Experimental and theoretical demonstration of the feasibility of global quantum cryptography using satellites

by

Jean-Philippe Bourgoin

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosohy
in
Physics

Waterloo, Ontario, Canada, 2014

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

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

Abstract

Information security is a growing concern in our modern world, where almost everything can be done online. To protect security, classical encryption protocols, such as RSA, are used. These encryption protocols are almost always based on mathematical problems that are computational difficult. Therefore, the security is only valid under limited computational resources, and therefore do not provide provable security. An exception is the one-time pad protocol, which is provably secure but requires an existing shared key that is as long as the information it must encrypt. The exchange of such a key can be challenging, often requiring the two partied to physically meet to exchange the key or the use a trusted courier to physically carry the key on a hard drive.

Quantum key distribution (QKD) offers a solution by utilizing quantum mechanics to grow a secure cryptographic key shared between two distant parties. The quantum nature of the particles used in the exchange ensure that any eavesdropper would leave signs of their presence, allowing the users to precisely quantify the security of the key that is produced. This allows secure generation of a random key which can be used for the one-time pad encryption protocol which, unlike most encryption protocols, does not rely on computational assumptions, and is secure regardless of available computational power.

Current implementations of QKD are limited to a single link distance of $\sim$200 km, preventing implementation of QKD on a global scale, or even between distant cities within a single country, without some additional techniques. One promising solution is the use of orbiting low Earth orbit satellite platforms as trusted nodes in a quantum communications network. The main purpose of this work has been to show the viability of this solution, trough theoretical performance modeling and experimental demonstrations.

Thorough numerical simulations have been developed to evaluate the performance and challenges in implementing QKD using a low Earth orbit satellite platform and determine an optimal approach to its implementation. The simulations include a realistic satellite orbit analysis, all expected loss mechanisms, estimates of background contributions and realistic simulation of quantum optical processes. This work addresses the questions of optimal wavelength and beam waist, the effect of the telescope design and pointing error, and the impact of detector degradation due to exposure to radiation in the space

environment. The simulation is used to determine the length of secure key for QKD and the performance of fundamental quantum optics experiments such as Bell tests and quantum teleportation. We compare the advantages and disadvantages of uplink and dowlink scenarios, and show that an uplink, despite having reduced performance compared to a downlink, offers more scientific freedom, by allowing changes to the quantum source, and benefits from a simpler satellite design with reduced pointing requirement. This work provides a theoretical foundation for ongoing design and development of quantum systems for satellite implementation of QKD.

In addition to theoretical analyses, experiments where developed and conducted corresponding to the challenges likely to be faced by a satellite uplink. Two main challenges where identified and experimentally overcome. First, the difficulty of operating in the high loss regime of a satellite uplink, which typically experience losses in the range of 40–50 dB when above 40° of elevation from the horizon, an elevation only reached by half of the satellite passes. This challenge was addressed by demonstrating full QKD protocols at losses exceeding 50 dB. Also, the ability to perform full QKD during the short duration of a satellite pass was shown by replicating the varying loss of archetypal passes and successfully extracting secure keys. Secondly, the difficulty of accurately tracking and pointing to a receiver platform traveling at the high angular speed of a satellite was overcome by successfully exchange quantum signals to a truck traveling at angular speeds exceeding that of a low Earth orbit satellite. This required the design, construction, and implementation of a transmitter system and a quantum receiver system capable of active pointing using a custom pointing system.

An additional experiment was also performed where we experimentally investigate the feasibility of performing QKD using light scattered by a diffusive screen. A system capable of doing so could be used to create QKD hot-spots, where a QKD source could be aimed at a diffusive screen to allow multiple users to simultaneously exchange secure keys with the source without the need for high precision pointing.

Through these analyses and experimental demonstrations we evaluated the performance of QKD using a satellite and have shown its technological readiness to be implemented. Implementation of such a system would allow QKD to be performed on a global scale, enabling communications security that is not based on computational assumptions without the need to physically transport the key from one party to the other.

Acknowledgements

I would like to thank my supervisor Dr. Thomas Jennewein for all his guidance and advice. I truly enjoyed the opportunity to be a part of the Canadian satellite QKD endeavor and hope to continue to contribute to it in the future.

I thank my committee members, Dr. Raymond Laflamme, Dr. Norbert Lütkenhaus, and Dr. Hamed Majedi for their advice and constructive criticism. I also thank Dr. Joshua Bienfang for agreeing to be part of my thesis defense committee.

Many thanks to my many colleagues who have all contributed to this work in one way or another, either directly or through helpful discussions, and have shared with me the agony of graduate school.

A huge thanks to Dr. Brendon Higgins for all his invaluable advice and contributions. I hope we can continue to take advantage of our complementary expertises and produce ideas that are better than either of us could produce alone.

I would like to acknowledge my colleagues who have directly contributed to this work. Dr. Brendon Higgins who designed the polarization compensation system and improved the QKD and pointing softwares. Nikolay Gigov who developed the QKD software used in the experiments. Evan Meyer-Scott who initially developed the MATLAB code used to predict the visibility and secure key rates, and initially developed the weak coherent pulse source. Dr. Zhizhong Yan who developed the intensity and polarization modulator system for the weak coherent pulse source. Bassam Helou who initially developed the background estimation program. Catherine Holloway who initially developed the tracking and pointing software. Christopher Pugh, Sarah Kaiser, Miles Cranmer, Christian Barna, Sasha Chuchin and Jennifer Fernic who helped during some of the moving receiver night tests. Chris Ervin, Hannes Hübel and Norbert Lütkenhaus who provided helpful advices.

I also want to acknowledge the contributions of our industry partners from the Canadian Space Agency (CSA), COMDEV, and from the National Optics Institute (INO). In particular I want to highlight the contributions of the following individuals. Balaji Kumar of COMDEV, who provided the orbit analysis using AGI's System Tool Kit. Jean-François Lavigne of INO, who gave useful advices in modeling atmospheric turbulence. Ralph Girard

of CSA, who thoroughly reviewing the link analysis code. Ian D'Souza and Danya Hudson of COMDEV, who on many occasions shared their expertize in satellite technologies.

Special thanks to Sarah Kaiser, Elena Anisimova and Aimee Gunther for catching a few typos in this thesis.

I acknowledge the many funding agency that have made this work possible: Canadian Space Agency, Defence Research and Development Canada, NSERC, CryptoWorks21, FEDDEV, CIFAR, CFI and Ontario's ERA program.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In this chapter, we briefly introduce classical and quantum cryptography, the challenges of applying quantum key distribution globally, and how satellites could be used to overcome these challenges.

1.1 Classical encryption

With the widespread use of computers and growing use of online services, our modern society as become heavily reliant on electronic communications and data transfer. Many of these activities, such as online banking, shopping and other activities that use personal information, require security and privacy. Protection is needed on all kinds of information, from personal data to trade secrets, which is regularly transmitted over public communication channels. To prevent unauthorized access to this information, many different cryptographic techniques are used.

Most of the cryptographic schemes used today do not provide provable security. Instead, these cryptosystems, such as RSA [1], are deemed secure by using assumptions about the limited computation power of an adversary [2]. These protocols use mathematical operations that are difficult to reverse, such as factoring of large integers. The size of these integers are chosen so that and adversary would typically be unable to break security within a certain time frame with realistic hardware, usually chosen several decades. The security therefore relies on estimates of the computational power available to an adversary. Because of the fast growth of computational power, these estimates have often proven to be too conservative. These underestimations have lead to secure communication, assumed unbreakable for decades, being broken in a fraction of that time [3].

In addition, some of the cryptosystem have been showed to be vulnerable to Quantum computers. Shor's algorithm [4] is a quantum computer algorithm that can be used to efficiently factor integers and find discrete logarithms, thus breaking some cryptosystem such as RSA. As a result, quantum computers have the potential to easily break many of the currently used cryptosystem. Not all cryptosystem have been shown to be efficiently breakable by quantum computers. These alternative cryptosystem, called post-quantum cryptosystem [5], are being actively studied to be implemented as alternatives. However, post-quantum cryptography is still based on computational assumptions, and thus still rely on accurate estimates of the computational power available in the near future. In addition, while these cryptosystem have not been shown to be efficiently breakable by either classical or quantum computers, there is no formal proof that an efficient algorithm cannot exist.

Not all cryptographic schemes are based on computational assumptions. The one-time pad, invented by Frank Miller in 1882 [6] and re-invented by Gilbert Vernam in 1917 [7], uses a secret key that is shared between two parties to encrypt and decrypt messages. Unlike RSA and other public cryptosystem, the one-time pad protocol does not provide any key distribution, and instead relies on a preexisting secret key. To ensure security, the key must be at least as long as the message, so that each bit is encoded randomly, and the key must be kept secret by both parties, and only used once. This protocol was proven optimal by Claude Shanon in 1949 [8], that is, no other encryption method can provide proven security with less key. The main limitation of this scheme as been the difficulty of securely distributing keys among the two parties. Classically, the most reliable way of doing this has been to physically transport the key, either by one of the two parties or with the use of trusted couriers. Quantum information has brought a solution to this problem called quantum key distribution.

1.2 Quantum key distribution

Quantum key distribution (QKD) allows the exchange of secure keys between two parties, typically referred to as Alice and Bob, by exploiting the fundamentally quantum mechanical nature of reality [9]. In QKD, the key is obtained by exchanging quantum states using a quantum channel. One peculiar property of quantum states compared to classical systems is superposition: a quantum state can be in many states simultaneously [10].

A good example of this phenomenon is observed in the double-slit experiment, first performed by Thomas Young. In this experiment, a beam of quantum particles are projected onto two small and closely spaced slits. If the particles are detected on a screen

placed a certain distance after the slit, they will show a wave-like interference pattern. This occurs even if the beam fires only one particle at a time, the particle can therefore interfere only with itself. This strange observation signifies that the quantum particle has passed through both slits simultaneously, meaning it's in a superposition of having passed through each slits. Even stranger, if one chooses instead to measure the particle at the slits, it will only be measured at either one slit or the other, never both. The effect of measuring the state has thus collapsed the superposition, forcing the quantum particle in either one state or the other. This effect of measurement on quantum states is what allows QKD to be provably secure.

If an eavesdropper, typically referred to as Eve, attempts to extract information from the quantum states in the quantum channel, she will be performing some form of measurement and will therefore, in general, modify the state. Alternatively, if Eve tries to copy the state, the no-cloning theorem [11] provides a formal proof that one cannot copy an arbitrary unknown state without disturbing the original. Therefore, any attempts made by Eve to extract information from the key will inevitably leave signs of her presence in the form of errors in the key. By sampling and revealing a random part of the key, which is later discarded, Alice and Bob can estimate the amount of errors and therefore detect the presence of an adversary. If an eavesdropper is detected, the compromised key is discarded. Because Eve cannot prevent signs of her presence, any key that shows no sign of an eavesdropper is provably secure with a certain ϵ probability, typically chosen on the order of 10^{-9}, i.e. the key has a probability ϵ of deviating from perfect security (where no bits are compromised).

In general, QKD can be performed with any quantum states. Implementations of QKD however, are almost always performed using photons [9]. The main reason for this is because light can be transmitted over long distances without decoherence, i.e. without unreversable change in its initial quantum state. In free-space applications of QKD, the information is typically encoded in the polarization state of light. These states are typically the horizontal ($|\mathrm{H}\rangle$), vertical ($|\mathrm{V}\rangle$), diagonal ($|\mathrm{D}\rangle$), and antidiagonal ($|\mathrm{A}\rangle$) polarizations, where $|\mathrm{D}\rangle$ and $|\mathrm{A}\rangle$ are superpositions of $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$:

$$|\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |\mathrm{V}\rangle) \tag{1.1}$$

$$|\mathrm{A}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle - |\mathrm{V}\rangle) \tag{1.2}$$

The photons are therefore encoded in two polarization bases: the H/V basis and the D/A basis. These two bases are mutually unbiased, meaning any state in one basis that is

measured in the other basis will give a random result with equal probability across all possible outcomes [12] (in this case there are two measurement outcomes, thus each will have a probability $\frac{1}{2}$). If either Alice, Bob or Eve attempt to measure the state in its proper basis, such as measuring $|\mathrm{H}\rangle$ in the H/V basis, they will gain information on the state of the photon without modifying it. If however they measure using the wrong basis, such as measuring $|\mathrm{H}\rangle$ in the D/A basis, they will perturb the state. When Bob measures in the wrong basis compared to Alice, the results is simply discarded. If there is no eavesdropper, the events where Bob measures in the right basis should be perfectly correlated with Alice. If however Eve is present, there is a chance that she will measures in the wrong basis, thus breaking the correlations. The results of Alice and Bob will then only randomly agree with each other. When a large number of photons are exchanged, the probability that Alice and Bob obtain completely correlated results in the presence of Eve becomes infinitesimally small.

In fiber implementations of QKD, photons are typically encode in phase [9]. This is mainly because propagation through fiber modifies polarization states. This change in encoding method does not affect the performance or security of QKD. In this work we focus on free-space QKD using polarization encoding of photons.

The original QKD protocol was proposed by Charles Bennett and Gilles Brassard in 1984 [13]. In this scheme, called the BB84 protocol, Alice generates single photons in a polarization state randomly chosen from a predefined set, typically $|\mathrm{H}\rangle$, $|\mathrm{V}\rangle$, $|\mathrm{D}\rangle$ and $|\mathrm{A}\rangle$. Bob receives the photons and measures them in one of the two nonorthogonal bases H/V or D/A, chosen randomly. Whenever Bob measures in the same basis which Alice prepared in, his measurement outcome will match the prepared state with unit probability (neglecting experimental imperfections). Alice and Bob then exchange information about the bases in which states were prepared and measured, but not the states themselves, across the public classical channel, allowing them to establish a secret key from their shared knowledge of the states. The additional steps of error correction and privacy amplification can then be employed to correct errors from background noise and other practical imperfections in the source and detectors, and to reduce the amount of information that may have leaked to Eve to an exponentially small amount.

One way to generate the BB84 states is to use a weak coherent pulse (WCP) source, i.e. a pulsed laser with each pulse attenuated to an average of less than one photon. A WCP source is only an approximate single-photon source, with a small probability of creating states consisting of two or more photons. To maintain security with a WCP source, one must either keep the probability of multi-photon events very small (by keeping the average photon number small, which also reduces the single-photon probability and thus reduces

the key rate), or by amending the protocol with a decoy state method [14].

In a decoy state protocol, the intensity of the pulses are randomly varied between a signal and a smaller decoy intensity, with the signal state typically having a higher probability of being produced. If Eve tries to take advantage of all the multi-photon pulses by measuring one photons when there are two or more and blocking the pulses with only one photon, she will block a higher ratio of decoy pulses (which have a lower chance of producing two or more photons) compared to signal pulses. By comparing the number of received signal and decoy states Alice and Bob can determine if they suffered the same attenuation and thus quantify the probability of an eavesdropper being present.

The BB84 protocol is known as a prepare-and-measure schemes because Alice prepares the photons in a randomly chosen state and Bob measures them. There exist a second main type of QKD schemes known as entanglement-based schemes, such as the Ekert91 protocol [15] or the simpler BBM92 protocol [16]. These schemes take advantage of quantum entanglement to perform QKD.

Quantum entanglement occurs when two or more particles, photons in the case of QKD, are in a combined quantum state that cannot be separate, i.e. one cannot express the state of one particle without the other. One example of entangled states are the Bell states [17]:

$$\left|\phi^{\pm}\right\rangle_{12} = \frac{1}{\sqrt{2}}(\left|\mathrm{H}\right\rangle_1 \left|\mathrm{H}\right\rangle_2 \pm \left|\mathrm{V}\right\rangle_1 \left|\mathrm{V}\right\rangle_2) \tag{1.3}$$

$$\left|\psi^{\pm}\right\rangle_{12} = \frac{1}{\sqrt{2}}(\left|\mathrm{H}\right\rangle_1 \left|\mathrm{V}\right\rangle_2 \pm \left|\mathrm{V}\right\rangle_1 \left|\mathrm{H}\right\rangle_2) \tag{1.4}$$

where the subscript 1 and 2 are used to indicate which particle is referred to. If we take, for example, the state $|\phi^+\rangle$ and measure one photon to be in the polarization state $|H\rangle$, the second photon will be immediately projected into the state $|H\rangle$, even if the particles are physically separated. This paradox of action at a distance became a source of debate in the early years of quantum mechanics [18, 19] but was later proven to be correct [20–24].

One remarkable results of quantum entanglement is that some of the entangled states, such as the Bell states, are capable of producing correlations that cannot be replicated classically using separable states. When using an entanglement-based QKD scheme, Alice and Bob can verify, by measuring these correlations, that their states where truly entangled. The presence of an eavesdropper would necessarily disrupt the entanglement and therefore would be revealed when Alice and Bob measure their correlation. This test of correlation is know as a Bell test because it's a measure of success is the violation of a Bell inequality [25].

In the BBM92 protocol [16], entangled pairs of photons are generated by a source, with one photon of the pair sent to Alice and the other to Bob. Alice and Bob each randomly

choose a basis in which to measure the photon they have received. In the cases that those bases align (which Alice and Bob reveal publicly after their measurement), entanglement ensures that Alice and Bob's measurement outcomes are fully correlated, thereby allowing them to establish a shared secret key. The difficulty in preparing and subsequently measuring high-quality entangled photons for entanglement-based QKD schemes is offset by a number of potential advantages; the most interesting of these is that the trustworthiness of the source can be determined by assessing the strength of the measured correlations via a Bell test [26]. Thus the source needs not be trusted and does not need to be located at either Alice's or Bob's site. In addition, QKD protocols based on entangled photons do not require random preparation of the state, as the correlation exists in all basis. Only the measurement bases need to be randomly chosen, something that can be achieved passively (using a non-polarizing beam-splitter). Therefore, these protocols do not require random number generators for secure implementation.

1.3 Global QKD

Various implementations of QKD have been performed [27–31] and technological advances have allowed, in the recent years, for QKD to reach the level of maturity sufficient for commercial implementation [32, 33]. Despite this, QKD currently suffers from a significant flaw: the method used to transmit the photon states are limited to distances of only a few hundred kilometers for direct links [34].

There are two practical methods of transmitting photons: through optical fibers or via free-space. Over short distances, optical fiber can often impart less loss than free-space. However, loss in fiber scales exponentially with distance and quickly renders long-distance transmission impractical. Current technologies allow QKD to be performed only at up to 250 km of fiber [35–37], with future advances predicted to only moderately extend this range to 400 km [34].

For free-space transmission, atmospheric absorption also scales exponentially, but other more significant loss contributors within this regime scale much slower—for example, beam divergence caused by diffraction, which scales quadratically. This gives free-space propagation the potential to be feasible at a larger distance regime than is currently possible with optical fiber. Yet, practical implementations on ground often exhibit atmospheric transmission losses that are too high for such long distances, and the difficulty of obtaining line-of-sight link between two points on Earth cannot be avoided. As of this writing, free-space QKD has been demonstrated up to 144 km [38, 39].

Three main strategies have been proposed to solve this long distance issue: networks of trusted nodes, quantum repeaters, and orbiting satellites. A network of trusted nodes would use a large number of individual QKD links, relayed between trusted nodes, to create a secure key between two parties [40–43]. As the distance between the two parties increases, the number of trusted nodes must also be increased. The drawback of this approach requires each of the trusted nodes to be secured, as a breach in even a single node would allow access to any key generated using the breached note.

Quantum repeaters utilize entanglement swapping [44] to effectively extend the distance of photon correlations without sending individual photons the entire distance [45]. Quantum memories, to store the photon state until it is required, are vital for this to take place efficiently, but despite extensive research and considerable improvements in recent years, this technology is not yet ready for practical application [46, 47].

In the orbiting satellite approach, a satellite is used to extend the range of QKD by acting as a node in a quantum network [48–55]. This general approach, with various potential implementations, is being actively studied by a number of groups worldwide [56–63] with projected launch dates as early as 2017 [60].

1.4 QKD using satellites

There are two approaches for using satellites to establish long-distance QKD links. The first approach takes advantage of the verifiability of entanglement correlations in schemes such as BBM92. This approach can be achieved by using an entangled source on a satellite to distribute photons to Alice and Bob. Alternatively, Alice and Bob can used a prepare-and-measure schemes to send photons to a satellite which performs an entangling Bell state measurement [64]. The result of this Bell state measurement allows Alice and Bob to determine, when they used the same basis, if their prepared states where the same or orthogonal (i.e. if one prepares $|\mathrm{H}\rangle$ the result of the measurement will indicate whether the other one prepared $|\mathrm{H}\rangle$ or $|\mathrm{V}\rangle$) without revealing either states. Both implementations of this approach allows QKD to be performed without the satellite gaining any information about the key, the satellite can therefore be untrusted. This approach is, however, challenging as it requires the satellite to establish and maintain two links simultaneously. In addition, the curvature of the Earth, which limits the distance between two parties who can both see the satellite, and the high loss experienced by both links significantly reduce the long distance capabilities of this approach, particularly when using lower orbit satellite.

In the second approach, both parties independently establish a secure key with a satel-

lite by using a single link when the satellite is in view. Once both keys have been exchanged, the satellite reveals a combination of the two keys, typically the bitwise sum. One user can then, knowing one of the keys, determine the other key. The two parties can then use this key to communicate securely. The other key is discarded since the known combination, which is revealed publicly, makes the two key related, i.e. using both keys would be equivalent to using the same key twice. The main drawback of this approach is the satellite also obtains a copy of both keys, and must therefore be trusted, that is, one must assume that an adversary is unable to manipulate the satellite. This is still the most common approach considered due to its simplicity, requiring only a single quantum link at a time. This makes it is technologically easier, more cost-effective, and therefore faster to deploy than the untrusted satellite schemes.

1.5 Demonstration of the feasibility of satellite QKD

To demonstrate the feasibility of satellite QKD using current technologies we first developed a detailed theoretical model to predict the performance of a such a system using a trusted node approach. This model, described in Chapter 2, includes a simulated satellite orbit, loss and background simulations, and an estimation of the secure key generation. The model is applied to both downlink and uplink scenarios and using both WCP (BB84) and entangled photon (BBM92) sources. In addition, we also investigate the capability of this satellite platform to perform long-distance Bell tests [25] and quantum teleportation experiments [44].

This theoretical feasibility was then demonstrated in the lab by implementing full QKD protocols at high losses using a free-space receiver similar in design to a quantum receiver on a satellite platform. This test, detailed in Chapter 3, showed the ability to perform full QKD at over 50 dB of constant loss. The experiment was also used to simulate a satellite pass by simulating the varying loss expected during such a pass.

With the ability to perform QKD at high loss came the concept of using a diffusive screen to perform "QKD off of a wall", where a QKD source is aimed at a diffusive screen, scattering the signal in a large angle. Multiple users would then be able to exchange keys simultaneously with little to no pointing. This concept was experimentally investigated and showed to be feasible but would require detectors with lower dark counts than those used in order to be demonstrated. The details of this concept, its feasibility, and its limitations, are briefly discussed in Chapter 4.

As a final experimental demonstration, a pointing system was built to demonstrate the

performance of QKD using a moving receiver platform. The QKD receiver was placed on a pickup truck and was driven along Westmount road, approximately 0.7 km from the transmitter, which remained at a fixed location on the roof of the Research Advancement Center 1. The receiver was moved at an angular speed similar to the maximum angular speed of a satellite platform. This work is detailed in Chapter 5.

The main results and conclusions are summarized in Chapter 6, and the future steps to enable the implementation of satellite QKD are discussed.

Chapter 2

Performance analysis of satellite QKD

This chapter describes the theoretical model used to predict the performance of satellite QKD. Section 2.1 explains the orbit used and how it is modeled. The estimation of the loss and background counts are detailed in Sections 2.2 and 2.3 respectively. In Section 2.4 we show how to estimate the secure key generation for QKD and the performance of two other important fundamental quantum experiments: Bell test and teleportation. Finally in Section 2.5 we show the important results and conclusions of the performance analysis.

Author contributions

Evan Meyer-Scott wrote the initial version of the MATLAB code used to predict the visibility and secure key rates. Bassam Helou wrote the initial version of the MATLAB code used to estimate the background. Brendon Higgins helped modify and improve various parts of the MATLAB codes used to estimate the loss and the background. Balaji provided the orbit analysis data. Thomas Jenewein, Brendon Higgins, Chris Ervin, Hannes Hübel, Jean-François Lavigne, Ralph Girard, Ian D'Souza and Danya Hudson provided advice on modeling the loss. I wrote the MATLAB code used to estimate the loss. I modified parts of the MATLAB code used to estimate the background and the code used to predict the visibility and secure key rates. I integrated the Matlab programs, and extracted and analyzed the results.

2.1 Orbit analysis

To predict the realistic performance of a satellite QKD we used a detailed one year orbit analysis that was provided by Balaji Kumar of COMDEV, using Systems Tool Kit (STK)

9 from Analytical Graphics, Inc. (AGI) [65]. The orbit considered is a circular, sun-synchronous noon/midnight low Earth orbit (LEO) at an altitude of 600 km. To reduce background noise, only nighttime passes are considered. A sun-synchronous noon/midnight orbit is defined as an orbit that crosses over the equator at noon and, after half of its orbital period, at midnight solar time. This orbit was therefore chosen because maximizes the nighttime passes by having the satellite intersect the Earths shadow during every orbit. The LEO orbit (500 km–1000 km) was chosen because of its lower loss, cost, and complexity; making this orbit a more realistic short term implementation of satellite QKD.

Low elevation angles typically exhibit losses too high to be used with any of the considered schemes, therefore we only incorporate satellite elevations greater than 10° above the horizon. Nights where the moon is strongly illuminated (full moon or close to it) are also ignored as the extra background light would prevent QKD. With these conditions we obtain a total of 713 usable passes over one year, or about 2 passes per night. We found that the results of the simulations are largely insensitive to the selection of orbit height—e.g. lowering the orbit to 500 km does improve the signal-to-noise ratio, but this effect is muted by the reduced contact time to the ground station.

Examples of passes for the 600 km orbit, including the best, upper quartile and median passes are illustrated in Figure 2.1. The best pass is the pass possessing the maximum usable duration, the upper quartile pass is the pass for which 25% of all satellite passes have longer usable duration, and the median pass is the pass for which 50% of all satellite passes have longer usable portions (and 50% have shorter usable portions). Figure 2.2 shows the range and elevation of these three pases over time.

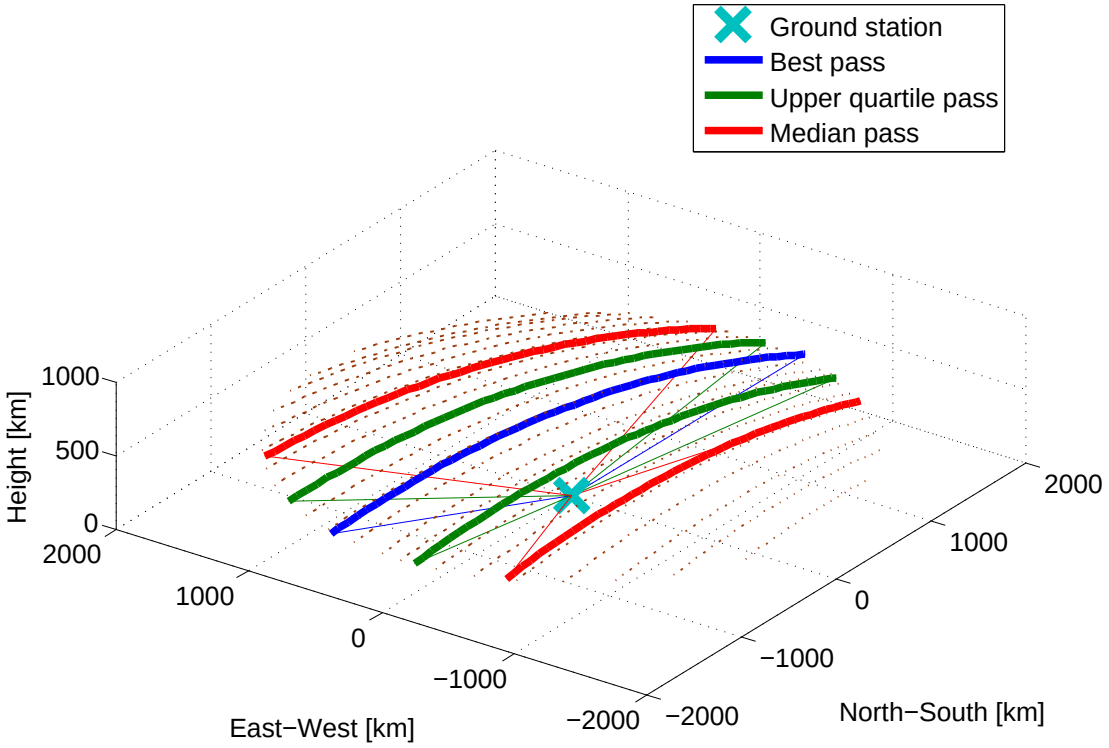

Figure 2.1: Illustration of satellite passes (top) over the ground location. Best, upper quartile, and median passes are shown as thick blue, green, and red lines, respectively (thin lines connect the ground station with the link termination points for these passes), with 20 additional example passes (brown dotted lines). The best pass transits directly over the ground station (i.e. reaching 90° elevation), while other passes fall to either side. The best pass, upper quartile pass, and median pass, are defined as having the longest, upper quartile, and median usable duration, respectively, of all passes over one year.

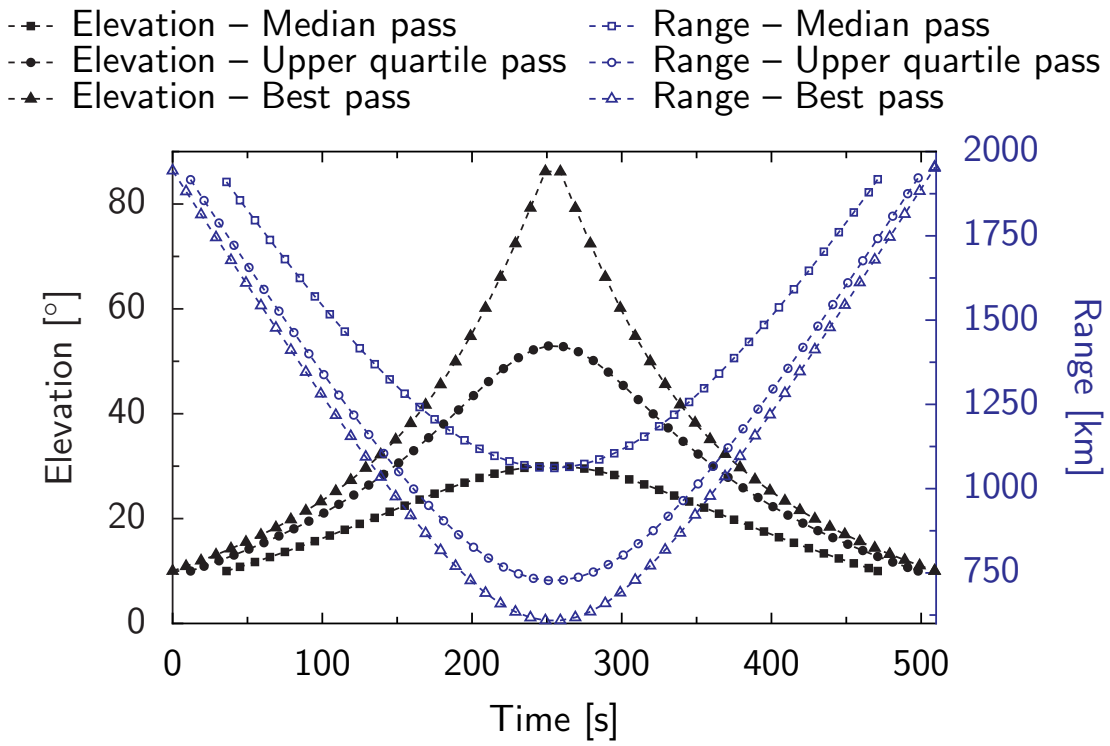

Figure 2.2: Range and elevation angle of the satellite relative to the ground location during the best pass, upper quartile pass, and median pass. Half of all passes have a duration of at least 450 s, only 80 s less than the best pass, yet less than 25% of passes reach 53° of elevation from zenith.

