°C\right)^{2}, \tag{2.29}$$

where $\alpha^{'} = 6.7^{-6} \pm 0.7$ and $\beta^{'} = 11^{-9} \pm 2$ and l and $l^{'}$ are crystal lengths at the reference

[4] The two optical axes are similar, so properties such as the refractive index or thermal expansion along those two directions will be nearly equivalent, i.e. $x \approx y$

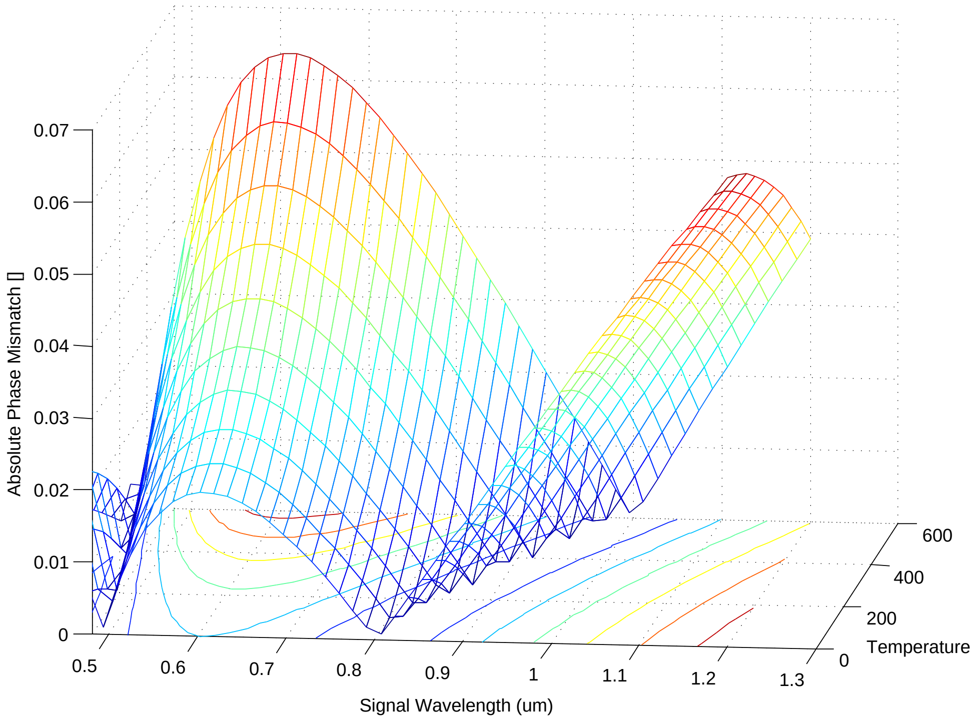


Figure 2.7: Absolute Phase Mismatching for Quasi-Phase Matched Type II Down Conversion in PPKTP. Note the characteristic parabolic dependence on temperature in the contour plot (drawn on lower plane).

temperature of 25° C and the temperature T respectively. Geometric expansion of the poling period will only effect the conversion wavelength by a factor of $\cong 10^{-1}$, as compared to a change in phase-matching due to refractive index gradients with T but are included for accuracy.

Now, substituting the expression for the wavenumber in a material

$$k_j = 2\pi n\left(\lambda_j, T\right)/\lambda_j$$

into the quasi-phase matching equation 2.7.2, including temperature dependence as the variable T, we have

$$\Delta_k = \frac{2\pi n_y\left(\lambda_p, T\right)}{\lambda_p} - \frac{2\pi n_y\left(\lambda_s, T\right)}{\lambda_s} - \frac{2\pi n_z\left(\lambda_i, T\right)}{\lambda_i} - \frac{2m\pi}{\Lambda l'/l} \tag{2.30}$$

which is plotted in absolute values in 2.7 based on values for the index which follow.

Form	A	B	C	D	crystal axis
one-pole	2.19229	0.83547	0.04970	0.01621	y
two-pole	2.12725	1.18431	5.14852×10^{-2}	0.6603	z
Form	E	F	-	-	crystal axis
two-pole	100.00507	9.68956×10^{-3}	-	-	z

Table 2.1: Sellmeier equation coefficients for the one pole and two pole equations for the refractive index of KTP.

The subscripts in $n_{y,z}$ account for the fact that the Type II process uses the pump in the y axis of the crystal, while the signal and idler are converted via the y and z axes, respectively. The pump wave, and daughter photons all travel in a collinear axis in this phase matching arrangement.

Turning attention to solve 2.7.2, accurate equations for $n\left(\lambda, T\right)$ must be used and the curves where $\Delta_k = 0$ are solved to find temperature tuning for constructive phase matching of the PPKTP arrangement. To account for $n\left(\lambda\right)$, a one pole Sellmeier equation of the form

$$n^2 = A + \frac{B}{1 - C\lambda^2} - D\lambda^2 \tag{2.31}$$

is found to be accurate for the refractive index in the y axis [43], and a two pole Sellmeier equation of the form

$$n^2 = A + \frac{B}{1 - C\lambda^2} + \frac{D}{1 - E\lambda^2} - F\lambda^2 \tag{2.32}$$

as is found to provide the best fits for the z axes [44] in the NIR and IR spectral regions. The coefficients are listed in table 2.1.

Finally, temperature dependent dispersion[5] which was experimentally investigated in [42] is introduced. Similar equations are also studied in [45] but these coefficients are not used. The refractive index follows a parabolic dependence with temperature

$$\Delta n\left(\lambda, T\right) = n_1\left(\lambda\right)\left(T - 25°C\right) + n_2\left(\lambda\right)\left(T - 25°C\right)^2 \tag{2.33}$$

[5] Also called thermo-optic dispersion.

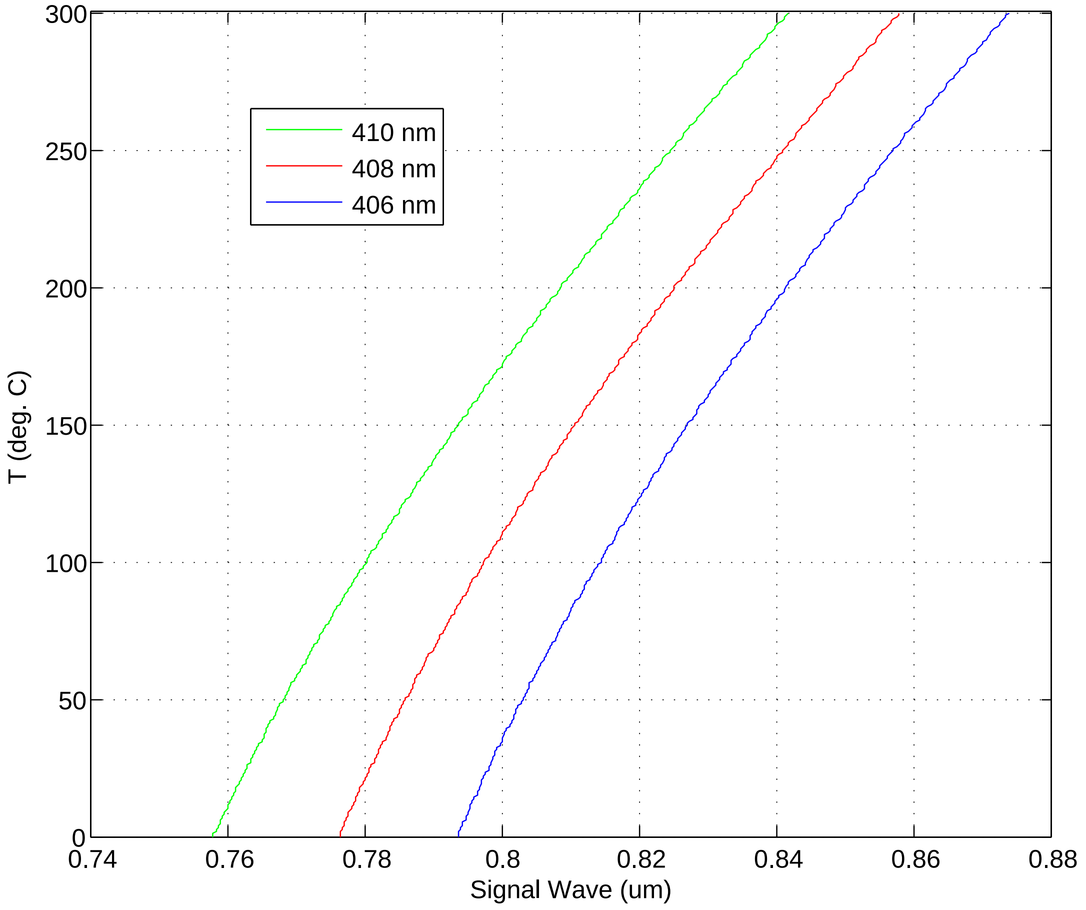


Figure 2.8: Temperature tuning curves for the signal wave for three different pump wavelengths. A small change in the wavelength of the laser diode leads to a large temperature shift required to select a particular wavelength for the signal photon.

with the coefficients

$$n_{1,2}\left(\lambda\right)=\sum_{p=0}^{3}\frac{a_p}{\lambda^p}$$

listed in table 2.2 for an expansion of third order. Taking the above factors into account, it is possible to generate the temperature tuning curves for Type II down conversion in the PPKTP crystal. The temperature and pump wavelength can be seen to have a strong effect on the phase matched signal and idler wavelength as in figure 2.8, where a change of $\approx 2\,\mathrm{nm}$ in pump wavelength requires a temperature change of $\approx 50°\mathrm{C}$ to maintain a particular signal wavelength.

For a blue diode chosen at $407\,nm$ which was selected for a narrow band Littrow

	n_1 (10^{-6})	n_2 (10^{-8})	n_1 (10^{-6})	n_2 (10^{-8})
Axis	z	z	y	y
a_0	9.9587	1.1882	6.2897	0.14445
a_1	9.9228	10.459	6.3061	2.2244
a_2	8.9603	9.8136	6.0629	3.5770
a_3	4.1010	3.1481	2.6486	1.3470

Table 2.2: Temperature dependence fit coefficients for KTP used in equation 2.7.2.

stabilized pump LASER [47] we can see the signal and idler wavelength dependence with temperature, as well as the frequency degenerate temperature in figure 2.9. The signal and idler are constrained by considering the energy conservation in vacuum from equation 2.24 which gives

$$\frac{c}{\lambda_p} = \frac{c}{\lambda_s} + \frac{c}{\lambda_i} \rightarrow \lambda_i = \frac{\lambda_s \lambda_p}{\lambda_s - \lambda_p}. \tag{2.34}$$

This allows us to relate the signal and idler spectra together as a set to a given temperature and pump wavelength directly from the crystal parameters.

The proposed source of entanglement using the PPKTP crystal requires a Sagnac loop interferometer [48] where the pump illuminates the crystal through both directions of the interferometer. This creates a spatial indistinguishability of the arrival of the signal and idler on the out port of the interferometer due to symmetry of their generation, and a entangled photon state in the polarization degree of freedom. The most recent version of this source created visibilities better than 98% in a narrow bandwidth of roughly $1nm$, with 10 times more coincident counts than in our present system [49]. A longer distance test, up to a few km's, should be possible using the PPKTP source. It would be very unlikely to acheive this distance using the BBO source due to the low pair generation rate, and atmospheric losses.

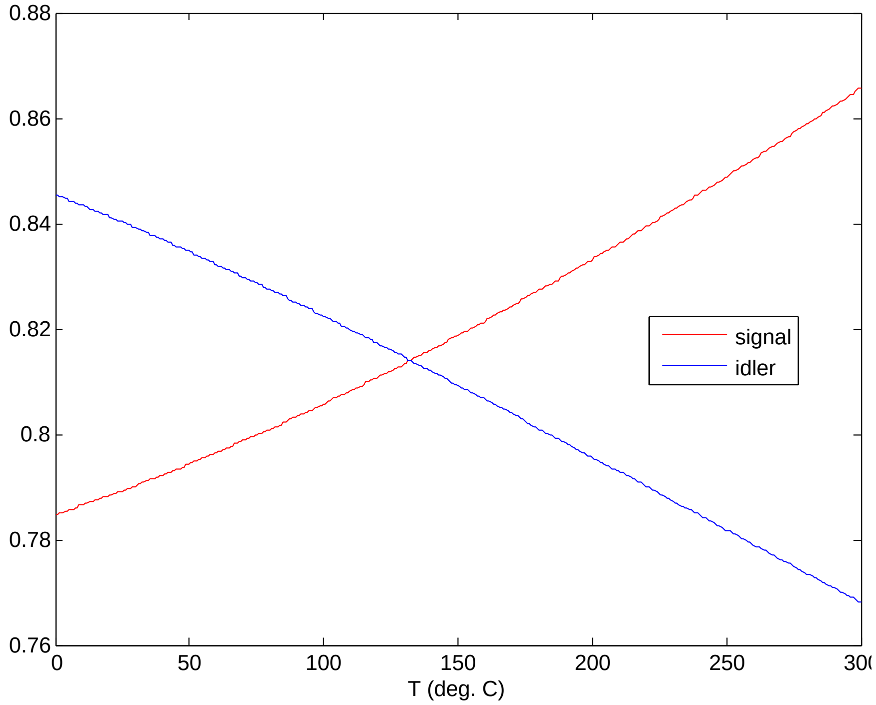


Figure 2.9: Temperature Tuning Curves for Type II (xy-y) Quasi-Phase Matching in a PPKTP Crystal. The temperature required for degenerate down conversion is at the cross over of both wavelengths near 140°C.

2.8 Atmosphere Absorption and Turbulence

Atmospheric losses must be considered for the free space channel. Here two main loss effects due to fluctuations in the refractive index of the air channel are described.

Fortunately, air has negligible birefringence so the use of polarization coding for the bits will mean there are negligible errors introduced in the bits through the atmospheric channel[6]. The use of a free-space optical channel has other limitations rising from turbulence in the air, which will effect the on the propagation of a the light beam. Signal loss is imminent due to absorption and scattering just like in a fiber optic channel, while

[6] In the case of a fiber optical channel, time-bin encoding is more often chosen due to stress induced birefringence of polarization in a typical silica fiber.

geometric coupling through the channel will fluctuate due to stochastic refractive index changes. These later losses will limit coupling and may also require active stabilization over a particular distance.

In air, fluctuations in the refractive index with temperature are on the order $\Delta n \approx 10^{-6}$ for a change of $1°C$ [54, 55] inside the free-space channel. Moreover, these fluctuations may be on the scale of a few millimeters, to as much as a kilometer. The former fluctuations would cause a distortion of the image pattern in a collimated beam of ≈10 cm diameter, while fluctuations a few times the size of the beam will tend to steer the beam around slightly. For free space QKD we are interested in maximizing tranmission across the channel. Thus, some of the effects of a turbulent atmosphere, such as image quality, may be ignored. Depending on the distance of the transmission, beam divergence, and the size of the beam diameter the effects originating from the turbulent atmosphere [55] include:

- beam wandering;
- beam spreading;
- coherence loss;
- pulse distortion or broadening;
- thermal blooming;
- scintillations.

Scintillations within the beam are not a concern since no image needs to be constructed from the transmission, however, they will lead to fluctuations above and below the mean intensity, or photon number in a random way. This is of concern when imaging celestial objects for example, but will not cause ultimate losses over our distance. As well, pulse distortion is negligible. Thermal blooming occurs with high energy beams, causing them to self focus or causing nonlinear effects, and it can be ignored as we transmit a source of single photons. Coherence loss is also negligible, leaving two main effects to be considered: beam wandering, and beam spreading.

2.8.1 Beam spreading and wandering

Two predominant effects of the turbulent atmosphere on transmission in a free space channel are described.

Purely diffraction based beam spreading of a Gaussian beam gives a radius of

$$\rho_d = \left[\frac{4L^2}{(k_s D_l)^2} + \left(\frac{D_l}{2}\right)^2\right]^{1/2} \tag{2.35}$$

in meters, which is negligible over the distance of this experiment, since the initial beam waist is 40 mm, the beam diameter changes less than one tenth a percent. Here $L = 350\,\text{m}$, $k_s = 2\pi/\left(810\right)\text{nm}$ and $D_l = 0.08\,\text{m}$. From turbulence theory [56] we get the equation

$$\rho_0 = \left[1.46k^2 \sec\varphi \int_0^L dz C_n^2\left(z\right)\left(1 - \frac{z}{L}\right)^{5/3}\right]^{-3/5} \tag{2.36}$$

which is the transverse coherence length, also know as Fried's parameter or the *diffraction limited aperture of the atmosphere* with units of length. This parameter depends strongly on the atmospheric structure constant C_n^2 which in most cases is numerically determined. C_n^2 depends on elevation, temperature, weather, wind speed and other factors which are hard to determine, and φ is the declination angle with respect to the zenith direction.

The structure constant C_n^2 is modeled in the Hufnagel-Valley 5/7 Model of Atmospheric Turbulence [57], however, this model shows C_n^2 at ground level spans a large range; with $C_n^2 \approx 10^{-3} - 10^{-7}$ over a few kilometers of elevation from ground level. Usually it is found empirically, for which we have some observations only of the beam wander. Here, at 1 km the beam wanders over an area with roughly twice it's original diameter. At a constant ground level, the C_n^2 is pulled from the integral, which then evaluates to $3L/8$. Assuming that $\sec\varphi \approx 1$, we then have $\rho_0 \approx 7.75 \times 10^{-9}\left(C_n^2 L\right)^{-3/5}$ m.

Beam spreading can be calculated as again from turbulence theory [58]:

$$\left\langle \rho_s^2 \right\rangle = \rho_d^2 + \frac{4L^2}{(k_s \rho_o)^2}\left[1 - 0.62\left(\frac{\rho_0}{D_l}\right)^{1/3}\right]^{6/5} \tag{2.37}$$

where ρ_d^2 is already shown to be negligible. Again we have to deal with the unknown parameter ρ_0 for diffraction of the atmosphere. An empirical expression for the beam diameter D was obtained by Buck [59]

$$D = \alpha L^{\beta} \tag{2.38}$$

with the dimensionless parameters $\alpha = 4.5 \times 10^{-6}$ and $\beta = 1.2$. This shows the turbulence model to overestimate the spreading with distance. In any case, in respect to a distance of $350\,m$ the atmospheric spreading evaluates to a small number. Given observations of the beam over distances in earlier experiments [2] it is clear that within the diffraction limit of the beam, spreading is not much of a concern. Note, the dependence of beam spreading with distance goes like $L^{11/3}$ owing to completely atmospheric turbulence, and is inversely proportional to the beam diameter sent. Thus, a larger beam diameter can be chosen for longer distances, however, the limit to the diameter will depend on the amount of background light input into the receiver during day.

A value of ρ_0 may be calculated from beam wandering observations. Beam wandering from the turbulence theory is

$$\left\langle \rho_c^2 \right\rangle = \frac{2.97 L^2}{k_s^2 \rho_0^{5/3} D_l^{1/3}}. \tag{2.39}$$

The Fried parameter is estimated to be $\rho_0 = \{1.45 \times 10^{-8}, 3.65 \times 10^{-6}\}\ m$ by taking a range of values for C_n^2 from the Hufnagel-Valley 5/7 Model of Atmospheric Turbulence [57] near ground level. We calculate $\langle \rho_c^2 \rangle$ for those parameters as $\langle \rho_c^2 \rangle \approx \frac{1.4 \times 10^{-8}}{\rho_0^{5/3}} = \{1.6 \times 10^5, 0.16\}\ m^2$. The later is of the order of the square beam diameter. Owing to the observations an estimated turbulence loss over 1 km is 50%, and in our short test range of 350 m losses of roughly $15 - 25\%$ by simply comparing average areas of the beam observed over a period of time, assuming there are no fluctuation in the stability of the sending telescope. Using $L'_{\langle \rho_c^2 \rangle} = 10 \log_{10} \left(\frac{D_l^2}{4 \left\langle \rho_{s,c}^2 \right\rangle} \right)$ which represents the dB loss based on a geometric overlap between the receiver aperture and the final beam diameter, we can estimate the parameter $\rho_0 = 5.8145 \times 10^{-5}\, m$ from the beam wander observed. Due to the large range of values prevalent from the model it may be most instructive to make measurements on site, and fit them to the expected exponential laws described. It would be instructive to reinterpret the turbulence theory for a ground to ground free-space communication channel.

Chapter 3

The Experiment

Previous reports of the hardware and software used in this experiment are in [55, 56]. The Quantum Key Distribution system is as well reported on from previous experiments [2, 27, 57] and otherwise any modifications are stated herein.