2.2 Estimating the loss

To accurately predict the loss that would be experienced by a quantum link between a satellite platform and a ground station, we had to include several effects that contribute to deterioration of the optical transmission. The first class of effects are geometric broadening caused by diffraction, systematic pointing error, and atmospheric turbulence. In addition, the optical transmission will be further reduced by atmospheric absorption and scattering, detector efficiency and the imperfections of the various optical components. This loss also depends on the telescope design, initial beam waist and type of source used. In this section we explain these loss contributers and show how each ones were taken into account in our analysis.

Figure 2.3 shows a sketch of the transmission from a satellite (left) and to a satellite (right), illustrating the various loss mechanisms encountered along the transmission channel. The variables used in the sketch corresponds to the variables that will be used in the equations. Not shown are the loss contributions that are not from the free-space channel: the detector efficiency (η_{d}) at the receiver and the optical losses (η_{o}) that combines the various imperfections in the polarization analyzer as well as those of both telescopes .

2.2.1 Diffraction

A collimated beam exiting a telescope will unavoidably have a certain divergence angle due to diffraction, causing it to expand as it propagates. This diffraction depends on the size and shape of the transmitting telescope aperture as well as the initial beam shape and its wavelength. To analyze this effect in detail we used the Rayleigh-Sommerfeld diffraction [66] to calculate numerically the beam profile after diffraction:

$$I_1(\vec{v}) = \left| \frac{d^2}{\lambda^2} \iint_{S_{\mathrm{t}}} \frac{\sqrt{I_0(\vec{v}\,')}}{|\vec{v} - \vec{v}\,'|^2} \exp\left(\frac{2\mathrm{i}\pi |\vec{v} - \vec{v}\,'|}{\lambda} \right) \mathrm{d}x\mathrm{d}y \right|^2 . \tag{2.1}$$

Here I is the intensity at the receiver, $\vec{v}$ is the location at the receiver, $\vec{v}\,'$ is the location at the transmitter, and we integrate over the surface of the transmitter, S_{t}. I_0 is the intensity at the transmitter, λ is the beam's wavelength, and d is the distance from the satellite to the ground station. By using the fact that the beam's profile has circular symmetry, we need only calculate the intensity at $y = 0$ (or $x = 0$) and determine $I(r)$ where r is the radius from the center of the beam.

The surface of the transmitter S_{t} can be be specified to any shape and size, allowing us to consider different telescope designs and properly determine their impact. Although it is

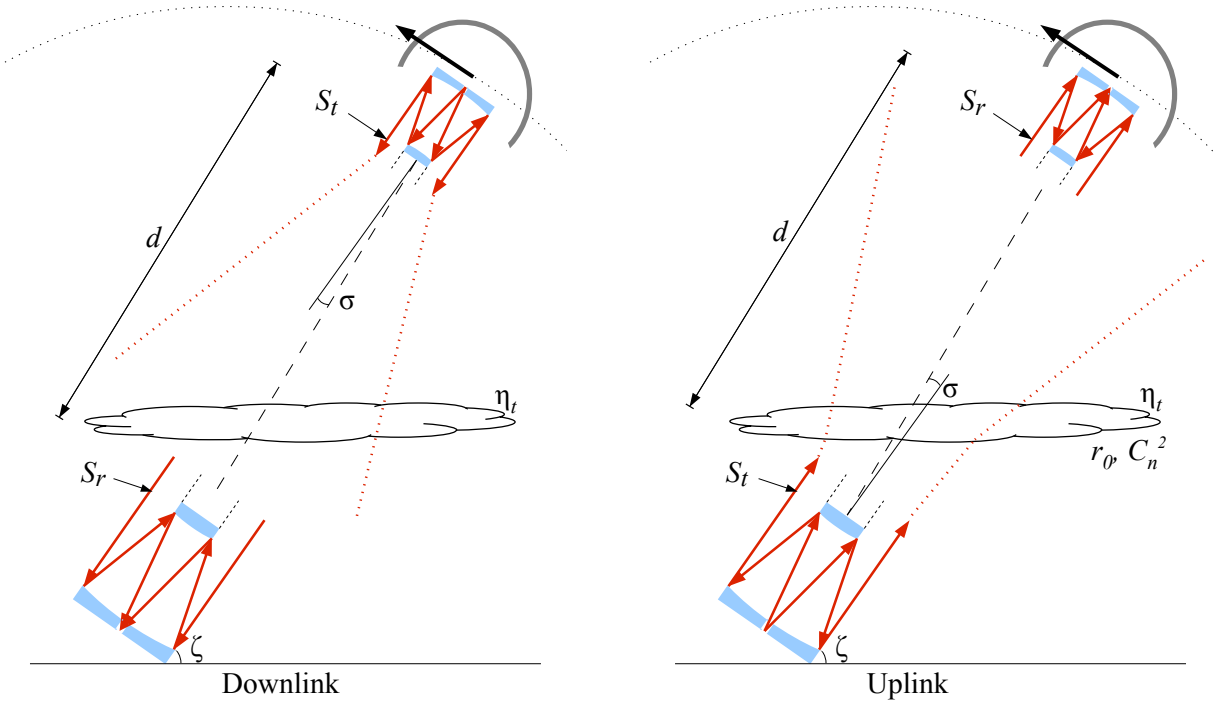

Figure 2.3: Sketch of the downlink (left) and uplink (right) transmission with a satellite. The variables follow those used in the text: S_t is the transmitter's surface, S_r is the receiver's surface, σ is the pointing error, d is the distance from the satellite to the ground station, and ζ is the elevation angle from ground. η_t is the atmospheric transmittance, and the atmospheric turbulence is characterized by r_0, the transverse coherence length, and $C_\mathrm{n}^2(z)$, the refractive-index structure constant.

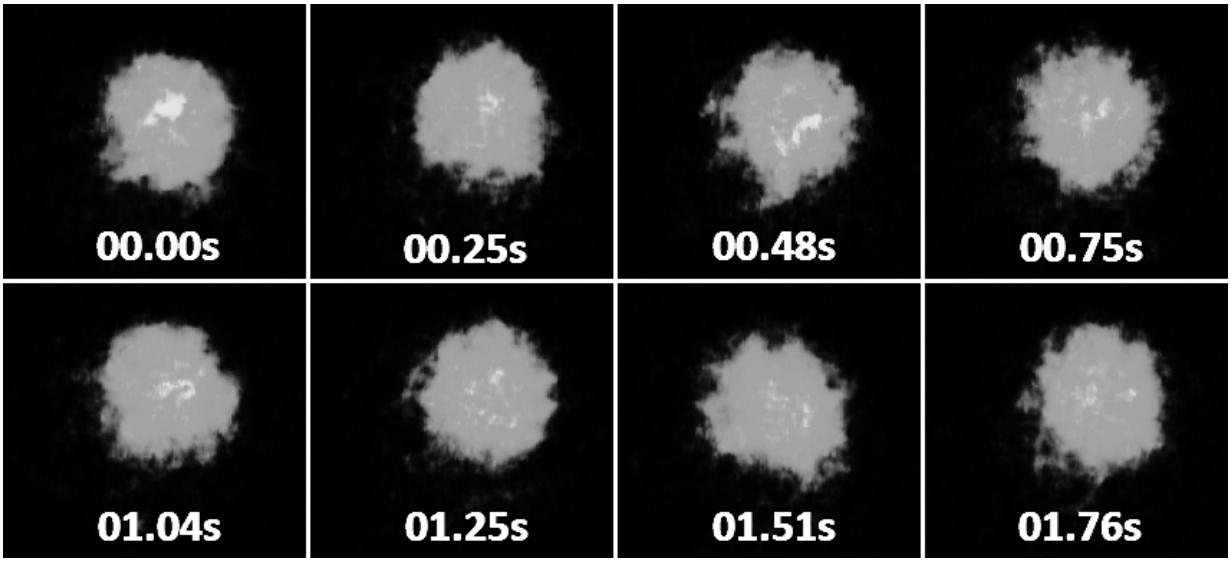

Figure 2.4: Effect of turbulence after 700 m on a beam. The shape of the beam and its intensity distribution rapidly change over time. The average beam size is approximately 30 cm in diameter. Wavelength of the beam used is 532nm. Timestamp in seconds

possible to reduce the effect of diffraction by using either a shorter wavelength or a bigger telescope, these solutions are not alway practical. A lower wavelength will suffer more from atmospheric turbulence and atmospheric attenuations due to Rayleigh scattering [67], while a larger telescope will come at an increased cost.

2.2.2 Atmospheric turbulence

Atmospheric turbulence is the beam broadening, beam wander and intensity fluctuations that occurs to a beam while it propagates through the atmosphere [67]. It is caused by local refractive index fluctuations that occur due to temperature variations. It as been shown that atmospheric turbulence has no negative effect on the polarization states used for QKD [68]. The effect of turbulence is thus limited to a source of additional loss. An example of the effects of turbulence is shown in Figure 2.4.

The beam broadening will cause divergence to the beam that will propagate until the beam reaches the receiver. Therefore, the effect of beam broadening will be much worse for an uplink, where the beam broadening occurs at the very beginning of the free-space channel. In contrast, a downlink will only encounter atmospheric turbulence during the last fraction of the free-space channel. The divergence from beam broadening will then only apply to this last fraction of the propagation path.

The beam wander caused by atmospheric turbulence can cause significant fluctuations in the received signal with time scales on the order of 10–100 ms. The signal fluctuation can have a significant negative impact on applications that require continuous signal (such as classical communications). This is not the case in QKD, where each photon contains information that is independent and uncorrelated to the other photons. The performance of QKD is therefore determined by the total received signal regardless to its distribution in time. Recent studies have even showed that short-term temporal fluctuations can increase the efficiency of QKD by using sophisticated filtering techniques to remove the periods of low signal, thus increasing the average signal to noise [69–72]. Here we have chosen to ignore temporal fluctuations and its possible improvement to obtain a lower bound on the performance of satellite QKD. When averaged over time, the beam wander can be modeled as more beam broadening.

The last effect of turbulence, intensity fluctuations, will cause the intensity distribution across the beam to fluctuate. This effect, also known as scintillation, does not increase the average loss. Since short-term temporal fluctuations in signal intensity do not have a negative effect on QKD, atmospheric scintillation effects can be ignored.

In addition to spacial fluctuations, atmospheric turbulence will also induce temporal fluctuations. This time-of-flight variation has been recently studied [73] and showed slow variations in the time of flight of ≈27 ps over the course of two hours with transmission distances of a few kilometers. This suggest that the time jitter due to atmospheric turbulence over the course of a satellite pass (5–10 min), where the atmospheric propagation distance is on the order of 20 km, would remain bellow 50 ps.

Calculating the time-averaged beam broadening due to turbulence is done by calculating the long term beam width w of the distribution at the receiver [67, 74]

$$w = \frac{2\sqrt{2}d\lambda}{\pi\rho_0}, \tag{2.2}$$

where ρ_0 is the transverse coherence length,

$$\rho_0 = \left[1.46\sec(\frac{\pi}{2} - \zeta)\left(\frac{2\pi}{\lambda}\right)^2 \int_0^h C_{\mathrm{n}}^2(z)\left(1 - \frac{z}{h}\right)^{\frac{5}{3}} \mathrm{d}z\right]^{-\frac{3}{5}}, \tag{2.3}$$

with ζ the elevation angle of the satellite from the ground, h the altitude of the receiver, and $C_{\mathrm{n}}^2(z)$ the refractive-index structure constant. The transverse coherence length can be related to the more widespread used atmospheric coherence length, or Fried coherence length, (r_0) with the relation $r_0 = 2.1\rho_0$ [67, 75]. Both quantities can be used to describe the strength of the turbulence. The atmospheric coherence length has the added advantage of

representing the the maximum size of the transmitter for which diffraction dominates over turbulence. In the limit of transmitter diameters much greater than r_0, diffraction will be negligible compared to turbulence and the beam divergence will be completely determined by turbulence, a process that is independent of the transmitter size. This imposes an effective limit on the size of the transmitter: transmitters with diameters larger than r_0 will have their geometric loss dominated by turbulence and increasing the transmitter size further will yield little to no improvement in performance.

This effect is shown in Figure 2.5 for an uplink with three different strength of turbulence (r_0=5 cm, 10 cm and 15 cm). Both figures show reduced gain from increasing transmitter size beyond the the atmospheric coherence length, with negligible gain for increases beyond 5 times r_0.

It can be seen from Equation (2.2) and 2.3 that the width of the distribution from turbulence scales as $\lambda^{-\frac{1}{5}}$. This small dependence on the wavelength means that shorter wavelength will be more affected by atmospheric turbulence. Because of this dependence, it is sometimes beneficial to use a higher wavelength to reduce atmospheric turbulence despite the increased diffraction caused by longer wavelengths.

The refractive-index structure constant ($C_{\mathrm{n}}^2(z)$) is a crucial parameter for atmospheric turbulence as it allows to predict the strength of turbulence for any propagation distance. There are many models designed to predict $C_{\mathrm{n}}^2(z)$, the most widely used being the Hufnagel-Valley model of atmospheric turbulence [67, 74]. This model of atmospheric turbulence predicts the profile of $C_{\mathrm{n}}^2(z)$ based on two parameters that depend on the atmospheric conditions: The upper level wind speed v, given as the root mean square wind speed averaged over the 5-20 km range, and the surface value of the refractive-index structure constant ($A = C_{\mathrm{n}}^2(0)$)

$$C_{\mathrm{n}}^2(z) = 0.00594(v/27)^2(z \cdot 10^{-5})^{10}\mathrm{e}^{-z/1000} + 2.7 \cdot 10^{-16}\mathrm{e}^{-z/1500} + A\mathrm{e}^{-z/100}. \tag{2.4}$$

For this work we used two typical values of these parameters at sea-level during night-time [76]: $A = 1.7 \times 10^{-14}$ $\mathrm{m}^{-\frac{2}{3}}$ and $v = 21$ m/s. These values produce atmospheric coherence length (r_0) between 5 cm to 15 cm for most elevation angles. In these conditions, increasing the telescope diameter beyond 25–75cm (5 times r_0) will have negligible impact on the performance of the system (see Figure 2.5).

The distribution from turbulence is a two-dimensional Gaussian distribution of width w:

$$g_t(r) = \frac{2}{\pi w^2} \exp\left(-\frac{2r^2}{w^2}\right). \tag{2.5}$$

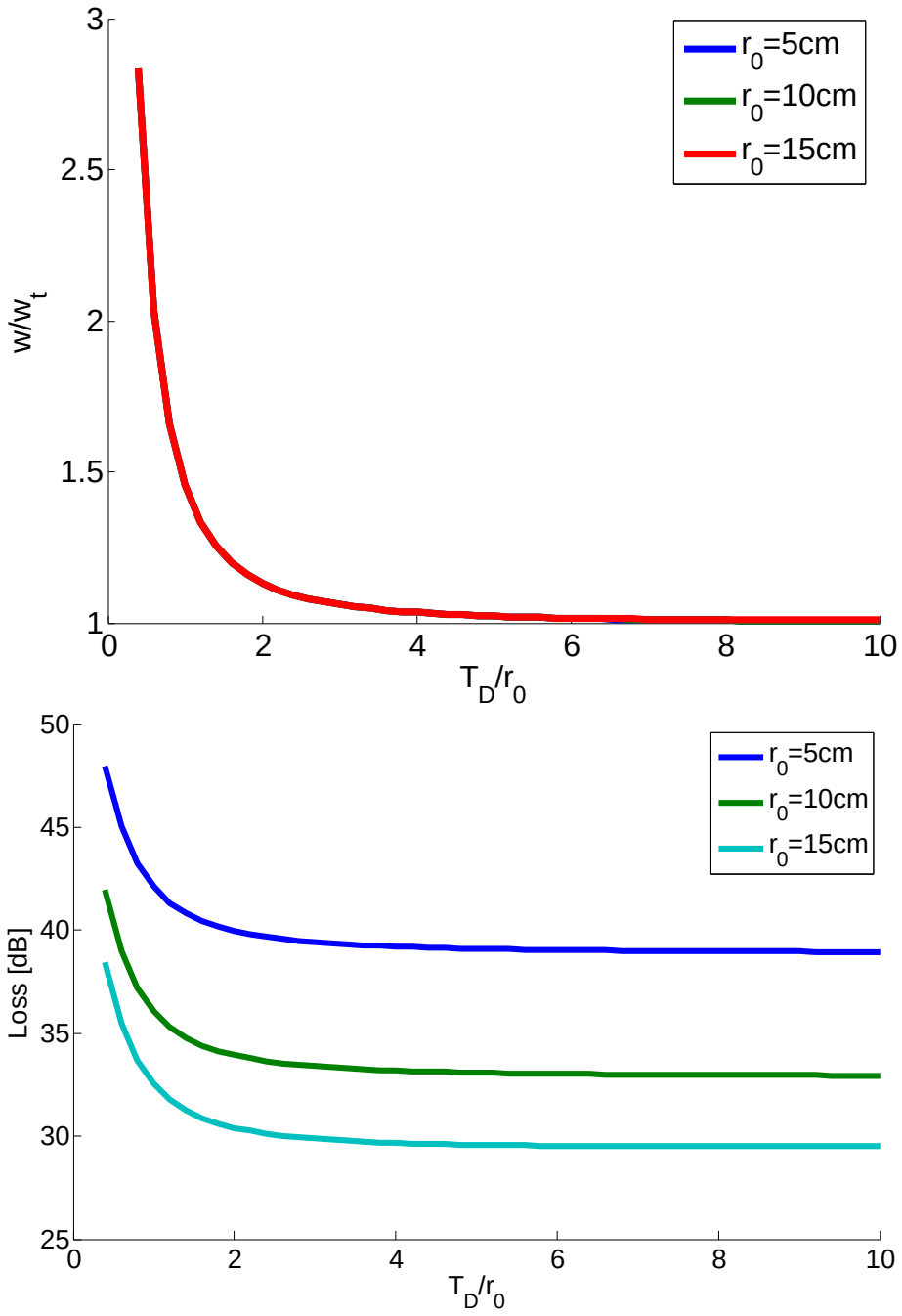

Figure 2.5: Effect of Increasing the transmitter diameter (T_D) beyond the atmospheric coherence length (r_0). The top figure shows the effect on the beam waist (w) to the turbulence distribution width (w_t) ratio (shown to be insensitive to r_0, with all three traces overlapping), and the effect on the link loss is shown in the bottom figure. The gain from increasing the transmitter size is reduces for transmitter diameters greater than r_0. Wavelength, 785 nm, satellite receiver diameter, 20 cm, propagation distance, 1000 km.

The beam profile with atmospheric turbulence $I_2(\vec{v})$ is then obtained by taking a two-dimensional convolution [77] of the beam after diffraction with the distribution of the beam at the receiver caused by atmospheric turbulence:

$$I_2(\vec{v}) = (I_1 * g_t)(r, \theta) = \int_0^{2\pi} \mathrm{d}\theta' \int_0^{\infty} I_1(r') g(r - r') \mathrm{d}r'. \tag{2.6}$$

As the density of the atmosphere gets smaller with increasing altitude, the atmospheric turbulence also gets weaker with the stongest turbulence occurring near the surface. The lower 20 km of the atmosphere is where atmospheric turbulence predominately occurs [67], thus its impact on a downlink will only occur during the last fraction of its propagation distance. The linear dependence of Equation (2.2) on d means that for the same turbulence strength (i.e. the same coherence length), the width of the distribution from turbulence in a downlink from a 600 km altitude LEO satellite will be roughly 20 km/600 km=1/30 times the width for an uplink. In this regime the contribution to geometric losses from turbulence is negligible compared to diffraction. We therefore ignore atmospheric turbulence in the case of a downlink ($I_2(\vec{v}) = I_1(\vec{v})$).

In the case of an uplink transmissions, the effects of turbulence propagate over the entire optical path leading to an important contribution to geometric losses. It is possible to reduce the effect of turbulence by choosing a ground station in a location with better atmospheric conditions or higher altitude. This improvement may not alway be possible as certain locations that would benefit from the implementation of a global QKD link will not have access to a good site for a ground station. An adaptive optics system could also be used to compensate the effects of turbulence [75], but would come at an increased cost.

2.2.3 Pointing error

The last geometric broadening effect is caused by misalignment between the transmitting and receiving telescopes. This is due to imprecision in the tracking system and jitter in the telescopes. This pointing error, typically fluctuating on a time scale of ∼0.1–1 s, can be averaged over time as additional beam broadening. This can be reduced with higher-quality tracking and pointing systems, which however incur increased cost and complexity. Controlling for jitter is more challenging on a satellite, thus a downlink will be more vulnerable to this effect.

The loss from the pointing error is calculated by first determining the distribution over time of the beam center at the receiver. We assume a two-dimensional Gaussian

distribution of pointing, given by

$$g_p(r) = \frac{1}{2\pi\sigma^2} \exp\left(-\frac{r^2}{2\sigma^2}\right), \tag{2.7}$$

where σ is the standard deviation caused by pointing error. As was the case for atmospheric turbulence, The beam profile with pointing error $I_3(\vec{v})$ is obtained by taking a two-dimensional convolution of the beam after diffraction and turbulence ($I_2(\vec{v})$) with the distribution of the pointing error:

$$I_3(\vec{v}) = (I_2 * g_p)(r,\theta) = \int_0^{2\pi} \mathrm{d}\theta' \int_0^{\infty} I_1(r')g(r-r')\mathrm{d}r'. \tag{2.8}$$

Once all geometric broadening effects have been taken into account, we can use the profile of the beam at the receiver ($I_3(\vec{v})$), to obtain the received optical power (P) by integrating the beam profile over the receiving area:

$$P = \iint_{S_\mathrm{r}} I_3(\vec{v})\mathrm{d}x\mathrm{d}y, \tag{2.9}$$

where S_r is the surface of the receiver. This surface can again be specified to any shape and size to accommodate various telescope designs. The resulting power is proportional to the average number of detected photons.

Figure 2.6 shows the excess loss due to transmitter systematic pointing error (the loss added to the system from pointing error compared to the same system with perfect pointing accuracy) for a downlink (top) and for an uplink (bottom). In a downlink, the impact depends strongly on the transmitter size which determines the contribution of diffraction. To minimize loss, it is sufficient to reduce the pointing error such that diffraction becomes the dominant source of broadening. In the case of an uplink however, the dominating beam broadening effect, for transmitters of 20 cm or more, is atmospheric turbulence. We then simply need to reduce pointing error below the influence of atmospheric turbulence. We have found that pointing accuracies of better than 2 μrad root mean square (RMS), would cause 1–4 dB of loss in a downlink for up to a 20 cm transmitter, and less than 1 dB of loss in an uplink for all transmitter sizes. This pointing accuracy as been demonstrated in previous satellite experiments [78] and is therefore feasible. For the rest of our analysis, this value is applied for the transmitter pointing accuracy.

The receiver pointing accuracy in much more relaxed as it only needs to point to an accuracy within its field of view which is typically much greater than 2 μrad. For our analysis we assume 50 μrad of field of view. This value was chosen to keep the received background light to a manageable level, while keeping the complexity of the system as low as possible.

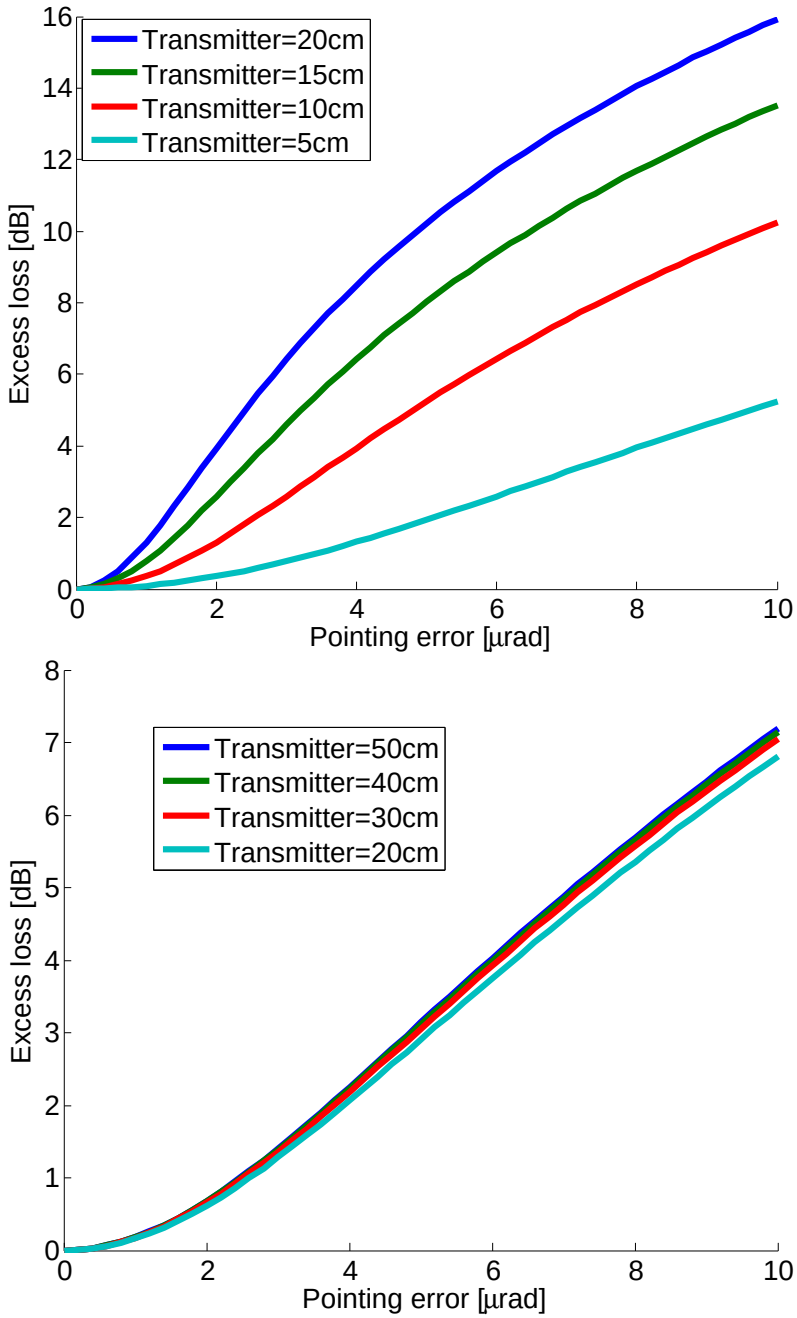

Figure 2.6: Excess loss due to systematic pointing error of the transmitter for various transmitter sizes at 40° from zenith in a downlink (top) and in an uplink (bottom) assuming a two-dimensional Gaussian distribution of the pointing error. For our performance analysis we assumed a pointing error of 2 μrad, inducing only up to 4 dB of loss in a downlink and less than 1 dB of loss in an uplink. For downlink: wavelength is 670 nm, ground receiver diameter is 50 cm. For uplink: wavelength is 785 nm; satellite receiver is 30 cm. In both cases, the orbit altitude is 600 km and the atmosphere is rural sea-level.

2.2.4 Atmospheric transmission

In addition to atmospheric turbulence, a beam propagating through the atmosphere will also suffer non-geometric losses due to scattering and absorption [67]. The two main types of scattering in the atmosphere are Rayleigh and Mie scattering. Rayleigh scattering are caused by small molecules and particles and are responsible for the sky's blue appearance. This type of scattering is more significant for light with a smaller wavelength, limiting the improvement one can obtain from reducing diffraction with a smaller wavelength. Mie scattering, responsible for the white glare around lights, is caused by larger particles and is largely wavelength independent [79].

Atmospheric absorption is largely dependent on the concentration of the various constituents of the atmosphere. Many molecules contribute to atmospheric absorption, creating widows of high and low transmission. Water vapor and carbon dioxide are the main contributors to molecular absorption in the visible and infrared ranges [67]. To ensure manageable loss it is crucial to chose a wavelength away from the low transmission windows.

Given the complexity of the atmosphere, several programs have been developed to predict atmospheric transmission with good accurately based on user given atmospheric composition. One widely used commercial program to predict atmospheric transmission is MODTRAN [80]. Using MODTRAN 5, we modeled atmospheric transmittance of a rural sea-level location with a visibility of 5 km. We chose this atmosphere type to reflect the possibility of a ground station close to a large city. There exist many locations with significantly better atmospheric conditions than the one described by this model. This type of atmosphere thus represents a worst case scenario of atmospheric transmission. The interest of having ground stations close to a city, despite the worst atmospheric conditions, is to enable the possibility of city-wide QKD networks globally connected using satellite QKD. The MODTRAN parameters we used are listed in Appendix D.

The results of the MODTRAN calculations are shown in Figure 2.7. The left side of the figure shows the dependence on wavelength, revealing several low-loss transmission windows. Of particular interest are the widows at 665–685 nm, 775–785 nm, 1000–1070 nm, and 1540–1680 nm, all of which support wavelengths of commercial laser diodes. The dependence on the transmission angle is shown on the right side of the figure.

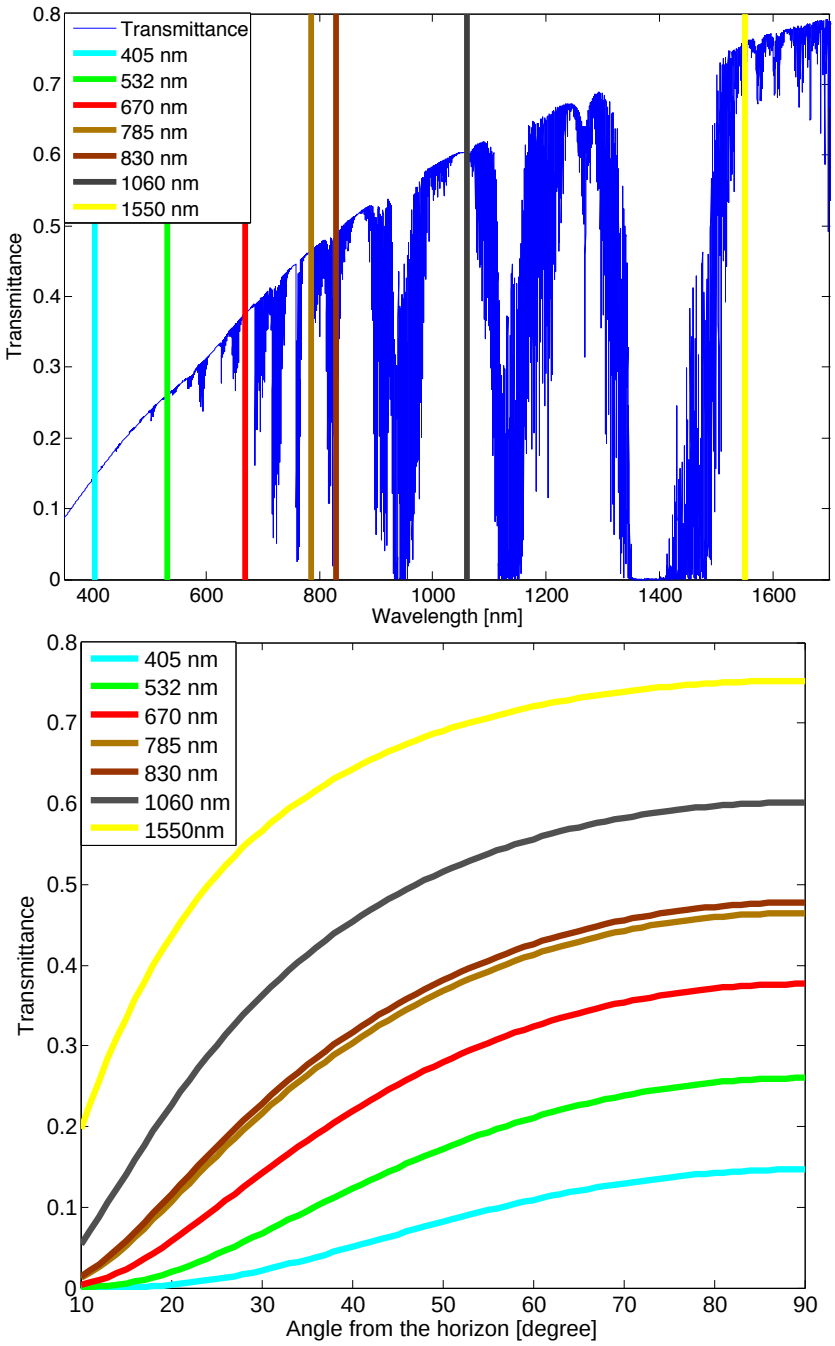

Figure 2.7: Simulated atmospheric transmittance at a typical rural location, for propagation at zenith (top) and for different elevation angles (bottom). Coloured lines represent wavelengths of commercially available laser systems. Several transmission windows are evident, within which optical transmission would experience low loss. Generally, the transmission tends to be better at higher wavelengths, but other factors (e.g. diffraction, sources, detectors) must be taken into account to properly determine the best wavelength choice.