3.1 Set-up

Here we describe the experimental setup, including hardware, alignment procedures, et cetera.

Optical Channel: The optical channel is aligned roughly $E16°S$, (16° *South of East*) along the horizon with the receiver pointing toward the morning sun as in figure 3.5. The minimal incident angle of the sun and the line of sight was thus about 16° which allows the experiment to be tested near the channel orientation where maximal coupling of daylight into the channel is expected. An ad hoc channel should not be limited to be perpendicular to the sun's projected daytime trajectory, so this case should be tested.

Detector units: Actively quenched avalanche photo diode (APD) detectors may be subject to irreversible destruction when exposed to an excessive amount of light; such a situation may occur if there is excessive scattering in the optical communication link. These detectors are attractive for their fast recovery times, however for a the daylight

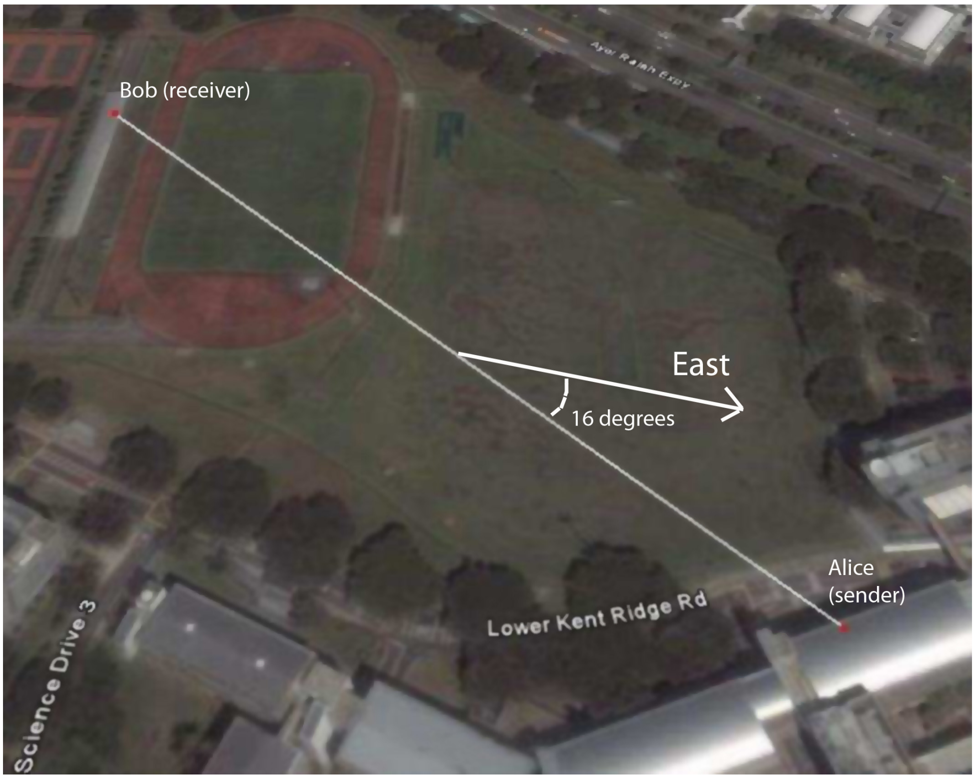


Figure 3.1: The free space optical channel spans a turbulent atmosphere of 350 m across the NUS campus. The receiver takes cover beneath the sports pavilion, while the sending telescopes are positioned behind the windows of the building. Negligible birefringence is introduced in air.

version of the experiment destruction of the device is a problem. For passively quenched APD's this is not a problem, since the electrical power deposited into the device can be limited to a safe operation regime at all times. We use passively quenched APD's for this experiment. The passively quenched APD's are configured in *Geiger mode* by setting an extra 15 V above the breakdown point while monitoring the device on an oscilloscope. This allows increased sensitivity so that a single photon may be detected, and such a device is commonly referred to as a single photon APD (SPAPD). Dark counts of each SPAPD are then compared to verify that the four SPAPD's all have an equal quantum efficiency. The detection unit is outlined in figure 2.2.

TCP/IP Channel: A classical channel using wire mesh antenna and a wireless modem using a TCP/IP link is setup. For this small distance the quality is very good, and is only limited by the bandwidth of the wireless channel which is 1 MB/second.

The link was tested up to 20 km and still shows good signal quality. Each antenna is mechanically stabilized and directed to optimize the signal. 250 mW of power are applied for the wireless link. This was used for public communications. All the software for the key generation was programmed by Christian Kurtsiefer and has been provided as open source[1].

Photon Pair Source: The polarization-entangled photon pairs are prepared from a source based on type-II parametric down conversion (PDC) in a non-collinear configuration similar to [40]. It is pumped with a CW free-running diode laser with power of 30mW and a center wavelength of 407 nm, producing pairs at a degenerate wavelength around 814 nm in single mode fibers. When directly connected to single photon detectors, we typically observe single rate per arm of 78 kcps and 71 kcps, with a coincidence rate of 12 kcps. The visibility as in equation 2.10 of polarization correlations in the HV and ±45° basis are $97.5 \pm 0.5\%$ and $92.1 \pm 0.8\%$, respectively. While these sources have been substantially surpassed in quality and brightness [47, 48], this particular device is both simple and robust. The next generation PPKTP source discussed above will allow further distances and higher count rates in future experiments.

Telescopes: As endpoints in our transmission channel, we use a pair of custom telescopes to transmit one member of the entangled photon pair across a distance of $350m$. The relative orientation of both telescopes is adjusted using manual tip/tilt stages with an angular resolution of $\approx 10\mu rad$, mounted on tripods intended for mobile satellite links. The telescopes are not actively stabilized, but this could be added for spanning larger distances, or to compensate for thermal drifts in the mounting stages. The sending telescope consists of fiber port, a small achromat with $f = 100\,\text{mm}$ to reduce the effective numerical-aperture of the single mode fiber, and a main achromat with $f = 310\,\text{mm}$ and 75 mm diameter, transforming the optical mode of the fiber to a collimated Gaussian beam with a waist parameter of 20 mm. Nominally this results in a Rayleigh length $2z_r = \pi\omega_o^2/\lambda$ of 1.6 km at our operation wavelength of $\lambda \approx$810 nm, well above our target distance over NUS campus pictured in figure 3.1.

[1] All the code is available under http://code.google.com/p/qcrypto

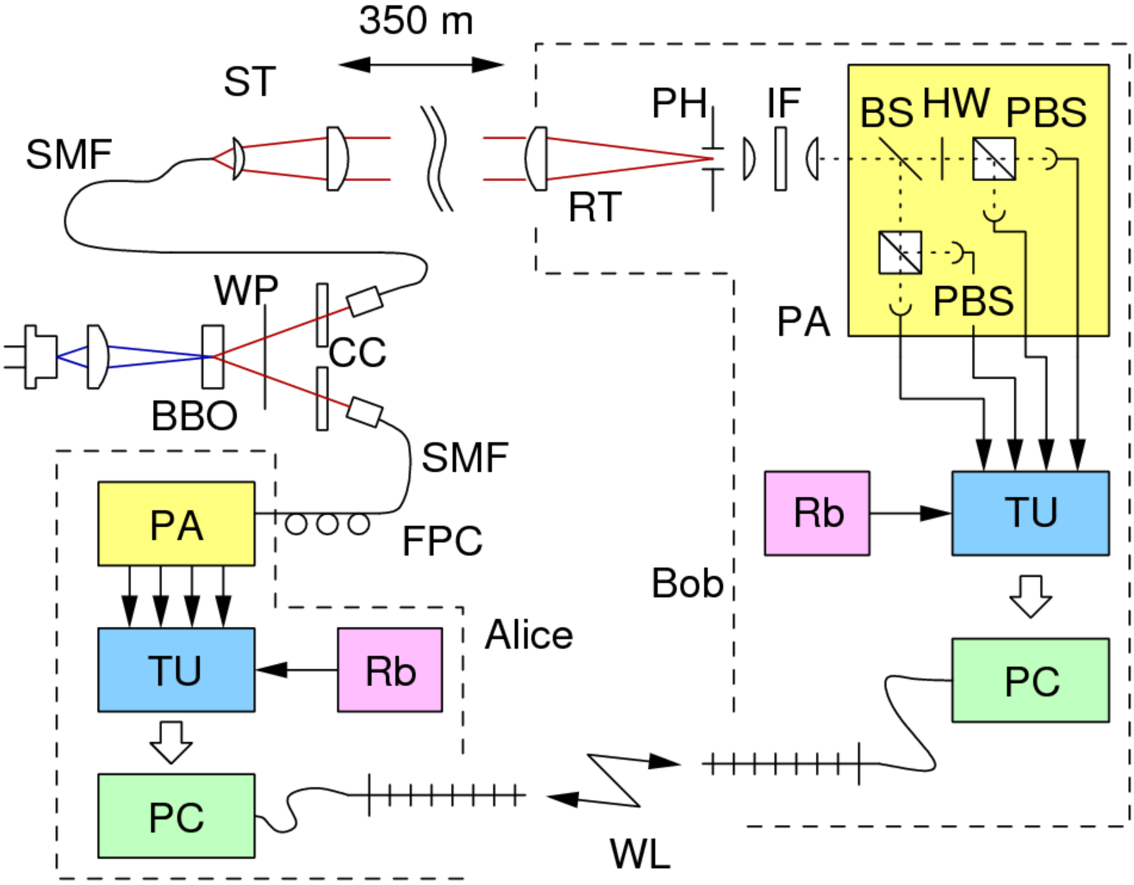


Figure 3.2: Schematic diagram of the QKD setup. Components are a sending telescope (ST) located at Alice (A), receiving telescope (RT) located at Bob (B), single mode fibers (SMF), a wave plate (WP), compensating crystals (CC) to address birefringent walk-off; polarization analyzer units (PA) comprising a 50:50 Beam splitter (BS), polarizing beam splitters (PBS) and a half wave plate (HW); a time stamp unit (TU) referenced to a Rb oscillator (Rb), a receiving telescope (RT) with a pinhole (PH) for spatial filtering and an interference filter (IF) for spectral filtering. A wireless link (WL) is used for classical communication.

3.2 Filtering Techniques

Spectral, spatial and temporal filtering methods are used to reduce the background rate at the receiver telescope to bring accidental coincidence rates low enough for secure QKD.

The filters used to remove background light to acceptable levels include the spatial filters, mounted internally and externally to the sending and receiving telescopes, a temporal filter applied in the software, and spectral filtering aligned in the lab and internal to the receiving telescope at Bob. Here we discuss their figures of merit, and describe the design and alignment procedures for each.

3.2.1 Temporal Filter

Due to the tight time correlation of the down-converted photons, it is expected that paired events on either side of the transmission will occur within a small time window. Public discussion of events at the onset of the data acquisition using a correlation method searches for the highest overlap to correctly match the pairs. The temporal filter acts to simply ignore any coincident events outside of a particular time delay, by choosing events in a smaller time window. This acts to remove unwanted detection of background in the optical channel along with a real event at the source side of the channel from the key. We limit our time window to roughly 2 ns, which is close to the minimum time acceptable owing to detector jitter.

Referring to figure 3.3, the overlap between detector pairs operating in the same basis is excellent, but there is approximately 0.5 ns difference between the two detector groupings. These groupings are just the two measurement bases, and are publicly announced during the sifting of the raw key, so will not compromise the security of key generation. The coincidence window of 2 ns is indicated in the graph, showing that that there are some key generating counts being lost outside of the time window. Unfortunately the delays for all of the detectors were not equalized during alignment, though not interfering with the success of the experiment, some coincidence counts are lost due to this error. If the detector groups were mutually compensated, the coincidence window could have been tightened with no loss of signal, but reducing the background proportionally. On the order of 10% more key may be generated correcting for this overlap, as estimated by inspection of figure 3.3.

It should be noted at Bob's side of the channel, i.e. the one exposed to a lot of background light, obtains more photon counts than the detection module which is coupled

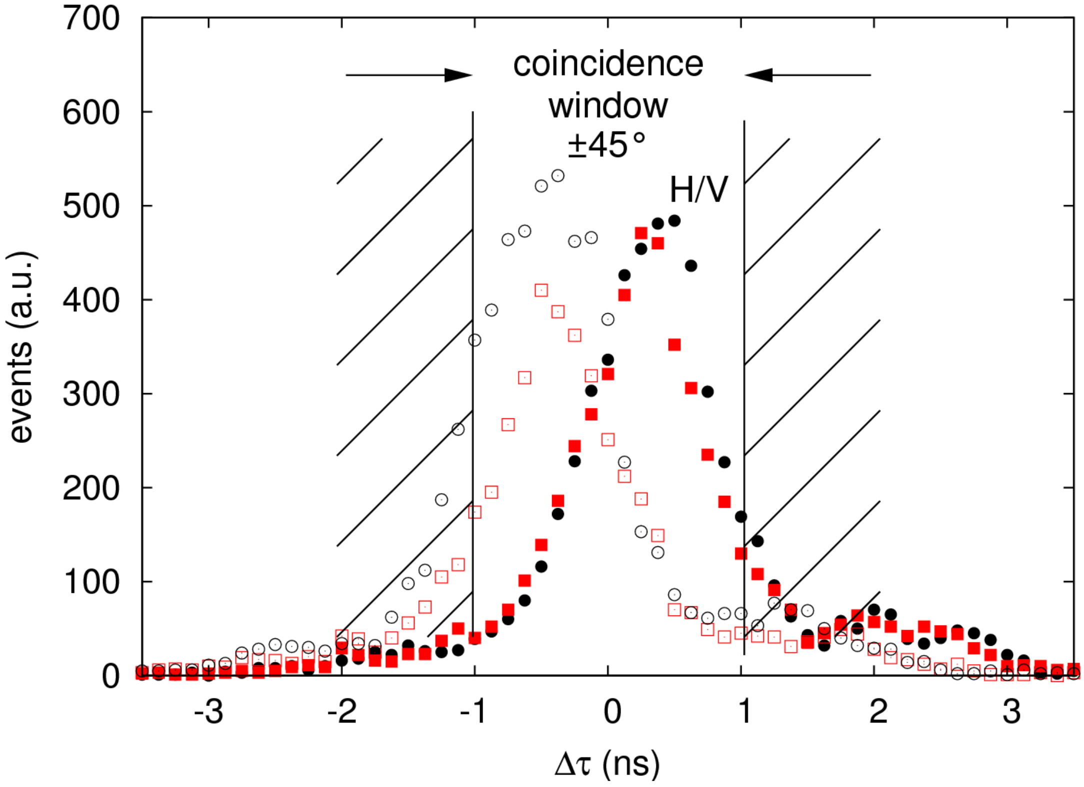


Figure 3.3: Histograms of time delays between the four main coincidence combinations contributing to the raw key. We can see that the two bases are overlapping very well, however, some signal loss occurs outside of this time window. By adjusting the two publicly announced bases to overlap in time some more correlation counts would be generated.

directly to the entanglement source. Each of these events corresponds to a time tag along with the result for the basis and the polarization. We found at first that sending Bob's counts over the classical channel quickly saturated the channel bandwidth of the TCP/IP communication link. Thus, it was most efficient to send information from Alice's side of the channel Bob's side of the channel (to the remote side) for the processing stages of the key generation protocol.

3.2.2 Spectral Filter

The source of entanglement was thermally stabilized in a lab using long single mode fibers to connect to our sending telescope. It was aligned through the particular interference filter we used by observing maximal correlation counts, and minimal correlation counts in the lower ±45° basis fringes as in section 2.4, which serves to maximize the visibility as long as the coincidence counts are maintained. The output was coupled into a spectrometer and a signal is measured both with and without the filter present and is illustrated in figure 3.4. A broadband scan is performed over the spectrum corresponding to the SPAPD's sensitive regime, and is averaged to estimate the blockage of ambient light. We find that the interference filter (IF) performs on average across the whole spectrum with and Optical Density (OD) of 2. Under the limiting assumption that the detector sensitivity and spectrum of the background are flat, this figure will underestimate the effectiveness of the spectral filter.

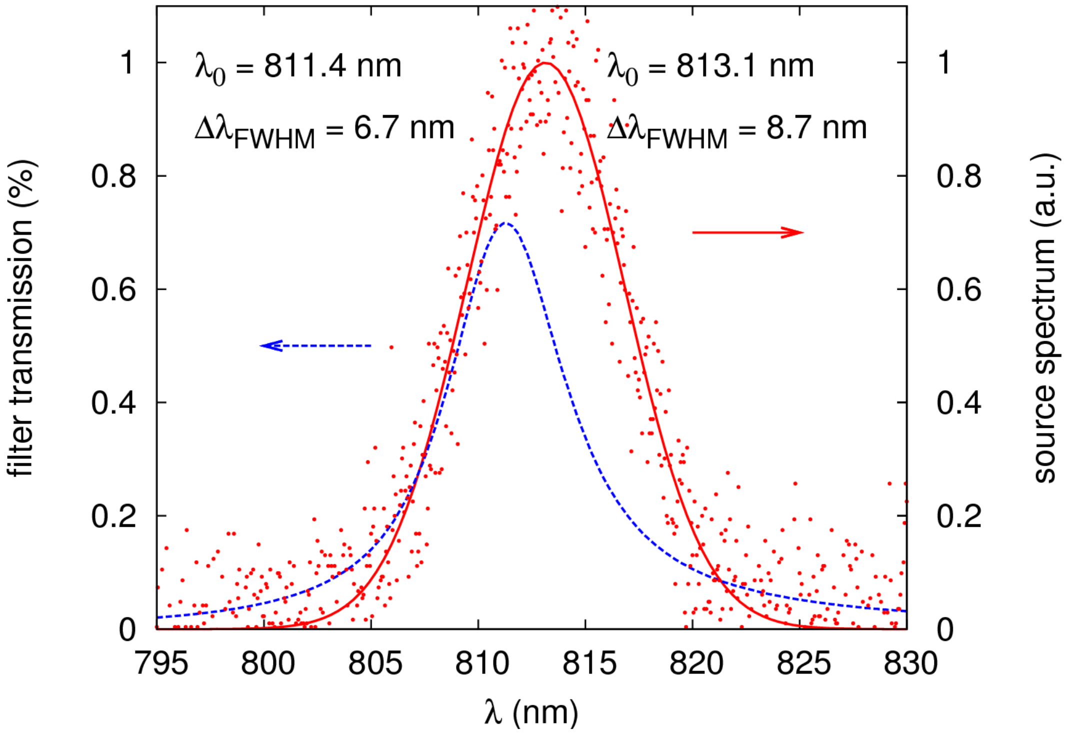


Figure 3.4: Spectral distribution of photons from the SPDC source, and transmission profile of the interference filter used to suppress background light outside that range. With this filter/source combination, a signal loss of 57% is introduced. In comparison, the PPKTP photon pair source has a bandwidth of ≈1 nm, which will couple with much higher transmission through the interference filter.

3.2.3 Spatial Filter

Spatial filters made a significant reduction of the background light. The spatial filters are described here and the spatial coupling of background light is discussed.

A significant reduction of background events was achieved by reducing the acceptance angle of the detector, reducing the light scattered from elements of the optical ports close to the optical channel and reducing the amount of noise coupled from outside of the acceptance angle. The main portion of daylight noise coming from the direct line of sight of the receiver is contributed by scattering in its field-of-view (FOV) as shown in the measurements of figure 3.6. This area can be reduced by choosing a smaller pinhole aperture as a spatial filter. We found a 30 μm pinhole to be the optimal choice when accounting for pointing accuracy and maintaining signal transmission for this distance, as in table 3.1. This gives a calculated FOV of 73 mm diameter which will strongly contribute to daylight noise counts.

Pinhole (μm)	Transmission	FOV (m^2)	SNR factor
20	32%	0.0076	42.1
30	72%	0.0095	**75.78**
50	82%	0.014	58.57
100	83%	0.0288	28.47
no pinhole	83%	≈ 4	≈ 0.2

Table 3.1: Transmission for various pinholes measured through both sending and receiving optics in the laboratory, and their relative merit considering signal transmission and background coupling in the FOV. Interference filter losses are not included in this measurement. A pinhole of 30μm is the optimal choice for the experiment.