Table 2.1: Summary of the comparison between single-photon detectors showing typical values of their main parameters. The manufacturer of the detector used for comparison is referenced in the detector column.

Detector	**Wavelength [nm]**	**Peak efficiency [%]**	**Dark counts [cps]**	**Timing jitter [ps]**	**Cooling method**
Thin Si APD [82]	550	50	20	50	Thermoelectric
Think SI APD [83]	700	70	20	350	Thermoelectric
InGaAs APD [32]	1300	20	200	200	Thermoelectric
PMT [84]	600	40	100	300	Thermoelectric
HPD [84]	500	45	30	120	Thermoelectric
MCP-PMT [84]	500	40	10	100	Thermoelectric
SSPD [85]	1550	90	100	50	Cryogenic

2.2.5 Detectors and optical components

The measurement of single photons requires very sensitive detection devices [81]. These devices suffer from imperfect detection efficiency that must be taken into account in the performance estimation. In addition to detection efficiency, the choice of detector is strongly affected by dark counts rate, i.e. the number of false counts per second caused by thermal processes. Two other important parameters are timing jitter (the uncertainty in the timing information of the detection) and the maximum count rate of the detector (which should be above the expected detection rate).

Single-photon detectors are an active area of research producing rapid improvements. However, a satellite mission requires detectors that are well tested to mitigate the risk of failure. For this overview, we focus on the currently available commercial single-photon detector, which could be tested and space qualified before a satellite mission.

There are two main ranges of wavelength with commercially available detectors. Silicon (Si) avalanche photodiodes (APD) technologies are typically used for the visible range (400–1000 nm) while the near-infrared wavelengths (950–1650 nm) are typically detected using Indium gallium arsenide (InGaAs) APD or, more recently, by superconducting single-photon detectors. A summary of typical detector characteristics is shown in table 2.1.

Si APD is a mature technology capable of >50% detection efficiency with low dark

counts, low timing jitter (<50 ps), and maximum count rates in the MHz range [9, 81, 86]. On the other hand, InGaAs APD currently suffer from lower detection efficiencies, higher dark count rates, and low repetition rates [9] limiting their usefulness for satellite QKD. This may change in the future as some new techniques, such as self-differencing [87], are improving InGaAs detectors.

Photomultiplier tubes (PMT) are a well established technology that can provide an alternative to APD [81, 84]. However, their detection efficiency is typically lower than Si-APD and PMT can contribute additional noise due to afterpulsing. Hybrid photodetectors (HPD) and micro-channel photomultiplier tubes (MCP-PMT) are promising technologies that incorporates PMT in their design but they also suffer from the same drawback.

Superconducting single-photon detectors (SSPD) are a promising technology that has made considerable progress over the last few years [85, 88–95], reaching high efficiency, low dark counts, and broad-spectrum sensitivity. Despite this progress, current superconducting detectors are in the research stage, and all such devices require cryogenic cooling to operate [9]. This makes them impractical for low cost satellite missions, particularly in the case of an uplink, where the detectors (and their cooling system) are located on the satellite.

Because of the current difficulties of measuring in the near-infrared ranged, we focus on the visible range, taking advantage of Si APD that have low technological requirements for a satellite mission and support wavelengths of multiple free-space transmission windows (see Figure 2.7). Two types of Si APDs were studied: thin APD (from Micro Photon Devices) detection efficiencies are used for wavelengths below 500 nm [82], and thick APD (from Excelitas Technologies) efficiencies for 500 nm and above [83]. Typical detection efficiency of these detectors are shown in Figure 2.8.

In addition to imperfect detection efficiency, there will also be various loss contributions from the various optical components of both telescopes. These include imperfect filter transmission at the signal wavelength, non-ideal beam-splitter, lens and mirror transmission and reflection, and imperfect coupling from the telescope to the detectors. These are typically low individual contributions (often no more than a few percents in one given component) but can add up to a non-negligible contribution. To ensure these extra contributions are taken into account we include an extra 3 dB of loss (≈50% transmission) due to optical components which is beyond what these various imperfections typically lead to.

The various non-geometric losses (atmospheric transmission, detector efficiency and optical losses) are then added to the geometric losses by multiplying the received power (P) with the atmospheric transmittance η_{t}, the detector efficiency η_{d} and the optical efficiency

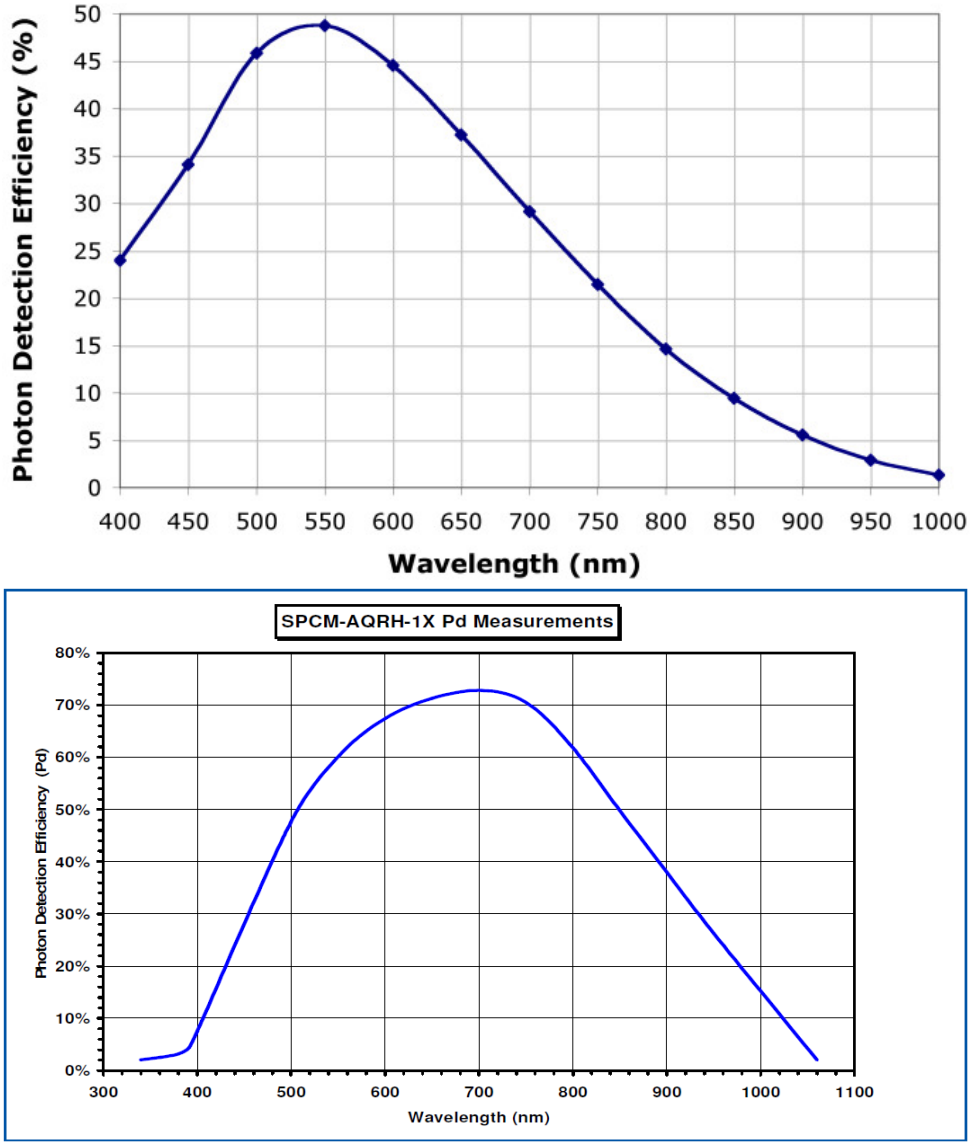

Figure 2.8: Detection efficiency curve for a thin Si APD (top) [82] and from a thick Si APD (bottom) [83]. A thin APD is better suited for shorter wavelength (400–500 nm) while the thick APD is better suited for longer wavelength (500–900 nm). Graphs taken from the detector's respective data sheets [82, 83]

.

η_o.

$$P_{\text{final}} = P\eta_t\eta_d\eta_o. \tag{2.10}$$

Finally the ratio of the final power to the initial power (P_0) is converted into loss in dB

$$L = -10\log_{10}\left(\frac{P_{\text{final}}}{P_0}\right). \tag{2.11}$$

2.2.6 Effect of the initial beam shape and telescope design

The numerical nature of the simulation used to calculate loss allow us to model the impact of the telescope design and the impact of the initial beam shape and size. Here we use this feature of our model to determine the optimal beam size and the impact of an aperture obstruction on in telescope design.

Optimal beam waist at the transmitter

The most common shape of laser beams is a Gaussian beam distribution of a certain beam waist. This beam waist can be engineered by changing the curvature of the lenses/mirrors of the telescope. This beam waist can therefore be optimize to reduce the loss. Using our model, we evaluated the loss performance when varying the initial beam waist of a Gaussian beam, measured as full width at half maximum (FWHM) of the intensity of the beam.

The results, shown in Figure 2.9, reveal a significantly different behavior for an entangled photon source compared to a weak coherent pulse (WCP) source. In a downlink, (Figure 2.9 top), an entangled photon source is shown to have optimal loss with a beam waist of half the diameter of the transmitter. This is consistent with existing literature [96] for classical communication to and from a satellite. This is because a beam that is too large will be clipped to the size of the transmitter telescope, while a beam that is too small causes exaggerated diffraction.

This behavior is not exhibited by a WCP source, where we find that the loss due to beam waist becomes effectively constant for any FWHM beam waist greater than the transmitter telescope diameter. The reason for this unusual behavior comes from the fact that the WCP source is attenuated to emit less than one photon per pulse (on average), and the loss from clipping the outer portion of the beam can be utilized as attenuation towards this end. Therefore, the clipping losses at the telescope can be compensated by increasing the intensity because only the outgoing intensity counts. The beam waist may be made so large, whilst increasing source intensity to compensate, that it essentially becomes a plane

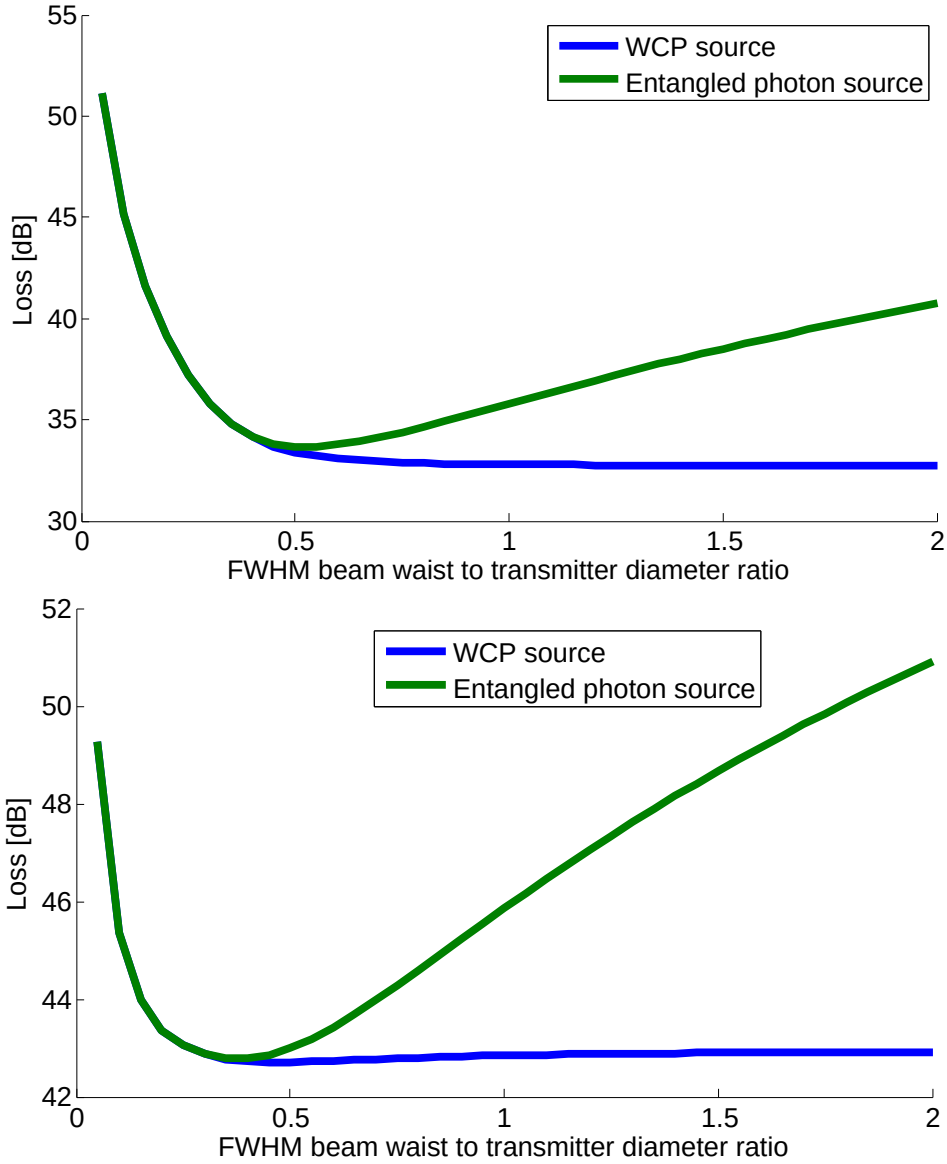

Figure 2.9: Loss at 40° from zenith as a function of the outgoing beam waist (FWHM) for a downlink (top) and an uplink (bottom). The WCP performs better than the entangled source at large beam waist because the loss from clipping can be included in realizing the required attenuation. The optimum for a downlink is to have a beam waist as large as possible for a WCP source and a beam waist of half the telescope diameter for an entangled photon source. In an uplink, the best beam waist for both sources is smaller then their corresponding value for a downlink because of atmospheric turbulence effects. For downlink: wavelength, 670 nm; satellite transmitter diameter, 10 cm; ground receiver, 50 cm. For uplink: wavelength, 785 nm; satellite receiver, 30 cm; ground transmitter, 25 cm. In both cases, orbit altitude is 600 km with no pointing error. Atmosphere is rural sea-level.

wave where diffraction is entirely due to the transmitter's size. Because the loss for large beam waist approaches a constant, it is sufficient to increase the beam waist up to the transmitter's diameter to achieve close to minimal loss.

In an uplink, diffraction broadening is dominated by atmospheric turbulence, reducing the advantage of a larger transmitting telescope. This limit on the effective telescope size is reflected in the optimal beam waist shown in Figure 2.9 (right). The optimal beam waist reflects the size of the beam where diffraction becomes negligible compared to turbulence, and increasing the beam size further has almost no effect on the final beam broadening from all sources. Because of this, it is actually better to keep the beam waist smaller, with less clipping, even if doing so increases diffraction. For a small telescope or weak turbulence, diffraction will dominate once more and we will enter the same regime as the downlink, where the optimal FWHM beam waist is the transmitter diameter for the WCP source and half of the transmitter diameter for the entangled photon source.

The influence of atmospheric turbulence depends on the propagation angle through the atmosphere. Propagations at elevation angles further from zenith will have a longer path through the atmosphere and will therefor experience more turbulence effects than propagations at elevation angles closer to zenith. Because of this, the optimal ratio of the beam waist to transmitter size in an uplink will be dependent on the elevation angle of the satellite. Since this elevation angle changes continuously during a satellite pass, keeping an optimal beam waist would also require continuous readjustment. Figure 2.9 (right) shows that the improvement in using the optimal beam waist is less than 1 dB compared to the performance of beam waists that were optimal without turbulence (FWHM equal to the transmitter diameter for a WCP source and half the transmitter diameter for an entangled photon source). Maintaining the optimal beam waist is therefore a significant complication that is unlikely to return major improvements.

For this work, we use the same FWHM beam waist for uplink as the optimal values for a downlink: a FWHM equal to half the transmitter diameter for an entangled photon source and a FWHM equal to the transmitter diameter for a WCP source. In these configurations the diffraction remains based on the telescope size and not on the beam waist. This represents a design where one desires to achieve small losses without the technically difficult re-optimization of beam waists with changing elevation angles.

Telescope design with an obstruction

There exists two main categories of telescope design: refractive telescopes, built using one or more lenses, and reflective telescopes, built using mirrors [97]. Large refractive

telescopes are difficult to manufacture because they require large high quality lenses with precisely shaped surface on both sides. Large mirrors only require one reflective surface to be precisely shaped making them much easier to manufacture. In addition, large lenses can be considerably heavier than mirrors and can only be mounted at their edge, leading to instability and the possibility of deformation. Mirrors however can be mounted using their back surface, proving far better stability. Because of these factors, most modern telescopes are typically made using a reflective design.

Telescopes with reflective designs use a primary mirror that reflect and focus the beam on a secondary mirrors, which then redirect the light where it can be analyzed [97]. Many such design have the secondary mirror placed in the path of the incoming beam, creating an obstruction (see Figure 2.10, top). The likelihood of such a design provides motivation to analyze the impact of such an obstruction on the loss performance. To analyze the maximum impact of an obstruction, we use a design where the obstruction is placed at the center of the beam, thus blocking the most intense part of the signal. This design then provides a lower bound on the performance when using a reflective telescope.

The obstruction caused by a secondary mirror in the transmitting telescope has two effects: it blocks a portion of the beam (Figure 2.10, bottom) and it alters the diffraction (Figure 2.11, top). Our analysis show that the resulting performance from both effects depends only on the ratio of primary and secondary mirror diameters. The additional loss from such an impact is shown in Figure 2.11 (bottom). For reasonable primary/secondary mirror ratios, the secondary obstruction has little impact. Just as was the case for the beam waist, the impact of blocking the central part of the beam is smaller for the WCP source than for an entangled source because the transmission power can be adjusted to counteract the obstruction loss.

The size of the beam reaching the receiving telescope is typically on the order of 10 m. This is much larger than any considered receiving telescope. In this regime, the part of the beam entering the telescope has an almost constant intensity distribution. The loss due to a reflective telescope design at the receiver is therefore almost entirely dependent on the area of the obstruction in the telescope. The additional loss in this case is then proportional to the ratio of the area with obstruction compared to the area without obstruction:

$$L_{\text{obstruction}} = L + (-10 \log_{10} \left(\frac{A_{\text{obstruction}}}{A} \right)), \tag{2.12}$$

where $L_{\text{obstruction}}$ is the loss with obstruction, L is the loss without obstruction, $A_{\text{obstruction}}$ is the area of the telescope when there is an obstruction (equal to the total area of the telescope minus the obstructed area), and A is the area of the telescope in the case with

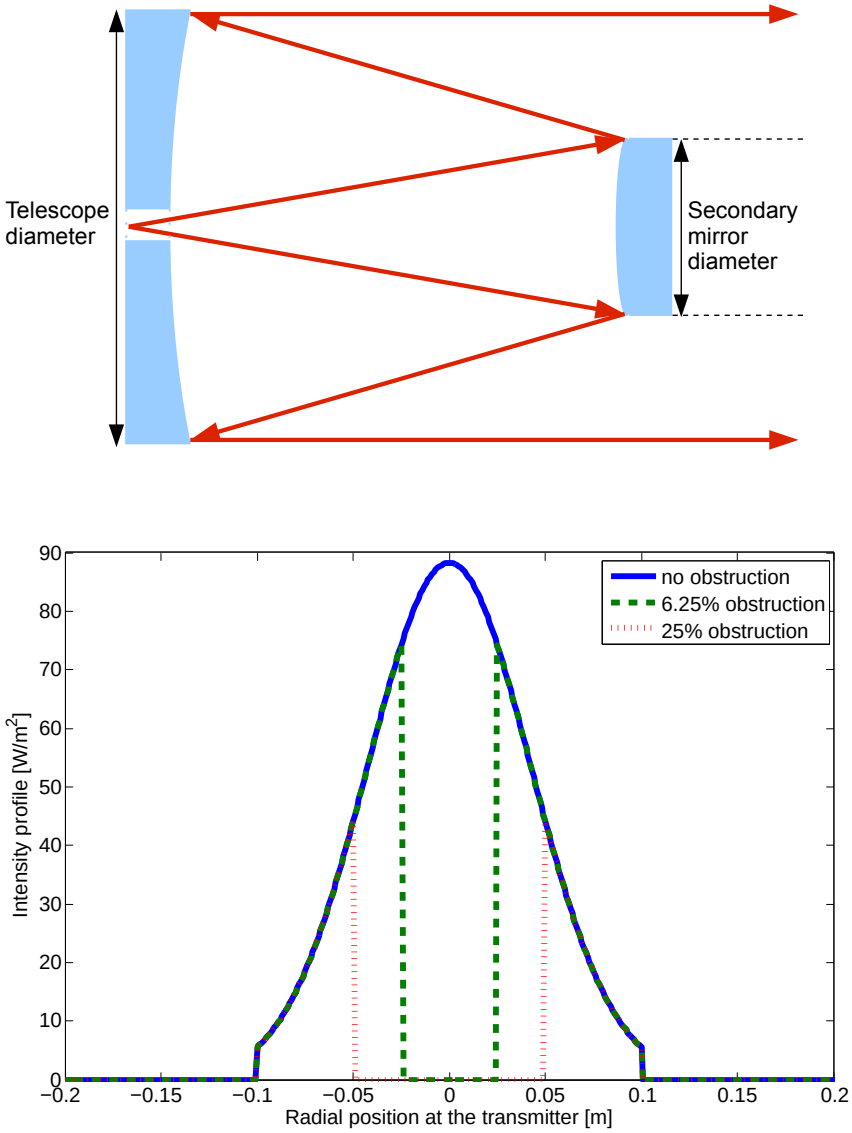

Figure 2.10: Cassegrain telescope design (top), which has a central secondary mirror blocking a portion of the outgoing beam, and the accompanying intensity profile at the transmitter (bottom).

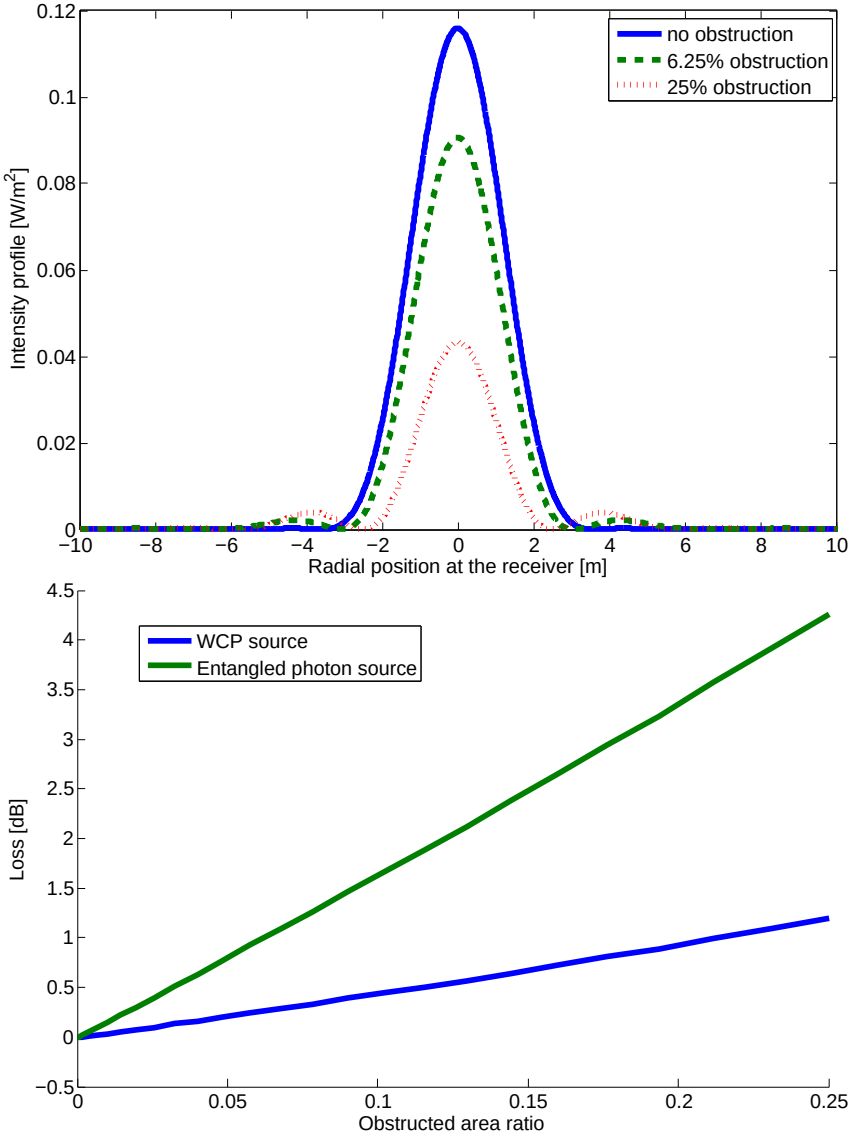

Figure 2.11: Beam intensity profile at the receiving telescopefrom a transmitter with a central secondary mirror blocking a portion of the outgoing beam (top) and the additional loss due to this type of transmitting telescope was evaluated for both WCP and entangled photon sources (bottom). The impact of this design is less than 1 dB for an obstruction of up to 6.2% of the area (i.e., a secondary mirror with a diameter of up to 25% the diameter of the primary mirror). Theses results are at a distance of 600 km, with a wavelength of 670 nm and a 20 cm transmitter. The additional loss (in dB) from this type of transmitter is independent of distance, wavelength, receiver and transmitter size, provided that we are in the regime where the received beam is larger than the receiver. In our case (distances greater than 500 km and visible wavelengths), this condition is valid for receivers of up to 1–2 m (for any transmitter size).

no obstruction.

2.2.7 Results of the loss analysis

Combining all loss mechanisms we can obtain the total loss expected from a satellite QKD link at any given point of the satellite passes. Figures 2.12 and 2.13 shows the total predicted loss (light blue) at various elevation angles (with the length of the transmission adjusted to correspond to a satellite at a 600 km orbit appearing at the given elevation angle). Also shown are the loss when we include only diffraction (dark blue), including all geometric effects (in green) and including all channel effects (in red).

Values of the losses for the various contributors are shown in Tables 2.2 and 2.3 for elevation angles of 90°, 55° and 30° from the horizon. The contributions of the individual geometric effects are shown as their contributions if they were the only geometric effect present, allowing us to better compare them and identify the dominant effect. In a downlink, the dominant effect is diffraction, which can be mitigated by increasing the size of the transmitter. In first order, doubling the transmitter (from 10 cm to 20 cm) would reduce the loss by a factor 4 (≈6 dB). Doing so would reduce the diffraction loss to less than the pointing error, and would require improvements to the pointing accuracy to further reduce the geometric loss. In an uplink, the geometric loss is dominated by atmospheric turbulence, which can only be mitigated by choosing a location with better atmospheric conditions or higher altitude, or by using an adaptive optics system to compensate the effect of turbulence [75]. The increase in diffraction loss with an entangled photon source is due to the smaller beam size (chosen to reduce loss from clipping). This reduced beam size causes diffraction to be limited by the beam waist rather than the transmitter.

The full MATLAB code used used to estimate the loss is shown in Appendix A.

2.2.8 Confidence in the loss analysis

Here we briefly discuss the accuracy of the various loss calculations and how well they represent an actual implementation. The transmitter clipping is based on the beam waist at the transmitter which can be adjusted with proper choice of lenses and their position. Therefore the beam waist can be manipulated to accurately match the desired value. In the case on a WCP source, the 0 dB of clipping loss relies on proper characterization of the output beam of the transmitter (to normalize the signal intensity). This may be difficult in practice and a more conservative normalization may use the signal intensity before the transmitter, thus causing the clipping loss to be non-zero and the optimal beam waist to

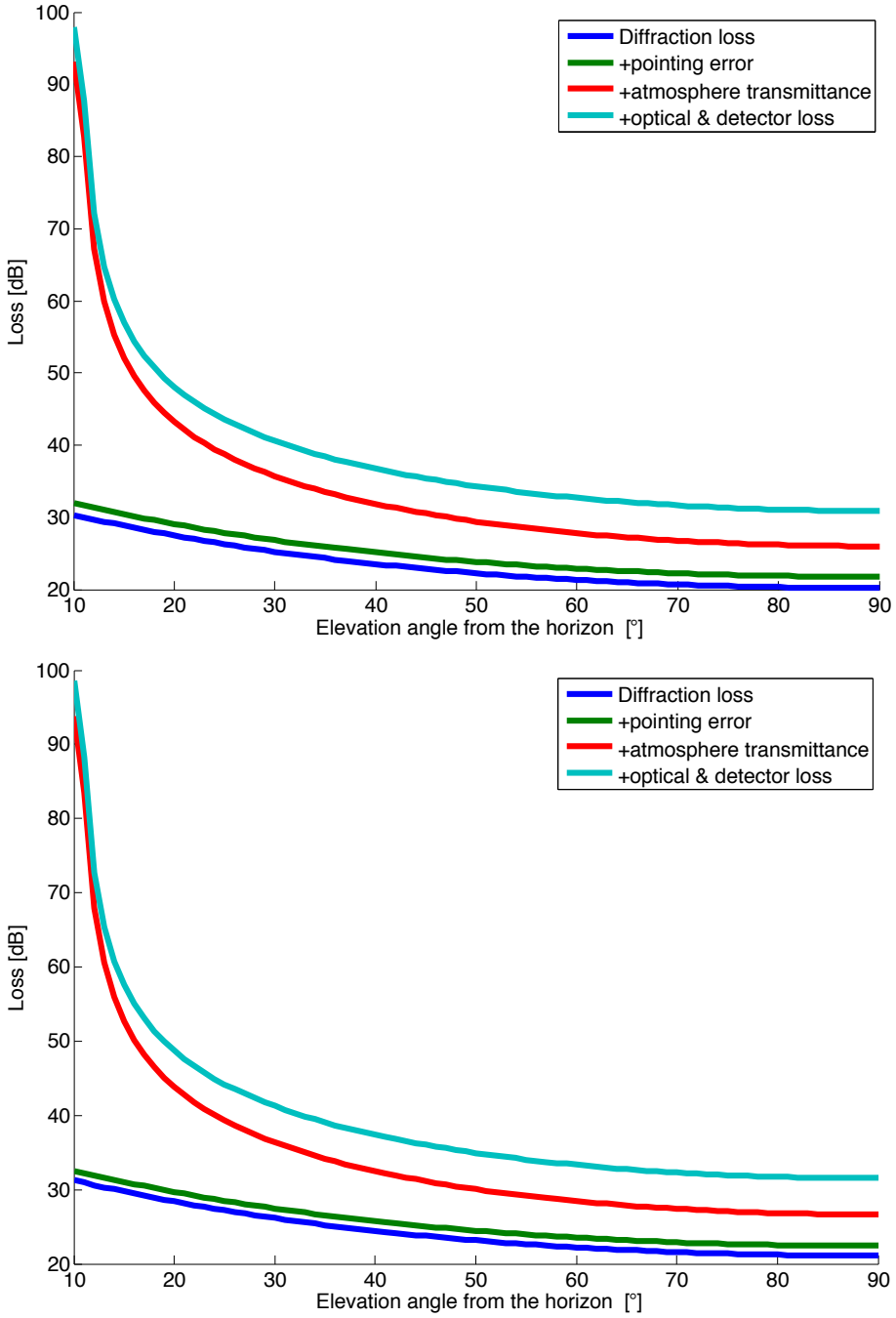

Figure 2.12: Predicted transmission loss from a satellite to a ground station using a WCP source (top) and an entangled photon source (bottom). Satellite transmitter telescope of 10 cm, ground receiver telescope of 50 cm, both circular with no obstruction. Wavelength of 670 nm, pointing error of 2 μrad with a 600km orbit and rural (5 km vis.) sea-level atmosphere.