Using black-out material, a dark area is constructed to extend over the FOV on the sending side, see figure 3.5. The internal parts of the sending telescope including the silver fiber couplers are also coated in black out material to reduce reflections anywhere inside

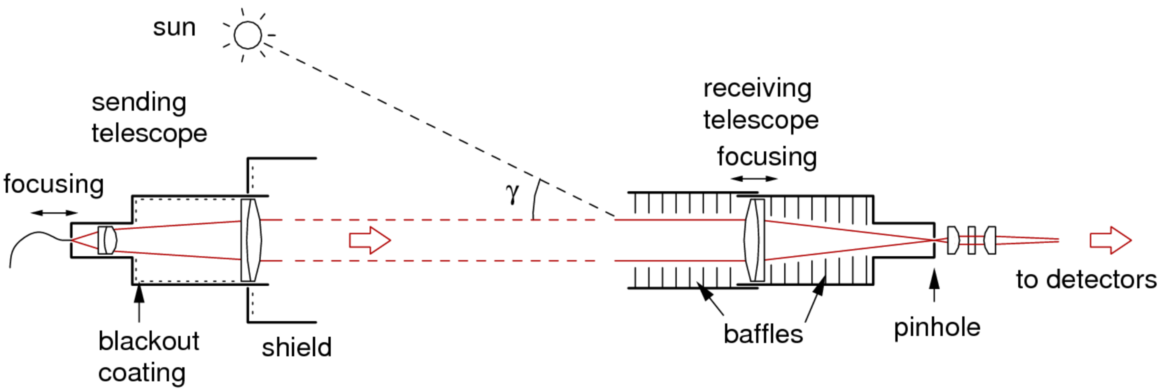


Figure 3.5: Schematic of telescope orientation with respect to the sun showing positioning of spatial baffles. γ reaches a minimum angle of 16° near dawn.

the channel. Shielding against direct sunlight on this area reduces the noise scattered from the lens of the sending telescope into the receiver telescope. Together these steps reduce the background counts by 12 dB.

A set of apertures placed periodically along the receiver telescope as light baffles removes scattered light coupled to the detector through the pinhole outside of the line-of-sight of the telescope. These angular spatial modes come from multiple reflections inside the receiver assembly. Seven concentric apertures internal to the receiver telescope, as well as five apertures extending 30 cm externally to the receiver telescope constructed to match the collimated beam, removed another $3-4$ dB of background light.

The FOV can be estimated using a ray tracing calculation. Assuming the outer perimeter of the FOV corresponds to a marginal ray tracing through the aperture of the lens and the pinhole, we perform analytical calculation of the diameter and area. Realistically, this area will estimate the maximal coupling as seen in the measurements presented in figure 3.6, while coupling will fall off exponentially outside of the area due to the wave nature of light, and atmospheric beam spreading.

Let D_l be the whole lens aperture, L be the distance of the optical channel, f the focal distance of the lens, D_p the diameter of the pinhole, and ξ the angular power of the lens as in figure 3.7. Then defining new terms $a = \frac{D_l}{2}^2 + f^2$ and $b = \left(\frac{D_l}{2} - \frac{D_p}{2}\right)^2 + f^2$ where

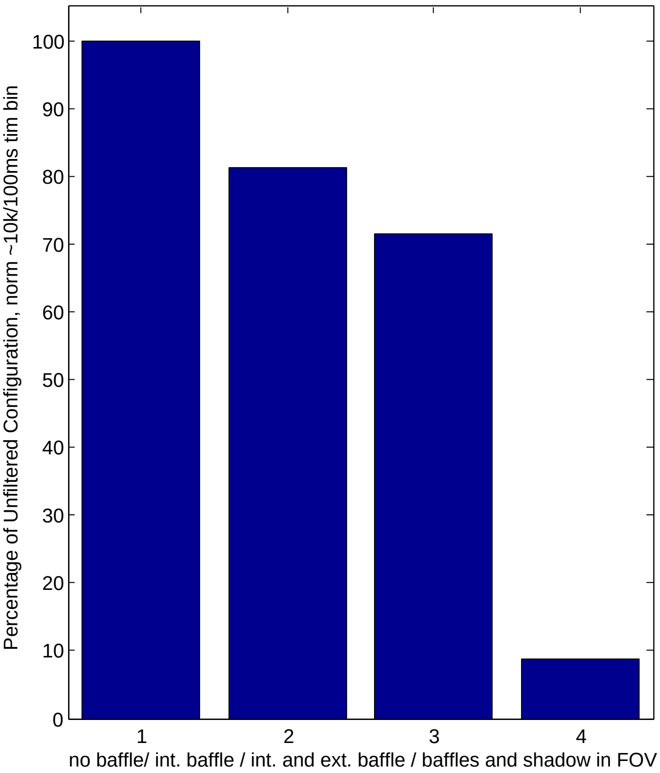


Figure 3.6: Relative reduction of background events using three different baffle configurations: 1 - no baffle, 2 - internal baffles, 3 - both internal and external baffles, and 4 - the largest reduction when light is absorbed directly in the FOV of the optical channel while both baffles are in place.

the lens diameter and focal length are fixed for our receiving telescope we have

$$\xi\left(D_p\right) = \arccos\left(\frac{\left(a + b - \frac{D_p^2}{4}\right)}{2\sqrt{a}\sqrt{b}}\right) \tag{3.1}$$

from which we obtain the equation for the FOV by solving for ξ as

$$D_{fov}\left(L, D_p\right) = D_l + 2L\tan\left(\xi\left(D_p\right)\right). \tag{3.2}$$

Overestimating the distance as 1200 m to construct a sending telescope which may be used for the longer distance tests, we find values for area and diameter (see figure 3.8) for a selection of standard pinholes sizes. These estimates were verified to be good in our test range. Over the distance of 350 m a diameter of approximately 9 cm for the FOV is

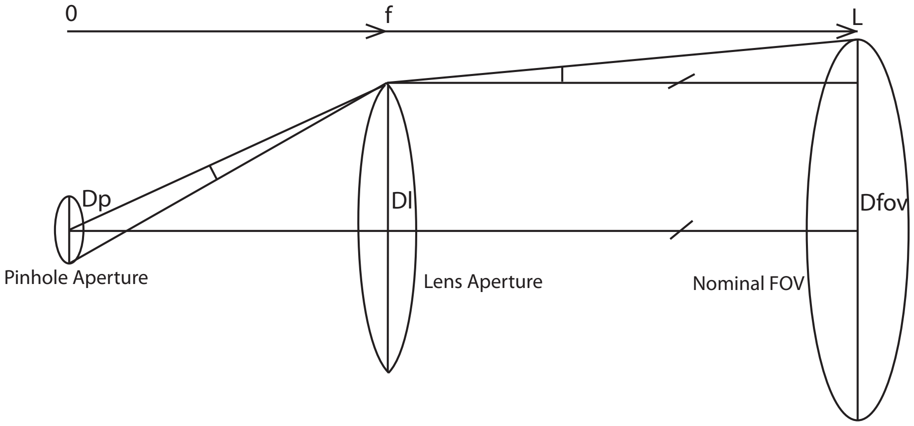


Figure 3.7: Geometry of ray tracing analysis for estimation of the field of views diameter D_{fov}. A marginal ray runs parallel to the optical axis originating at the center of the pinhole. The marginal ray from the edge of the pinhole is projected over the target distance L. f is the focal length of the lens, while D_p and D_l are diameters of the pinhole and the lens respectively.

observed by using a white sheet to introduce photon counts, fitting well to the calculated value of 7.37 cm. While the receiver telescope is coupled on center to the sending telescope, the distance from the center of the channel to the sharp edge of the sheet is recorded while a spike in singles counts is monitored remotely. This is only a rough estimate and includes errors associated with mechanical stability.

The pinhole transmission for various sizes was investigated and is listed in table 3.1. This is measured by simply comparing optical powers from a collimated beam coupled through the receiving telescope with no pinhole, to the optical power measured with a pinhole aligned at the focus, to estimate the signal coupling parameter. The amount of background coupling for a particular pinhole is estimated by using the diameter of the FOV from equation 3.2.3. This is justified because the FOV is where 90% of the daylight background originates, as observed in figure 3.6. From these parameters, a figure of merit to estimate a Signal to Noise Ratio for a particular pinhole diameter is calculated and presented in table 3.1. We can see a 30 μm pinhole is the best choice under these

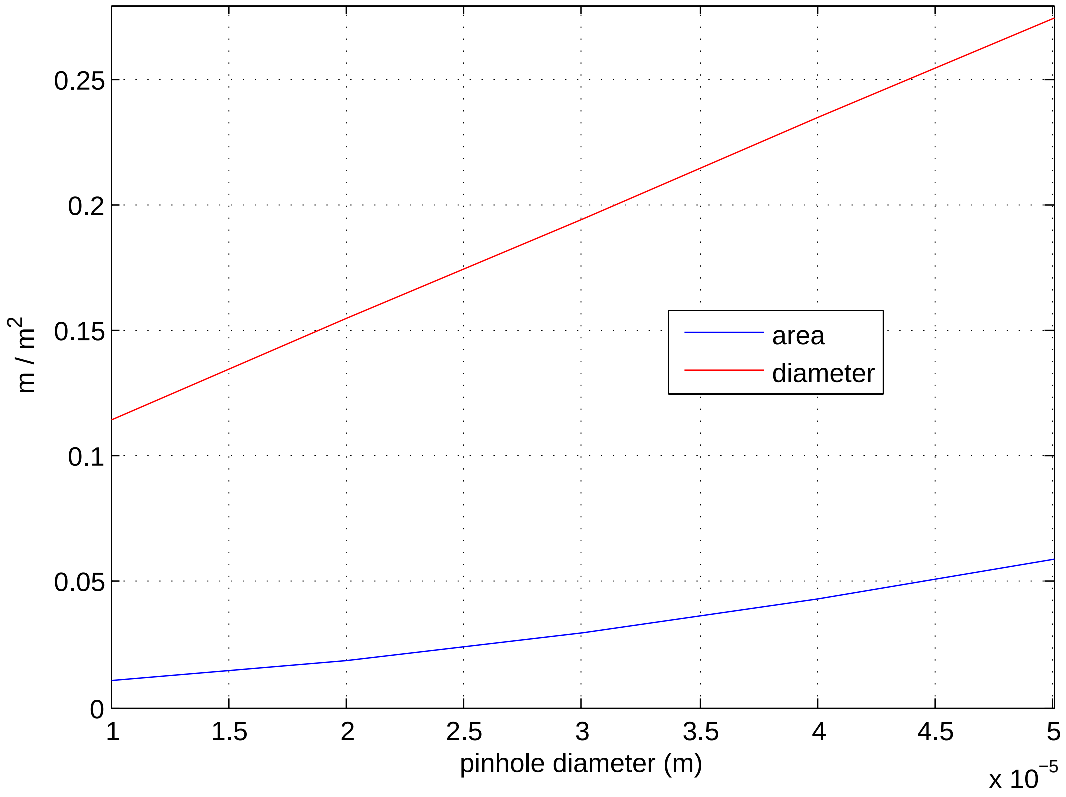


Figure 3.8: The area and diameter plotted for various pinhole sizes, based on a distance of 1.2 km. A 30 μm pinhole was chosen for our experiment having a distance of 350 m, as the optimal decrease in background counts, while maintaining the robustness of the alignment.

considerations[2].

3.3 Alignment Procedure

The alignment procedure used to prepare the source of polarization entangled photon pairs, and achieve maximal transmission through the free space channel is described herein.

[2] We did test the 20 μm pinhole in the field but found alignment accuracy poor, and signal loss too large, for stable key generation.

3.3.1 Source

The source of entangled photon pairs was initially exposed to outdoor environmental conditions through an open office window at the sending side. Large fluctuations in the total coincidences over periods of a few hours were observed. To compensate for the degradation of the source parameters, a long single mode fiber optic cable was run to the sending telescope from the photon pair source in a laboratory with a stable temperature. We then found upon the initial source alignment that parameters did not degrade throughout the experiment.

The pump is focused down in the crystal, and by back propagating signals, the fiber coupler aperture is matched to the size of the pump [63]. Single count rates are maximized in the operating bandwidth using the interference filter from our receiving telescope, until correlation counts are observed. These correlation counts are maximized toward an expected ratio of ≈1:5-6 to single counts, representing the source efficiency parameter.

The visibility in the ±45° basis, where $V_{\pm 45^\circ} = (R_{max} + R_{min}) \, / \, (R_{max} - R_{min})$ as described in equation 2.10 for average minimum and maximum rates observed is then measured and optimized by rotating two polarizers in the signal and idler path. The down conversion crystal is tilted to minimize those counts further, effectively maximizing the fringe size, or maximizing the collection of a singlet bell pair. It was observed previously that tilting the conversion crystal within the range of the fringe minimum has little effect on the total number of coincidence counts, thus using the crystal tilt in this way does not lead to other misalignments. Then, using a compensation crystal in both beam paths we finally minimize coincidence counts further in the ±45° and achieve visibilities of $V_{\pm 45^\circ} \approx 92 - 93\%$ which are observed over a series of alignment stages during the experiment. Thus, these parameters for the quality of entanglement are assumed to be indicative of the source throughout the entire experiment.

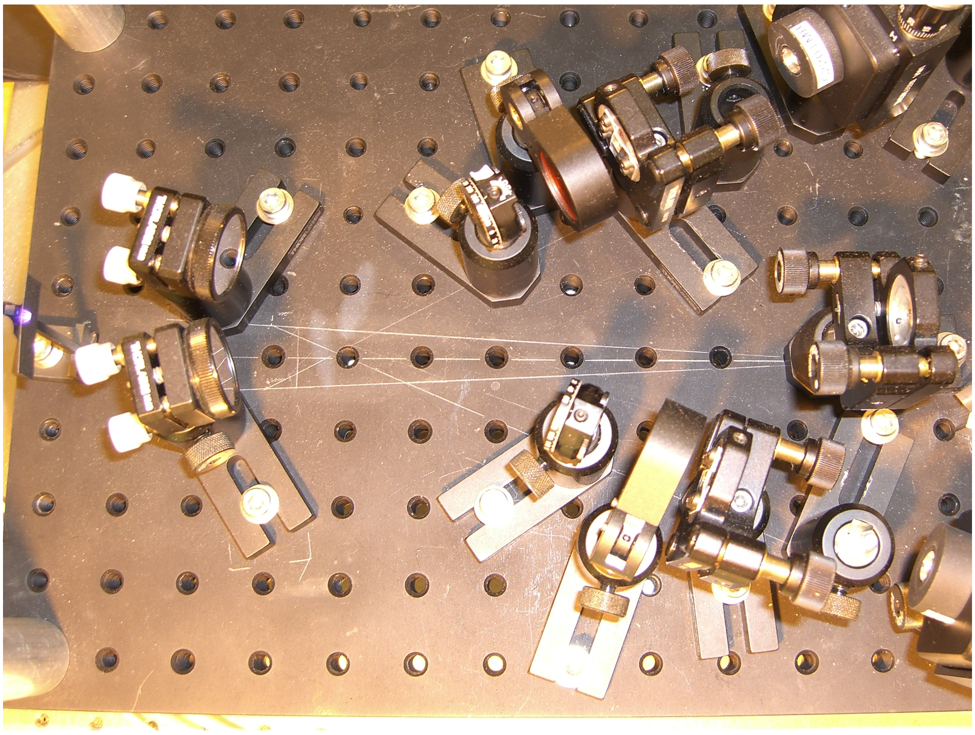


Figure 3.9: Polarization Entanglement Source based on a BBO crystal. Non-collinear signal and idler beams are collected into single mode fibers. Compensation crystals are used to remove timing distinguishability of the photon pairs.

3.3.2 Free Space Coupling

Alignment of the two telescopes in the optical link requires a few stages before the source signal is coupled. The key is that the small pinhole on the order of ten μm's which is required for removing quite a lot of background must be coupled across the channel. Although in some experiments performed at night a pinhole is not used for ease of alignment [29], a pinhole is required to act as a spatial filter of daylight background.

Two bright laser diodes, one at 650 nm, and one at 810 nm, spectrally near the photon pair source wavelength, are used for coarse and fine alignment. They are coupled to the sending telescope for alignment using an aspherical lens focused into a single mode fiber and plugged into the telescope. The diodes are used to observe the collimated beam size, the location of the focal point in the receiving telescope, and coupling rates on the receiving telescope detector unit while adjustments are made. Collimation must be maintained such that the beam is not clipped at the receiver. In fact, the initial alignment had roughly 50% unexpected losses from a misalignment of the collimator. Using a raytrace, the position of the two collimator lenses was corrected by projecting a set of marginal rays to distances of 500 m and 1500 m. The beam waist was optimized by forcing the equality of the beam diameter in a merit function to find the best positioning of the lenses of the sending telescope (ST) as in figure 3.2. The final collimated beam can be finely adjusted by translating the single mode fiber tip along the optical axis at the input of the collimator.

For rough alignment of the telescopes the red diode is used. The beam is guided to the receiving lens and the focal point of the red light may be observed by eye by looking into the receiving telescope unit through the 3 inch lens. Both sending and receiving units axes are set parallel to the axis of the free space channel[3]. In most cases some light is seen coupled through the pinhole after this procedure is complete, and the tilt and pan of each telescope unit is adjusted to maximize photo-counts. If no counts were observed, the position of the pinhole with respect to the lens was realigned. The collimation of the beam is adjusted roughly over the channel since it was only aligned over a short distance in the laboratory.

The 810 nm laser diode is then switched into the sending telescope port, and observed across the channel on a ruled sheet using an infrared viewer. It is set to the appropriate beam width. With the 810 nm diode now coupled, photo-counts are re-optimized to correct any misalignment from the re-collimation or chromatic effect of the lens. A series of adjustments of the pinhole position and the tip tilt stages is then performed to maximize photo-count rates. This is performed while periodically unplugging alignment diodes and plugging in the photon pair source. If the source is found with a sufficient count rate, it is used for fine alignment of the pinhole. It was found that during the day, should the link become decoupled, it is possible to turn up the power on the (preferably IR) laser diodes used for alignment and observe their photo detection above the background rate through

[3] This process could be automated with a compass, a small CCD array and a control system

the channel. In this condition it is found that the telescopes could be aligned through the free space channel in daylight conditions by maximizing the diode coupled photo-counts as far as possible using the micrometer pins of the telescopes. By iterating this procedure while lowering the intensity of the diode, optimal coupling was established during day and the source could be plugged back into the channel to resume key generation.

For this test, the long duration of the experiment requires that the system is periodically maintained, as we observed a gradual reduction of signal coupling through the channel over periods of a few hours and at particular points of the day. Should the signal for key generation be lost for a long period, the system must be halted and resynchronized, which is possible only up to a limiting ratio of coincidence counts to background counts[4]. This procedure is explained in more detail in the paper by Caleb Ho of reference [64]. It was observed that the signal rate dropped most often during sunrise or during periods of temperature change during sunset, and in rainy conditions. Thermal expansion was the likely cause of this observation, as the absorption of heat by the telescope mechanics while the sun was striking it would induce some expansion. Luckily this expansion was small enough to keep the pinhole and lens at the proper distance from each other and the sending telescope was not affected as it was protected from strong sunlight. By adjusting the tilt it was possible to compensate slowly for this drift and maintain coincidences at the expected rates[5].

[4] See synchronization in the results section below.

[5] Horizontal adjustment was not often required, maybe because less effect due to symmetric forces in this dimension weakened the effect of decoupling with thermal expansion. The vertical tilt of the sending and receiving telescopes was used.

Chapter 4

Experimental Results

We present the final data of the QKD experiment which ran during both night and day, and compare the data to the expected outcomes as estimated from the theory section above.

A cryptographic key generation protocol based on BBM92 is demonstrated using entangled photon pairs in a free-space channel during daylight hours. The first test similar in motivation is by Seward [60] where no key was generated. Preliminary results of this test were presented in the conference proceedings for CLEO [57]. This is the first report of a daylight operating QKD system using entangled photons over a continual cycle period of 24 hours, in both day and night conditions. We generated key over four days at both day and night, creating roughly 3.75 MB of key per day, or roughly 350 (bits/s), over a distance of 350 m. During this three day period, very sunny conditions and a few serious rain storms were endured. We found reduction of transmission in the channel during rain and higher error rates during sun. But throughout this period we maintain an error rate allowing us to create secure key, as the system recovered during any events where source was completely attenuated [3].