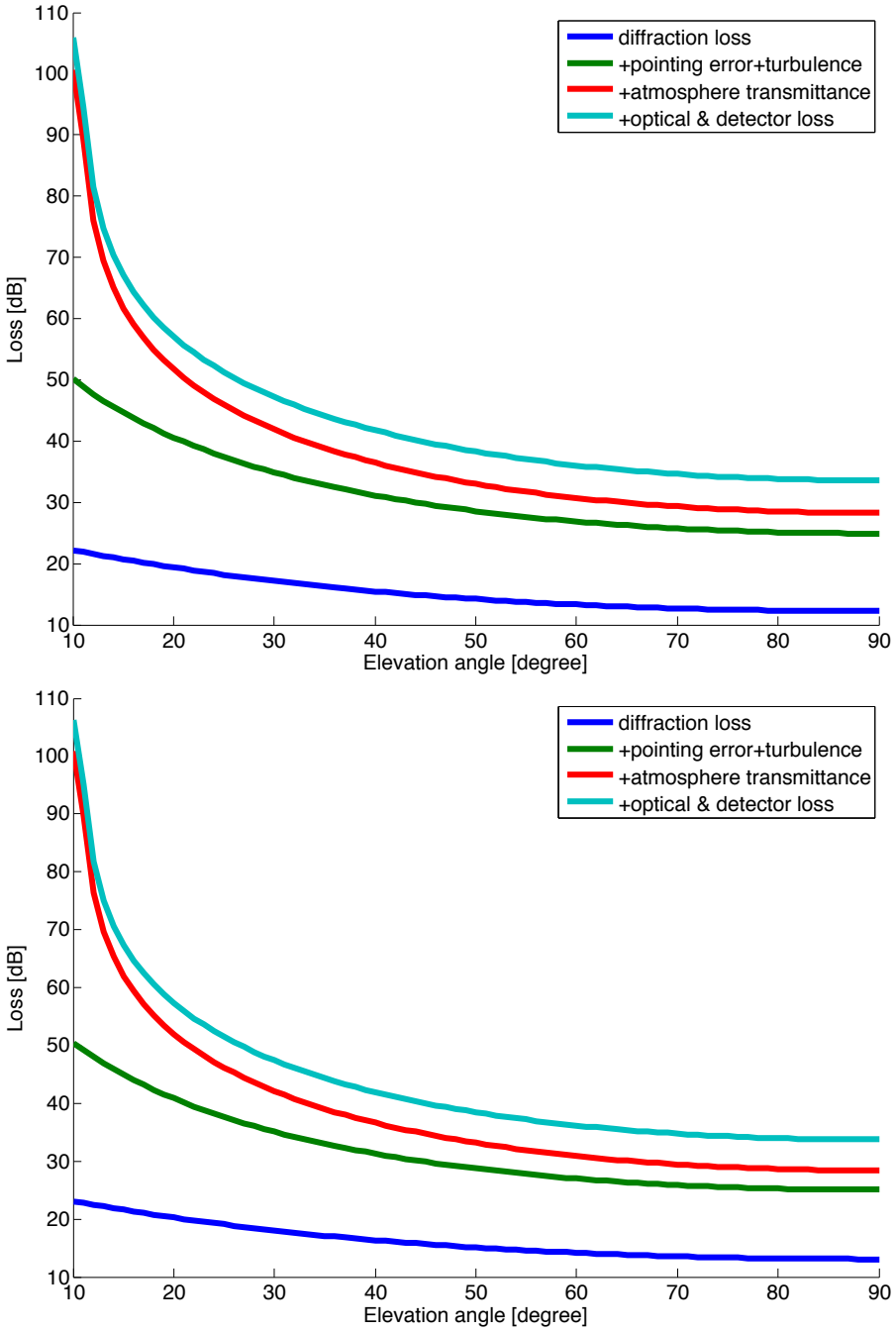

Figure 2.13: Predicted transmission loss from a ground station to a satellite using a WCP source (top) and an entangled photon source (bottom). Ground transmitter telescope of 50 cm, satellite receiver telescope of 30 cm, both circular with no obstruction. Wavelength of 785 nm, pointing error of 2 μrad with a 600km orbit and rural (5 km vis.) sea-level atmosphere.

Table 2.2: Contributions of loss for elevation angles of 90°, 55° and 30° from the horizon in a downlink. These elevation angles correspond to the maximum elevation angles of the best, upper quartile and median pass respectively. To help compare the relative importance of the geometric losses (diffraction, pointing error and atmospheric turbulence), their individual values are given as if they where the only geometric loss present. The total geometric loss is the loss when all geometric effects are properly combined to find the final beam distribution from which loss is computed. Conditions are the same as in Figure 2.12.

Source of loss	**WCP source loss [dB]**			**Entangled photon source loss [dB]**		
	90°	**55°**	**30°**	**90°**	**55°**	**30°**
Transmitter clipping	0.0	0.0	0.0	0.3	0.3	0.3
Diffraction	20.2	21.7	25.2	20.8	22.3	25.8
Pointing error	16.4	17.9	21.5	16.4	17.9	21.5
Atmospheric turbulence	0.0	0.0	0.0	0.0	0.0	0.0
Total Geometric	21.8	23.3	26.8	22.1	23.6	27.1
Atmospheric transmittance	3.4	4.1	7.0	3.4	4.1	7.0
Optical losses	3.0	3.0	3.0	3.0	3.0	3.0
Detector efficiency	1.9	1.9	1.9	1.9	1.9	1.9
Total	30.1	32.3	38.7	30.7	33.0	39.3

Table 2.3: Contributions of loss for elevation angles of 90°, 55° and 30° from the horizon in a uplink. These elevation angles correspond to the maximum elevation angles of the best, upper quartile and median pass respectively. To help compare the relative importance of the geometric losses (diffraction, pointing error and atmospheric turbulence), their individual values are given as if they where the only geometric loss present. The total geometric loss is the loss when all geometric effects are properly combined to find the final beam distribution from which loss is computed. Conditions are the same as in Figure 2.13.

Source of loss	**WCP source loss [dB]**			**Entangled photon source loss [dB]**		
	90°	**55°**	**30°**	**90°**	**55°**	**30°**
Transmitter clipping	0.0	0.0	0.0	0.3	0.3	0.3
Diffraction	12.2	13.7	17.1	12.8	14.3	17.7
Pointing error	18.6	20.1	23.7	18.6	20.1	23.7
Atmospheric turbulence	23.4	26.6	34.5	23.4	26.6	34.5
Total Geometric	24.9	27.6	34.9	24.9	27.6	34.9
Atmospheric transmittance	3.4	4.1	7.0	3.4	4.1	7.0
Optical losses	3.0	3.0	3.0	3.0	3.0	3.0
Detector efficiency	2.3	2.3	2.3	2.3	2.3	2.3
Total	33.6	37.0	47.2	33.9	37.3	47.5

decrease to the same value as the entangled photon source. In such a case, the WCP source would suffer the same losses as the entangle source.

Diffraction is a well studied phenomena, and is modeled with high accuracy. The average loss of pointing error is also very accurate, but the actual effect of pointing error will result in fluctuations of the loss around the average value. Since QKD is based on the transmission of single pulses rather than a continuous data stream, the variation induced by pointing error does not negatively impact QKD beyond the increase in average loss. However, the variability can cause similar passes to have different performance based on the fluctuations of the pointing error (some will perform better than expected, others will perform worse), decreasing the reliability of the performance.

Atmospheric turbulence is based on a complex but well studied model, providing good accuracy. However, the model depends strongly on the parameters that characterize the atmosphere, which can vary significantly over different locations and time of year. For example, a study that measured the parameters at the Canary Islands [98] found that the monthly average values of the parameters A and v of Equation (2.4) varied by up to 68% and 39% respectively from their average value. The average values were found to be $A = 9.75 \times 10^{-15}$ $\mathrm{m}^{-\frac{2}{3}}$ and $v = 17.47$ m/s, compared to the sea-level values of $A = 1.7 \times 10^{-14}$ $\mathrm{m}^{-\frac{2}{3}}$ and $v = 21$ m/s used in our analysis. Using these measured values of atmospheric turbulence parameters we find atmospheric turbulence contributions (in an uplink) of 21.2 dB, 24.4 dB and 32.3 dB for 90°, 55° and 30° respectively, corresponding to 2.2dB less loss for each angles. The best month of the year (June, $A = 3.09 \times 10^{-15}$ $\mathrm{m}^{-\frac{2}{3}}$ and $v = 17.1$ m/s) reduce the losses by an additional 3.2 dB (18.0 dB, 21.2 dB and 29.1 dB for 90°, 55° and 30° respectively). It is thus clear that while atmospheric turbulence is likely to remain the dominant source of geometric loss in an uplink, it's impact can vary significantly based on location and time of year. In addition to increasing the average loss, atmospheric turbulence will increase the variation of the link loss due to the beam wander and scintillation effect of atmospheric turbulence. In the same way as pointing error, this variability can decrease the reliability of the performance.

Atmospheric transmittance is another well studied model that provide good accuracy but can vary significantly over locations, air composition and atmospheric conditions. For example, a maritime model yields losses of 1.2 dB, 1.5 dB and 2.4 dB for 90°, 55° and 30° respectively, corresponding to 2.2 dB, 2.6 dB and 4.6 dB less loss compared to our modeled rural atmosphere. Atmospheric transmittance is thus another parameter that can vary widely based on location.

Optical losses depend on the chosen optical components. The optical loss of the free space receiver used in Chapter 5 was measured to be 2 dB (see section 5.2.1). Our chosen

value of 3 dB is therefore likely to be an overestimate and better efficiency can and have been achieved. Finally, the detector efficiency is based on existing Si APDs and is therefore very accurate. However, the final detector model may be different and can thus have a different detection efficiency.

In summary, our model provides high accuracy in determining the average loss but some components, particularly atmospheric turbulence and transmittance, can have loss contributions that vary significantly from those in our current estimates. In addition, pointing error and atmospheric turbulence could add variations to the link, causing some passes to behave better or worse than expected, reducing the reliability of the expected performance.

2.3 Estimating the background counts

Having a good signal to noise ratio is crucial for QKD because there is no way to distinguish between noise and errors introduced by an eavesdropper. All noise must therefore be attributed to the presence of an eavesdropper. By revealing parts of the received signal the two parties performing QKD are able to estimate the number of errors, caused by either noise or an eavesdropper, and place a limit on the amount of information that an eavesdropper may have acquired. To ensure security, QKD can only proceed if this limit is below a certain threshold. It is therefore crucial for the noise of a QKD system to be small enough for this limit the be below the threshold when there is no eavesdropper. In addition, security requires to reduce the size of the key to wash out any information that may have been learned by an eavesdropper. More noise will then lead to a greater reduction in the size of the key, thus reducing the performance.

For these reasons, it was crucial to develop a program to estimate the amount of background light received. This program is a modified version of a background counts program developed by Bassam Helou.

2.3.1 Sources of background noise

Most background noise comes from background light originating from both natural and artificial sources. Natural sources come from the Sun, reflected by the Moon, and from stars. Artificial sources consist of light pollution from human activities. The light pollution was characterized over the surface of the Earth during 1996 and 1997 by the Defence Me-

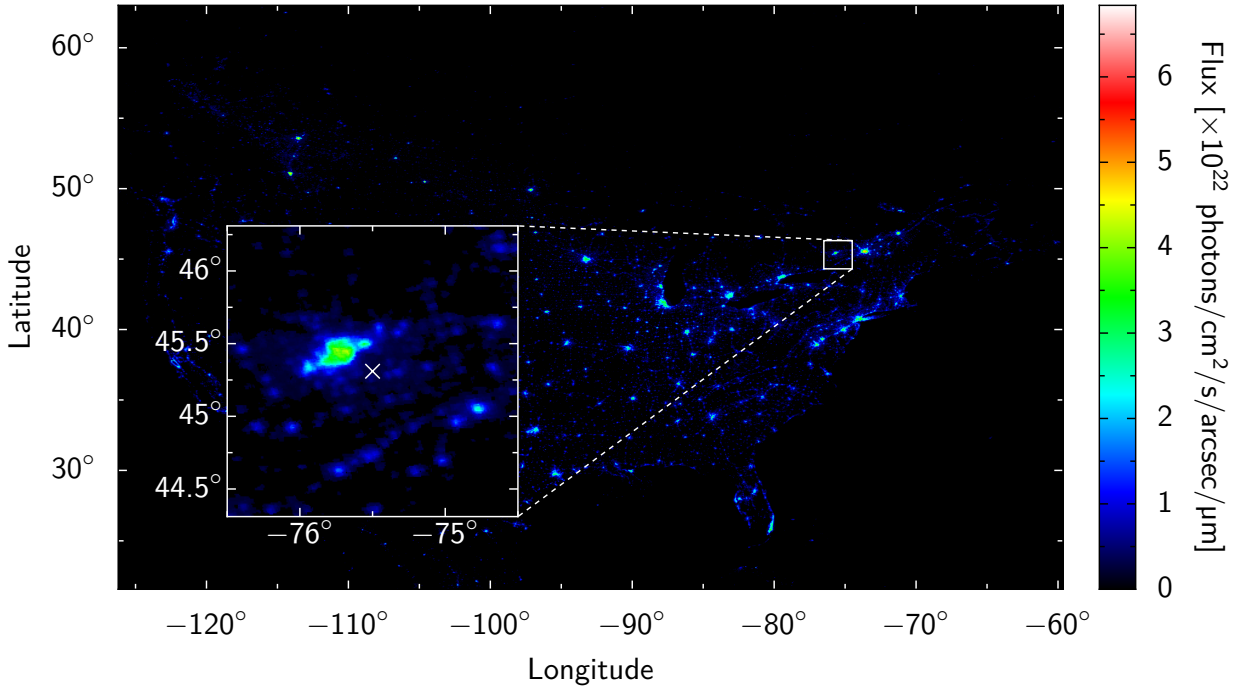

Figure 2.14: Light pollution from human activities in North America, data from World Atlas of Artificial Sky Brightness (Ref. [100]). The inset shows a closer view of the location of the simulated ground site, marked with a cross, approximately 20 km outside Ottawa.

teorological Satellite Program's (DMSP) Operational Linescan System (OLS) [99]. Light pollution data is partly shown in Figure 2.14.

The location used for calculating the artificial light pollution was 20 km from the city of Ottawa, Canada, with a latitude of approximately 45° North. This location, at the the edge of the city, represents a scenario where the ground station may be linked to a city's ground-based secure QKD network, with the satellite acting as a trusted node to establish global quantum-secured links. We also assume a half-moon at 45° elevation, representing a worst case for most night that are considered, and a receiver field of view (FOV) of 50 μrad. Finally a 1 nm bandwidth filter is assumed to eliminate background not at the signal wavelength.

From our choice of orbit (sun-synchronous noon/midnight LEO orbit), and our choice of ground location (latitude around 45° North), the satellite will always be in the Earth's shadow during nighttime passes. We can therefore ignore all contribution to the background light that would arise from the satellite being illuminated by the sun.

Other contributions to the noise are from detector count rates and polarization misalignment between the source and the receiver. In this work, we used a detector dark count

rate of 20 cps per detectors, in line with the capabilities of the Si APD detectors [82, 83]. The polarization misalignment will be considered in Section 2.4.

The full MATLAB code used to estimate the background counts is shown in Appendix B.

2.3.2 Background for a downlink

In a downlink, the receiver will be on the ground pointing towards the sky. The natural brightness of the sky has been well characterized by astronomers for various different locations [101–103]. Similarly, the contribution of the Moon to the night sky brightness has also been studied [104]. There also exists theoretical models and computer algorithms to predict the night sky brightness. We use one of these computer algorithms [105] to determine the natural sky brightness (H_{nat}).

A ground receiver will also receive artificial light contribution from scattered light originally emitted by human activities. This nighttime sky brightness due to light pollution can be calculated from the DMSP-OLS data which specifies the measured upward flux emitted at a given ground location [106]. This data, reproduced in Figure 2.14 can be used to directly determine the upward flux at the location of interest which can be converted to artificial sky brightness (H_{art}).

The overall sum of these contributions amounts to the total number of background counts per second:

$$N_{\text{tot}} = \frac{1}{E_{\nu_0}} \left\{ (H_{\text{nat}} + H_{\text{art}}) \times \pi(\text{FOV})^2 \times \pi r^2 \times B_{\text{filter}} \right\} + D_{\text{dark}}, \tag{2.13}$$

where ν_0 is the mean frequency of the laser emitted towards the receiver, E_{ν_0} is the energy of a single photon of frequency ν_0, r is the telescope's radius (assumed circular, alternatively πr^2 can be replaced by the total area of the receiver). FOV is the angular field of view of the receiving telescope, B_{filter} is the bandwidth of the filter an D_{dark} is the summed dark counts from all detectors. Figure 2.15 shows the predicted total background counts (red) at various elevation angles and the contributions from natural (blue) and artificial (green) light sources.

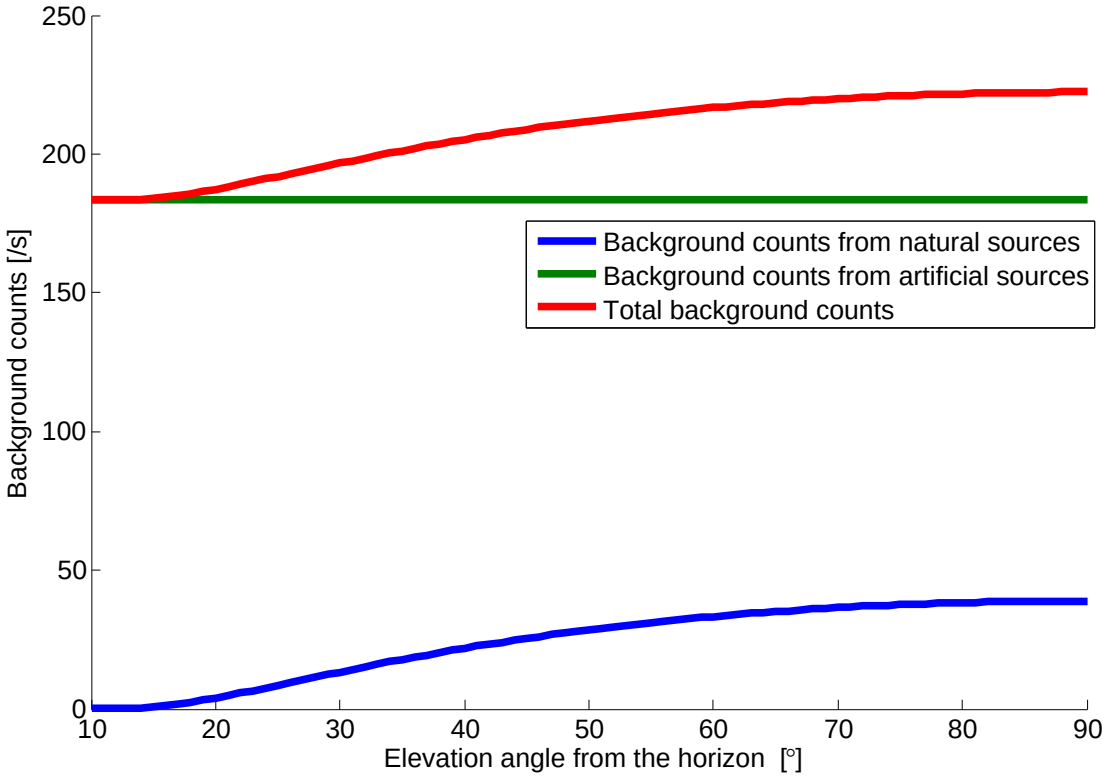

Figure 2.15: Predicted background light at a ground station 20 km from the city of Ottawa. Ground receiver telescope of 50 cm, circular with no obstruction, wavelength of 670 nm, 600 km orbit and rural (5 km vis.) sea-level atmosphere. Filter bandwidth of 1 nm, half-moon at 45° elevation and FOV of 50 μrad. Detector dark counts are not included.

2.3.3 Background for an uplink

In an uplink, the receiver is on a satellite pointing towards the ground. In this configuration, reflected light from stars is negligible. The main source of natural light is the light from the Sun reflected first off the Moon, and then off the surface of the Earth towards the satellite. The amount of light emitted by the Sun (to be reflected by the Moon) is obtained using Planck's law for blackbody radiation [107],

$$I(\nu, T) = \frac{2h\nu^3}{c^2} \left(\exp(h\nu/kT) - 1\right)^{-1}, \tag{2.14}$$

where ν is the frequency of the emitted radiation, h is the Planck constant, c is the speed of light, k is the Boltzmann constant, and T is the temperature of the emitter. Using this equation at the temperatures of the surface of the Sun (about 5778 K on average [107]) we obtain an accurate estimate of the spectrum of emitted light.

The Moon's albedo (quantifying how strongly its surface reflects light) depends primarily on the lunar phase. For this work, we assumed a moon half illuminated and used empirical data to obtain the amount of light reflected at a certain lunar phase [108]. The average Earth albedo is 30% [107]. We assumed Lambertian diffusion [74], meaning the radiance of reflected light is independent of angle. The number of photons reflected by the Moon N_{M} is given by

$$N_{\mathrm{Moon}} = a_{\mathrm{Moon}} \frac{I\left(\nu_0, T_{\mathrm{Sun}}\right)}{E_{\nu_0}} \pi R_{\mathrm{Moon}}^2, \tag{2.15}$$

where a_{Moon} is the Moon's albedo, T_{Sun} is the Sun's temperature and R_{Moon} is the Moon's radius. If the Moon is at normal incidence, the solid angle to the area on Earth Λ seen from the Moon is $\Lambda/d_{\mathrm{EM}}^2$, where d_{EM} is the distance between the Earth and the Moon. The number of background photons reaching the telescope after Lambertian reflection from the surface of the Earth is then

$$N_{\mathrm{Sun}} = B_{\mathrm{filter}} \eta_{\mathrm{t}} \eta_{\mathrm{t}}^{\mathrm{Moon}} \left[a_{\mathrm{Earth}} N_{\mathrm{Moon}} \left(\frac{\Lambda}{d_{\mathrm{EM}}^2} \right) \Omega \right], \tag{2.16}$$

where η_{t} is the atmospheric transmittance from the ground to the satellite, $\eta_{\mathrm{t}}^{\mathrm{Moon}}$ is the atmospheric transmittance from the moon to the ground, a_{Earth} is the Earth's albedo and Ω is the solid angle from which the telescope can be seen from the Earth. η_{t} and $\eta_{\mathrm{t}}^{\mathrm{Moon}}$ are both required to take into account the traversal of light through the atmosphere twice: First, light reflected from the Moon reaches the surface of the Earth. Then, this light is reflected into the receiving telescope.

The number of background counts due to light pollution is estimated using the DMSP-OLS data [99]. This data takes the form of a high-resolution image, with each pixel

coordinates of the image correspond to physical locations on the surface of the Earth, and the pixel values denote the nighttime radiance. With this we can obtain the average radiance $\bar{L}$ emitted by a certain location due to nighttime activities. We can then directly obtain light pollution emitted into the receiver:

$$N_{\text{night}} = B_{\text{filter}}\eta_{\text{t}}\left(\frac{\bar{L}}{E_{\nu_0}}\Lambda\Omega\right). \tag{2.17}$$

One limitation with this result is that the artificial light contribution is based on data taken almost a decade ago, and its accuracy varies seasonally due to changes in composition of the atmosphere. In addition, because there is little data on the composition of the types of lamps used in a certain region, we assume that the radiance $\bar{L}$ is constant at all frequencies. Some information about the composition of lighting types is expected to arrive in the future when the Nightsat mission becomes operational [109]. Nevertheless this data is accurate enough to give a reasonable estimate of the expected magnitude of background counts.

The total number of background counts is then obtained by summing the contributions from all sources:

$$N_{\text{BG}} = N_{\text{Sun}} + N_{\text{night}} + D_{\text{dark}}. \tag{2.18}$$

Figure 2.16 shows the predicted total background counts (red) at various elevation angles and the contributions from natural (blue) and artificial (green) light sources.

2.3.4 Wavelength considerations

The choice of wavelength can greatly influence the background counts experienced by our system. Notably, the spectrum of the Sun is affected by the absorption lines of the molecules in the solar atmosphere. These cause regions of lower solar spectrum, called Fraunhofer bands [110]. Taking advantage of such bands for QKD systems, such as the H-α band [111], has been proposed and showed a reduction of ≈50% in the solar background. Using a wavelength in such a line could significantly reduce the background in a downlink, which is mainly due to solar background reflected off the moon. Despite this possible improvement, typical QKD downlink will not be significantly affected by background. The predicted losses of a downlink (around 30–40 dB, see Section 2.2.7) correspond to a signal detection probability of 10^{-3}–10^{-4} while the predicted background contribution (200–300 cps, see Figure 2.15) corresponds to a background detection probability on the order of only 10^{-7}–10^{-6} with a typical detection window of 1 ns. Reducing the background

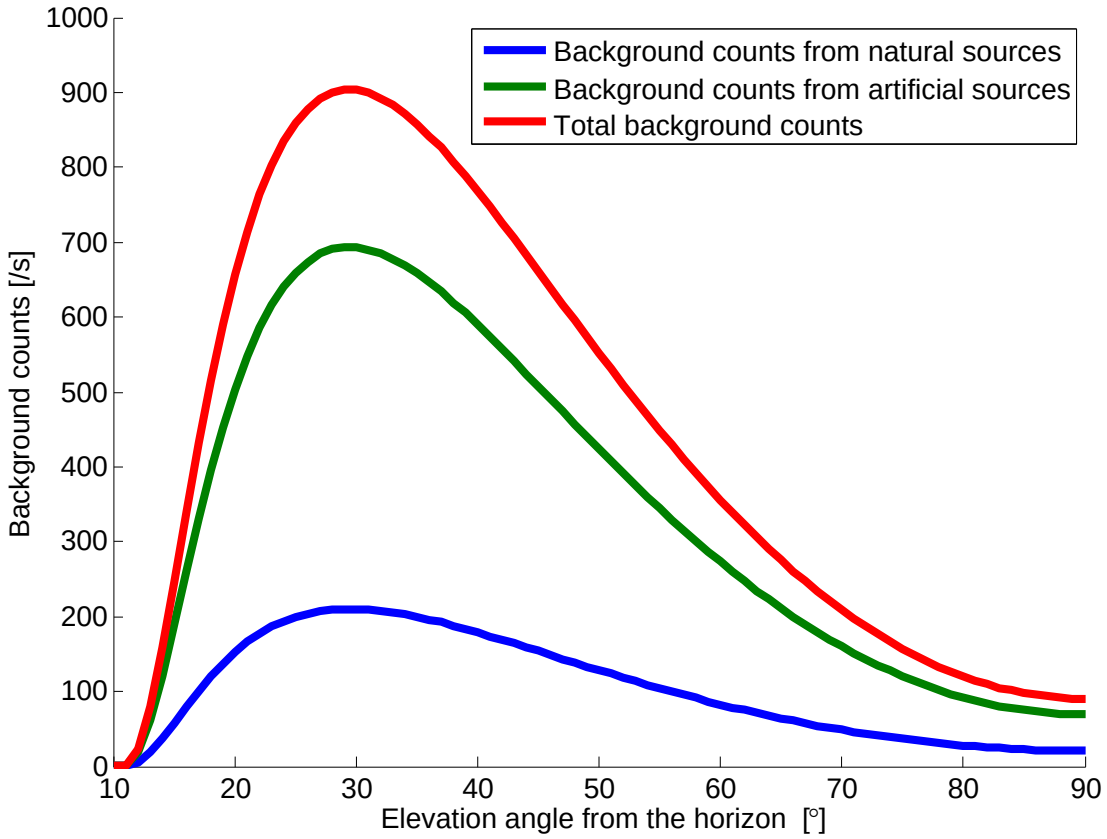

Figure 2.16: Predicted background light for a satellite pointing to a ground station 20 km from the city of Ottawa. Satellite receiver telescope of 30 cm, circular with no obstruction, wavelength of 785 nm, 600 km orbit and rural (5 km vis.) sea-level atmosphere. Filter bandwidth of 1 nm, half-moon at 45° elevation and FOV of 50 μrad. Detector dark counts are not included.

counts by choosing a wavelength in one of the Fraunhofer bands is thus unlikely to yield significant improvements.

In an uplink, the main background contribution comes from artificial lights. These lights have their own spectrum that can included regions of low emission. For example, high pressure sodium lamps, which are often used as streetlight, have a significant spectral emission drop around 595 nm [112]. Artificial light sources vary greatly between locations, choosing a wavelength that reduces artificial light pollution therefore requires good knowledge of the artificial light sources at potential locations. In our analysis, we chose not to make assumptions on the artificial light spectrum to ensure our predicted performance would not be limited to specific locations. We also chose to ignore the Fraunhofer bands because the background from the solar spectrum is much smaller than the artificial spectrum.

2.4 Estimating the key generation and the performance of fundamental experiments

To comprehensively evaluate the performance of a quantum link between the ground and a satellite we developed a realistic, numerical, quantum optics simulation. This allows us to accurately predict effects such as multi-photon emissions, optical losses and non-ideal detection [113]. Figure 2.17 illustrates the system we simulate, consisting of source, quantum channel, and detection.

In these simulations, polarization states are represented by modes, one for $|\mathrm{H}\rangle$ and one for $|\mathrm{V}\rangle$ with $|\mathrm{D}\rangle$ and $|\mathrm{A}\rangle$ represented as linear combination of $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ as shown in equations 1.1 and 1.2. This leads to two modes with a WCP source and four modes with an entangled source (two for Alice and two for BOB). Each mode contains its photon number distribution expressed in a Fock space of finite dimension. Fock space is a orthonormal Hilbert space in the photon number basis [114]. These basis states, called Fock states ($|n\rangle$), are fixed photon number states, i.e. $|0\rangle$ is the vacuum state (no photons), $|1\rangle$ is the one photon states, $|2\rangle$ is the two photon states, etc. [115].