The first tests of the filtered count rates in the receiver during day showed that the daylight photon counts did not saturate the detectors. See figure 4.1. This showed the daylight operation was in principle possible and that background rates r_{bg} did not saturate the detectors. QKD test runs during the morning began to be successful once the correct

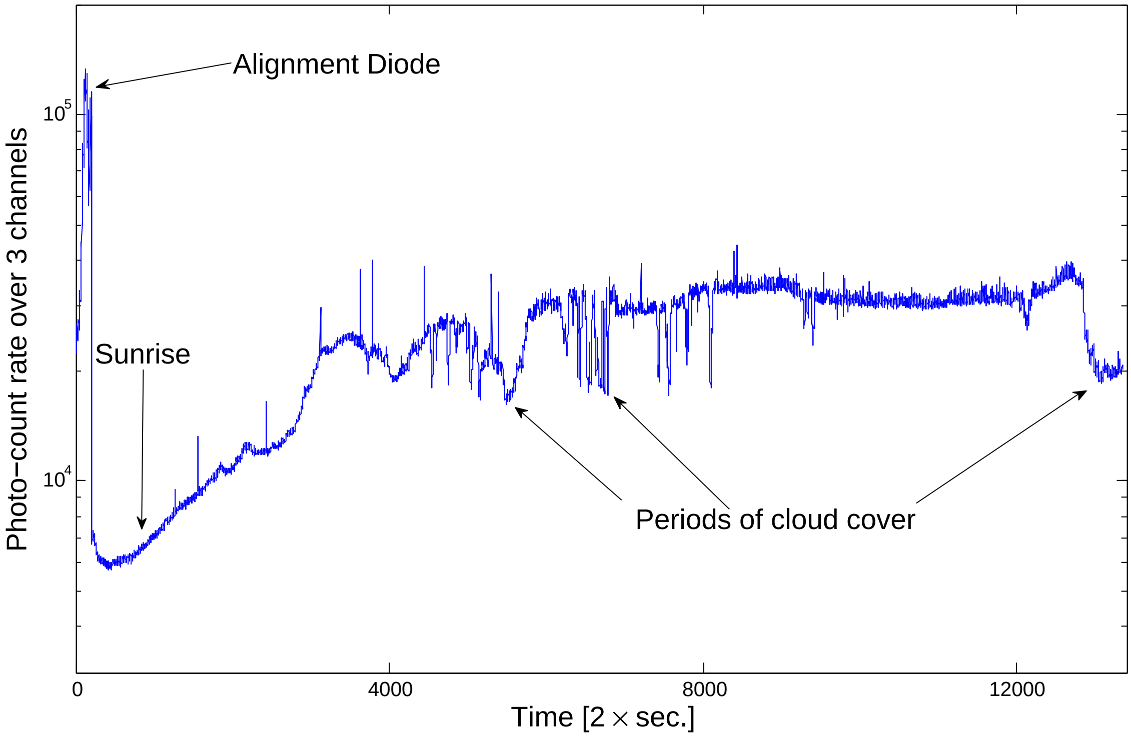


Figure 4.1: Preliminary tests during daylight hours from 7am to 3pm 15/5/2008. The photo-count rate is sampled every two seconds. Fluctuations in the count rates mid-day arise from intermittent cloud cover. We find there is no saturation of the photo detector units and rates between 20 000 and 100 000 counts/sec. Background counts from the experiment are larger because this test result was over a different channel orientation and a shorter distance. Note, the bright alignment diode was switched off before sunrise as seen on the left of the graph.

symmetry of the classical communication was used. The high bandwidth of information at the detector receiving large background rates initially saturated the classical channel. Thus, data was send from the side of the channel connected to the detectors in the laboratory, not exposed to high background counts.

Baffles external to the receiving telescope were re-constructed after the initial QKD test runs for a reduced aperture size which was 40 mm in diameter instead of 80 mm in diameter to exactly match the diameter of the collimated beam from the sending telescope. At this point, data was generated and monitored remotely for the entire test period.

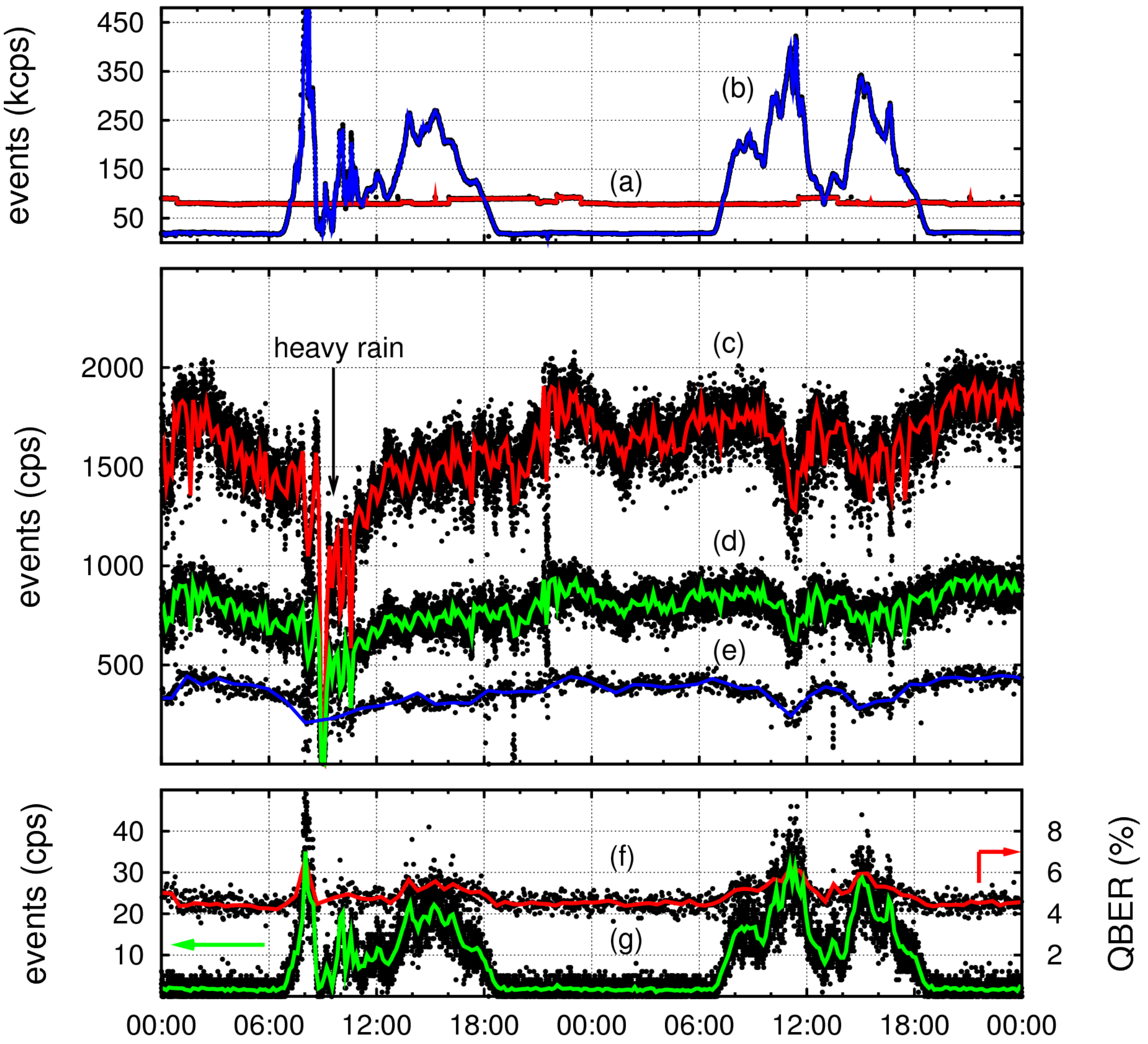


Figure 4.2: Experimental results for 10th and 11th November, 2008. All experimental points are sampled down, and the solid lines represent a moving average as a guide to the eye. Top panel: (a) in red, photon detection events on Alice's detector; (b) in blue, photon detection events on Bob's detector. Middle panel: (c) in red, the rate of raw key events; (d) in green, the sifted key; (e) in blue, the final key rate after privacy amplification and error correction stages. Bottom panel: (f) in red, the QBER as a percentage; (g) in green, the estimated rate of accidental counts.

4.1 48 Hours of Key Exchange

Referring to figure 4.2, the top panel records the firing rate of the single photon detectors at Alice and at Bob. The stable trace labeled (a) in red corresponds to Alice's detector connected directly to one arm of the entanglement source, which is isolated from changes in ambient light. The other trace (b) in blue on the remote side, or Bob's side, is the detector coupled to the entanglement source arm through the free space channel. We can see the background rate as single photon counts in Bob's detector rise during day above 150 kcps and fall to less than 10 kcps at night. The middle panel traces show (c) the number of raw pair events collected in red, (d) the sifted events in green whereupon roughly half the raw key is removed as the measurement bases did not coincide, and (e) in blue, which are the final key bits after error correction and privacy amplification, to be used for the creation of the cipher. The lower panel shows the number of *accidental* pair events detected (g) in green, which is estimated by using correlated detection events that fall outside of the timing window. The QBER level as a percentage (f) in the red trace of the bottom pane is shown, and can be seen to rise with accidental rates, but never crosses the secure threshold at QBER $\approx 11\%$.

The experiment was run continuously over a period from 9.11.2008, 18:00 SGT to 14.11.2008, 2:00 SGT over four consecutive days. In this period we saw extremely bright sunlight, tropical thunderstorms and partly cloudy weather; over the whole period the

Events	H	+45°	V	−45°
H	599	22 791	34 032	18 409
+45°	18 647	2 894	17 512	44 841
V	29 062	16 422	2 125	25 246
−45°	14 635	40 558	22 280	1 498

Table 4.1: Correlation events between each of the four detectors on both sides. Though anti-correlation is clear, there is some higher than expected correlations due to contributions from sunlight.

figure 4.2 we show the results collected over two consecutive days. On the second day we identified $14.72 \cdot 10^7$ raw coincidences. After sifting, this resulted in $7.18 \cdot 10^7$ of raw uncorrected bits, with a total of $3.5 \cdot 10^6$ errors corrected using a modified CASCADE protocol [61], which was carried out over blocks of at least 5 000 bits to a target bit error ratio of 10^{-9}.

We do observe that during severe rainstorms which brought $\eta_t \approx 1 - 2\%$ the QBER began to rise approching $\approx 9 - 10\%$. Luckily, during these storms the background was also lower than during intense sunlight, due to the overhead cloud coverage. Yet, these weather conditions are not necessarily the norm and it must be considered that some periods of key generation will be insecure.

For the privacy amplification step, we arrive at a knowledge of an eavesdropper on the error-corrected raw key determined by (a) the actual information revealed in the error correction process, and (b) the asymptotic (i.e. assuming infinite key length) expression for the eavesdropping knowledge inferred from the actually observed QBER q_T, $I_E = -q_t \log_2 q_t - (1 - q_t) \log_2(1 - q_t)$ of an equivalent true single photon BB84 protocol as in equation 2.9. Privacy amplification itself is carried out by binary multiplication/addition of blocks of raw key vectors with a length of at least 5 000 bits with a rectangular matrix filled with a pseudo random balanced bit stream from a 32 bit linear-feedback shift register, seeded with a number from a high-entropy source for each block. We are left with $3.33 \cdot 10^7$ of secure bits for this 24 hour period, corresponding to an average key generation rate of 385 bits per second (bps). In these conditions, the raw key generation rates are far from uniform during the acquisition period; we see a maximum secure key generation rate of 533 bps in darkness and a minimum of 29 bps around noon in rainy conditions. A few blocks of the final key over the entire two day test period contain no secure bits, but this is very rare.

Referring to equation 4.4, the *detected* background rate r'_{bg} shows saturation, due to the intrinsic dead time of the four detectors. Less coincidence counts are detected for higher background count rates. The observed background rate increases up to ≈ 450 kcps, which leads also to a reduction of the sifted key rate, r_{sig}, by 20% and an increase of the

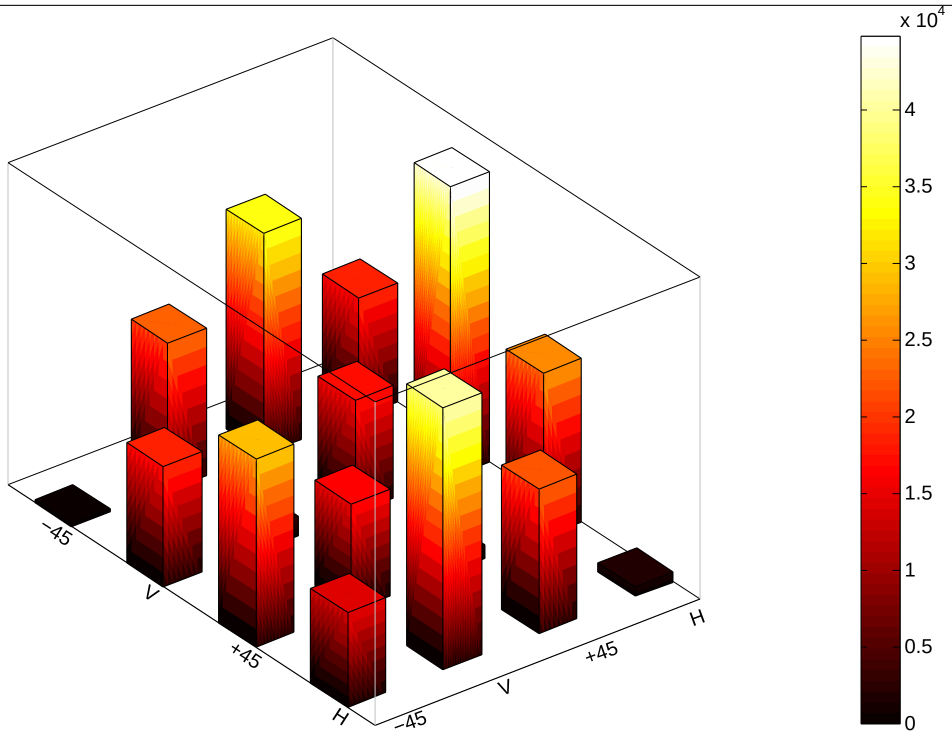


Figure 4.3: Correlation events between each of the four detectors as in table 4.1 for visual reference.

resulting QBER q_{t} up to 6.5%. The efficient filtering of the ambient light prevents a higher background, which would lead to an increase of the QBER above the threshold of 11% where no private key can be established between the two parties. This threshold is not reached during the whole experiment, thus continuous operation is possible when the transmission of photon pairs between the parties is maintained.

The raw key compression ratio in the privacy amplification step should actually also take care of a limited entropy in the raw key due to part-to-part variation in detector efficiencies. This information was obtained before the main key generation process by establishing the complete correlation matrix (see table 4.1) out of an ensemble of 148 493 coincidence events with matching bases.

The asymmetry between 0 and 1 results in the HV basis is $53.9 : 46.1 \pm 0.2\%$, and in the ±45° basis $52.5 : 47.5 \pm 0.2\%$. Using again entropy as a simple measure of information leakage, this detector asymmetry would allow an eavesdropper to obtain 0.45% of the raw key for events in the HV basis, and 0.18% in the ±45° basis. At the moment, however, it is not obvious that a simple reduction of the final key size in the privacy amplification step due to various information leakage channels would be sufficient to ensure that the eavesdropper has no access to any elements of the final key. We also note that the choice between the two measurement bases is not completely balanced; the ratio of HV vs. ±45° coincidences is $42.5 : 57.5 \pm 0.1\%$. Furthermore, this asymmetry varies over time. For the combined asymmetry between logical 0 and 1 bits in the raw key we find around 51.5% during night time, and 54.0% during daytime. A system which captures this variability in detection efficiencies (and also would allow to discover selective detector blinding attacks) would have to monitor this asymmetry continuously.

We can estimate how well the experiment performs for a given number of background events. Figure 4.4 shows theoretical values for background and signal rates according to equations 2.15 and 2.18, and experimental data for the coincident detection events and error ratios output from the error correction module during all two days of the experiment. The dead-time affected detector response is also shown assuming $\tau_d = 1\,\mu$s in equation 2.16 to visualize the saturation effect of the background light on the detector. This effect contributes to the reduction of coincidence counts and key generation rates with higher background levels.

The night time periods with $r_{\text{sig}} \approx 12\,$kcps and a total dark count rate of 7 kcps contribute to events on the low background regime of the experiment forming a vertical line to the left of figure 4.4. We cannot differentiate between fluctuations due to changes in the source and those in the transmission channel, but since the source itself was protected against thermal fluctuations, we attribute them to variations in transmission η_t due to changes in the coupling of the telescopes.

The strongly fluctuating background during daytime contributes to the broadly scattered data between $r_{\text{bg}} = 20$ and 500 kcps. If the source properties and channel coupling were constant, the deviation of q_t and r_{sig} from the theoretical value would be both randomly distributed. Figure 4.4, however, shows more structure in r_{sig} than in q_{t} which we attribute to changes in the coupling between the telescopes due to thermal expansion. Nevertheless, the experimental values fit the theoretical prediction well. We note that

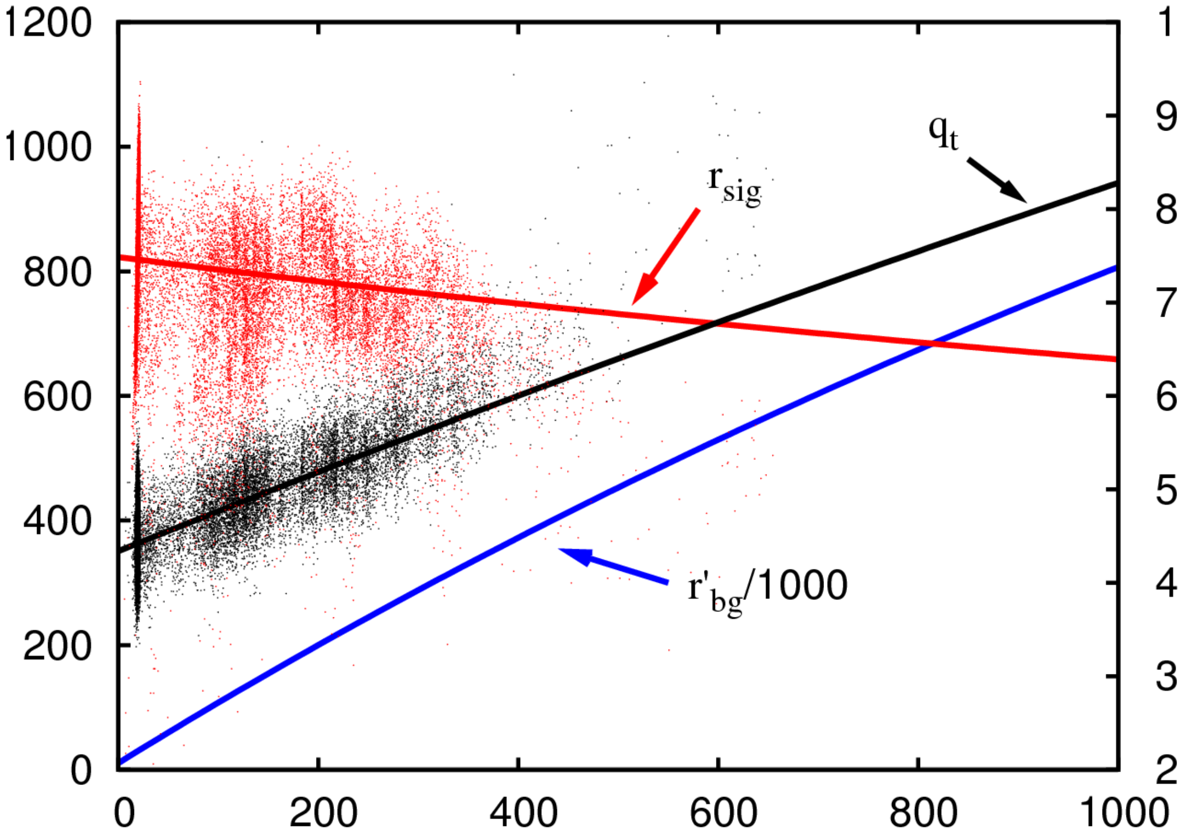


Figure 4.4: Detection behavior due to an external background rate r_{bg} for parameters representative for our experiment. The dense points at the left of the plot correspond to events obtained at night, whereas daylight events are spread out to the right, showing key generation rates and the QBER with respect to the background level. We can see that the drift of the coupling through the channel during the 48 hours of key exchange causes a large spread of key rates and QBER values. For reference, the scaling function for the detectors as in equation 2.6 is plotted to show the effect of dead time.

saturation of the detectors is never a problem.