The dimension of the Fock space used in the calculations determines the maximum number of photons we can simulate in each modes. To limit the computation time we chose a dimension of 7 when using a WCP source, allowing us to perform the simulation with 0–6 photons in each mode considered, and 4 when using an entangled photon source, allowing 0–3 photons in each mode considered. The difference in the number of dimensions

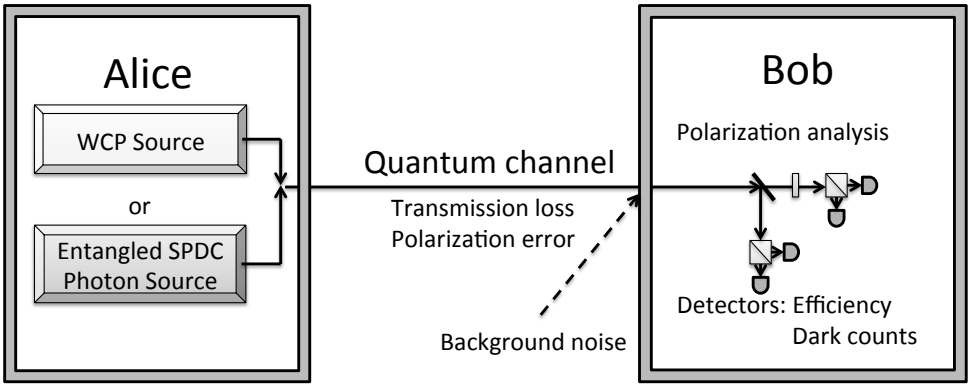

Figure 2.17: Devices considered in the quantum optics simulation. Each source is modelled separately using the appropriate quantum unitary operator. Optical losses are added in the quantum channel, accounting for atmospheric losses, and finally the polarization state of the photons is analysed and the photon detection probability evaluated. For the WCP source, Alice chooses the polarization to send for each pulse, whereas for the entangled photon source, Alice measures one photon of the pair to determine its polarization state. Bob's polarization analysis consists of four detectors in a passive polarization analysis apparatus arranged for QKD states.

considered is because the WCP source only needs to consider 4 modes (two outcomes in two bases) while the entangled photon source requires 8 modes (two outcomes in two bases for each of the two users). Using a dimension greater than 2 allows us to incorporate the effects of multi-pair emission from Poissonian statistics in weak coherent pulses and from down-conversion in entangle sources.

Imperfect source and polarization analysis components are simulated by adding a rotation to the polarization modes. Realistic non-number resolving detector models are used to estimate the probability of a detection based on the photon state, loss and background counts. Finally, total key length is calculation based on the total number of detection events and the correlation between Alice and Bob (to estimate the probability of an eavesdropper). This is done for both prepare-and-measure (using WCP source) and entanglement-based schemes.

In addition, we simulate the performance of two fundamental quantum experiments that could be performed using a quantum link between the ground and a satellite: Bell test [24] and quantum teleportation [116]. Both experiments utilize an entangled photon source, with quantum teleportation also utilizing a WCP source. Our model allows us to determine, for various telescope sizes, the maximum ground-satellite distance over which these experiments are possible. The dimension of the Fock space used for teleportation

is 5, allowing us to simulate up to 4 photons in each mode. The Bell test is based on an entangled photon source and uses the same simulation to calculate visibility (Fock space of dimension 4).

The programs described in this section were written by Evan Meyer-Scott with some simulations modified from programs written by Thomas Jennewein. [113]. Some additional modifications to the programs were done in collaboration with Evan. Some of these simulations use the quantum optics and computation toolbox by Sze Tan [117].

The full MATLAB code used to estimate the key generation, and the performance of Bell test and teleportation experiment, is shown in Appendix C.

2.4.1 QKD with a WCP source

A WCP source emits laser pulses with a Poissonian distribution of photon number. The photon number in each pulse can be represenly by using the coherent state ($|\alpha\rangle$) [114]. The coherent state produces a state with a Poissonian distribution of photon number where the mean photon number values is α^2:

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{2.19}$$

This state can be simulated by applying the displacement operator to the vacuum state:

$$|\alpha\rangle = D(\alpha) |0\rangle \,, \tag{2.20}$$

with the displacement operator defines as

$$D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a). \tag{2.21}$$

Here, a and $a^\dagger$ are the annihilation and creation operators [114] and $|\alpha|^2 = \mu$ is the average photon number per pulse. The annihilation and creation operator are non-Hermitian operators that add or remove a photon [118]. Their effect on the photon number states is thus:

$$a |n\rangle = \sqrt{n} |n-1\rangle \,, \quad \text{with} \quad a |0\rangle = 0, \tag{2.22}$$

$$a^\dagger |n\rangle = \sqrt{n+1} |n+1\rangle \,. \tag{2.23}$$

Both polarization based QKD and the single-photon counting detectors are insensitive to the phase factor $\mathrm{e}^{-|\alpha|^2/2}$. This is because the phase information is only accessible using

interference with a reference. Since polarization measurements do not employ interference, it is insensitive to global phases. We note that some implementation can cause a polarization dependent phase which could be used by an eavesdropper. It is therefore important for security to either ensure the phase is constant for all polarization states (so the phase cannot be used to extract any information), or to randomize the phase for each pulses [9]. The coherent states therefore also describes the incoherent Poissonian photon number distribution assumed in security proofs [119].

The security of QKD relies on its ability to detect the presence of an eavesdropper by comparing the correlations between the state prepared by one party, Alice, and the state measured by the other, Bob. These correlations are characterized by the polarization visibility:

$$V_{Polarization} = \frac{N_{\mathrm{E}} - N_{\mathrm{U}}}{N_{\mathrm{E}} + N_{\mathrm{U}}}. \tag{2.24}$$

Here, N_{E} is the number of detections with polarization parallel to the state that Alice sent (the expected counts), and N_{U} is the number of detections with perpendicular polarization (the unexpected counts). The polarization visibility relates to the more commonly used quantum bit error ratio (QBER) with the following relation:

$$\mathrm{QBER} = \frac{N_{\mathrm{U}}}{N_{\mathrm{E}} + N_{\mathrm{U}}} = \frac{1 - V_{Polarization}}{2}. \tag{2.25}$$

To account for imperfections in the source and in Bob's polarization analyzers we simulate the effect of a small polarization misalignment by applying a unitary rotation to Bob's photon, leading to some "unexpected" counts and hence to degraded visibility. We chose this unitary rotation to limit the polarization visibility to 98% in the ideal case, i.e. without loss or background. This is a pessimistic case, as better alignments have already been achieved experimentally [120].

To obtain the correlation we use realistic photon counting detectors [113]. Our simulated detectors do not resolve photon number, in line with current commercial detectors. The detector models use the total link loss, described Section 2.2, as their detector efficiency. The total received background counts, described in Section 2.3, is divided by the number of detectors used and serves as the detector dark count. From this the polarization visibility is obtained as well as the total number of counts received (including expected and unexpected detection events). This allows us to obtain the correlations between Alice's prepared states and the results of Bob's measurement.

Some examples of the calculated polarization visibility and count rate for a WCP source QKD system are shown in Figure 2.18. The drop in visibility from the ideal $V_{Polarization} =$

100% is due to the signal to noise ratio in the detectors, to multi-photon emissions, due to the Poissonian distribution of photon number produced, and to the slight polarization misalignment. The reduction in visibility from the multi-photon emissions is caused by the increased probability of multiple detector clicks, in which case the result is randomly assigned, causing an average of 0% visibility for multiple detection events.

Because laser pulses have Poissonian photon number statistics, some pulses will possess more than one photon. This makes WCP source QKD vulnerable to the photon number splitting attack [122, 123], where an adversary (Eve) splits off one photon from the pulse and stores it (in a quantum memory) to measure only after Bob reveals his measurement basis. Eve can then measure the stored photon in the same basis, thereby gaining full information about multi-photon pulses in an undetectable manner. This vulnerability reduces the performance of WCP source QKD by requiring the average photon number to be low, thereby reducing to multi-photon probability below a certain threshold, while also reducing the single-photon probability, thereby reducing the key generation rate. The key rate can be given as [124]

$$R \geq q\{Q_\mu \left[1 - \eta_{\text{EC}} H_2(E_\mu)\right] - (R_1 I_1(D_1) + R_{multi}\}, \tag{2.26}$$

where $q = 1/2$ is the basis reconciliation factor, Q_μ is the signal gain (i.e. the ratio of Bob's detections to pulses sent by Alice for average photon number μ), E_μ is the quantum bit error rate (QBER) for signal pulses. η_{EC} is the error correction efficiency for practical error correction codes (we assume 1.22, achievable with cascade and low density parity check codes [125]), $H_2(x)$ is the binary entropy function, R_1 (R_{multi}) is the rate of single-photon (multi-photon) detection events that are detected by bob and $I_1(D_1)$ is the information an eavesdropper can gain on single-photon events while introducing a disturbance D_1 (which increases the QBER E_μ). Intuitively, the first term (qQ_μ) represents the rate of received photons, the second ($qQ_\mu \eta_{\text{EC}} H_2(E_\mu)$) represents the information lost during error correction and the final term $R_1 I_1(D_1) + R_{multi}$ represents the amount of information gathered by an Eavesdropper which must be removed during privacy amplification. An eavesdropper will gain partial information from single-photon events (while disturbing the state, introducing errors) and full information on multi-photon events. In this model, the optimal average photon number for a WCP source is approximately the transmission of the channel [124], requiring lower average photon number when the channel transmission decreases. This typically limits WCP source QKD to channel losses of 10–20dB [124].

One way to combat this attack is for Alice to change the average photon number μ of randomly interspersed pulses (decoys) which are not utilized in generating the secure key. This method, called the decoy pulse method, enforces a much stricter bounds on how

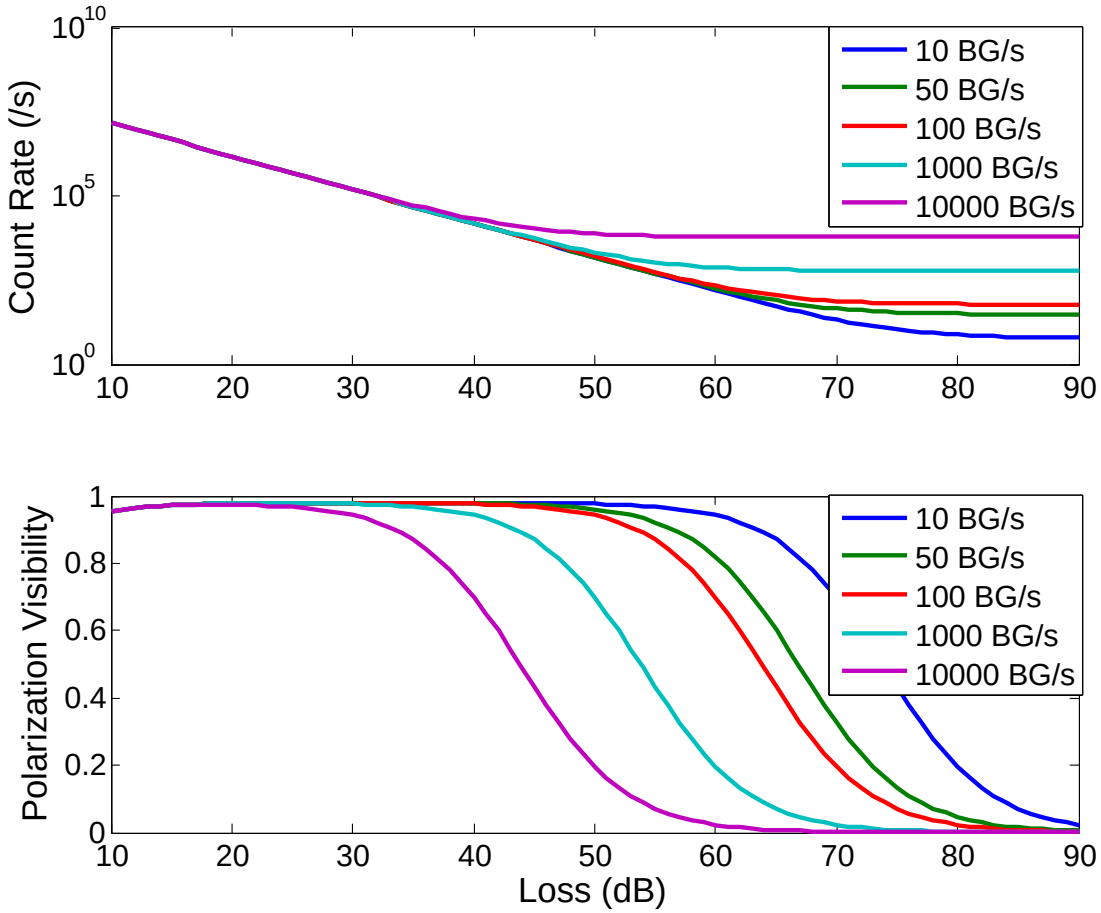

Figure 2.18: Weak coherent pulse photon polarization visibility and count rate as a function of channel loss in Bob's arm, for various background count rates (BG/s) per detectors. The source operates at a repetition rate of 300 MHz, with an average photon number per pulse of 0.5. The count rate here includes only detections that arrive within 1 ns of an expected laser pulse from Alice. Multi-photon emissions and the slight polarization misalignment lead to imperfect entanglement visibility at low loss. At high loss, the visibility goes to zero, and the count rate approaches the product of background count rate per detector, the number of detectors (four), and the ratio of the detection window (1.0 ns) to the repetition period (3.3 ns). The detection window is limited by the sources pulse width (typically 1–100s of ps), the timing jitter of the detectors (typically 100s of ps) the timing jitter of the electronics (typically 100s of ps or better) and the uncertainty in the variation of time of flight due to GPS uncertainty (typically 100s of ps) and atmospheric transmission through the atmosphere (typically on the order of a few ps [121]).

much information can be gained from multi-photon signals; since Eve cannot know *a priori* whether a given pulse is a signal or decoy. This strengthens the security of WCP source QKD and reduces the amount of privacy amplification that must be performed. The lower bound on asymptotic (i.e. in the limit of an infinite key generation time) key rate per laser pulse using the decoy pulse method is [126]

$$R \geq q\{-Q_\mu \eta_{\mathrm{EC}} H_2(E_\mu) + Q_1 \left[1 - H_2(E_1)\right]\}, \tag{2.27}$$

where Q_1 and E_1 are the estimated gain and error rate for single-photon pulses. The key rate is then the gain of signal pulses (qQ_1), minus the information leaked from error correction on all signal pulses ($qQ_\mu \eta_{\mathrm{EC}} H_2(E_\mu)$), minus the privacy amplification on signal pulses ($qQ_1 H_2(E_1)$). This key rate is multiplied by the system clock rate or laser pulse rate to obtain secure key bits per second. The use of decoy state allows the average photon number to be independent of the transmission loss (typically with an optimal value around 0.5), allowing WCP source QKD at losses of up to 40–60dB [126].

In our calculations we considered the one-decoy protocol from [126]. In this protocol, Alice randomly chooses to send either a signal pulse with average photon number μ or a decoy pulse with average photon number $\nu < \mu$. In this protocol, Q_1 and E_1 can be estimated from measurable quantities as

$$Q_1 = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu - \nu^2} \left(Q_\nu \mathrm{e}^{\nu} - Q_\mu \mathrm{e}^{\mu} \frac{\nu^2}{\mu^2} \right), \tag{2.28}$$

$$E_1 = \frac{E_\nu Q_\nu}{Q_1}. \tag{2.29}$$

Here, Q_μ and Q_ν are the gains of signal and decoy pulses, respectively. In this protocol, a factor $N_\mu/(N_\mu + N_\nu)$, where N_μ and N_ν are the number of Bob's received signal and decoy counts, must multiply the key rate in Equation (2.27) since only signal pulses contribute to the final key.

Equation (2.27) quantifies the asymptotic key rate over an infinitely long key generation time, but in actual implementations the key generation time will be finite. To account for this finite time, and allow the generation of a key on a single pass, finite-size statistics of the observed parameters must be incorporated. A rigorous finite-size analysis for WCP QKD is still incomplete, but an *ad hoc* version can be developed as follows. Firstly, We assume no bits are required for error rate estimation as the error correction algorithm identifies the number of errors precisely [127]. Secondly, the parameters used to calculate Q_1 and E_1 must be modified to account for the chance of statistical fluctuation in their values. Specifically, 10 standard deviations [128] are incorporated into Q_μ, Q_ν, E_μ and E_ν such

that the worst case scenario is considered, and the probability that the actual values fall outside this range is less than 10^{-25}. Finally, the following security parameter, described in [129] must be added to the secure rate equation (Equation 2.27):

$$\Delta = 2\log_2 1/[2(\epsilon - \bar{\epsilon} - \epsilon_{\mathrm{EC}})] + 7\sqrt{N_\mu \log_2[2/(\bar{\epsilon} - \bar{\epsilon}')]}, \tag{2.30}$$

where ϵ is the total allowable probability that the final key is insecure, chosen to be $\epsilon = 10^{-9}$, $\epsilon_{\mathrm{EC}} = 10^{-10}$ is the error correction failure probability, and $\bar{\epsilon}$ and $\bar{\epsilon}'$ can be optimized numerically with the constraint $\epsilon - \epsilon_{\mathrm{EC}} > \bar{\epsilon} > \bar{\epsilon}' \geq 0$. The first term of this security parameter is due to the fact that, in the non asymptotic case, the error correction and the privacy amplification may fail. The second term comes from the smooth min-entropy, a conditional entropy that characterizes an Eavesdropper's uncertainty.

The final key rate for a WCP source with finite-size effects is then lower-bounded by

$$R \geq q\frac{N_\mu}{N_\mu + N_\nu}\{-Q_\mu \eta_{\mathrm{EC}} H_2(E_\mu) + Q_1\left[1 - H_2(E_1)\right] - Q_\mu \Delta/N_\mu\}. \tag{2.31}$$

Given the known μ, ν, N_μ, N_ν, ϵ, ϵ_{EC}, bounded Q_μ, Q_ν, E_μ, E_ν and estimated Q_1, E_1 from our quantum optics simulations, a secure key length can be calculated for each satellite passage. In our simulations we used $\mu = 0.5$ and $\nu = 0.1$.

2.4.2 QKD with an entangled photon source

Entangle photon sources used for QKD are typically created using spontaneous parametric down-conversion (SPDC). The state produced by this process is known as a two-mode squeezed state ($|\varepsilon\rangle$) [118].

$$|\varepsilon\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(-1)^n \mathrm{e}^{\mathrm{i}n\theta}\tanh^n r\,|n\rangle_1\,|n\rangle_2\,, \tag{2.32}$$

where $\varepsilon = r\mathrm{e}^{\mathrm{i}\theta}$ contains the pump power and probability of down-conversion. The $|n\rangle_1$ and $|n\rangle_2$ are the photon number states in mode 1 and 2 respectively. In the two-mode squeezed state photons in modes 1 and 2 always exist in pairs. This state can be simulated by applying the two-mode squeezing operator to the vacuum state:

$$|\varepsilon\rangle = S(\varepsilon)\,|0\rangle_1\,|0\rangle_2\,, \tag{2.33}$$

with the squeezing operator defined as

$$S(\varepsilon) = \exp\left(\varepsilon(a_1^\dagger a_2^\dagger - a_1 a_2)\right), \tag{2.34}$$

where $a_m^\dagger$ and a_m are the creation and annihilation operators respectively for mode m. To create an entangled state we use two squeezed states (with the same ε) to represent the two polarizations of each modes. The first two modes arise from the first squeeze state and the last two from the second squeezed state. This creates the state:

$$\frac{1}{\cosh^2 r}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}(-1)^{n+m}\mathrm{e}^{\mathrm{i}(n+m)\theta}\tanh^{n+m} r\,|n\rangle_1\,|n\rangle_2\,|m\rangle_3\,|m\rangle_4\,. \tag{2.35}$$

In modern SPDC sources of entangled photon pairs, the entangled state is created directly, but here we achieve this entanglement by permuting the photons from mode 2 and 4 creating the state

$$\frac{1}{\cosh^2 r}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}(-1)^{n+m}\mathrm{e}^{\mathrm{i}(n+m)\theta}\tanh^{n+m} r\,|n\rangle_1\,|m\rangle_2\,|m\rangle_3\,|n\rangle_4\,. \tag{2.36}$$

The four modes correspond to H in channel one, V in channel 1, H in channel 2 and V in channel 2. This permutation trick achieves the polarization entanglement in a way that is computationally much simpler. The variable ε is chosen so that there is a low probability of n and m being both greater than zero (and therefore a very low probability of either being greater than one). In the special case where n or m is 1 and the other is 0, this state approximates the $|\psi^+\rangle$ maximally-entangled Bell state

$$\left|\psi^+\right\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1\,|\mathrm{V}\rangle_2 + |\mathrm{V}\rangle_1\,|\mathrm{H}\rangle_2). \tag{2.37}$$

As is the case for a real SPDC source, Equation (2.36) shows the possibility of multiple uncorrelated photon pairs being created simultaneously, leading to errors. This model can be applied to both a pulsed or continuous wave pumping scheme, with the former having detection probabilities defined per pulse, and the latter per coincident detection window of the detectors. The pumping scheme was modeled in our simulations because it is easier to simulate, requiring only to analyze the coincidences during pump pulses.

When using entanglement-based schemes, the correlations between Alice and Bob are characterize using the entanglement visibility,

$$V_{Entangled} = \frac{C_\mathrm{E} - C_\mathrm{U}}{C_\mathrm{E} + C_\mathrm{U}}. \tag{2.38}$$

Here, C_E is the coincident photon counts detected possessing the expected polarization, and C_U is the coincident counts detected with unexpected. For the maximally entangled $|\psi^+\rangle$ state used, the expected polarizations are perfect correlation in the H–V basis and perfect anti-correlation in the A–D basis, leading to visibility of $V_{Entangled} = 100\%$. Again, the entanglement visibility can be related to the QBER:

$$\mathrm{QBER} = \frac{C_\mathrm{U}}{C_\mathrm{E} + C_\mathrm{U}} = \frac{1 - V_{Entangled}}{2}. \tag{2.39}$$

Similarly to the case of a WCP, we simulate realistic degradation in entanglement visibility due to imperfect sources and polarization analyzers by applying a unitary rotation to Bob's photon (but not Alice's), leading to some "unexpected" coincident counts and hence to degraded visibility. We again chose an entanglement visibility of 98%, with better alignment previously achieved experimentally [130].

The correlations are again obtained using realistic detector models with Bob's detectors using the calculated loss and background counts as detector efficiency and dark counts. On Alice's side, the photons do not travel the free-space link and are assume to be measured locally. The detection apparatus is assumed to be the same as Bob's, shown in Figure 2.17, consisting of four detectors with passive polarization analysis. The total efficiency on Alice's side is then the efficiency of the detectors and optical components described in Section 2.2.5. This total efficiency ($\eta_{\mathrm{d}}\eta_{\mathrm{o}}$) is then used as the modeled detector's efficiency. For simplicity, the detector efficiency is taken at the same wavelength as the photon transmitted to Bob. In addition, Alice will also not receive the background counts from natural and artificial light sources. The dark counts in the detector models for Alice is the simply the dark counts D_{dark} of her detectors. Because D_{dark} as defined in Section 2.3 is the summed dark counts from all detectors, it must once again be divided by the total number of detectors.

Some examples of the calculated polarization visibility and count rate for an entangled source QKD system are shown in Figure 2.19. Similarly to the case of a WCP source, the ideal entanglement visibility, $V_{Entangled} = 100\%$, is reduced by the signal to noise ratio in the detectors and by the slight polarization misalignment. However, this visibility is also reduced by multi-pair emission, i.e. the simultaneous emission of multiple uncorrelated pairs. The probability of multi-pair emission can be reduced by reducing the probability of emission, thereby also reducing the single pair production and thus the count rate. There thus exists a trade-off between maximizing the pair production rate and reducing the entanglement degradation due to double-pair emissions to a minimum. In our simulations we use $\varepsilon = 0.22$ (the strength of the SPDC operator in Equation 2.34, corresponding to an average number of pairs per pulse of 0.1 [131]). This value has been experimentally demonstrated in the pass [132] and gives a probability of double pair emission of 0.01.

The entangled source is slightly more resilient against background noise than the WCP source, i.e. the entangled source produces better visibility at high loss. This can be seen by comparing Figure 2.19 with Figure 2.18, which show a shift in the visibility curves of $\approx$3 dB, with the entangled source dropping at later losses than the WCP source. This is because a noise count must arrive in coincidence with a detection on Alice's side to be considered in an entangled scheme, whereas for a WCP source every noise count that

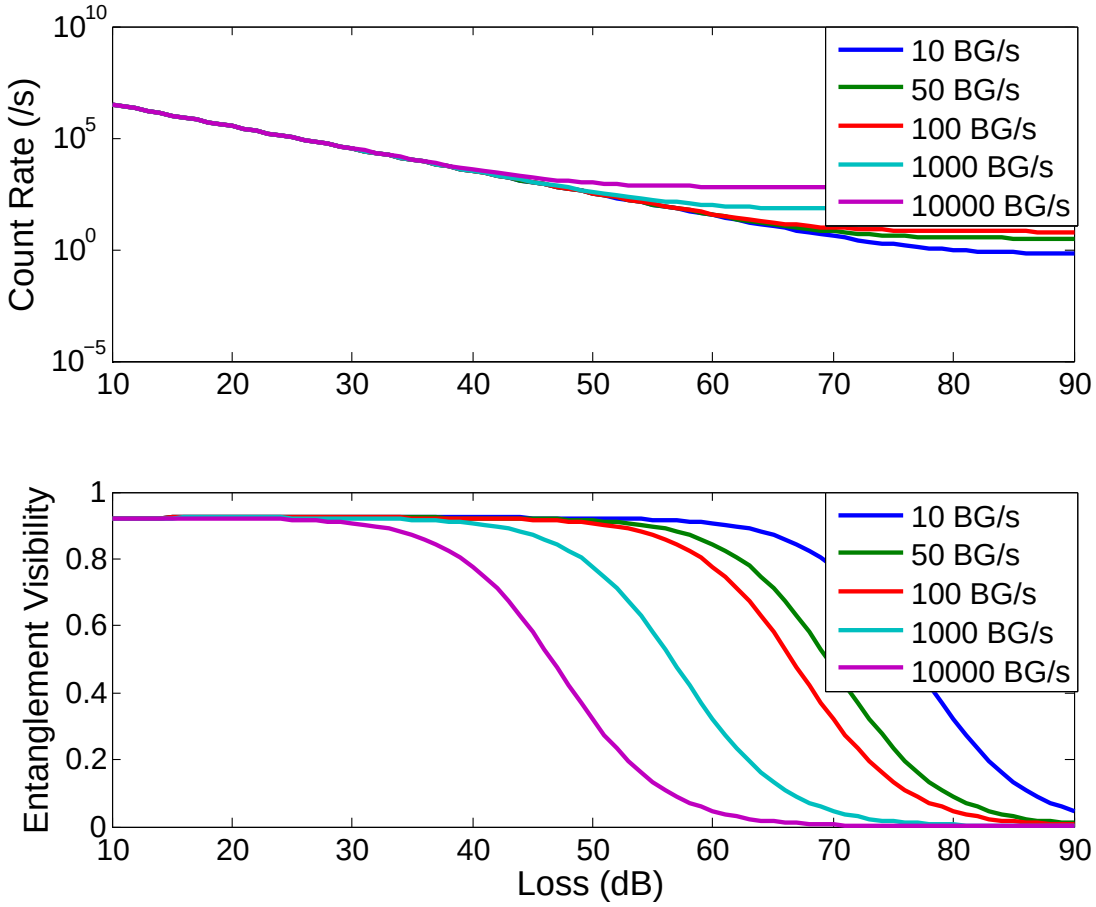

Figure 2.19: Entangled photon visibility and coincidence count rate as a function of loss in Bob's channel, for various background count rates (BG/s) per detectors. The entangled source operates at a pair production rate of 100 MHz; double-pair emissions and the slight polarization misalignment lead to imperfect entanglement visibility at low loss. At high loss, the visibility goes to zero, and the count rate approaches the product of background count rate per detector, the number of detectors (four), the ratio of the detection window (1.0 ns) to repetition period (10 ns), and Alice's detection efficiency (0.25), i.e. only background counts that arrive in coincidence with a photon detected by Alice are included in the rate.

arrives in coincidence with a laser pulse time-slice is accepted.

The secure key rate, based on the count rate and entanglement visibility, can be calculated following [129]. The final key rate per detected coincident pair is

$$R = q\left[1 - H_2(E+\xi) - f(E)H_2(E) - \Delta/N\right], \tag{2.40}$$

where $q = 1/2$ is the basis reconciliation (sifting) factor, E is the QBER, ξ is a security parameter from [129], $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, $f(E) = 1.22$ is the error correction efficiency, and N is the length of raw key. Similarly to Equation 2.30, The security parameter Δ given in by

$$\Delta = 2\log_2 1/[2(\epsilon - \bar{\epsilon} - \epsilon_{\mathrm{EC}})] + 7\sqrt{N\log_2[2/(\bar{\epsilon} - \bar{\epsilon}')]}, \tag{2.41}$$

where we again chose $\epsilon = 10^{-9}$ and $\epsilon_{\mathrm{EC}} = 10^{-10}$ with $\bar{\epsilon}$ and $\bar{\epsilon}'$ optimized numerically with the constraint $\epsilon - \epsilon_{\mathrm{EC}} > \bar{\epsilon} > \bar{\epsilon}' \geq 0$. The key rate in (2.40) can then be used, when combined with the output of the link analysis, to calculate the secure key length for each satellite passes.

2.4.3 Bell tests

Entangled states have the peculiar property of being linked. When one particle is measured, all particles of the entangled state are projected onto a new state based on the measurement outcome of the first particle. This phenomenon occurs instantaneously even when the particles are space-like separated. This paradoxical action at a distance of entangled states [18] led to the introduction of hidden variable theories. In these theories, the measurement outcome of any particle is predetermined by certain variables which we do not have access to.

There are two classes of hidden variable theories: local and non-local. In local hidden variable theories, the measurement outcome of one particle cannot affect space-like separated particles faster than the speed of light. In 1964, John Bell mathematically formulated the idea of local hidden variable theory and showed that they lead to inequalities that contradict the results of entangled states measurement predicted by quantum mechanics [25]. These inequalities have later been shown to be experimentally violated [21–24], thus proving no local variable theories can be used to explain quantum mechanics.

Non-local hidden variable theories, while removing the indeterminism of quantum mechanics, allow the paradoxical faster than light correlations between particles. These theories can lead to predictions that are always identical to the predictions of quantum mechanics. It was recently shown that, under the assumption that measurements can be chosen

freely, any hidden variable theories cannot give more information about the outcomes of future measurements than quantum theory itself [133].

The Bell inequalities have to date been violated experimentally up to a separation of 144 km [134]. The separation of these Bell inequality tests suffers from the same limitations as QKD. A quantum satellite platform therefore has the potential to greatly extend this distance, thereby testing the validity of quantum mechanics in a new regime [135].

A Bell test is performed in a similar fashion as entanglement base QKD, with one photon of the entangled pair measured locally at the source, while the other is sent to the receiver. The main difference lies in the measurement settings, which can be obtained from the QKD polarization analyzer (see Figure 2.17) by adding wave plates to change the measurement basis. The correlations are then compared and used to violate a Bell type inequality. Experimental implementations typically use the Clauser-Horne-Shimony-Holt (CHSH) inequality [136] as the Bell type inequality:

$$S_{\mathrm{CHSH}} = |E(\phi_{\mathrm{A}}, \phi_{\mathrm{B}}) - E(\phi_{\mathrm{A}}, \phi'_{\mathrm{B}})| + |E(\phi'_{\mathrm{A}}, \phi_{\mathrm{B}}) + E(\phi'_{\mathrm{A}}, \phi'_{\mathrm{B}})| \leq 2, \tag{2.42}$$

where

$$E(\phi_{\mathrm{A}}, \phi_{\mathrm{B}}) = (N_{++} - N_{+-} - N_{-+} + N_{--})/N_{\mathrm{meas}} \tag{2.43}$$

is the joint correlation at Alice and Bob's measurement angles ϕ_A and ϕ_B, respectively. The N_{ij} are the number of coincident counts between Alice's i and Bob's j detectors, where $i, j \in \{+, -\}$ and the $+$ detectors are set to the measurement settings $(\phi_{\mathrm{A}}, \phi_{\mathrm{B}})$ and the $-$ detectors are set orthogonally to those measurement settings. N_{meas} is the total number of measured counts for the measurement settings ϕ_A and ϕ_B.

Entangled states may violate this inequality, in particular for the set of polarization angles $(\phi_{\mathrm{A}}, \phi'_{\mathrm{A}}, \phi_{\mathrm{B}}, \phi'_{\mathrm{B}}) = (0°, 45°, 22.5°, 67.5°)$, which result in a maximal violation of $S_{CHSH} = 2\sqrt{2}$ for any of the four maximally entangled Bell states (Equation 1.3 and 1.4). This violation is significantly greater than the classical limit of 2.

Because the CHSH inequality is a measure of the correlations of an entangled pair, the violation of the inequality can be estimated with the entanglement visibility as defined in Equation 2.38. A reduction in the entanglement visibility will produce an equivalent reduction in the maximal violation of the inequality [137]:

$$S_{Experiment} = S_{CHSH} \times V_{Entangled} = 2\sqrt{2}V_{Entangled}. \tag{2.44}$$

The minimum entanglement visibility that is required to achieve violation of the Bell-inequality, in the asymptotic assumption that an infinite number of photons can be collected, is then

$$min(V_{Entangled}) = \frac{2}{2\sqrt{2}} = 70.7\%. \tag{2.45}$$

To include statistical fluctuations we consider a Bell test successful only if it violates the classical bound by at least three standard deviations, i.e. the experimental value must be larger than the classical value by at least three times the uncertainty:

$$S_{Experiment} - 3\Delta S_{Experiment} \geq 2, \tag{2.46}$$

where $\Delta S_{Experiment}$ is the uncertainty in the Bell parameter $S_{Experiment}$. The validity of this choice of 3 standard deviation (or even the validity of quantifying a bell violation using the number of standard deviations) is debatable [138]. We chose this method of standard deviations because it has been widely used in the past and provides a good bound to analyze while demonstrating our model. Our model is not limited to this method and a different method to quantify the deviation can be incorporate in our model if desired.

As photon pairs are created randomly, they follow Poisson statistics and the uncertainty of an average counts $\bar{N}$ is $\Delta\bar{N} = \sqrt{\bar{N}}$. Applying this uncertainty in Equation 2.43 and using error propagation for independent variables [139] yields

$$\Delta E(\phi_A, \phi_B) = \frac{2\sqrt{(N_{++} + N_{--})(N_{+-} + N_{+-})}}{N_{\text{meas}}\sqrt{N_{\text{meas}}}}. \tag{2.47}$$

The effect of a decrease in visibility can be seen as the states transitioning to a completely mixed state due to a depolarizing channel [140]:

$$|\psi'\rangle\langle\psi'| = (1-p)\,|\psi\rangle\langle\psi| + p\frac{I}{4}, \tag{2.48}$$

where $|\psi\rangle\langle\psi|$ and $|\psi'\rangle\langle\psi'|$ are the density matrix [17] of the state before and after depolarization, I is the sum over all two photon states (corresponding to 4 times the mixed state) and p is the probability of depolarization. Comparing this to the definition of visibility (Equation 2.38), the first part $(1-p)\,|\psi\rangle\langle\psi|$ will lead to perfect correlations while the second part $p\frac{I}{4}$ will lead to equal distribution of coincidence counts:

$$V_{Entangled} = \frac{C_{\text{E}} - C_{\text{U}}}{C_{\text{E}} + C_{\text{U}}} = \frac{(1-p+p\frac{1}{2}) - (p\frac{1}{2})}{(1-p+p\frac{1}{2}) + (p\frac{1}{2})}, \tag{2.49}$$

$$V_{Entangled} = 1 - p. \tag{2.50}$$

Using Equation 2.48, the number of measured coincidence when using the initial state $|\psi^+\rangle$ will be:

$$N_{++} = N_{--} = N_{\text{meas}}\left(\frac{1-p}{2}\sin^2(\phi_A + \phi_B) + \frac{p}{4}\right), \tag{2.51}$$

$$N_{+-} = N_{-+} = N_{\text{meas}} \left(\frac{1-p}{2} \cos^2(\phi_A + \phi_B) + \frac{p}{4} \right), \tag{2.52}$$

where ϕ_A and ϕ_B are the measurement settings of the detectors. The uncertainty in the joint correlation is then

$$\Delta E(\phi_A, \phi_B) = \frac{2\sqrt{\left((1-p)\sin^2(\phi_A+\phi_B) + \frac{p}{2}\right)\left((1-p)\cos^2(\phi_A+\phi_B) + \frac{p}{2}\right)}}{\sqrt{N_{\text{meas}}}}. \tag{2.53}$$

For our measurement settings $(\phi_{\text{A}}, \phi'_{\text{A}}, \phi_{\text{B}}, \phi'_{\text{B}}) = (0°, 45°, 22.5°, 67.5°)$, this leads to:

$$\Delta E(\phi_A, \phi_B) = \sqrt{\frac{\frac{1}{2} + p - \frac{p^2}{2}}{N_{\text{meas}}}}, \tag{2.54}$$

or written in terms of the visibility:

$$\Delta E(\phi_A, \phi_B) = \sqrt{\frac{1 - \frac{V^2_{Entangled}}{2}}{N_{\text{meas}}}}. \tag{2.55}$$

Using error propagation we obtain the uncertainty in the bell parameter:

$$\Delta S_{Experiment} = 2\sqrt{\frac{1 - \frac{V^2_{Entangled}}{2}}{N_{\text{meas}}}}, \tag{2.56}$$

where the number of measured counts in each measurement settings is assumed to be the same, i.e. $N_{\text{meas}} = N_{\text{total}}/4$, giving

$$\Delta S_{Experiment} = 4\sqrt{\frac{1 - \frac{V^2_{Entangled}}{2}}{N_{\text{total}}}}. \tag{2.57}$$

Using Equation 2.57 and 2.44 into Equation 2.46 we obtain the success criteria for violating a Bell test of at least three standard deviations:

$$2\sqrt{2}V_{Entangled} - 12\sqrt{\frac{1 - \frac{V^2_{Entangled}}{2}}{N_{\text{total}}}} \geq 2. \tag{2.58}$$

Figure 2.20 shows the total number of counts necessary to violate a Bell test, which is given by

$$N_{\text{total}} > \left(\frac{12}{2\sqrt{2}V_{Entangled} - 2} \right)^2 \left(1 - \frac{V^2_{Entangled}}{2} \right). \tag{2.59}$$

The entanglement visibility and count rates can be calculated in the same way for QKD with an entangled photon source (Section 2.4.2). Equation 2.58 is then used to verify if the Bell test can be succesfully violated based on the visibility and counts.

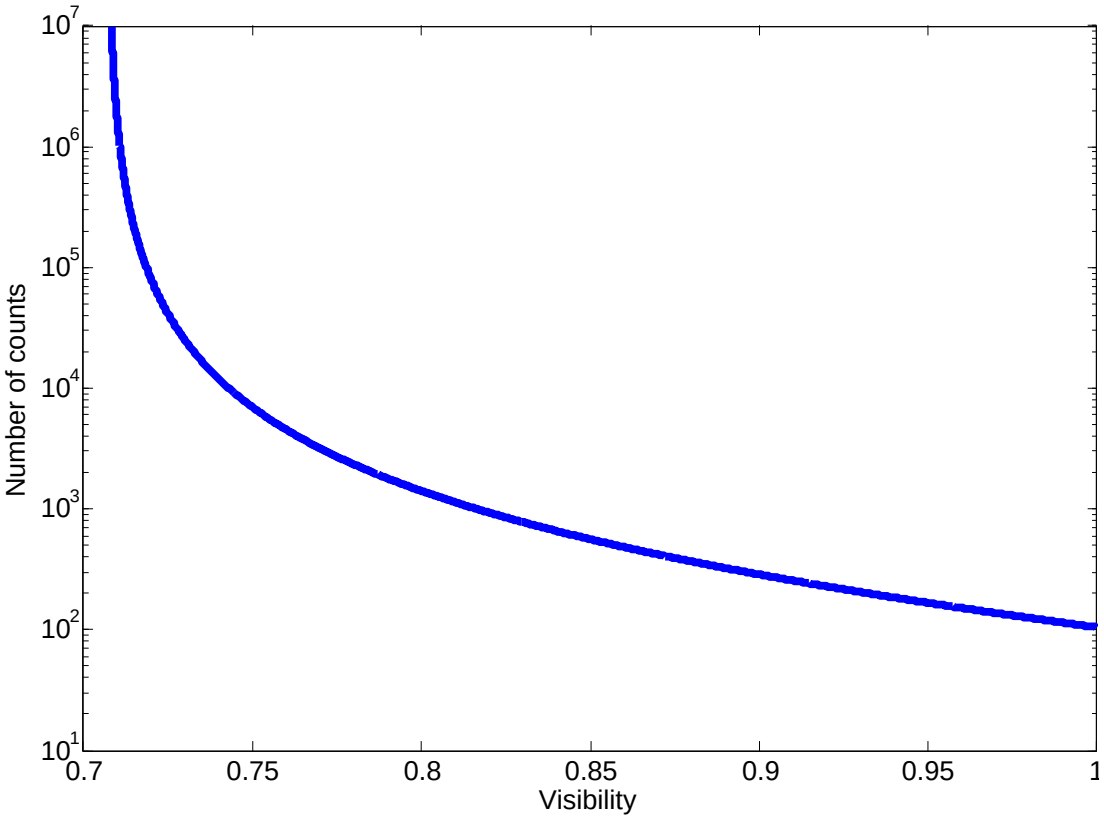

Figure 2.20: Required number of measured photon pairs to violate the CHSH inequality by three standard deviations with non perfect visibility. The number increases rapidly as we approach the minimum visibility of $V_{Entangled} = 1/\sqrt{2}$.

2.4.4 Quantum teleportation

Quantum teleportation allows one to instantly transfer a quantum state from one location to another [44]. This process, impossible classically, takes advantage of the unique properties of quantum entanglement and requires both parties to share an entangled state. By interfering one part of the entangled pair with the single state to be teleported and performing the right measurement, the single state can be teleported to the other part of the entangled pair.

The protocol can be explained as follow: take any maximally entangled Bell state, such as $|\psi^+\rangle$, and a general single-photon state to be teleported,

$$|\psi\rangle = \alpha\,|\mathrm{H}\rangle + \beta\,|\mathrm{V}\rangle\,. \tag{2.60}$$

The full three-photon state is then

$$|\psi\rangle_1\,|\psi^+\rangle_{23} = (\alpha\,|\mathrm{H}\rangle_1 + \beta\,|\mathrm{V}\rangle_1)(\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_2\,|\mathrm{V}\rangle_3 + |\mathrm{V}\rangle_2\,|\mathrm{H}\rangle_3)), \tag{2.61}$$

Which can be rewritten as

$$\begin{aligned}|\psi\rangle_1\,|\psi^+\rangle_{23} = \frac{1}{2}(\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1\,|\mathrm{V}\rangle_2 + |\mathrm{V}\rangle_1\,|\mathrm{H}\rangle_2))(\alpha\,|\mathrm{H}\rangle_3 + \beta\,|\mathrm{V}\rangle_3)\\ +\frac{1}{2}(\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1\,|\mathrm{V}\rangle_2 - |\mathrm{V}\rangle_1\,|\mathrm{H}\rangle_2))(\alpha\,|\mathrm{H}\rangle_3 - \beta\,|\mathrm{V}\rangle_3)\\ +\frac{1}{2}(\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1\,|\mathrm{H}\rangle_2 + |\mathrm{V}\rangle_1\,|\mathrm{V}\rangle_2))(\alpha\,|\mathrm{V}\rangle_3 + \beta\,|\mathrm{H}\rangle_3)\\ +\frac{1}{2}(\frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1\,|\mathrm{H}\rangle_2 - |\mathrm{V}\rangle_1\,|\mathrm{V}\rangle_2))(\alpha\,|\mathrm{V}\rangle_3 - \beta\,|\mathrm{H}\rangle_3),\end{aligned} \tag{2.62}$$

or equivalently

$$\begin{aligned}|\psi\rangle_1\,|\psi^+\rangle_{23} = \frac{1}{2}\,|\psi^+\rangle_{12}\,(\alpha\,|\mathrm{H}\rangle_3 + \beta\,|\mathrm{V}\rangle_3) + \frac{1}{2}\,|\psi^-\rangle_{12}\,(\alpha\,|\mathrm{H}\rangle_3 - \beta\,|\mathrm{V}\rangle_3)\\ +\frac{1}{2}\,|\phi^+\rangle_{12}\,(\alpha\,|\mathrm{V}\rangle_3 + \beta\,|\mathrm{H}\rangle_3) + \frac{1}{2}\,|\phi^-\rangle_{12}\,(\alpha\,|\mathrm{V}\rangle_3 - \beta\,|\mathrm{H}\rangle_3).\end{aligned} \tag{2.63}$$

If one then measures the first two photons in the Bell state basis, thereby measuring which Bell state the first two photons are in, the third photon is then projected into one of four states. Each of those states can then be transformed into the original state of the first photon by using, at most, a phase flip (inversing phase between H and V) and a bit flip (switching H and V polarizations). The state of the first photon is thus teleported onto the third photon. The projected state of the third photon and the operation needed to transform it to the original state of the first photon is shown in Table 2.4 for all four Bell measurement outcomes.

Table 2.4: Projected state of the third photon after a Bell measurement on the first two photons and the operation needed to transform the this third photon into the original state of the first photon, thus completing the teleportation.

Measured Bell state	**Projected state of the third photon**	**Operation needed**
$\|\psi^+\rangle$	$\alpha\|\mathrm{H}\rangle + \beta\|\mathrm{V}\rangle$	Nothing
$\|\psi^-\rangle$	$\alpha\|\mathrm{H}\rangle - \beta\|\mathrm{V}\rangle$	Phase flip
$\|\phi^+\rangle$	$\alpha\|\mathrm{V}\rangle + \beta\|\mathrm{H}\rangle$	Bit flip
$\|\phi^-\rangle$	$\alpha\|\mathrm{V}\rangle - \beta\|\mathrm{H}\rangle$	Phase flip and bit flip

It is noteworthy that the quantum state is only transfered, not copied, therefore quantum teleportation does not violate the no-cloning theorem [11]. Any information about the state of the first photon is destroyed in the process of the Bell measurement, leaving the information in the third photon only. In addition, this cannot be used to transmit information faster than light because the teleported state requires correction, based on the measured Bell state, and the information on the specific correction cannot be sent faster than light.

Quantum teleportation has been performed in full, with the entangled pair distributed before the Bell measurement, up to 550 m [141]. A simplified version, with the Bell measurement done at the entanglement source, before the third photon is fully transfered, has also been performed up to 143 km [142, 143]. In both cases the correction is made after the teleported state is transfered. The use of satellites could potentially extend this distance by an order of magnitude (beyond 1000 km).

The choice of using the simplified version comes from the high quality mode overlap required for the Bell measurement. Both of the two photons measured in the Bell analyzer must be indistinguishable in spatial, temporal and spectral modes. This requires very precise alignment and filtering, which is made more difficult when one photon is transfered over a long distance. In addition, the full version will have the transmission attenuation on one of the photons in the Bell measurement reducing the success rate of the Bell measurement. The performance will then be limited by the double pair emission of the other photon in the Bell measurement (which can lead to false Bell measurement, where two photons from the same source are measured instead of one from each source as intended). In the simplified version, the attenuation will reduce the detection efficiency of the teleported photon while the success rate of the Bell measurement will remain the same, limiting the rate of teleportation with a false Bell measurement.

The first limitation is purely experimental, there are no fundamental effects that limit the quality of the mode overlap. In the interest of finding the limit of quantum teleportation to a satellite with current technologies, we focus on the performance with perfect mode overlap. In addition, we consider the more interesting full teleportation protocol, where the entangled pair is distributed before the Bell measurement.

In the case of a downlink, the entangled source is located on the satellite, with one photon being transmitted to the ground where the Bell measurement is performed, teleporting the state from the ground to the satellite. In an uplink, the situation is reversed, with the entangled photon source on the ground and the Bell measurement on the satellite, teleporting the state from the satellite to the ground.

The hallmark of teleportation is that the visibility of the final state (which was teleported) averaged over all signal states should be higher than that possible with an optimal quantum cloner, i.e. the maximum visibility achievable by quantum cloning ($V_{Polarization} > V_{\text{cloner}} = 2/3$) [144]. Here, V is defined as in (2.24) with N_{E} being the number of detections with polarization parallel to the polarization of the original state (that was teleported), and N_{U} being the number of detections perpendicular. Similarly to the Bell test, statistical fluctuations are included by requiring that the visibility violates the optimal quantum cloner bound by at least three standard deviations:

$$V_{Polarization} - 3\Delta V_{Polarization} \geq 2/3. \tag{2.64}$$

Using the uncertainty of an average count $\Delta\bar{N} = \sqrt{\bar{N}}$ and error propagation for independent variables [139] in Equation 2.24 we obtain:

$$\Delta V_{Polarization} = \sqrt{\frac{4N_{\text{E}}N_{\text{U}}}{(N_{\text{E}}+N_{\text{U}})^3}} = \frac{2\sqrt{N_{\text{E}}(N_{\text{total}}-N_{\text{E}})}}{N_{\text{total}}\sqrt{N_{\text{total}}}}. \tag{2.65}$$

From Equation 2.24, $N_{\text{E}} = N_{\text{total}}(V_{Polarization}+1)/2$, leading to

$$\Delta V_{Polarization} = \sqrt{\frac{1-V_{Polarization}^2}{N_{\text{total}}}}. \tag{2.66}$$

The success criteria is then, from Equation 2.64 and 2.66,

$$V_{Polarization} - 3\sqrt{\frac{1-V_{Polarization}^2}{N_{\text{total}}}} \geq 2/3. \tag{2.67}$$

One flaw of Equation 2.67 is that when $V_{Polarization}$ approaches 1, the success criteria is always met, even when N_{total} is very small. In experimental implementations, a very low

count rate will cause an inaccurate estimate of the average value of both $V_{Polarization}$ and N_{total}, making Equation 2.67 invalid as it is based on an accurate mean value of these two variables. This imposes a restriction on the minimum number of counts for a successful quantum teleportation experiment

In our simulations, the estimate of the mean value of $V_{Polarization}$ is based on the probability of detection, making it valid even in the regime of low detections. We note that the results of the performance of teleportation when taking into account orbit, loss and background, show a total number of counts of $N_{\text{total}} > 100$ for each satellite passes that were deemed successful.

Figure 2.21 shows the total number of counts necessary for a successful teleportation, which is given by

$$N_{\text{total}} > 81 \frac{1 - V_{Polarization}^2}{(3V_{Polarization} - 2)^2}. \tag{2.68}$$

The simulations for quantum teleportation require both an entangled photon source and a single-photon source to produce the photon state to be teleported. The single-photon source can be a WCP source, an heralded photon from a spontaneous parametric down-conversion (SPDC) source (an SPDC source where one photon from the pair is measured to confirm the presence of the other), or a sub-Poissonian source (such as the single-photon emission from a quantum dot). All three sources were simulated, with both the WCP source and heralded SPDC source yielding performances too low for most satellite experiments. This low performance is due to the double emission rates (two photons or two photon pairs emitted in the same time window). The sub-Poissonian source was based on recently published results of a single-photon source based on a quantum dot in a photonic nanowire [145]. The results reported a second-order quantum correlation function of $g^{(2)}(0) < 0.008$. The second-order quantum correlation function is proportional to the probability that, when a photon is emitted, a second photon is also emitted [118]. This function is defined by:

$$g^{(2)}(0) = \frac{\langle\psi| a^\dagger a^\dagger a a |\psi\rangle}{(\langle\psi| a^\dagger a |\psi\rangle)^2}. \tag{2.69}$$

The single-photon state is represented by a mixture of Fock states:

$$|\psi\rangle = \sqrt{1 - p_1 - p_2}\,|0\rangle + \sqrt{p_1}\,|1\rangle + \sqrt{p_2}\,|2\rangle\,, \tag{2.70}$$

where p_1 is the probability of a single-photon emission, p_1 is the probability of a two photon emission, and all other multi-photon emissions have been ignored. Using this state in the definition of $g^{(2)}(0)$ yields:

$$g^{(2)}(0) = \frac{2p_2}{(p_1 + 2p_2)^2}. \tag{2.71}$$

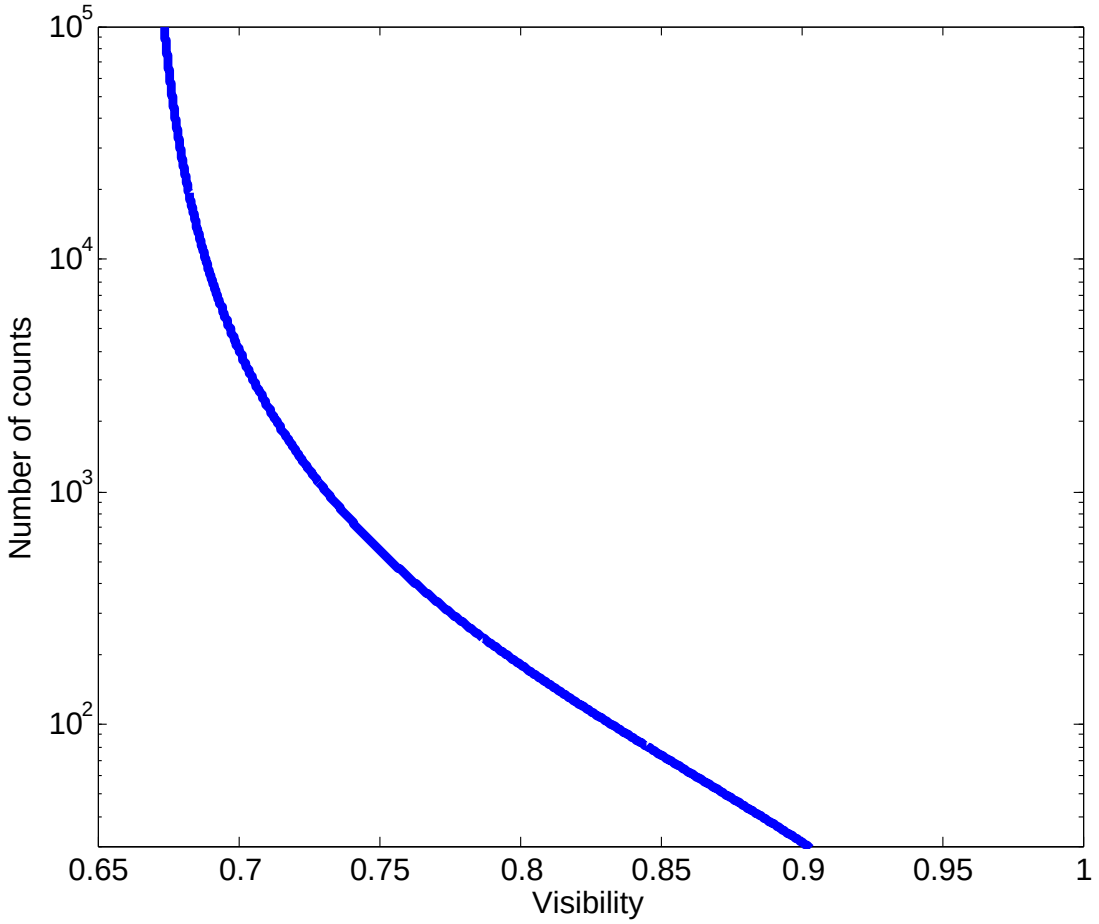

Figure 2.21: Required number of measured photon for a successful teleportation accounting for three standard deviations with non perfect visibility. The number increases rapidly as we approach the minimum visibility of $V_{Polarization} = 2/3$. This relation is only valid when used with accurate estimates of $V_{Polarization}$ and N_{total} and therefore cannot be used in experimental implementations if the total number of counts is too low to produce accurate estimates.

From this the probability of two photon emission is:

$$p_2 = \frac{1 - \sqrt{1 - 4p_1 g^{(2)}(0)}}{\sqrt{8g^{(2)}(0)}}. \tag{2.72}$$

In the simulations, one photon from the entangled photon source (Equation 2.36) is sent through the optical link before being measured, along with the photon from the single-photon source (Equation 2.69), in the Bell basis. The Bell analyzer consists of a non-polarizing beam splitter, with each of the two photons going to one input, one polarizing beam splitter at each output of the non-polarizing beam splitter (two in total) and one detector at each output of the polarizing beam splitters (four in total). This arrangement allows for the measurement of two of the Bell states (leaving the other two indistinguishable), thereby reducing the efficiency to half. This is the maximum achievable efficiency of a Bell analyzer when using linear optics [146]. The result of the measurement dictates the correction on the last photon before its measured. We note that higher teleportation success probabilities can be achieved by increasing the number of modes of the prepared entangled state [147], at the cost of increased complexity.

The prediction of the measurement outcome is again done using realistic detectors with the link loss applied to the transmitted photon (using a lossy non-polarizing beam splitter) before the Bell analyzer. The detection efficiency of the two non-transmitted photons (photons 1 and 3) is taken to be the efficiency of the detector and optical components ($\eta_d \eta_o$). Finally the received background is distributed among all four detectors of the Bell analyzer and the detector dark counts (D_{dark}) is included in the detection of the final teleported state (photon 3).

The performance of the teleportation is strongly dependent on the strengths of the SPDC (ε) and single-photon source (p_1) states, as shown in Figure 2.22. The optimal value of ε tends to increase with loss, while the optimal value of p_1 decreases. This is because the number of photons from the entangled photon source that reaches the Bell analyzer decreases with higher loss. This increase in ε mitigates this reduction while the reduction in p_1 reduces the number of double pair emission which cause false Bell measurement. A successful teleportation requires both high visibility (high number of true Bell measurement compared to false Bell measurement) and high count rates (to minimize the uncertainty).

For our simulations, two representative sets of parameters were chosen: $\varepsilon = 0.15$ and $p_1 = 0.007$ for downlink simulations (where the usable part of a pass is typically around 35–40 dB of total loss with 180–200 background counts) and $\varepsilon = 0.3$ and $p_1 = 0.0045$ for uplink simulations (usable part possessing around 40–45 dB loss and 250–750 background counts). The parameters lead to entangled pair production rates of ≈22.5 MHz in a

downlink and ≈90 MHz in a uplink with single-photon emission rates of ≈7 MHz and ≈4.5 MHz respectively.

Some examples of the calculated teleportation polarization visibility and count rate for the optimized parameters are shown in Figure 2.23 and 2.24. Similarly to the case of QKD, the ideal polarization visibility, $V_{Polarization} = 100\%$, is reduced by the signal to noise ratio in the detectors, the slight polarization misalignment and the multi-pair emissions. A unique feature is that the polarization visibility drops significantly at low losses. This drop is due to the multi-pair emissions of the entangled source. In the low loss regime, the false Bell measurement caused by these multi-pair emissions becomes comparable to the true Bell measurements, limited by the low rate of the single-photon source (optimized for higher loss regimes).

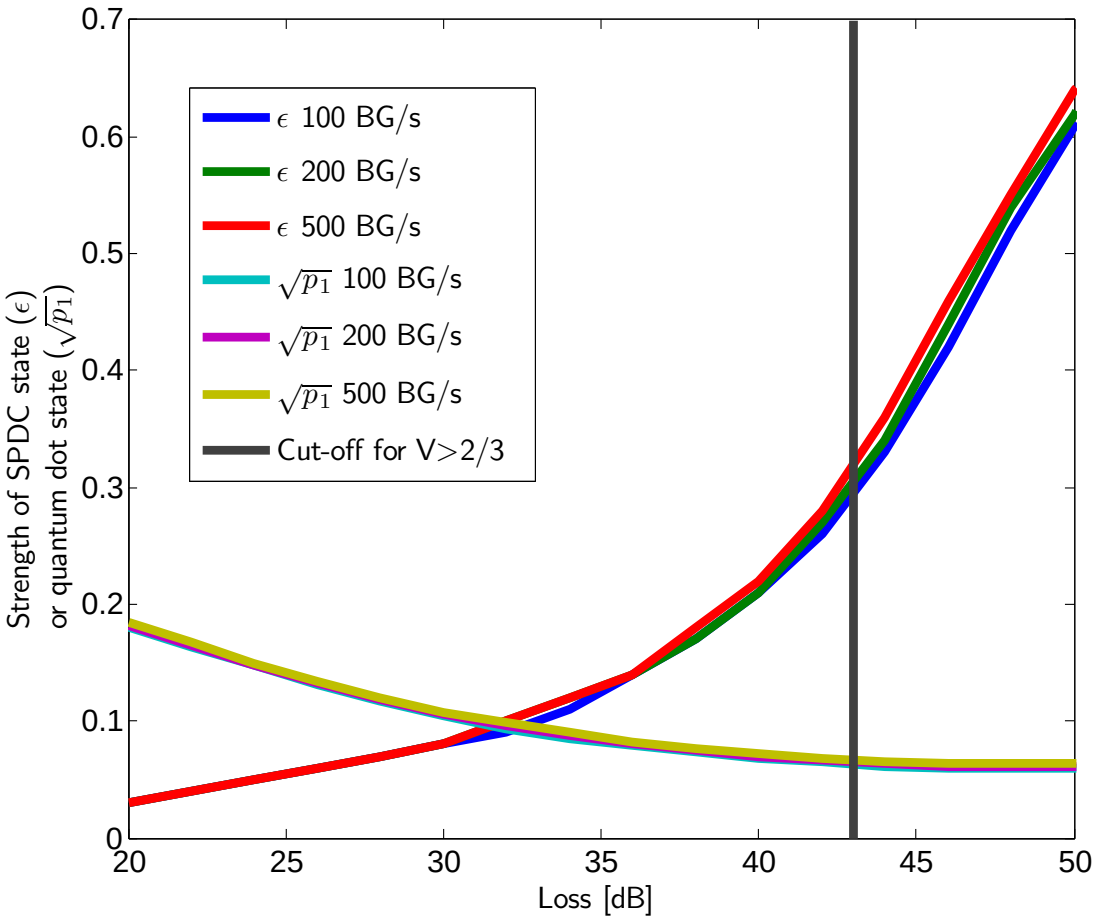

Figure 2.22: Optimized parameters ε and p_1 for teleportation as a function of channel loss, for various background counts per second per detector (BG/s). Here p_1 is the probability of a single-photon emission from the single-photon source, (2.69), whose polarization is teleported. Similarly, ε is the strength of the entangled photon state from SPDC, (2.34), with average number of pairs per pulse $2\sinh^2\varepsilon$. As the loss increases, the optimal value ε increases while the optimal value of p_1 decrease. Above 43 dB (grey vertical line) the teleportation is no longer able to produce the required visibility of $V \geq 2/3$. Both sources are pumped at a frequency of 1 GHz, leading to an entangled pair production rate of $\approx\varepsilon^2\times 10^9$ Hz and a single-photon emission rate of $\approx p_1\times 10^9$ Hz.