There are two contributors to the variability in key generation rate: First, atmospheric conditions such as rainfall reduce the transmission and thus the number of raw key events before the error correction and privacy amplification steps, but the QBER remains unchanged. On the other hand we have extremely bright conditions where accidental coincidences increase significantly. In this regime, as the background rises, the signal rate is reduced due to the dead time of the detectors. Furthermore, the QBER increases according to equation (2.15), occasionally preventing the generation of a secure key. But even under bright conditions, the system still keeps track of the time drift between the two reference clocks with the time-correlated coincidences from the source without a need for re-synchronization.

4.2 Synchronization

This describes the test used to estimate the level of background light that a synchronization algorithm can operate in. The ratio of total photo-detection counts to the number of coincident counts when no background light is coupled is found to be 250 ± 10 *beyond which the synchronization algorithm will not work.*

The first few seconds of key generation requires that the detection events of each photon pair are matched in time. This is performed in a synchronization stage at the beginning of each test run, where we compare $10\,s$ of data from both sides, long enough to cope with added background counts. A correlation algorithm looks for the maximum overlap of the timing of events to record the offset between photons at the local side, to those traveling through the channel to the remote side. In fact, the algorithm alone is active research in clock synchronization [59]. This makes sure that the correct pairs are matched up in the key at both sides. The software continuously checks the overlap in case of any drift.

It is instructive to test a threshold where it will be successful in the presence of background counts. It was required during the real data acquisition that we restart the program during day, and synchronization was successful. However, we seek a more controlled method to explore the upper level for the algorithm to be robust against added background counts in the correlation algorithm. Laboratory tests are done using a simulated background by coupling a broadband flash lamp into the receiver to set background rates by geometric coupling, and tested at a level where synchronization is possible. The background is then raised for each successive test, until synchronization is unsuccessful.

Each time the background light level is set, the algorithm is run and the success of the synchronization is recorded as true of false. Three tests are performed, where the source is initially coupled while $r_{\text{bg}} = 0$ to coincidence rates of 3400 /s, 2100 /s, and 1000 /s. For each of these coincidence count levels, five tests are averaged for an estimate of the ratio of coincidences to background levels where synchronization becomes unsuccessful. The values for three selected tests are presented in tables 4.2.

We report in table 4.2 on the ratio of the total singles counts to coincidence counts which are reduced as the total level rises as in equation 2.16 and the ratio of total singles counts to the initial coincident count rate. The total singles S follows from the previously introduced terms, $S = r_{\text{bg}} + r_1 + r_{\text{dc1}}$ where r_1 is the singles photo-detection rate from the source, including coincidence events. The ratio of total singles to initial count near the failure is averaged over 15 sets of tests to be roughly 250 ± 10.

Notice, this value is for the case of an embedded detector at the local side, but in the case of two free space optical links [29] with background levels as in figure 2.4) the synchronization algorithm would need to cope with large coincidence rates due to background light. Failure would be at a much lower ratio.

Coincidences	Singles	Synchronization	$\frac{\text{Singles}}{\text{Coincidences}}$	$\frac{\text{Singles}}{\text{Initial Coincidences}}$
(3400)	32000	T		
2600	500000	T	192	147
2200	780000	T	355	229
2200	820000	T	373	241
2000	900000	T	450	265
-	920000	F	-	-
-	1120000	F	-	-
(2100)	24000	T		
1400	500000	T	357	238
-	540000	F	-	-
1400	540000	T	386	257
-	600000	F	-	-
(1000)	16000	T		
900	180000	T	200	180
900	200000	T	222	200
800	220000	T	275	220
-	250000	F	-	-

Table 4.2: Synchronization tests recorded near the point where synchronization failure occurs. Singles are the total counts on the detector including both background and signal counts. Here initially 3400 /s (top table), 2100 /s (middle table), and 1000 /s (bottom table) coincidences are coupled while $r_{\text{bg}} = 0$, and the computed ratio is referred to above as '$\frac{Singles}{InitialCoincidences}$'. Once the background light is turned on coincidence counts are measured again and the computed ratio is referred to as '$\frac{Singles}{Coincidences}$'. The coincidences are reduced when background levels rise by the saturation of the detector, as described in equation 2.6. Averages of these tests are taken to find the ratio of $\approx 250\pm10$ single counts to coincident counts as a maximal level for successful synchronization.

4.3 Applying Random Number Tests to the Key

Here we present data obtained from the random number tests performed on the raw data of the key. Each algorithm is given some discussion and a conclusion is outlined at the end. Some of the tests discussed in this section are plotted and included in the appendix.

In the ideal case, the cryptographic device will output an identical key to both parties which is a statistically independent and unbiased binary digit. As discussed previously, the beauty of QKD is that quantum correlations act to distribute the random key symmetrically, distributing a resource for a one-time-pad, while errors in the correlation denote the presence of an eavesdropper. But, regardless of the QBER measured, if the key generation is biased due to the physical device for example, an eavesdropper can induce no errors in the correlation but by knowledge of a systematic bias, obtain some knowledge of the key with a high probability. Therefore, security relies on the ability to generate unpredictable, or random, keys. Randomness tests must be used to ensure the proper function of the cryptographic system, including hardware and software.

QKD requires a mix of both algorithmic steps, and the randomness of a physical system. In our case, the randomness of the physical system is obtained through everything including the random quantum nature of state collapse, and measurement, as well as any bias within the entire atmospheric channel and optical components; from generation of single photons to their detection at the passively quenched SPAPD's. In particular, excess counts due to the high background during day may contribute to the key in a predictable way. The algorithm used for EC and PA are assumed to be optimal. Hence, failure of any of the following randomness tests will be attributed to physical origins, namely the optical hardware including the detectors, beam splitters, etc. In particular it is important for the four analyzers as depicted in figure 2.2 to be well aligned for balanced measurements to result.

Typically, random numbers can be obtained from a random number generator (RNG) such as a coin toss or, through some deterministic but random process which delivers a number satisfying most tests of randomness. They are deterministic, in the sense that given the same input, the algorithm will produce the same output. Such sources of randomness are known as *pseudo*-random number generators (PRNG), and are said to pass all polynomial time statistical tests if no polynomial time algorithm can distinguish between a sequence output from the generator and a random sequence, with a probability of greater than 1/2 [63]. An example is the FIPS 186 algorithm used for DSA or the ANSI X9.17 generator. The QKD device based on the collapse of the polarization state in a projection measurement is a random number generator, because it is not deterministic, relying only on a random physical process. It of course has the added benefit of inherently distributing the random numbers, while usually random physical processes are localized. As an example, typical RNG's devised from a physical system include:

- Johnson noise from a diode or resistor,
- a single photon incident on a half silvered mirror,
- user input through keystrokes or movement of a mouse.

In the following we present tests of randomness on the **raw** key generated over the 48 hour period presented in this experiment. The tests are applied to the raw key, not the final key, because the software can act to remove some of the biased behavior of a RNG. This requires that the raw key be compressed to a final key, the less randomness in the raw key, the more compression that is required to generate a random final key so these tests show us as well how much key is lost due to systematic behavior of the QKD system[1]. Results of the tests are summarized at the end of this chapter in table 4.3.

Randomness tests are classified as hypothesis or decision tests, and by their nature are probabilistic, not deterministic. The strength of the test is measured by the p-value output from the following algorithms and are plotted in blue. The p-value is computed by comparing the results of a particular statistical test to expected results and testing

[1] The algorithms for this compression step which was applied in our test, referred to as the privacy amplification (PA) step, are reported in [62, 64, 57, 65] although other more sophisticated algorithms have been developed [66, 67].

how far away the result is from expectations using a χ^2 or normal distribution, leading to a *two-sided* or *one-sided* hypothesis test, respectively. Above a threshold for 1% or $p > 0.01$, the test is considered true, below it, the test is false. This corresponds to a significance for the test of 1%, or that in 100 such tests only one random number will appear to be non-random to the test, giving a confidence or 99%.

The entire two day long key is broken into blocks of various sizes depending on the test. The first set of tests is performed directly on a single block of key as output from the software, including the frequency tests, the runs test, approximate entropy, and CUSUM test, all of which require only ≥ 100 bits of key per test to function appropriately. We then proceed to fill larger blocks for tests such as the binary matrix rank test, random excursion tests, or Maurer's Universal Compression test, requiring larger blocks and longer test times. Each block represents a sample of the RNG, and the test result is plotted in time at the beginning of it's generation during the key exchange. Since each bit should be unbiased and independent, the block size does not matter outside of the requirements of a particular algorithm used for testing. Table 4.3 summarizes the test requirements, as well as their results.

In particular, we also focus on a few short string template matching schemes since QKD systems frequently suffer from the generation of repetitive short strings, due to for example after-pulsing or conversely detector saturation, upon the detection of a bit. Such signatures are common in QKD systems, and need to be detected and corrected for. This may include balancing the efficiency of detectors, modifying the optical density of the different paths in the detector analyzer, or correcting for unbalanced polarization effects in the optical path.

The following results are performed using a package of algorithms available via NIST at [67, 68]. In the plots, the horizontal axis is time, and the plots shows the p-value which is the strength of the test, as well as the result of the test. The actual true/false success of the test is plotted as a 1 for true, and a 0 for false, where a false value means the input sequence does not satisfy the test statistic of a random number. Since the density of tests is usually large a moving average on 50 such tests of the decision outcome is plotted,

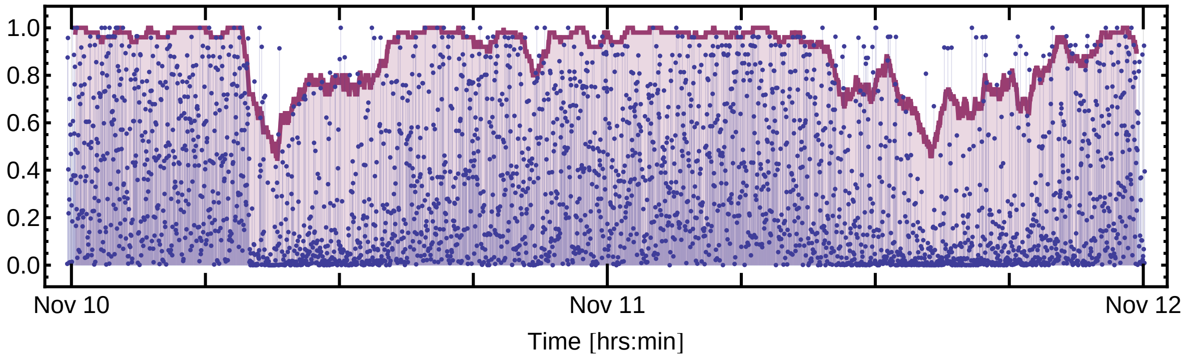


Figure 4.5: The Monobit Frequency Test: The p-value and moving average of the decision test.

except for lower density tests which required a large number of input bits. The p-value is blue point, while the results of the test are in red, where a moving average is applied in some cases, as specified.

4.3.1 Frequency Tests

Frequency tests probe the ratio of zeros or ones assuming the distribution should be equal. For example the binary string 111000 will pass a frequency test. This string is not representative of a random number generator though, and serves and example to illustrate the need for a variety of tests to achieve confidence in the randomness of the key. In the next section we will see a string which follows a random looking sequence or runs, may pass the runs test but still have a large asymmetry in its frequency. Therefore, some of the following tests, such as the runs test, require that the frequency test has already validated randomness to be valid. See figure 4.5.

These measurements show a 51.5% asymetry during night, and 54.0% asymetry during day. The majority of tests are successful, with some asymetry which rises during day. This is due to the background light incident on a slightly unbalanced set of detectors in the polarization analysers. Unbalance may be due to an amount of absorption in either spatial mode of the polarization analysers, for example the waveplate (see figure of detectors), which can be corrected using a piece of neutral glass or a weak ND filter in the corresponding arm. Different efficiencies of each detector after the analysers is another likely culprit. Dark counts on the detectors are unlikely to contribute a large amount bias in the key, but may be somewhat responsible when background rates coincide with the dark counts.

The block frequency test is a frequency test over a block M bits long. For these tests M=10.

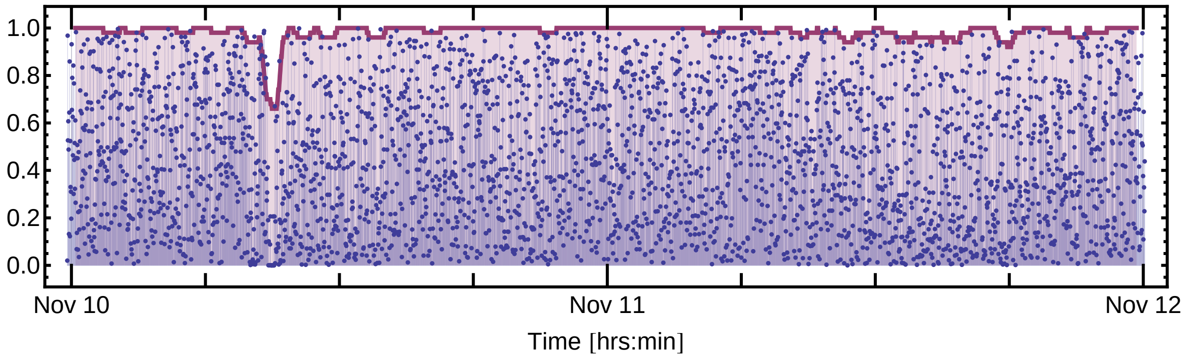


Figure 4.6: Block Frequency Test: The p-value (blue) and a moving average of the result (red).

4.3.2 Runs Tests

The *Wolf-Wolfowitz* runs test focuses on the number of uninterrupted sequences of identical bits, or runs, and compares this to the expectation of a random sequence. To be valid, this test requires that the frequency test is successful. The test in particular will determine if the oscillation from sequences of 1's to 0's is to fast or too slow. For example a string like 0101010101 oscillates very quickly, while the string 1111100000 is a slow oscillation. Neither of these strings will pass the runs test. As can be seen in figure 4.7, most of the key generated passes the runs test.

4.3.3 Binary Matrix Rank Test

The binary matrix rank test checks for independence of given length substrings of the entire sequence. The rank of the array is compared to the expectation of a random number to generate the statistic. We use 3×3 matrices for the test, although other sizes may be used, this size was recommended in the test suite. This test is performed on

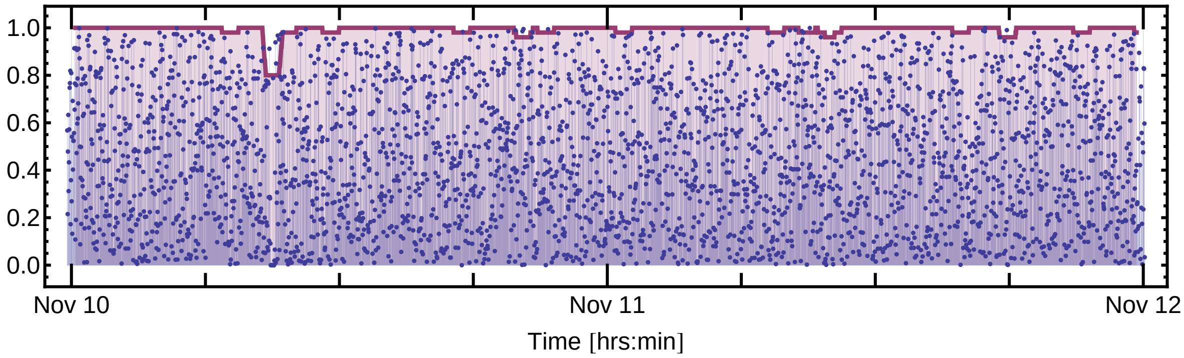


Figure 4.7: Runs Test: The p-value (blue) and a moving average of the decision test (red).

blocks each of equal length of 50000 bits. The key is being sampled every 100 seconds from which 50000 bits are drawn out for the test. There may be minimal overlap of the bits in the blocks at times where key generation is low. Referring to figure 4.8, it can be seen that the majority of tests using the binary matrix rank test are successful.

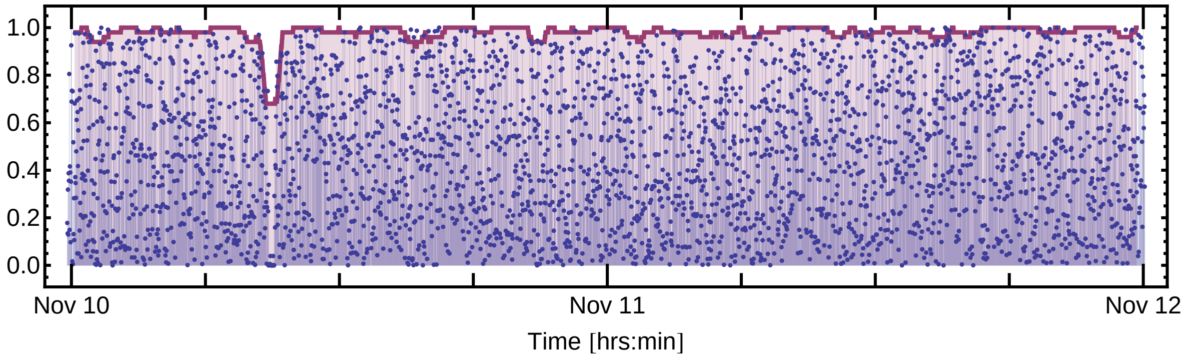


Figure 4.8: Binary Matrix Rank Test: The p-value (blue) and moving average of the decision test (red).

4.3.4 Approximate Entropy Test

This test compares the empirical number of adjacent overlapping blocks of bits to the statistic expected for a random sequence. Another way of looking at the test is to say it is concerned with the frequency of different patterns in the string. The test has often been used in comparing time series in biological functions, namely irregular repetitions of a normal functioning heart beat, but may be applied in randomness test generally. The principal assumption in generating the test statistic is that a pattern of fluctuations in a random process should not be followed by observations of similar patterns of fluctuations [69]. The test is called with the recommended string partition size of 3, and applied on each block of key of approximate size 200-400 bits, and figure 4.9 shows that most of the key is random by the approximate entropy statistic.

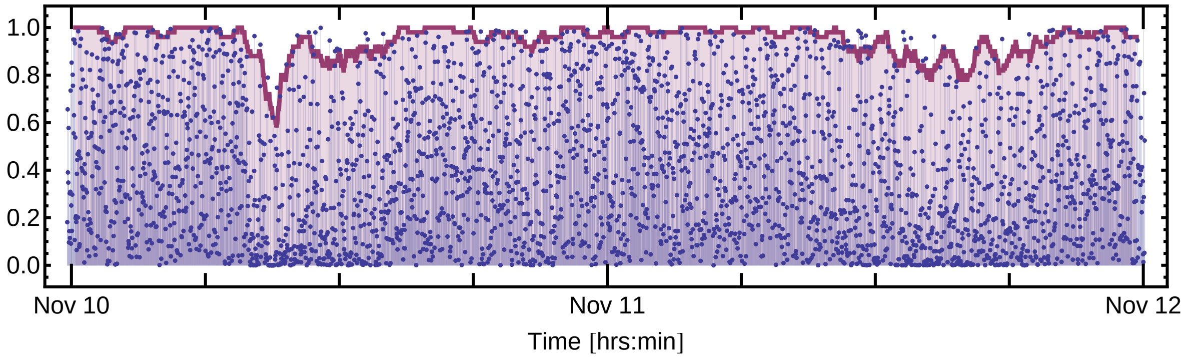


Figure 4.9: Approximate Entropy Test: The p-value and moving average of the decision test.

4.3.5 Compression Tests

Compression tests look to compress the random string by encoding patterns with simpler strings. For a true random number, it should not be possible to find any patterns withing the string which can be coded in a simpler way. Two such tests are the *Maurer's Universal Statistical Test* and the *Lempel-Ziv Complexity Test.* Results for the Maurer's Universal Statistical Test are presented below. Maurer's test is considered universal to a wide range of statistical tests, but depends on the heuristic approximation [70].

The Maurer's Universal Statistical Test is performed for all of the block sizes, including 500, 50000 and 1000000 bits. Figure 4.10 uses the correct number of bits and the confidence of this test satisfies the setting for the p-value. For an example, a somewhat low level of bits is input to the Maurer's Test and is presented in figure 4.11. It is apparent that the key does not pass the Maurer's test with as large a p-value when comparing the smaller number of bits input to it, as can be seen in figures 4.10 and 4.11. This feature of the test is most prominent during the portion of key generated in rain. In any case, the majority of tests are successful for randomness.