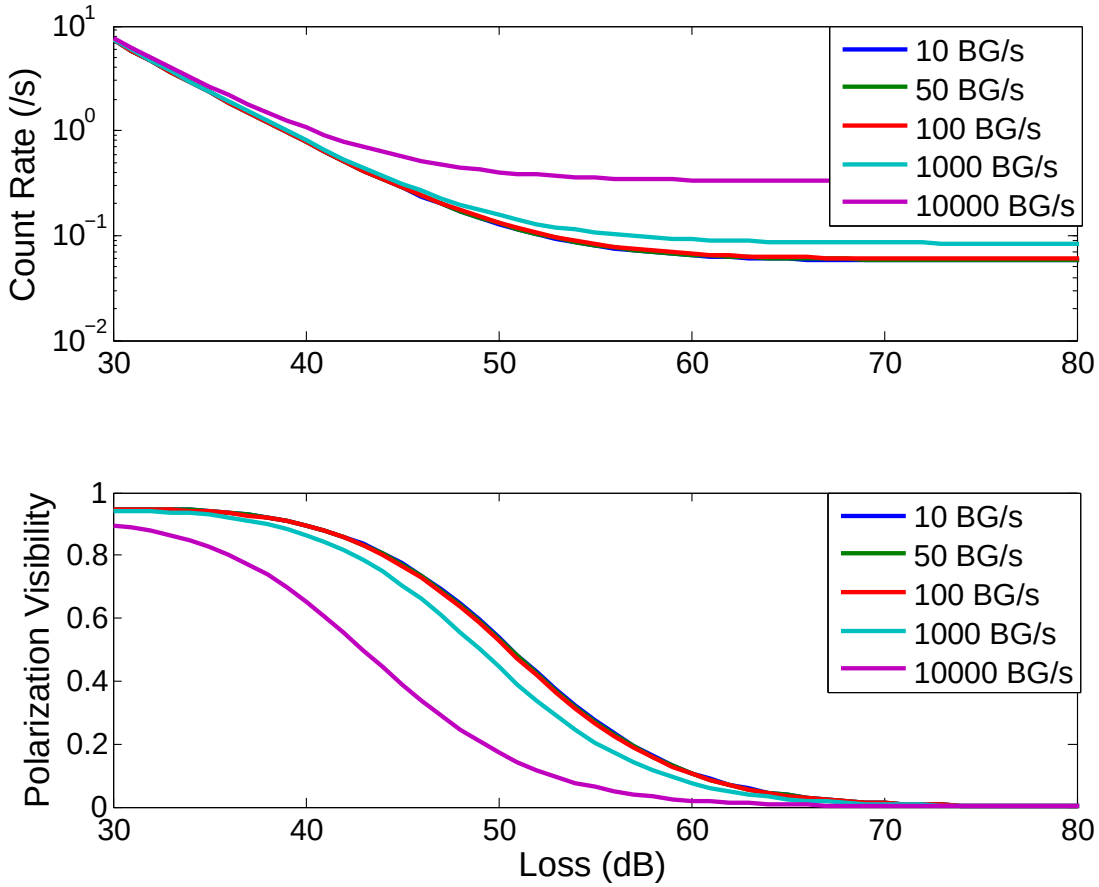

Figure 2.23: Teleportation polarization visibility and count rate as functions of channel loss, for various background count rates (BG/s) per detectors, using the parameters optimized for a downlink ($\varepsilon = 0.15$ and $p_1 = 0.007$). Both sources are pumped at a frequency of 1 GHz. In addition to the reduction from background and polarization misalignment, visibility is reduced at low loss because of double-pair emissions in the entangled source.

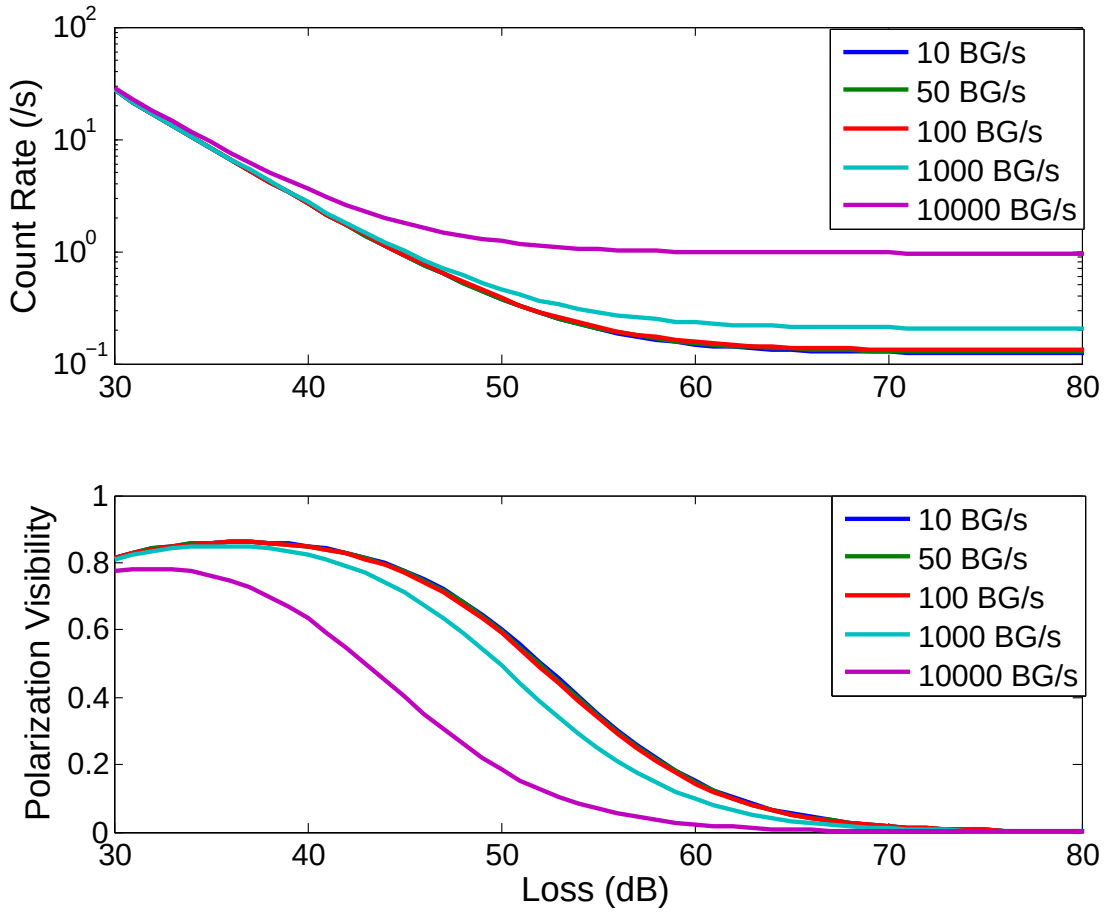

Figure 2.24: Teleportation polarization visibility and count rate as functions of channel loss, for various background count rates (BG/s) per detectors, using the parameters optimized for a an uplink ($\varepsilon = 0.3$ and $p_1 = 0.0045$). Both sources are pumped at a frequency of 1 GHz. Once again visibility is reduced by background and polarization misalignment, and double-pair emissions in the entangled source at low loss. The visibility suffers more degradation at low loss compared to the visibility in the downlink optimized parameter because the strength of the SPDC (ε) is higher. This causes more double-pair emissions which lead to a higher rate of false Bell measurement, where the Bell measurement is due to two photons from the entangled source rather than one photon from the entangled source and one photon from the single-photon source.

2.5 Results of the performance analysis

Each parts of the performance analysis (orbit, loss, background, quantum optical simulations, and calculation of the key rate or performance of the fundamental experiment), comes together to give a realistic estimate of the performance. With the orbit (Section 2.1), loss (Section 2.2) and background (Section 2.3), we obtain the the total loss and projected background counts for each nighttime satellite passes in one year. The loss and background for some example passes are shown in Figure 2.25. Even with an increase of the satellite telescope's diameter by a factor of 3, the atmospheric turbulence causes the uplink to experiences more loss (by ≈5 dB) than a downlink. The artificial light pollution also causes the background count rate for an uplink to be almost an order of magnitude higher than a downlink.

In both cases, the loss decreases as the satellite approaches zenith, mainly due to the decrease in atmospheric transmission (and turbulence) but also because of the shorter distance between the satellite and the ground (reducing diffraction and pointing error losses). This also means lower loss for background photons, thus leading to an increase in background counts. In an uplink however, the ground area imaged by the satellite also reduces near zenith, reducing the background photons collected overall.

The loss and backgound for each passes is then used in the simulation of photonic quantum communication (Section 2.4) to calculate the QBER and raw key rate for QKD, and the visibility and count rate for fundamental experiments. Examples of the QBER and raw key rate for different passes are shown for a WCP source in Figure 2.26 and for an entangled photon photon source in Figure 2.27. A WCP source can have a higher repetition rate than an entangled photon source, on the order of GHz [148, 149] compared to MHz for the entangled photon source [150]. For our simulations, we use a source rate for the WCP of 300 MHz and an entangled photon source pair production rate of 100 MHz.

The polarization visibility and count rates of teleportation are shown in Figure 2.28. Because of the similarity between a Bell test and entanglement-based QKD, they will produce the same visibility and count rates, with $V_{Entangled} = 1 - 2\,\mathrm{QBER}$ (Equation 2.39) and the count rate equal to the raw key rate.

With the QBER (visibility) and raw key rate (count rate) we can finally calculate the final key length (success of fundamental experiment) for each nighttime passes in our one year orbit analysis. Before proceeding to the final results we first look at determining the optimal wavelength that will yield the best performances.

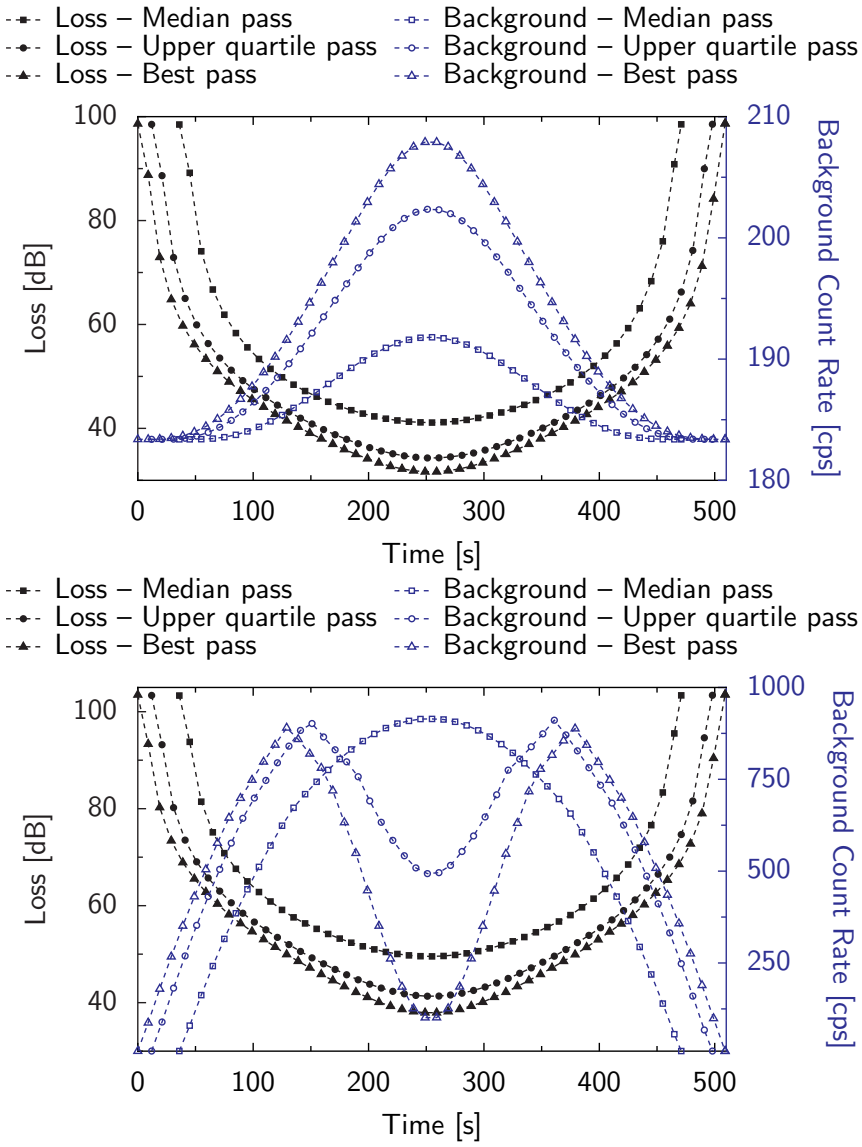

Figure 2.25: Loss and detected background count rate during the best pass, upper quartile pass, and median pass for a downlink (top) and an uplink (bottom). The uplink background is mainly due to artificial light and is lower at high elevation angle, when the satellite has a smaller field of view area on the ground. Orbit altitude is 600 km. For downlink, wavelength is 670 nm and satellite transmitter telescope diameter is 10 cm. For uplink, wavelength is 785 nm and satellite receiver telescope diameter is 30 cm. In both cases, the receiver applies an optical filter with 1 nm bandwidth on the background. The possible extra loss from this filter is assumed to be contained in the optical losses of the polarization analyzer (see 2.2.5). Ground telescope is 50 cm with pointing error of 2 μrad and rural sea-level atmosphere. The range and elevation of these passes are shown in Figure 2.2.

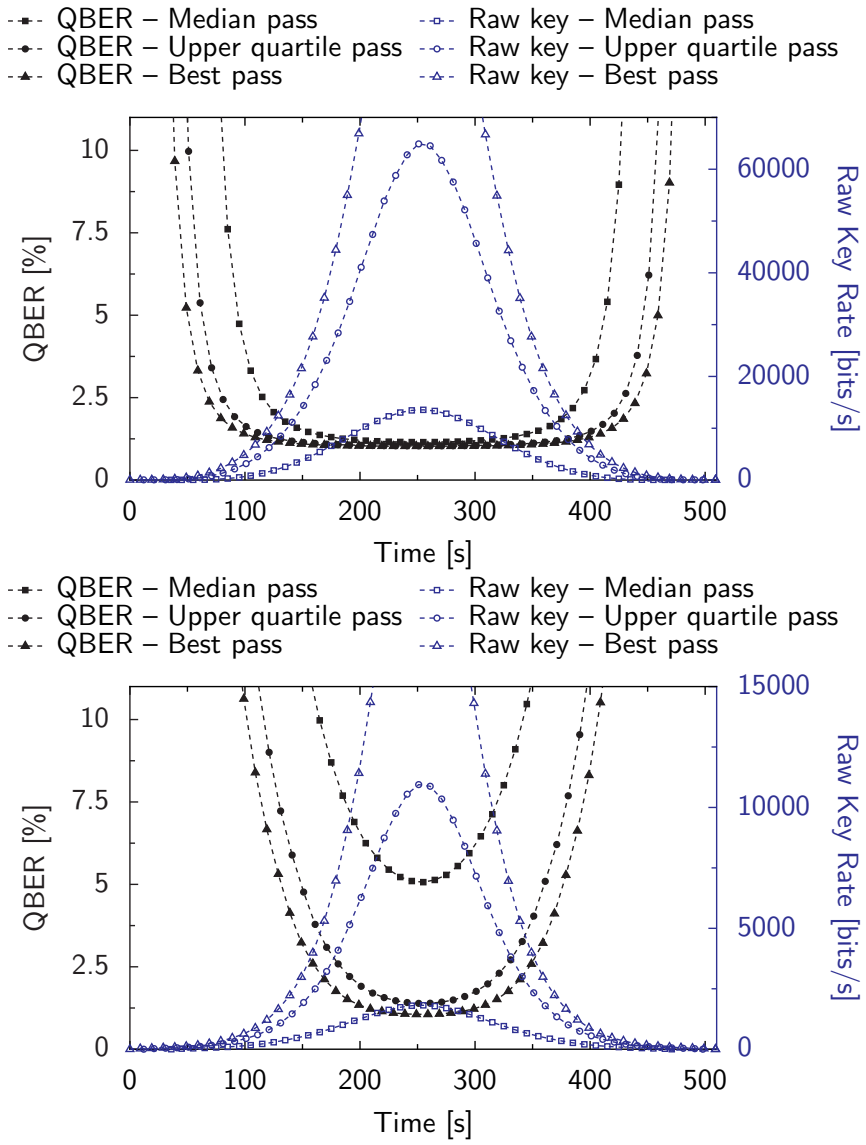

Figure 2.26: QBER and raw key rate during the best pass, upper quartile pass, and median pass for a downlink (top) and an uplink (bottom) utilizing a WCP source. The QBER is significantly higher at low elevations, preventing the generation of secure key from the raw key for most protocols when the QBER is above 11%. Altitude, wavelength, telescope and atmospheric conditions follow Figure 2.25. Source rate: 300 MHz; detector dark count rate: 20 cps; detection time window: 0.5 ns.

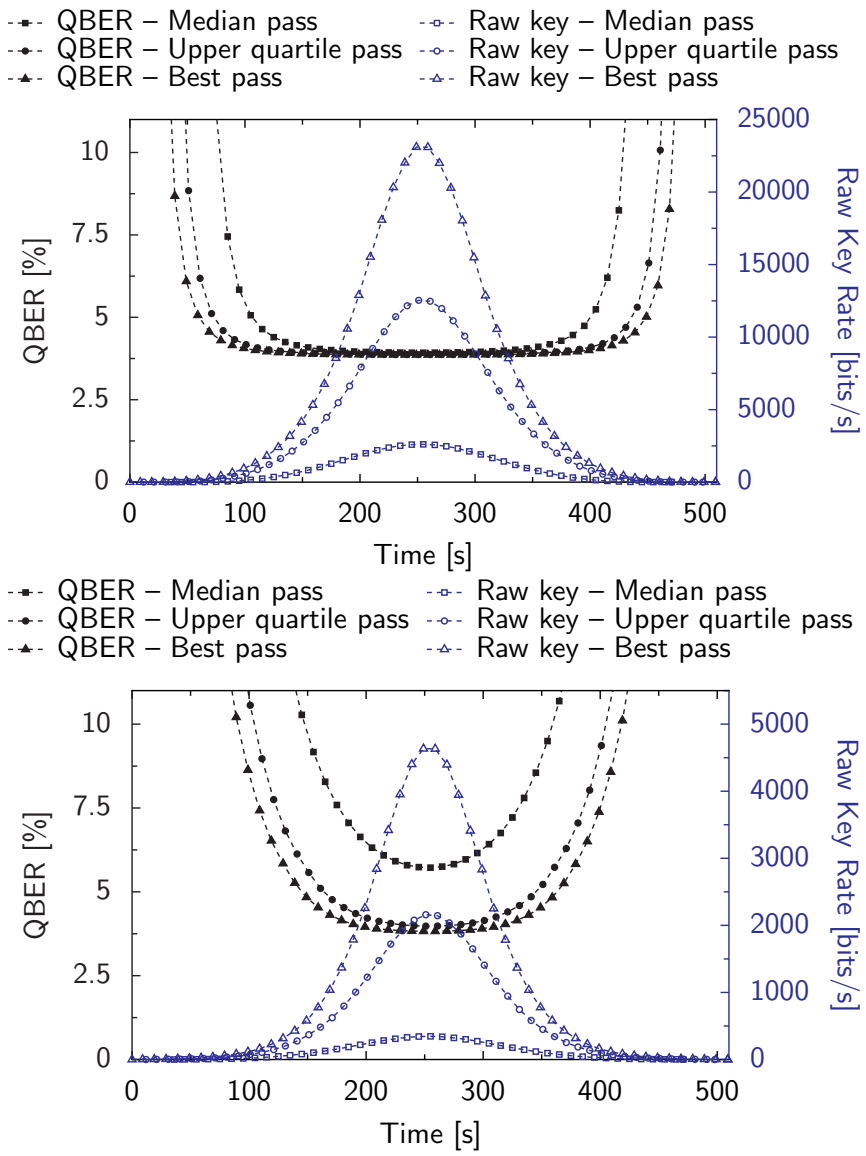

Figure 2.27: QBER and raw key rate during the best pass, upper quartile pass, and median pass for a downlink (top) and an uplink (bottom) utilizing an entangled photon source. The entangled photon source has a higher intrinsic QBER than the WCP source, primarily because of multi-pair emissions and a lower source rate. Altitude, wavelength, telescope and atmospheric conditions follow Figure 2.25. Source rate: 100 MHz; detector dark count rate: 20 cps; detection time window: 0.5 ns.

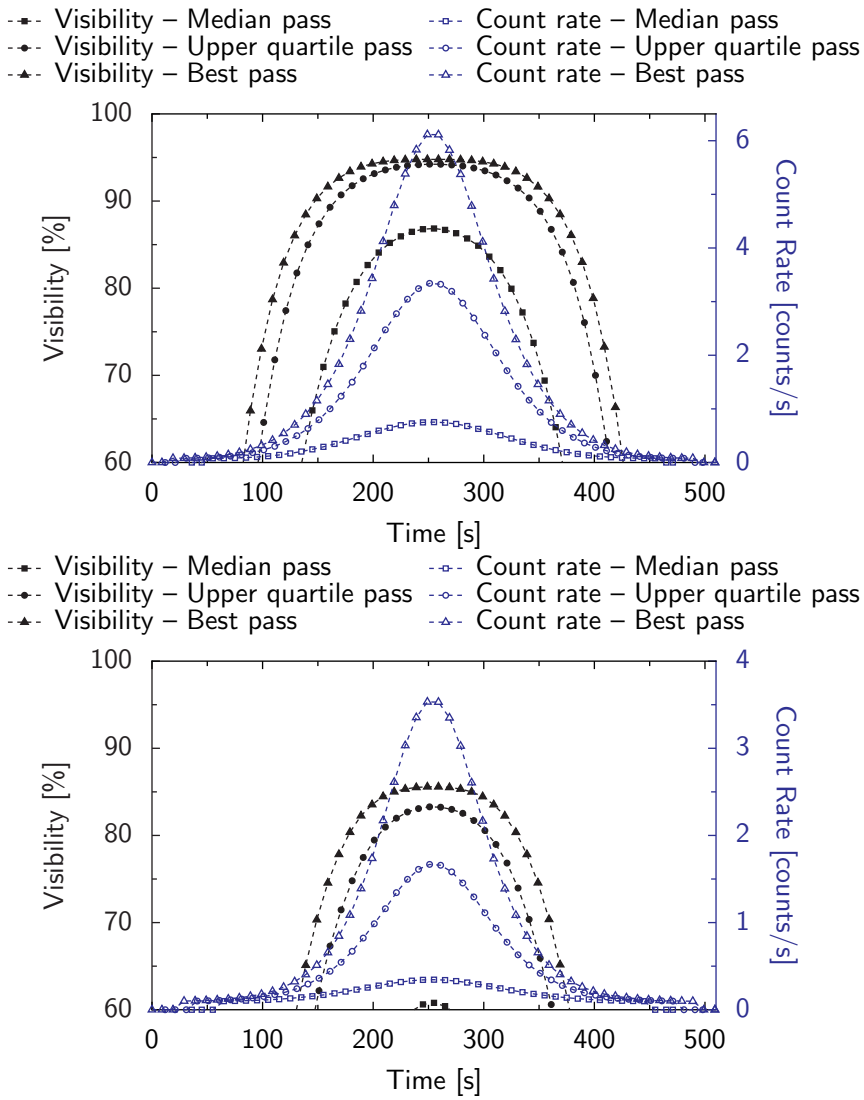

Figure 2.28: Polarization visibility and count rate of teleportation during the best pass, upper quartile pass, and median pass for a downlink (top) and an uplink (bottom). Altitude, wavelength, telescope and atmospheric conditions follow Figure 2.25. A successful teleportation requires a visibility of at least 2/3 and the part of the pass below this minimum visibility will be unable to contribute positively to the success of teleportation. Pump rate: 1 GHz with the optimized parameters obtained from Figure 2.22; detector dark count rate: 20 cps; detection time window: 0.5 ns.

2.5.1 Determination of the optimal wavelength

Several effects are influenced by wavelength: Longer wavelengths will increase diffraction losses, whereas atmospheric transmittance and turbulence losses will be reduced. As the magnitudes of these depend on transmitter and receiver telescope sizes, so too will the wavelength that minimizes the total loss from both effects. For a satellite incorporating a downlink, it is preferable to use a robust and space-qualified laser either as a WCP source or as part of an entangled photon source. Ideally this would consist of a diode laser module, capable of producing a certain wavelength or wavelengths within a very small bandwidth range. However, diode lasers exist only for certain specific wavelengths, limiting the choices available (wavelengths we considered are shown in Figure 2.7). Finally, the detector efficiency will also be wavelength dependent.

To properly determine the optimal wavelength, we examine the secure key length that can be obtained during an upper quartile pass. The results (Table 2.5) suggest that the common 670 nm laser line is a highly suitable wavelength for a downlink, be it using a WCP or an entangled photon source. The optimal wavelength for the uplink is higher, closer to the laser line at 785 nm, owing to the reduction of atmospheric turbulence. Table 2.5 also shows that ≈800 nm, typical of spontaneous parametric down-conversion entangled photon sources, would work well in both cases. The examples presented so far have used the optimal wavelengths of 670 nm and 785 nm.

2.5.2 Performance of satellite quantum communication

The performance of QKD is obtained by accumulating key rate statistics for the full one-year set of satellite passes, with various transmitter and receiver telescope sizes, to determine the expected number of secure key bits generated each month. Each pass generates a secure key independently—gradual accumulation of cryptographic key bits from each satellite pass ensures these bits are available for use when required.[1]

We further assume that only half of the nights have clear skies, automatically rendering half the passes unusable due to cloud coverage. Actual cloud coverage will depend on the ground station location ultimately chosen. The average global cloud coverage on land is between 50–90%, with over 25% of clouds having a thin density [151]. Many areas, particularly in drier or more elevated regions, experience less than 20% cloud cover, some having

[1] One could obtain a larger monthly secure key by combining the raw keys of several passes, thereby reducing finite-size effects, at the cost of a reduction in the frequency of key accumulation/usage.

Table 2.5: Calculated length of distributed cryptographic key for various wavelengths with a WCP (left) and an entangled photon (right) source. Of the laser-line wavelengths studied, 670 nm produces the longest key for a downlink, while 785 nm produces the longest key for the uplink. Downlink is with a 10 cm transmitter and a 50 cm receiver; uplink is with a 50 cm transmitter and a 30 cm receiver. Simulations are of the upper quartile satellite pass (in terms of pass duration) with a 600 km orbit, pointing error of 2 μrad, and rural atmosphere (5 km visibility) at sea-level. Source rate: 300 MHz for WCP and 100 MHz for entangled photon source; detector dark count rate: 20 cps; detection time window: 0.5 ns.

Wavelength [nm]	**Secure key length obtained for the upper quartile satellite pass [kbit]**			
	Downlink, WCP source	**Uplink, WCP source**	**Downlink, entangled photon source**	**Uplink, entangled photon source**
405	236.8	8.0	10.8	0
532	914.7	88.5	128.1	12.1
670	1606.4	235.1	306.7	57.4
785	1582.2	301.0	269.9	68.5
830	1090.5	215.8	146.9	39.5
1060	604.6	187.0	32.6	12.4
1550	415.9	254.5	20.2	20.6

near 0% cloud cover [152]. A location with 50% cloud coverage would likely represent a worst case of any site that would be reasonably considered.

The results, illustrated in Figures 2.29 and 2.30, show that a downlink can generate more secure key bits than an uplink for the same ground and satellite telescopes. Furthermore, the WCP source outperforms the entangled photon source, due in part to the higher source rate for WCP, and in part to the inefficiency of detecting the transmitter's photon in the entangled pair.

From these results, a downlink with a satellite transmitter telescope as small as 10 cm and a receiver of 50 cm could be used to successfully exchange a key of 4.3 Mbit per month with an entangled photon source, and 23 Mbit per month with a WCP source. In an uplink, a 30 cm receiver telescope on the satellite and a ground transmitter of at least 25 cm could produce 0.4 Mbit key per month with an entangled photon source and 2.2 Mbit per month with a WCP source.

In addition, varying the size of the ground transmitter telescope in an uplink has little effect on the number of key bits generated. This is because, for a transmitter telescope of 25 cm or more, turbulence dominates the beam divergence, limiting any gains that could otherwise be found by reducing diffraction via increasing the transmitter telescope diameter. This behavior was shown in Figure 2.5.

In the long-distance performance of fundamental quantum experiments (Bell tests and quantum teleportation), we analyse each satellite pass independently to determine which pass can perform a successful Bell test or teleportation with 3σ certainty. Since data from an entire pass is needed for success, we calculate the minimum ground-satellite distance of each successful pass. Finding the greatest of these minima from all passes gives the longest distance test achievable with our parameters. That is, at least one pass from our simulated year of orbits will be capable of performing the experiment with a 3σ violation while maintaining, for the entire experiment, a distance at least the "maximum distance" reported. These maximum distances are shown in Figures 2.31 and 2.32.

These results show that a downlink with a satellite transmitting telescope of 10 cm and a receiver of 50 cm reaches a distance of 1650 km in a Bell test and 1080 km for teleportation. In an uplink, a 30 cm receiver telescope on the satellite and a ground transmitter of 25 cm would be capable of performing a Bell test at 1225 km and teleportation at 745 km. Both are significantly beyond that which can be achieved on the ground alone.

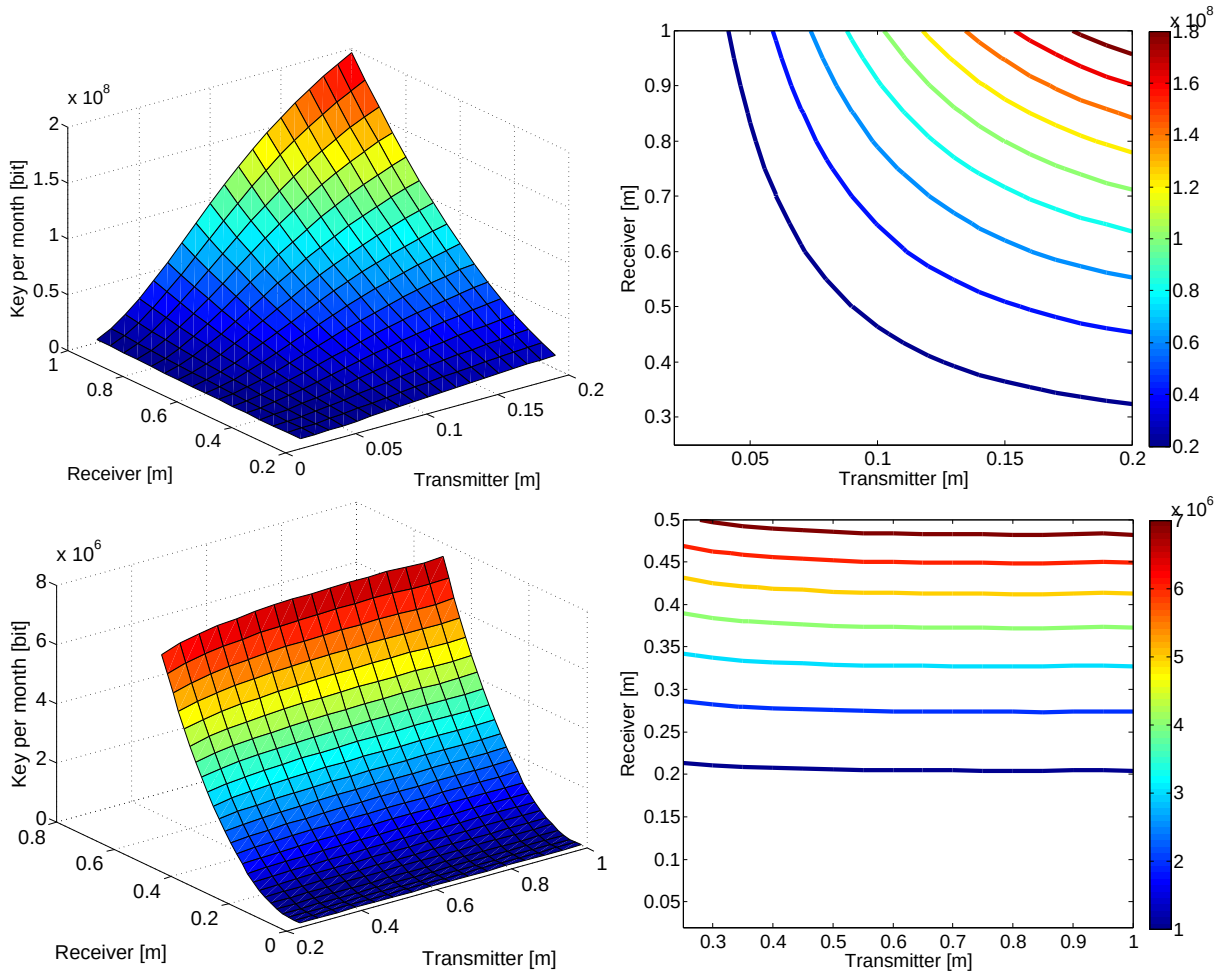

Figure 2.29: Estimated key per month with a WCP source for various telescope sizes, assuming half the passes are unobstructed by cloud cover. Top: downlink; bottom: uplink. A downlink with a satellite transmitter telescope of 10 cm and a receiver of 50 cm could be used to successfully exchange a key of 23 Mbit per month, while an uplink with a 30 cm receiver telescope on the satellite and a ground transmitter of 25 cm could produce 2.2 Mbit per month. In an uplink, the size of the ground transmitter has little importance because atmospheric turbulence dominates diffraction. Conditions are as in previous figures, with a downlink wavelength of 670 nm, uplink wavelength of 785 nm, and source rate of 300 MHz.