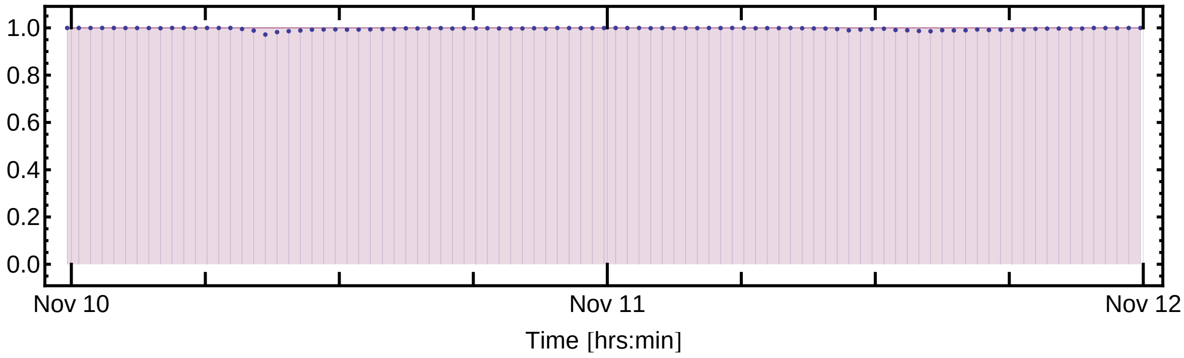


Figure 4.10: Maurer's Universal Compression Test: The p-value (blue) and moving average of the decision test (red) for 10^6 bit blocks.

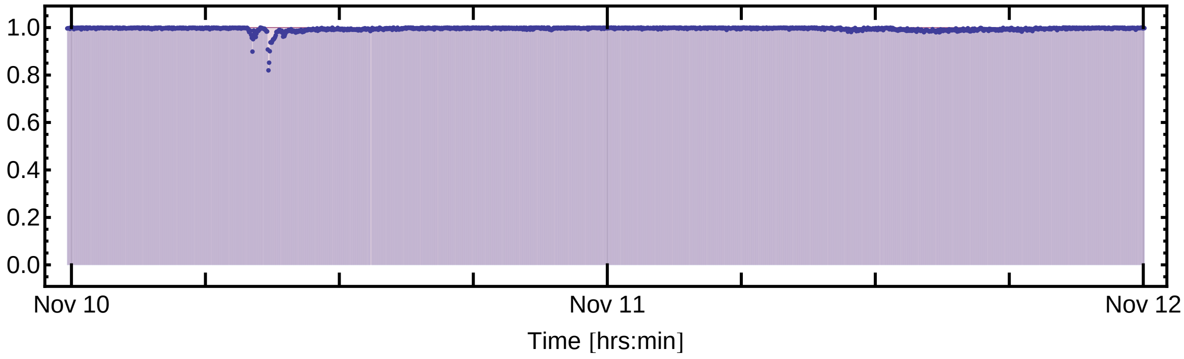


Figure 4.11: Maurer's Universal Compression Test: The p-value (blue) and moving average of the decision test (red) for 5×10^4 bit blocks.

4.3.6 Excursions Tests

The purpose of the excursions tests are to compare the resulting key to expectations of a random walk. A random walk is a studied process with known statistics. A good overview of the random walk including statistics and expectations of the random excursion can be found in Chapter 3 of the book by Feller [71]. Using a random key, a random walk can be easily simulated. In the Random Excursions tests, the sequence coming from the random number generator is turned into an equal length random walk by equating 0 and 1 with -1 and +1, and then doing a partial sum of the bits along the key while keeping tally of the result. This will result in a trajectory stepping up or down randomly in equal measures, in series with the index of the sequence. The random walk has known properties such as the maximal departure from zero, the number zero crossings which should occur for a given length, or the tendency of a walk to trend in one direction for some time, and mean revert. All of these properties can be used to find statistical tests of the sequence by assuming the walk is purely random and then observing the differences in behavior.

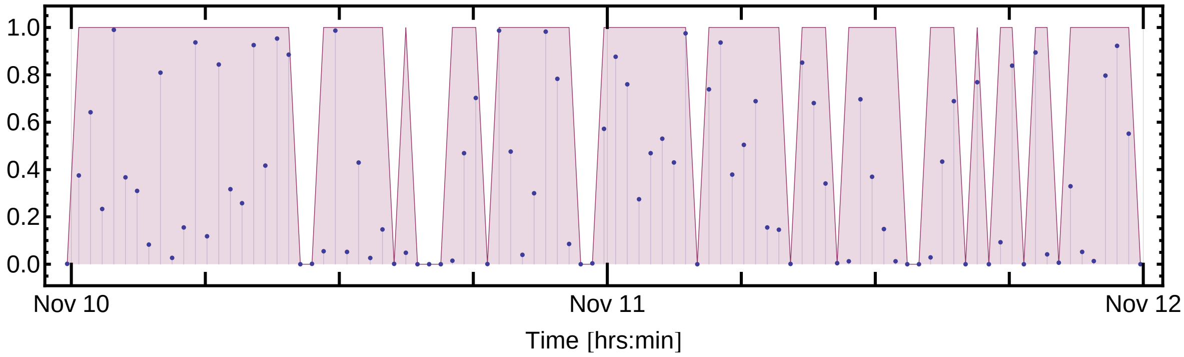


Figure 4.12: The random excursion test for the first state -4. The test is among the most poorly performing of the 8 tests, with 19 out of 93 tests giving false outcomes.

There are three tests below which are based on random walk excursions, the CUSUM test, the random excursions, and random excursions variant tests. Each of these tests focus on the total number of times the random walk visits a particular state. The excursion test performs a series of 8 sub-tests based on the number of times a particular state occurs in the random walk. The states are $\{-4, -3, -2, -1, +1, +2, +3, +4\}$. For example, given the input string 00101101, we would have sums of partial subsets moving along the sequence, giving a random walk starting from zero, with the result $\{-1, -2, -1, -2, -1, 0, -1, 0\}$. This visits states -1 four times, and -2 twice. The total number of times the states are visited is compared to the expectation of a random number, which would give a purely Gaussian random walk.

The random excursions test uses 10^6 bits, resulting is a series of test for our 48 hours of key that are mainly indicative of a random number generator. The p-value is based on the χ^2 distribution, or two sided test form. Not all the 8 states are plotted for brevity, although inspection shows each is similar. Four plots of the best and worst tests are plotted in figures 4.12, 4.13, 4.14 and 4.15 which are from excursions of the 1^{st}, 2^{nd}, 6^{th} and 7^{th} states.

The random excursions variant test is similar to the random excursions test, only using a larger number of states, here spanning from -9 to +9 and so outputting 18 different tests. As well, this test does not form a partition of the sequence to look at the number of times a state is visited in a cycle, but instead considers the number of times the state is visited in respect to the length of the entire sequence. The test also requires a minimum of 10^6 bits. Two such tests for states not checked in the original excursions test are plotted in figure 4.16 and 4.17.

The *Cumulative Sums Test* (CUMSUM) adjusts the binary digits to be -1 and 1, and compares the result of the sum of all digits, to the expected result of 0, for a random walk. In contrast to the random excursions test and random excursions variant test, it is the *maximum* cumulative sum for a given length of key is thus tested to fall within the expected statistic of a random walk in the CUSUM test. It is in the class of excursions tests, since it compares the statistic of the random walk generated from the key to average statistical expectation of a real random walk.

The CUSUM test can be considered similar to frequency tests. Should a key generate to large a number of ones (zeros) then the maximal excursion will be larger than expected for a true random number, befitting some non-random sequences. Moreover, it may detect a random number generators tendency to trend by giving many ones followed by many zeros, in a cyclical manner, which may not show up in a frequency test. As well, oscillations of the key may in some cases be detected as mean reverting processes (faster than average) by the test, where the expected maximum state of the random walk is not

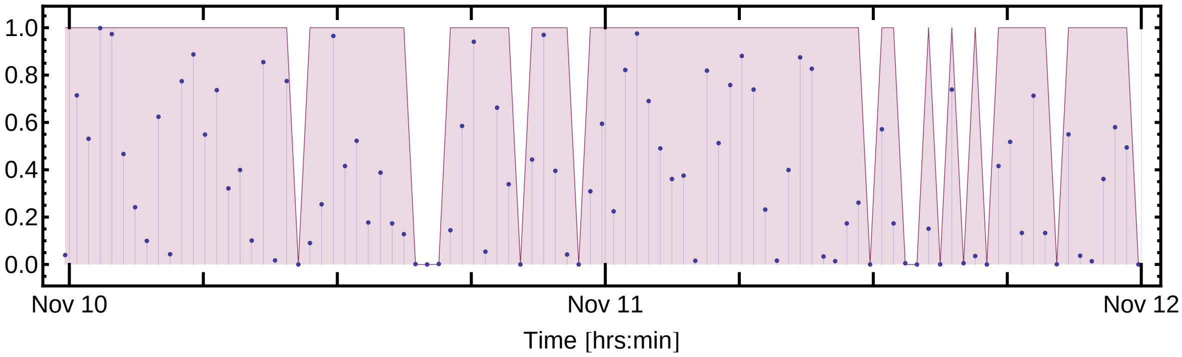


Figure 4.13: The random excursion test for the second state, −3, which is true but shows 14 of 93, or 15% tests failed.

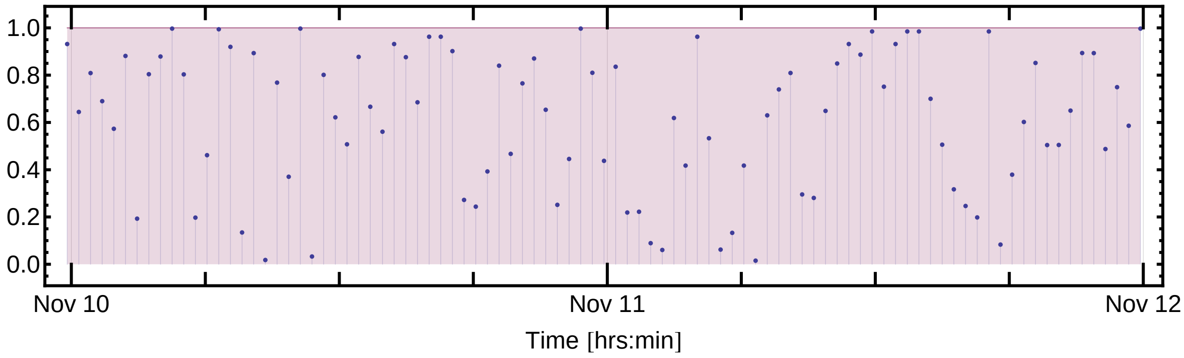


Figure 4.14: The random excursion test for the state +2, which is mainly true but shows some false tests.

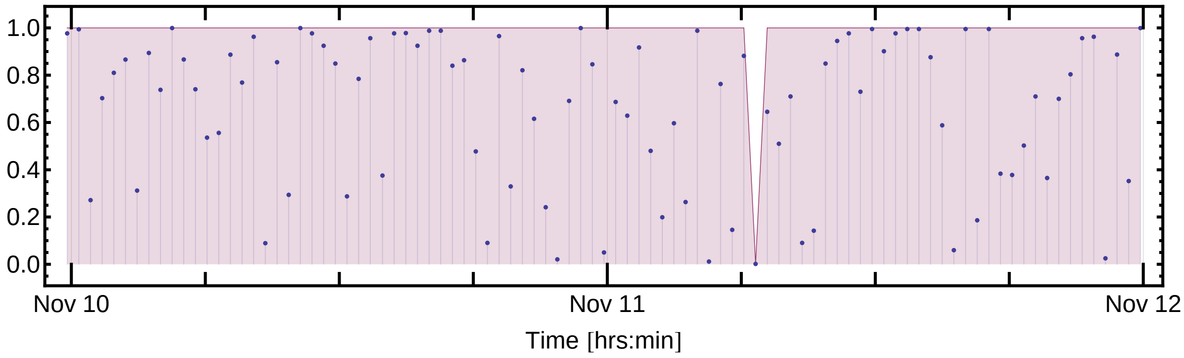


Figure 4.15: The random excursion test for the seventh state, +3, which shows one false test.

reached often enough. The test is applied in the forward cumulative summing mode on blocks of $\approx$200-400 bits output directly from the QKD system, and it can be seen in figure 4.18 that the key passes the majority of such tests.

4.3.7 Template Matching Tests

Template matching tests seek to find the number of matches to a specific m-bit long pattern within a window of particular size n. The input pattern is compared to the expectation of a random string to generate a statistic. A non-overlapping test differs from an overlapping test simply in the algorithm. In the overlapping template test if the pattern is found the algorithm selects the last bit of this pattern to place the beginning of the new window while it searches for a string. In the Non-overlapping version, the window moves along without regard to the occurrence of a pattern so that each window

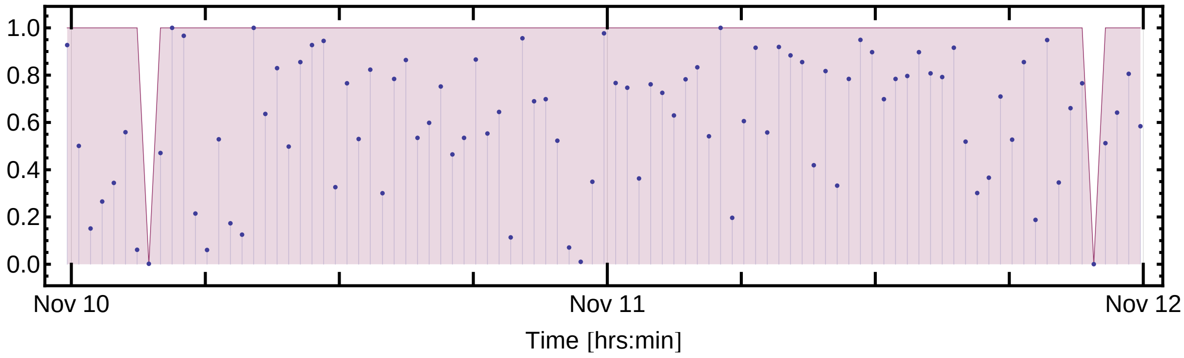


Figure 4.16: Random Excursions Variant Test for the state −8.

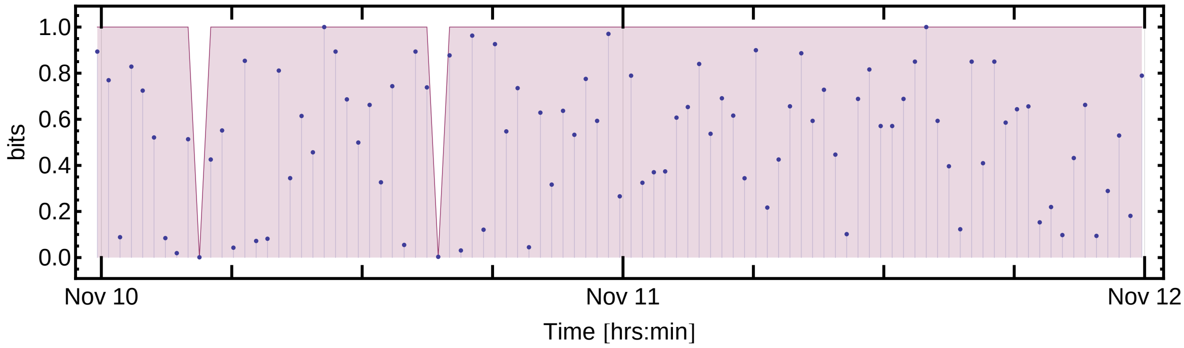


Figure 4.17: Random Excursions Variant Test for the state −4.

in the test is separate from the others. For both these tests many strings are tested so they are included in the Appendix from figure A.4 to figure A.26.

The template matching test is an important one since it may find small systematic patterns in the detection hardware. In particular, referring to the BBM92 detector diagram in figure 2.2 we should be concerned with the balance across each detection mode. There are four modes, each including some polarization optics and a Avalanche Photon detector. Note that there is some imbalance as the wave plate that sets the measurement in the ±45° basis will lead to more absorption in those two modes. This can be corrected for by adding a plate of glass, or a neutral density filter in the HV modes. Each Avalanche Photon detector should behave in a similar way. As well, some polarization effects due to small variations in the geometry of optical elements may be a problem. Small deviations within the tolerance specified for an optical element, or misalignments in the detectors may lead to polarizations effects. Finally, the polarization analyzers do

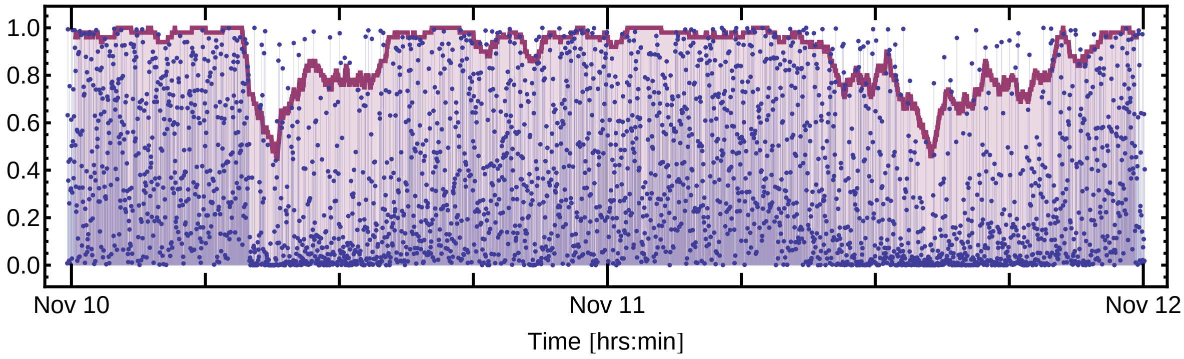


Figure 4.18: Cumulative Sums Test: The p-value (blue) and moving average of the decision test (red).

not separate polarization perfectly so some photons will go into the wrong ports in a systematic way.

Refer to figures A.4 to A.26 in the appendix. We see that the raw key has some systematic patterns in the key. These occur for small bit strings while longer bit string patterns in the non-overlapping template matching tests, but not for longer strings. The reverse appear for the overlapping template matching tests, longer strings fail while shorter ones pass the test for randomness. It would be appropriate to balance the whole set of detectors especially when extraneous light during the daytime generation of key will lead to further biases in the bit string. Although for small patterns the tests failed, this is the key prior to compression. The final key resulting after privacy amplification will likely pass these randomness tests with a larger p-value. However, to optimize the amount of key generated, small corrections of the detectors are an important improvement.

4.3.8 Discussion of the random number tests

Although the majority of tests show that the quantum cryptographic device behaves as a true random number generator, it is clear that the randomness of the key is decreased in daylight, when a large background incident in the optical channel will lead to erroneous key generation. This is observed especially at the portion of key when the signal was attenuated in a rain storm, at 9:00 AM on the first day. In these conditions $\eta_t \to 0\%$ and so $r_c^{'} \to r_a$, so $q_t \to 1/2$.

The background in the channel may also serve to bias the efficiency of particular single

Test	Result	Minimum bit size	Type
Frequency	T	100	Normal
Block frequency	T	100	χ^2
Runs	T	100	Normal
Binary Rank	T	38912	χ^2
Non Overlapping Template Matching	F	10^6	χ^2
Overlapping Template Matching	T	10^6	χ^2
Maurer's Universal Compression	T	904960	Normal
Approximate Entropy	T	100	χ^2
CUSUM	T	100	Normal
Random Excursions	T	10^6	χ^2
Random Excursions Variant	T	10^6	Normal

Table 4.3: Requirements and results of the random number tests.height

photon avalanche photo detectors (there are 4 detectors) leading to a slight asymmetry of key generation, since the different detectors may have varying saturation behavior. If this asymmetry is a part of the publicly discussed information it will not affect the security of the key. The portion of the asymmetry which gives an unbalanced key string will lead to information leakage to the potential eavesdropper. This is observed in most of the tests as a drop in the p-value during daytime hours, and can be observed in the monobit frequency test; figure 4.5, the approximate entropy test; figure 4.9, and the cumulative sums test; 4.18.

Chapter 5

Conclusion

The experiment and the main discoveries of this experiment are summarized here. A short outlook for improvements to the current QKD system is discussed.

5.1 Final Discussion

This report shows that it is possible to perform QKD with spectrally broad entangled photon pairs over a free-space optical link in daylight ambient background light conditions. A combination of temporal, spectral, and spatial filters are adequate to suppress the background light levels below the level of detector saturation, and below the levels where accidental coincidence contributions would bring the QBER above the threshold for secure key distribution. Moreover, we found that filtering only reduced the final daytime key generation rate in comparison to night time by a small factor; less than 2.

Spectral filters must be carefully matched to the source signal to maximize signal transmission across the channel and reject the large spectrum of sunlight which is transmitted through the atmosphere. Ideally, the source wavelength should be chosen so that a strong absorption in the earth's atmosphere, due to for example water molecules, does not occur. This could correspond to a Fraunhofer line of the sun or absorption line of the upper atmosphere, where background light will be at lower levels [72]. Additional filters may be used outside of the source signal to further reduce counts, but in our case an average optical density of OD2 was enough to suppress light to reasonable levels, while coupling roughly 8 nm spectral bandwidth. Color filters may also be used for reduction of background by extra densities outside of the signal spectrum. In regards to the choice of a pair source, the bandwidth may be reduced using longer crystals, in particular periodically poled crystals. This will also allow spectral filtering by larger densities through the selection of a narrow interference filter.

Spatial filters play an important role in removing stray light which is introduced into the receiving telescopes by way of multiple reflection in the telescope barrel or the lens, or just being scattered near the optical ports into the free space channel. Baffles extending both upstream and downstream to the receiving lens proved effective in reducing extraneous counts from modes outside of the free-space channel. Spatially, most of the background light coupled into the detectors falls within a small circular area surrounding the sending ports, namely, the FOV of the receiver. This FOV, including the optical ports, must be covered in diffuse black out material to reject unwanted scatter of background light into the free-space optical channel. Limiting the pinhole is an important factor to reduce the FOV, though a minimum size must be set where it will still be possible to align the optical channel efficiently.

The temporal filtering can be resolved to a minimum window for accepted counts to slightly more than the detector jitter. Adjusting for timing delays carefully optimizes the amount of coincident photons which are accepted into the data processing routine. As well, synchronization was achieved in the field tests during day. The laboratory tests found the ratio of total counts to real coincidences of approximately 250 beyond which synchronization will break down. Thus, with next generation sources, synchronization should always be possible in daylight conditions.

This opens up the possibility of QKD based on either of the BBM92 and E91 protocol which uses an entanglement source to operate continuously day and night over a free space optical channel. Using brighter sources, both larger key generation rates and further distances are possible. For example, these studies open up the option for 24 hour communication security using an intra-city QKD system, or possibly satellite based QKD operating during day, even when an entanglement source is used.

5.2 Improvements

A longer distance test and higher key rate are both possible. Periodically poled materials for χ^2 sum frequency generation will allow higher spectral filtering of sunlight due to their narrow bandwidth, may be temperature tuned for signal wavelength selection, and give higher count rates [48]. This will be an advantage for long distance QKD. Preliminary measurements for this source were begun while this experiment was run.

Adaptive optics may be used for stabilization to cope with atmospheric turbulence or thermal expansion of the hardware to improve transmission through the channel. Active coupling using simple tip and tilt controllers would cope for small mechanical misalignments due to the change in temperature from day and night. Although over short distances beam wander and spreading can be ignored, distances larger than a few kilometers will require active stabilization where atmospheric turbulence begins to have a strong effect on the collimated beam.

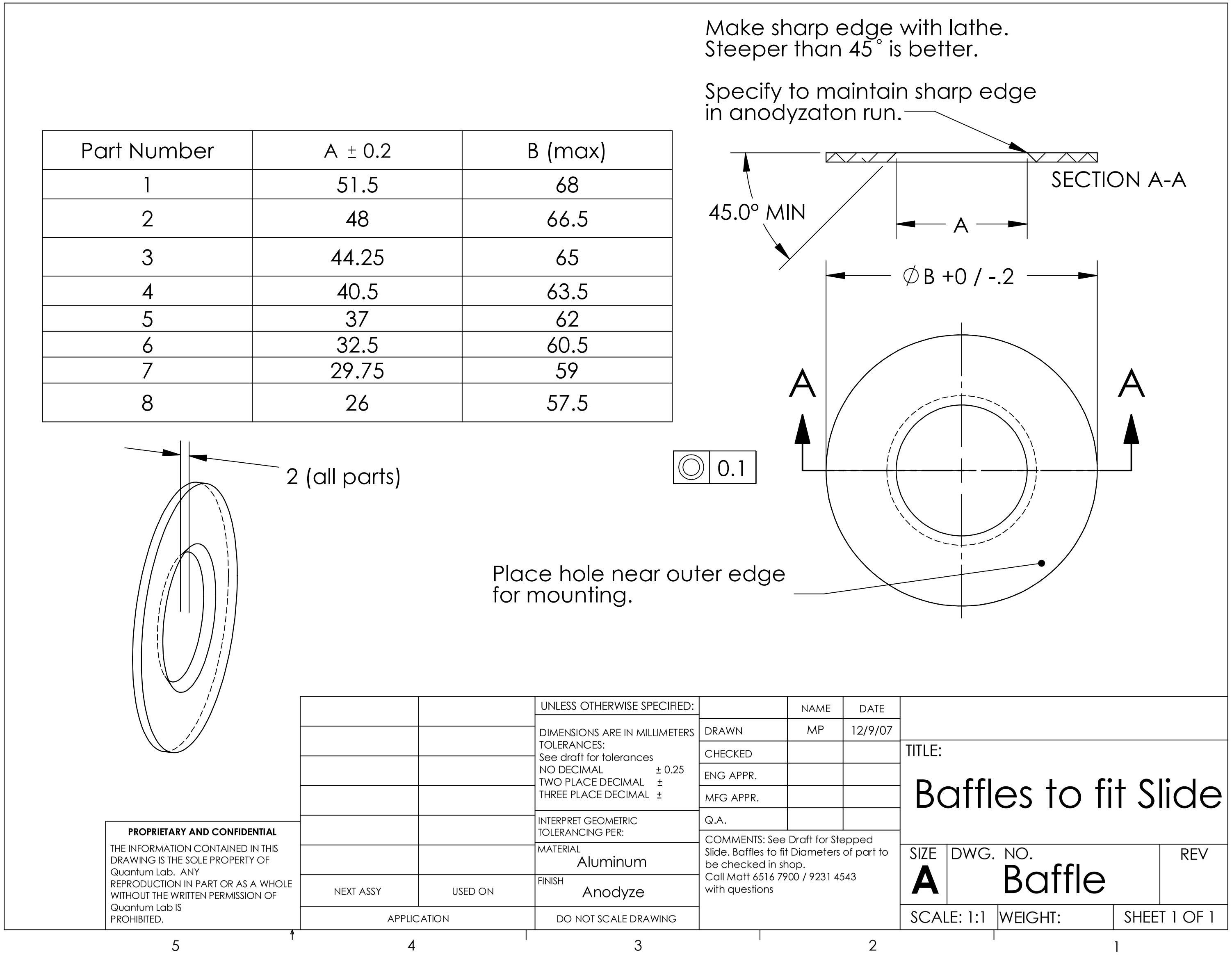
A more costly approach would be to use a beam splitter and deformable mirror to actively couple the signal through a smaller pinhole. This would reduce the background even further due to spatial filtering. Keep in mind that the Rayleigh range for a longer distance means the optical ports will be required to be large. It is not clear that daytime communication to and from geostationary earth orbiting (GEO) and low earth orbiting (LEO) satellites would be possible, since receiving apertures over these distances need to be of the order of a meter in diameter, and would collect a large amount of sunlight.

One minor improvement would involve design of a transmissive lens with dichroic properties. This could work in parallel to the interference filters as a spatial method to filter spectrally: by having a poor focus for the spectral range outside the signal bandwidth. This is much like placing a prism in the receiving telescope, but without introducing polarization rotations in the beam.

Appendix A

Appendix

A.1 CAD - Solid Models and Drafts for Optical Mechanics


Make sharp edge with lathe.
Steeper than 45° is better.
Specify to maintain sharp edge
in anodyzaton run.
SECTION A-A
45.0° MIN
A
∅B +0 / -.2
A
A
0.1
2 (all parts)
Place hole near outer edge
for mounting.
5
4
3
2
1

Part Number	A ± 0.2	B (max)
1	51.5	68
2	48	66.5
3	44.25	65
4	40.5	63.5
5	37	62
6	32.5	60.5
7	29.75	59
8	26	57.5

PROPRIETARY AND CONFIDENTIAL
THE INFORMATION CONTAINED IN THIS DRAWING IS THE SOLE PROPERTY OF Quantum Lab. ANY REPRODUCTION IN PART OR AS A WHOLE WITHOUT THE WRITTEN PERMISSION OF Quantum Lab IS PROHIBITED.

NEXT ASSY | USED ON
APPLICATION

UNLESS OTHERWISE SPECIFIED:
DIMENSIONS ARE IN MILLIMETERS
TOLERANCES:
See draft for tolerances
NO DECIMAL ± 0.25
TWO PLACE DECIMAL ±
THREE PLACE DECIMAL ±
INTERPRET GEOMETRIC TOLERANCING PER:
MATERIAL Aluminum
FINISH Anodyze
DO NOT SCALE DRAWING

	NAME	DATE
DRAWN	MP	12/9/07
CHECKED		
ENG APPR.		
MFG APPR.		
Q.A.		

COMMENTS: See Draft for Stepped Slide. Baffles to fit Diameters of part to be checked in shop.
Call Matt 6516 7900 / 9231 4543 with questions

TITLE:
Baffles to fit Slide

SIZE A | DWG. NO. Baffle | REV
SCALE: 1:1 | WEIGHT: | SHEET 1 OF 1

Figure A.1: Mechanical Draft of the Concentric Baffle Apertures for Daylight QKD.

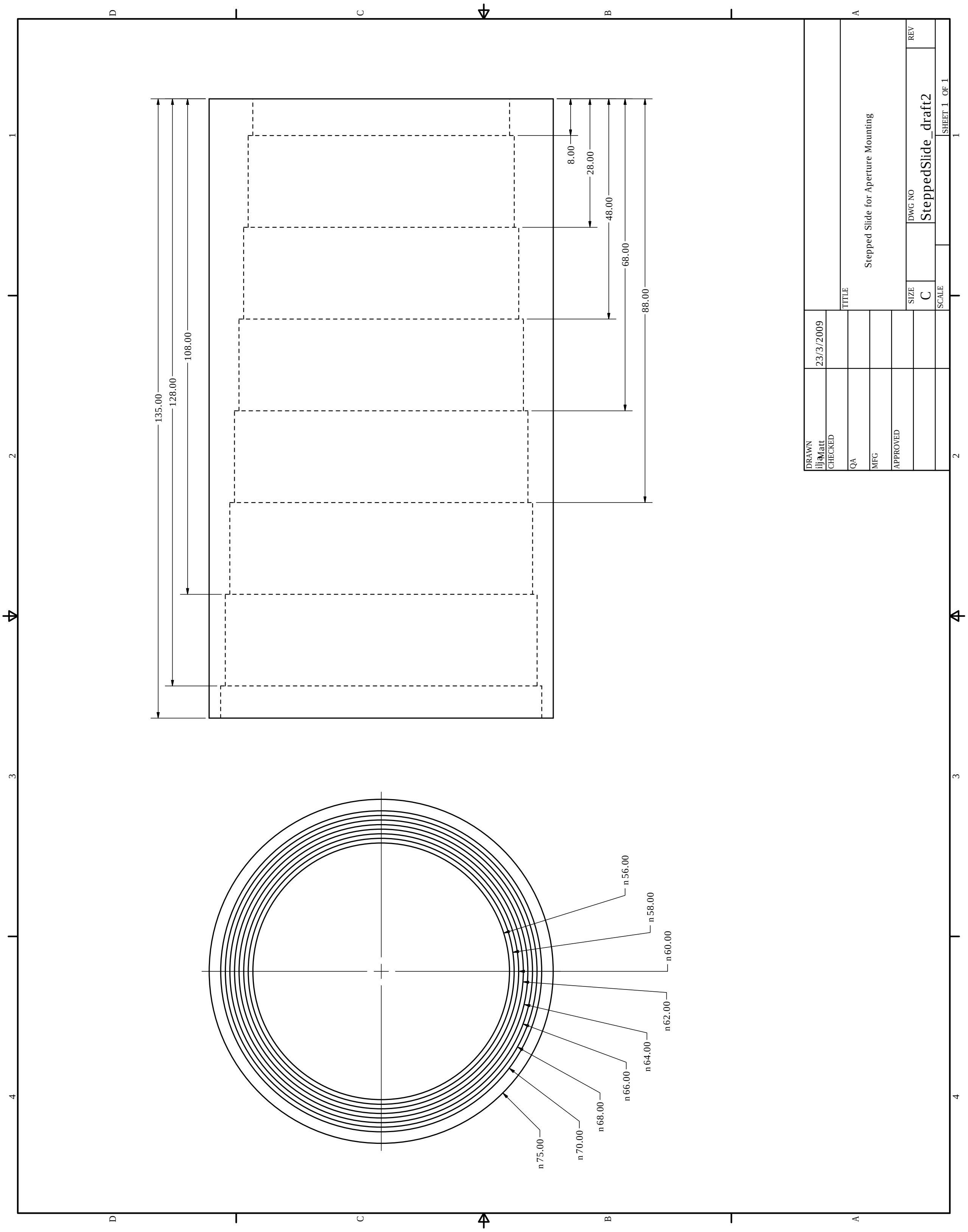


Figure A.2: Mechanical Draft of the Concentric Baffle Mount.

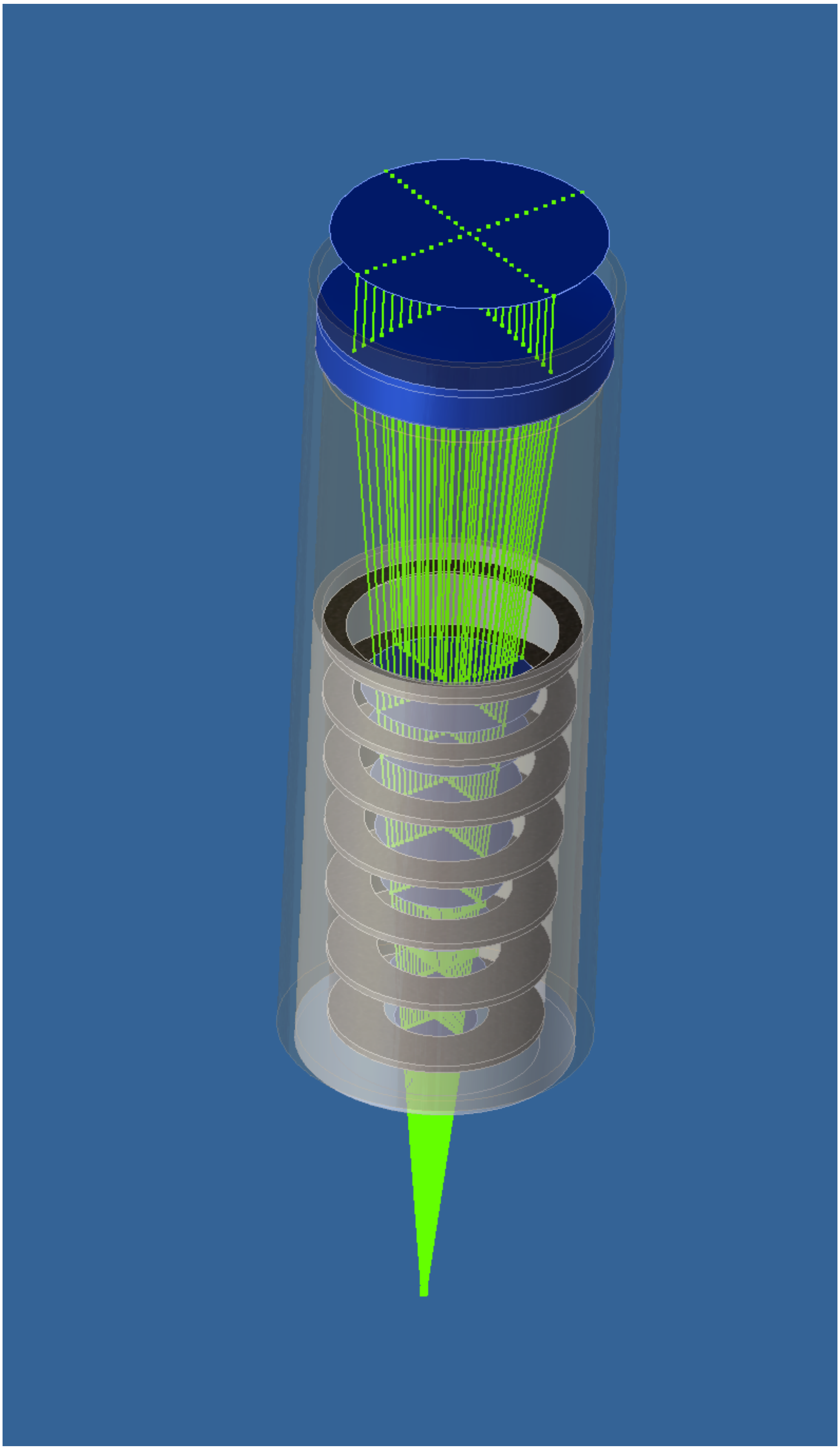


Figure A.3: Assembly including the Raytracing Wires for the the Receiver Lens, the Receiver Lens, the Baffle Mount, and Concentric Apertures.

A.2 Template Matching Tests

A.2.1 Non-Overlapping Template matching Tests

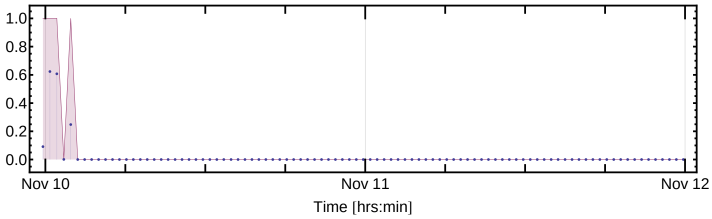


Figure A.4: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '001' performed on blocks of 1 × 10^6 bits.

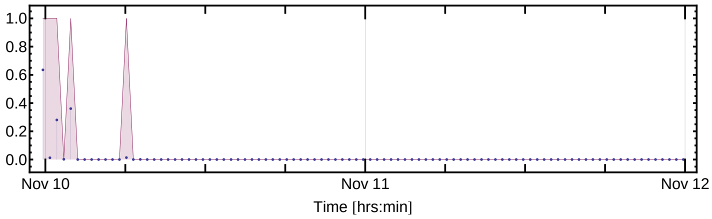


Figure A.5: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '011' performed on blocks of 1 × 10^6 bits.

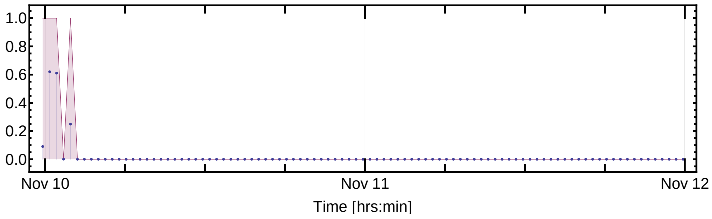


Figure A.6: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '100' performed on blocks of 1 × 10^6 bits.

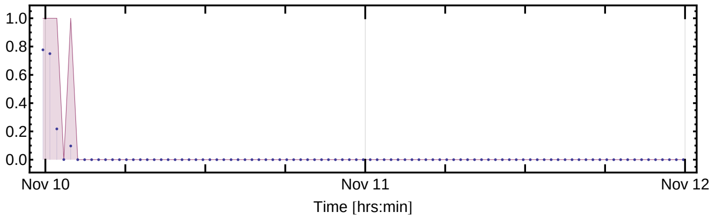


Figure A.7: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '1000' performed on blocks of 1×10^6 bits.

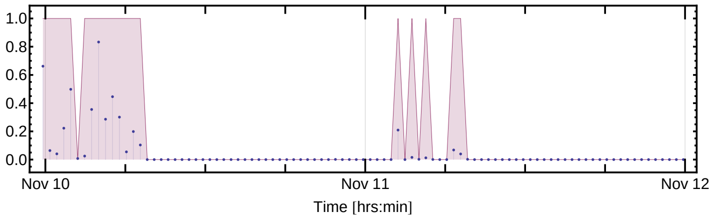


Figure A.8: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '10101010' performed on blocks of 1×10^6 bits.

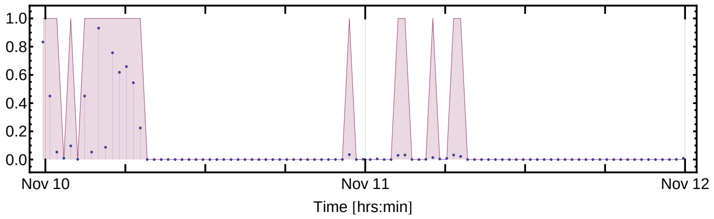


Figure A.9: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '00011001' performed on blocks of 1×10^6 bits.

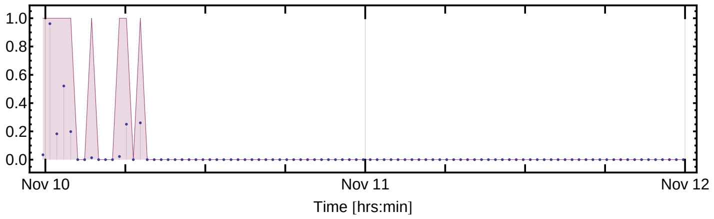


Figure A.10: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '000000001' performed on blocks of 1×10^6 bits.

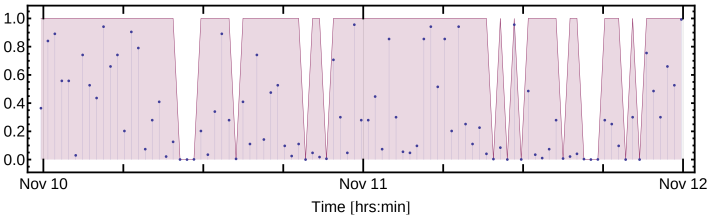


Figure A.11: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '100100100101' performed on blocks of 1×10^6 bits.

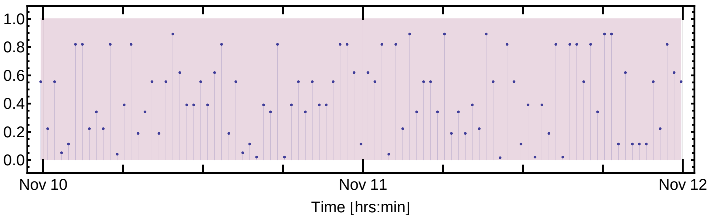


Figure A.12: Non-overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '100100101101100101' performed on blocks of 1×10^6 bits.

A.2.2 Overlapping Template Matching Tests

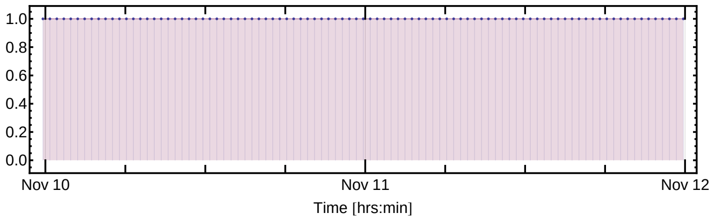


Figure A.13: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '01' performed on blocks of 1×10^6 bits.

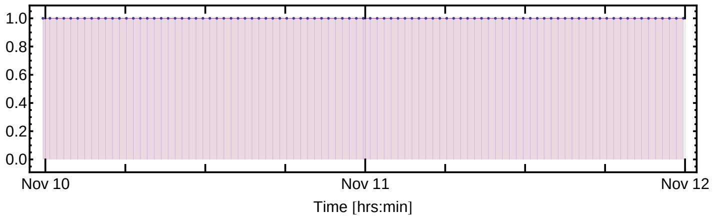


Figure A.14: Overlapping Template Matching Test: the p-value (blue) and the decision test (red) for the pattern '111' performed on blocks of 1×10^6 bits.

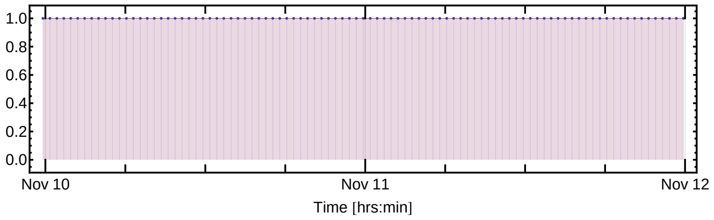


Figure A.15: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '101' performed on blocks of 1×10^6 bits.

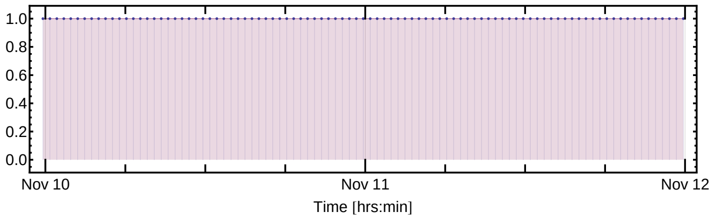


Figure A.16: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '011' performed on blocks of 1×10^6 bits.

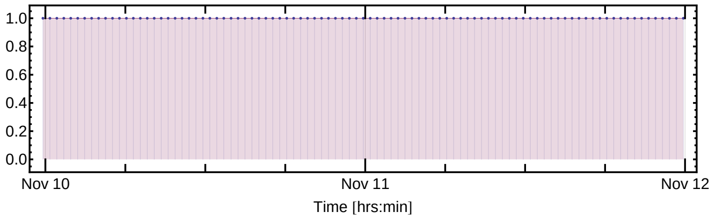


Figure A.17: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '001' performed on blocks of 1×10^6 bits.

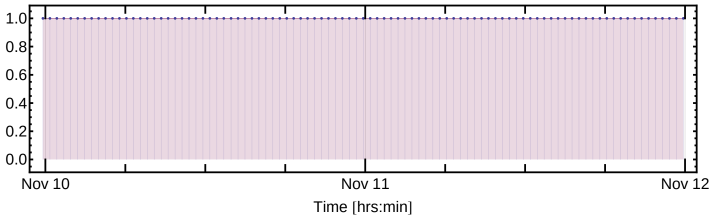


Figure A.18: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '0011' performed on blocks of 1×10^6 bits.

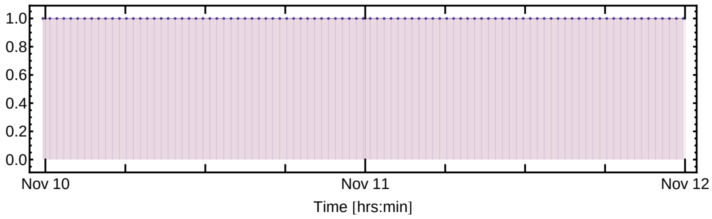


Figure A.19: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '0110' performed on blocks of 1×10^6 bits.

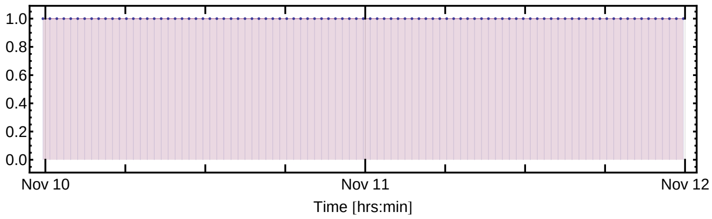


Figure A.20: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '1001' performed on blocks of 1×10^6 bits.

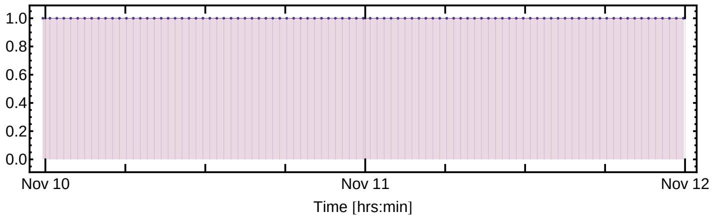


Figure A.21: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '1110' performed on blocks of 1×10^6 bits.

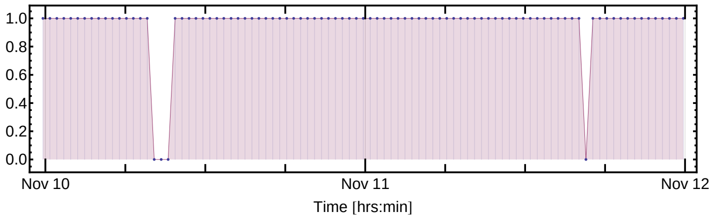


Figure A.22: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '11011' performed on blocks of 1×10^6 bits.

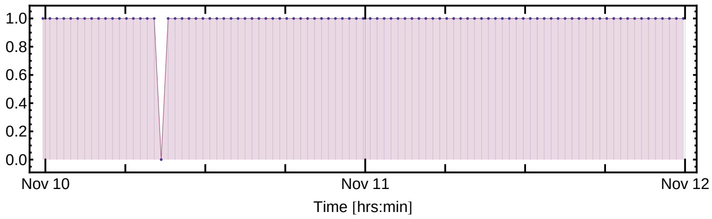


Figure A.23: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '01110' performed on blocks of 1×10^6 bits.

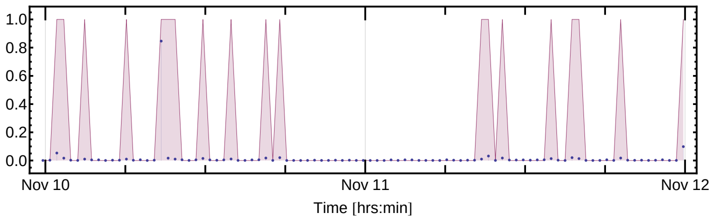


Figure A.24: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '010101' performed on blocks of 1×10^6 bits.

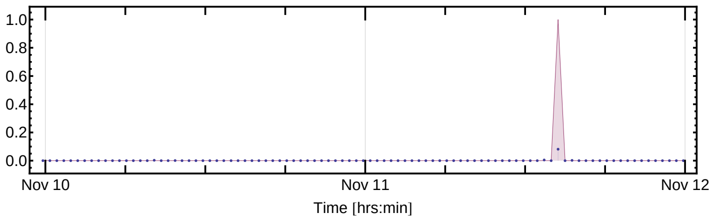


Figure A.25: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '1010101' performed on blocks of 1×10^6 bits.

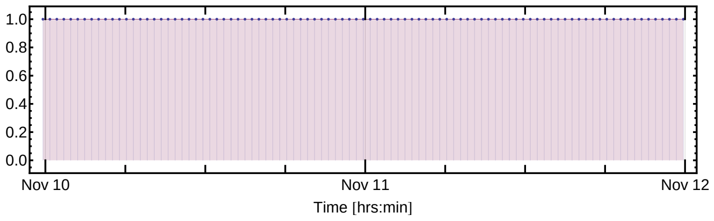


Figure A.26: Overlapping Template Matching Test: The p-value (blue) and the decision test (red) for the pattern '1000000' performed on blocks of 1×10^6 bits.

Bibliography

[1] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[2] Alexander Ling, Matthew P. Peloso, Ivan Marcikic, Valerio Scarani, Antia Lamas-Linares, and Christian Kurtsiefer. Experimental quantum key distribution based on a bell test. *Physical Review A*, 78:020301 (R), 2008.

[3] M Peloso, I Gerhardt, C Ho, A Lamas-Linares, and C Kurtsiefer. Daylight operation of a free space, entanglement-based quantum key distribution system. *The New Journal of Physics*, 11, April 2009.

[4] D. Martell. Intel's moore muses on end of technology maxim. *Reuters*, 2007.

[5] G. Moore. Cramming more components onto integrated circuits. *Electronics magazine*, 4, 1965.

[6] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46, 2001.

[7] J.I. Cirac and P. Zoller. Quantum computation with cold trapped ions. *Physics Review Letters*, 74:4091, 1995.

[8] J.A. Jones. Nmr quantum computation. *Progress in NMR Spectroscopy*, 38:325–360, 2001.

[9] C. H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physics Review Letters*, 69:2881, 1992.

[10] Stephen Weisner. Conjugate coding. *ACM SIGACT News*, 15:78–88, 1983.

[11] Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE Int. Conf. On Computer Systems and Signal Processing (ICCSSP)*, page 175. Bangalore, India, 1984.

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

[13] G.S. Vernam. Cypher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.*, 55:109, 1926.

[14] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittle, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[15] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557559, 1992.

[16] Artur Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[17] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[18] JS Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38:447, 1966.

[19] John S Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1:195–200, 1964.

[20] A Aspect, P Grangier, and G Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47:460–463, 1981.

[21] A Aspect, P Grangier, and G Roger. Experimental realization of Einstein–Podolsky–Rosen–Bohm *Gedankenexperiment:* a new violation of Bell's inequalities. *Physical Review Letters*, 49:91–94, 1982.

[22] N. Luetkenhaus. Security of quantum cryptography with realistic sources. *Phys. Rev. A*, 59:3301, 1999.

[23] W.Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, 2003.

[24] A. Lamas-Linares and C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Optics Express*, 15:9388–9393, 2007.

[25] C. Kurtsiefer. Spying on a quantum key distribution system through a timing side channel. In *Workshop on Theory and Realisation of Practical Quantum Key Distribution (TROPICAL QKD), 11.-14. June 2007, Waterloo (Canada)*, 2007.

[26] X Ma, CHF Fung, and HK Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007.

[27] Cheng-Zhi Peng, Tao Yang, Jian-Wei Pan, and et al. Experimental free-space distribution of entangled photon pairs over a noisy ground atmosphere of 13km. *Phys. Rev. Lett.*, 95:030502, 2005.

[28] Ivan Marcikic, Antia Lamas-Linares, and Christian Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89:101122, 2006.

[29] R Ursin, F Tiefenbacher, T Schmitt-Manderbach, and H Weier. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481–486, 2007.

[30] C. Erven, C. Couteau, R. Laflamme, and G. Weihs. Entangled quantum key distribution over two free-space optical links. *Optics Express*, 16:16840, 2008.

[31] Hughes RJ, Nordholt JE, Derkacs D, and Peterson CG. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4:Article Number: 43, JUL 12 2002.

[32] Richard J Hughes, William T Buttler, Jane E Nordholt, and C Glen Peterson. Free-space quantum key distribution in daylight. *Journal of Modern Optics*, 47:549, 2000.

[33] Jürgen Audretsch. *Entangled Systems: New Directions in Quantum Physics.* Wiley-VCH, 2007.

[34] Keiichi Edamatsu. Entangled photons: Generation, observation, and characterization. *Japanese Journal of Applied Physics*, 46(11):7175–7187, 2007.

[35] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Reviews of Modern Physics*, 77:1225– 1256, 2005.

[36] E.T. Jaynes. Information theory and statistical mechanics. *Physical Review*, 106:620–630, 1957.

[37] C.E. Shannon. Communication theory of secrecy systems. *Bell Technical Journal of ACM*, 28:441, 1949.

[38] D Mayers. Unconditional security in quantum cryptography. *Journal of ACM*, 48:351–406, 1998.

[39] H-K Lo and F Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.

[40] Peter Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett. 85, 441-444 (2000)*, 85:441–444, 2000.

[41] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *arXiv.org:0802.4155*, 2008.

[42] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, September 2005. available at http://arxiv.org/abs/quant-ph/0512258.

[43] David N. Klyshko. *Photons and Nonlinear Optics.* Gordon and Breach Science Publishers, 1988.

[44] Ravinder R. Puri. *Mathematical Methods of Quantum Optics.* Springer-Verlag, 2001.

[45] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, and Anton Zeilinger. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337 – 4341, 1995.

[46] V.G. Dmitriev, G.G. Gurzadyan, and D.N. Nikogosyan. *Handbook of Nonlinear Optical Crystals.* Springer-Verlag, 1999.

[47] S Emanueli and A Arie. Temperature-dependent dispersion equations for ktiopo4 and ktioaso4. *Applied Optics*, 42(33):6661–6665, 2003.

[48] Tso Yee Fan, R. S. Feigelson, and et al. Second harmonic generation and accurate index of refraction measurements in flux-grown ktiop04. *Applied Optics*, 26(12):2390–2394, 1987.

[49] K. Fradkin, A. Arie, A. Skliar, and G. Rosenman. Tunable midinfrared source by difference frequency generation in bulk periodically poled ktiopo4. *Applied Physics Letters*, 74(7):914–916, 1999.

[50] Kiyoshi Kato and Eiko Takaoka. Sellmeier and thermo-optic dispersion formulas for ktp. *Applied Optics*, 41(24):5040, 2002.

[51] KC Harvey and CJ Myatt. External-caviity diode laser using a grazing-incidence diffraction grating. *Optics letters*, 16:910–913, 1991.

[52] Taehyun Kim, Marco Fiorentino, and Franco N. C. Wong. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Phys. Rev. A*, 73:012316, 2006.

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

[54] H Hodera. *Trudy IIER*, 54 (3):36, 1966.

[55] Vladimir Evseevich Zuev. *Propagation of visible and infrared radiation in the atmosphere.* John Wiley and Sons, Ltd., Chichester, 1974.

[56] RL Fante. Electromagnetic beam propagation in turbulent media. *Proc. IEEE*, 63:1669, 1975.

[57] G. Gilbert and M. Hamrick. Practical quantum cryptography: A comprehensive analysis (part one). *Mitre Technical Report*, 51MSR837:91–102, 2000.

[58] F.G. Smith, editor. *The Infrared and Electro-Optical Systems Handbook Volume 2: Atmospheric Propagation of Radiation.* SPIE Optical Engineering Press, Bellingham, Washington USA, 1993.

[59] A.L. Buck. Effects of the atmosphere on laser beam propagation. *Applied Optics*, 6:703, 1967.

[60] QIT. Deliverable 2: Report on light sources for quantum key distribution. Technical report, NUS, april 2005.

[61] QIT. Deliverable 3: Report on clock synchronization and error correction and privacy amplification. Technical report, NUS, september 2005.

[62] Antia Lamas-Linares, Matthew P Peloso, and Christian Kurtsiefer. Free space distribution of entangled photons pairs in daylight conditions. *2007 Pacific RIM Conference on Lasers and Electro-Optics*, VOLS 1-4:945–946, 2007.

[63] Christian Kursiefer, Markus Oberparleiter, and Harald Weinfurter. High efficiency entangled photon pair collection in type ii parametric fluorescence. *Physical Review A*, 64:023802, 2001.

[64] Caleb Ho, Antia Lamas-Linares, and Christian Kurtsiefer. Clock synchronization by remote detection of correlated photon pairs. *arXiv:0901.3203*, 2009.

[65] S.F. Seward, P.R. Tapster, J.G. Walker, and et al. Daylight demonstration of a low-light-level communication-system using correlated photon pairs. *Quantum Optics*, 3(4):201–207, 1991.

[66] G Brassard and L Salvail. Secret-key reconciliation by public discussion. *Advances in Cryptology - Proc. Eurocrypt'94*, pages 410–423, 1994.

[67] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Inc., 1997.

[68] Tomohiro Sugimoto and Kouichi Yamazaki. A study on secret key reconciliation protocol "cascade". *IEICE Trans. Fundamentals*, E83-A(10):1987–1991, october 2000.

[69] C.H. Bennett, G. Brassard, , and J. Roberts. *SIAM Journal of Computing*, 17:210, 1988.

[70] C.H. Bennett and et al. Generalized privacy amplification. *IEEE Trans. Inform. Theory*, 41:1915–1923, 1995.

[71] G. Brassard and L. Savail. Secret-key reconciliation by public discussion. *Lect. Notes Comp. Sci.*, 765:410–423, 1994.

[72] NIST. Guide to the statistical tests. csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html, 2009.

[73] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dra, and San Vo. *Special Publication 800-22 Revision 1 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.* National Institute of Standards and Technology, 2008.

[74] S.M. Pincus. Approximate entropy as a measure of system complexity. *Proc Natl Acad Sci USA*, 88:2297–2301, 1991.

[75] U. Maurer. A universal statistical test for random bit generators. *Journal of Cryptology*, 5:89–105, 1992.

[76] W Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. New York: Wiley, 1968.

[77] D. J. Rogers, J. C. Bienfang, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, L. Ma, D. H. Su, Carl J. Williams, and Charles W. Clark. Free-space quantum cryptography in the h-alpha fraunhofer window. In *Free-Space Laser Communications VI, edited by Arun K. Majumdar, Christopher C. Davis, Proc. of SPIE Vol. 6304, 630417*, 2006.