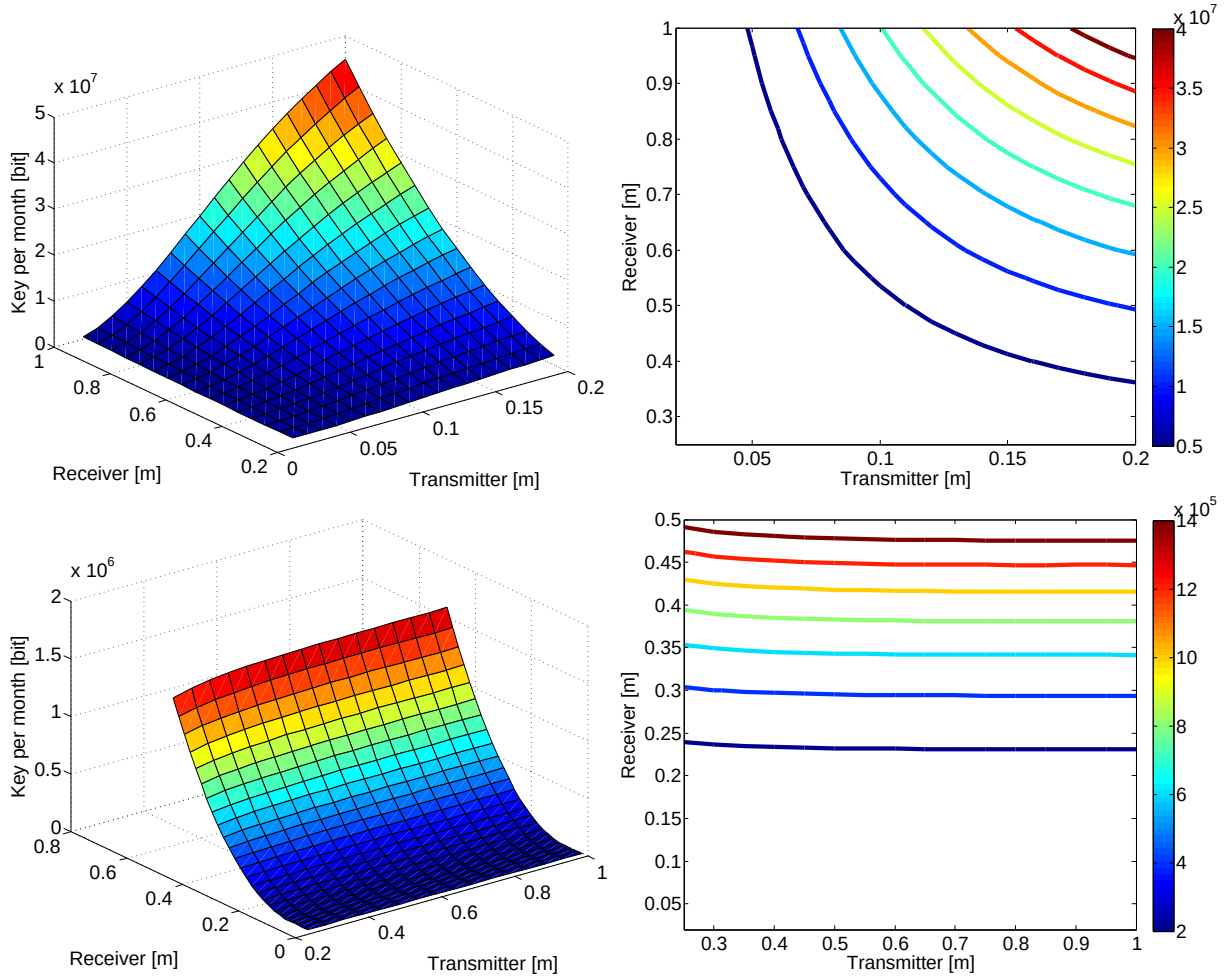

Figure 2.30: Estimated key per month with an entangled photon source for various telescope sizes, assuming half the passes are unobstructed by cloud cover. Top: downlink; bottom: uplink. A downlink with a satellite transmitter telescope of 10 cm and a receiver of 50 cm could be used to successfully exchange a key of 4.3 Mbit per month while an uplink with a 30 cm receiver telescope on the satellite and a ground transmitter of 25 cm could produce 0.4 Mbit per month. Again, the size of the ground transmitter in the uplink has little importance because atmospheric turbulence dominates diffraction. Conditions are as in previous figures, with a downlink wavelength of 670 nm, uplink wavelength of 785 nm, and source rate of 100 MHz.

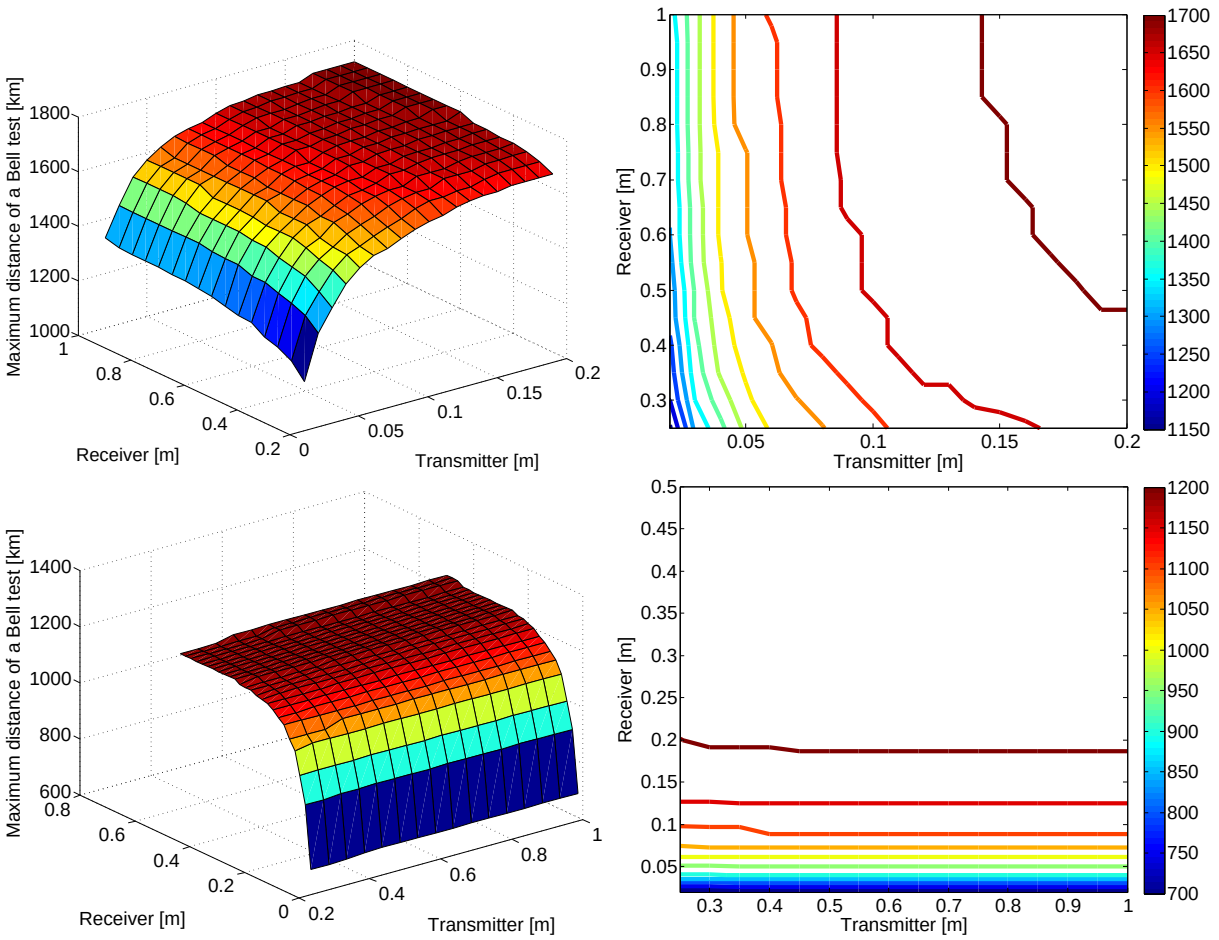

Figure 2.31: Maximum distance of a complete Bell test in a downlink (top) and an uplink (bottom) for various telescope sizes. A downlink with a satellite transmitter telescope of 10 cm and a receiver of 50 cm could be used to successfully violate the CHSH inequality at 1650 km, while an uplink with a 30 cm receiver telescope on the satellite and a ground transmitter of 25 cm could violate it at 1225 km. Jagged contours are an artifact of the finite sample of passes for the one year duration, leading to a discrete spectrum of possible distances. Conditions are as in previous figures for an entangled photon source (100 MHz).

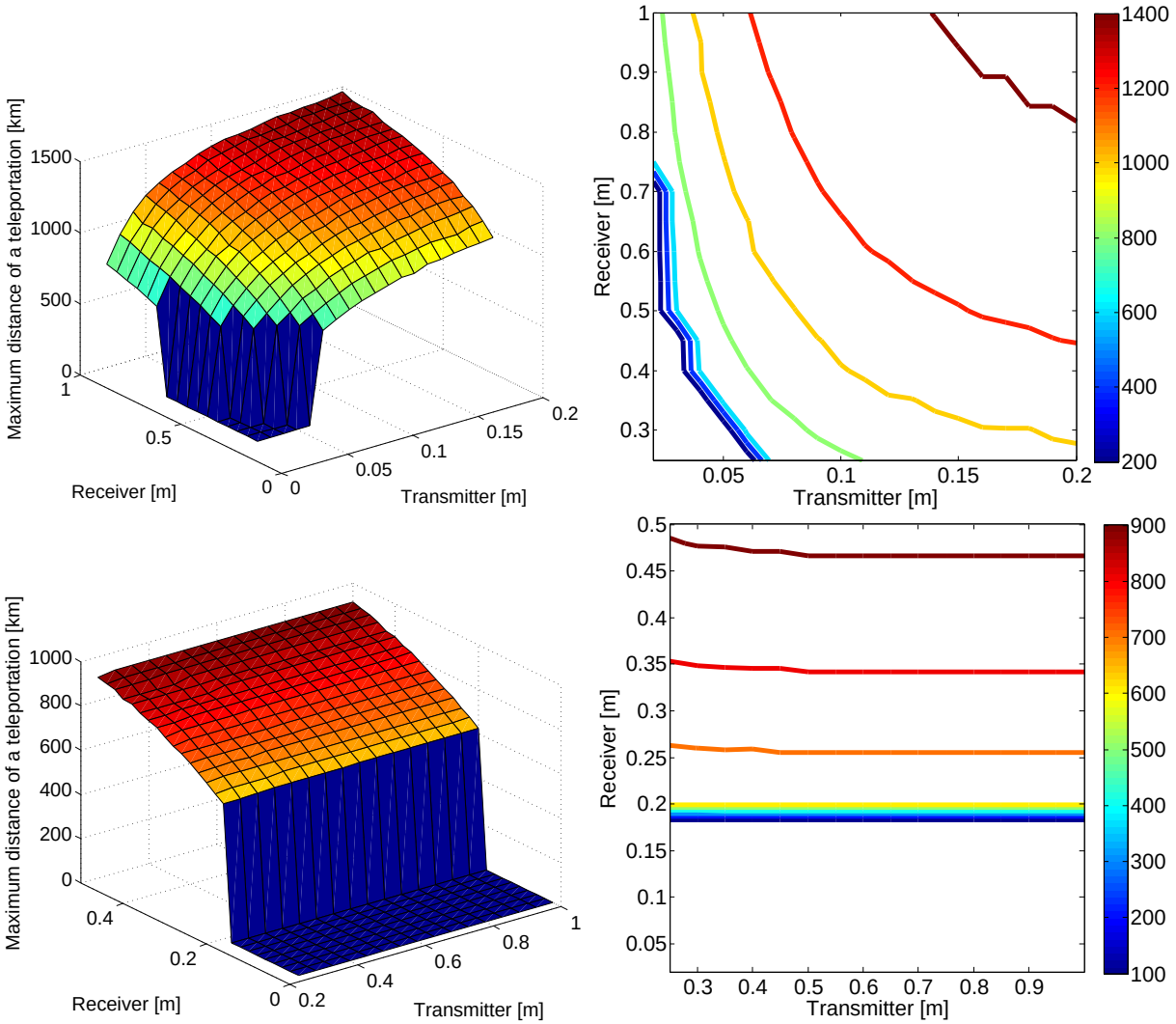

Figure 2.32: Maximum distance of a complete teleportation experiment in a downlink (top) and an uplink (bottom) for various telescope sizes. A downlink with a satellite transmitter telescope of 10 cm and a receiver of 50 cm could be used to successfully perform teleportation at 1050 km, while an uplink with a 30 cm receiver telescope on the satellite and a ground transmitter of 25 cm could perform it at 675 km. For small telescope sizes, teleportation cannot be performed with sufficient statistical certainty for any satellite pass studied. Again, jagged contours are due to the finite sample of passes. Other conditions are as in previous figures using the optimized teleportation parameters (Figure 2.22).

2.5.3 Effect of detector degradation in space

For experiments involving detectors on the satellite, the exposure to radiation in the space environment is expected to lead to an increase in the dark count rate over time [153, 154], the degree to which can be mitigated by appropriate shielding. To account for these effects we performed a preliminary analysis of the effect of increased detector dark counts on the performance of satellite quantum communication.

For QKD with a WCP source, only the receiver contains detectors and this detector degradation will only occur in an uplink. For both QKD with an entangled source and Bell test, the detection of one photon from the pair must be performed at both the transmitter and the receiver, leading to the same effect of detector degradation in both uplink and downlink.

Finally, in teleportation, the transmitter performs the measurement of the final teleportated state (using two detectors) while the receiver performs the Bell measurement on the other two photons (using for detectors). Because of the loss suffered by the transmitted photon used in the Bell test, the Bell measurement will be much more sensitive to noise. Therefore, in all considered experiments, the uplink will suffer from detector degradation at least as much (if not more) than the downlink. It was thus sufficient to limit our analysis to the uplink, placing an upper bound on the effects for a downlink.

The results of this preliminary analysis are summarized in Table 2.6. These show that a dark count rate on the order of 1000 cps would only cause a major effect on the performance of QKD when using a WCP. All other experiment only suffer small degradation in performance. This is because they rely on coincidence counts with the ground, which is far more robust to noise. Unfortunately, a dark count rate on the order of 10000 cps prevents all experiment from being performed successfully. These results provide important guidelines for determining the requirement of radiation hardening.

2.5.4 Advantages of an uplink

It is evident from our analysis that a downlink outperforms an uplink in general, and would thus be the preferred option for global QKD implementation. However, it should be recalled that a downlink requires finer pointing of the satellite than an uplink. In addition, a downlink would require the (complicated) quantum source to be on the satellite while the uplink only requires the (simpler) detectors to be on the satellite. These factors make an uplink technologically simpler.

Table 2.6: Effect of higher dark counts in the detectors on the key generation and on the maximum distances of fundamental experiments. QKD (with either a WCP source or an entangled photon source), Bell tests and teleportation are resistant to detector dark count rate increase of up to 1000 cps. Wavelength 785 nm, 50 cm transmitter and a 30 cm receiver. Orbit 600 km, pointing error 2 μrad, and rural atmosphere (5 km visibility) at sea-level. Source rate: 300 MHz for WCP and 100 MHz for entangled photon source; detection time window: 0.5 ns.

Detector dark [cps]	**WCP source key [Mbit/-month]**	**Entangled source key [Mbit/-month]**	**Max. Bell test distance [km]**	**Max. teleportation distance [km]**
20	2.431	0.417	1225	747
100	2.161	0.396	1162	747
1000	0.695	0.241	918	700
10000	0	0	0	0

An uplink also allows the source to be easily interchangeable, permitting a wider range of experiments and tests. With these considerations in mind, a strong argument can be made that an uplink is the better choice to scientifically study global-scale QKD implementations (and other experiments) prior to implementing a full-scale (possibly downlink) global QKD system.

Chapter 3

Demonstration of QKD at High losses

To show the experimental feasibility of satellite QKD we performed full QKD protocols at the high losses expected for a satellite uplink. A similar experiment was performed in 2011 where the feasibility of QKD was demonstrated at up to 57 dB of loss [59]. While this was a great step toward demonstrating high loss QKD, this demonstration did not perform the necessary QKD protocols, such as error correction and privacy amplification to extract any secure key from the system. In addition, the quantum receiver consisted of only one measurement basis (H/V or D/A). The measurement basis could be manually changed between data collection using a half-wave plate but remained fixed during each runs, making the system insecure. Finally the analysis was done in asymptotic limit (see Equation (2.27)) and did not take any finite-size statistics into account, making the 57 dB result impractical in real life applications where the key generation time is finite. Because of these shortcomings, the initial demonstration was insufficient in demonstrating high loss QKD in a realistic regime. This investigation focuses on high average loss, a future investigation could explore the effect of a varying channel loss by simulating turbulence [155], but since QKD is only dependent of the total received signals, a varying loss will not negatively impact the performance.

The experiment described in this chapter aims to improve over the initial 2011 demonstration by correcting these shortcomings. We implemented a two-basis measurement with passive basis choice, full decoy state QKD protocols and finite-size effects. While these improvements represent an important and necessary milestone in demonstrating secure QKD at high loss, further improvements will still be necessary in the future. Notably, we do not implement a fully random sequence of polarization and intensity states, instead implementing a repeating sequence of 128 bits. A truly random sequence would be require to ensure an eavesdropper cannot gain any information on the states. We also do not

implement true vacuum pulses, instead measuring the background between pulses, which could be manipulated by an eavesdropper. While the security flaws do not affect the lab demonstration of QKD at high loss (where we know there where no eavesdropper present), they will need to be addressed before deployment to ensure a truly secure system.

The experimental setup used for this demonstration includes a weak coherent pulse (WCP) source, a free-space quantum channel with adjustable loss and a quantum receiver. These components are described in Section 3.1. Section 3.2 details the software used to perform the full QKD protocols and its performance under the limited computing power of a satellite receiver. Lastly, in Section 3.3 we show the capabilities of our system to extract secure key both at fixed high loss communications and when simulating the varying loss of a satellite pass.

Author contributions

Nikolay Gigov developed the QKD software and analysed its performance. Evan Meyer-Scott built the WCP source. Zhizhong Yan built the intensity and polarization modulator. Brendon Higgins designed and built the automated polarization compensation system, analyzed its predicted performance, as well as designed and built the quantum receiver. Thomas Jenewein, Brendon Higgins and Norbet Lütkenhaus provided advice on the security analysis for QKD. I aligned the optical systems. Nikolay Gigov and I performed the experiment. Nikolay Gigov, Brendon Higgins, and I analyzed the results.

3.1 Experimental setup

Our high-loss QKD system is composed of a WCP source, a quantum channel with adjustable loss and a quantum receiver. The source generates photon states at a wavelength of 532 nm using up-conversion of a pulsed 810 nm laser and a continuous-wave 1550 nm laser. The pulsed laser allows for short pulses with good timing while the intensity and polarization states are set using fast modulators on the continuous-wave 1550 nm laser. The loss of the system is adjusted using a movable lens and the signals are detected using 4 avalanche photodiodes in two bases with a passive basis choice. Each sent and received pulse is time tagged and recorded using signals from a Global Positioning System (GPS) to synchronize both clocks. These tags are then processed with our QKD software to extract a key. A schematic overview of the setup is shown in Figure 3.1.

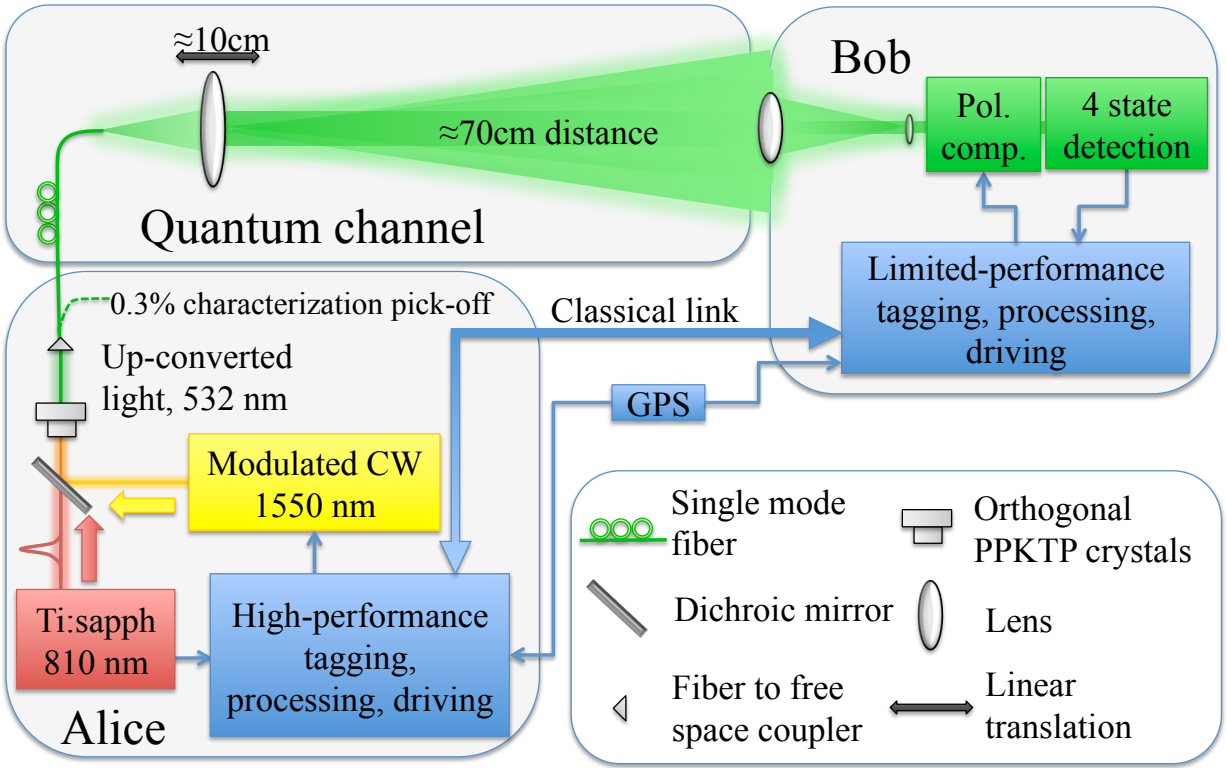

Figure 3.1: Schematic overview of the high-loss QKD system. A WCP source produces photons at 532 nm and transmits them to a quantum receiver via a free-space quantum channel that includes a movable lens to adjust the loss. Computational performance of the tagging, processing and driving in Bob is limited to simulate the available resources of a satellite-based QKD receiver payload.

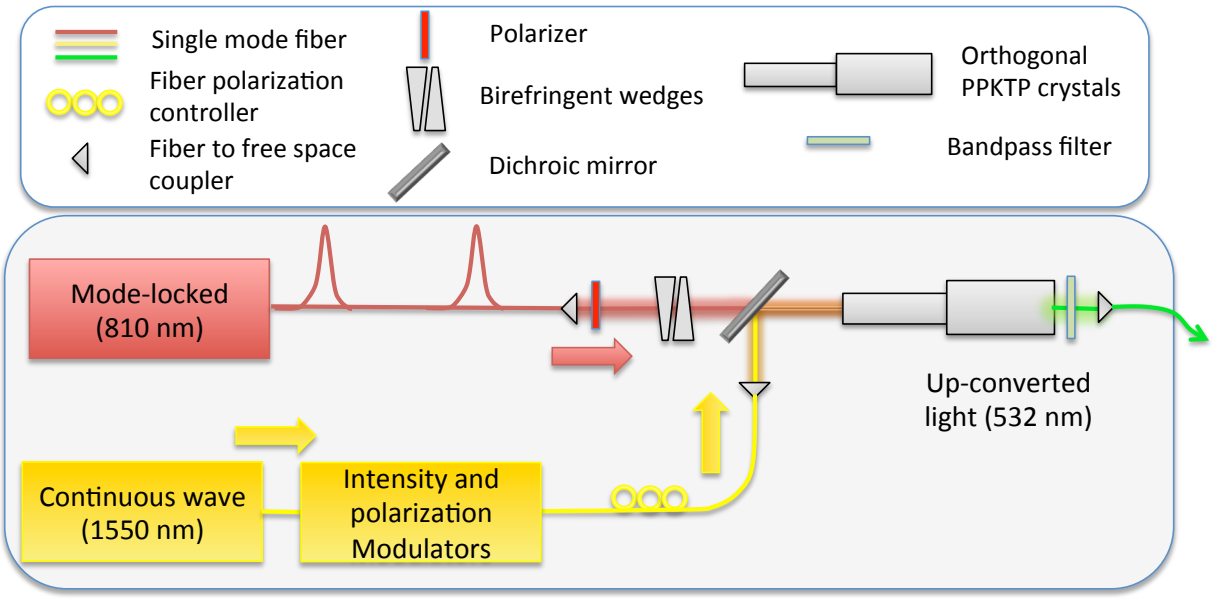

Figure 3.2: Schematic of the WCP source. A pulsed laser at 810 nm is combined with a continuous-wave 1550 nm laser using up-conversion to create photons at 532 nm. The photons produced will have the short pulse and timing of the 810 nm laser while the intensity and polarization will be that of the modulated continuous 1550 nm laser.

3.1.1 WCP Source for 532 nm photons

The WCP source used was originally built by Evan Meyer-Scott [156] and produces photon pulses at 532 nm. While 532 nm is not the optimal wavelength for a quantum transmission to a satellite (as shown in Table 2.5), it was chosen to take advantage of the peak efficiency of silicon avalanche photodiodes (APD) available at the time. The detectors where chosen because they are capable of high timing accuracy, low dark counts and high count rates without the requirement of cryogenic cooling. Recent technological advances are allowing the detectors to operate with high efficiency in the 600–800 nm rage while maintaining low dark counts and low timing jitter [157, 158]. The proof of concept of operating in high loss regime can therefore be applied to the 600–800 nm rage which is better suited for satellite QKD. A schematic diagram of the source is shown in Figure 3.2 and a photo of it is shown in Figure 3.3.

The 532 nm pulses are generated by combining a mode-locked titanium sapphire laser at 810 nm, operating at a pulse repetition rate of 76 MHz, with a continuous-wave 1550 nm laser by using up-conversion in two orthogonally oriented type-I periodically poled potassium titanyl phosphate (PPKTP) crystal. The 810 nm laser is diagonally polarized ($|D\rangle$) and birefringent wedges are used to precompensate for temporal walkoff in the PPKTP

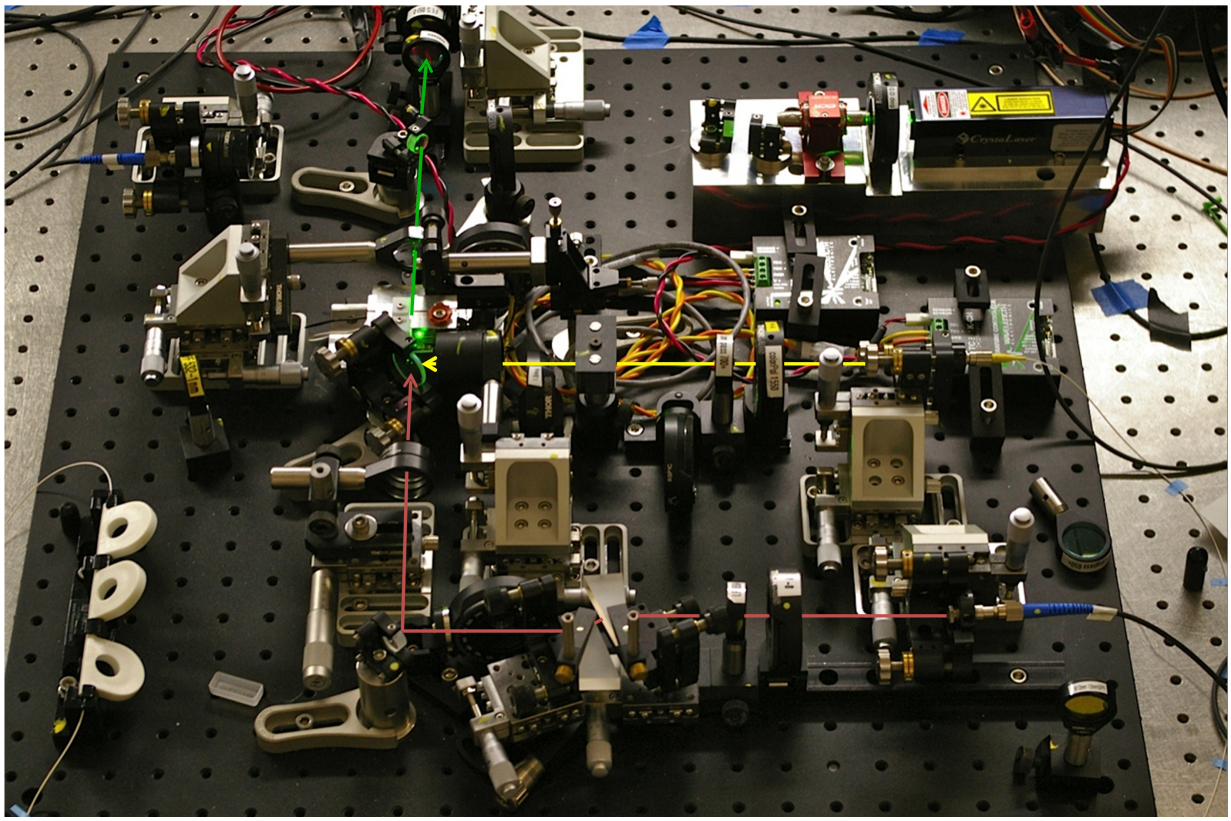

Figure 3.3: Photo of the WCP source. Colored lines show the path of the lasers (red for 850 nm, yellow for 1550 nm and green for 532 nm).

crystals. Efficient telecommunication waveguide modulators [159] are used to modulate the polarization and intensity of the 1550 nm laser.

Because the PPKTP is a type-I crystal at our wavelength, up-conversion will only occur for one polarization. One crystal will allow for up-conversion of horizontally polarized light ($|\mathrm{H}\rangle_1 |\mathrm{H}\rangle_2 \rightarrow |\mathrm{H}\rangle_3$) while the other, being turned orthogonally, will allow for up-conversion of vertically polarized light ($|\mathrm{V}\rangle_1 |\mathrm{V}\rangle_2 \rightarrow |\mathrm{V}\rangle_3$). By having both crystal following each other we can allow for diagonal ($|\mathrm{D}\rangle$) and antidiagonal ($|\mathrm{A}\rangle$) polarizations to be created. Having the 810 nm laser set to diagonal allows the polarization of up-converted 532 nm pulses to be completely determined by the polarization of the 1550 nm laser:

$$|\mathrm{D}\rangle_1 |\mathrm{H}\rangle_2 = \frac{1}{\sqrt{2}} |\mathrm{H}\rangle_1 |\mathrm{H}\rangle_2 + \frac{1}{\sqrt{2}} |\mathrm{V}\rangle_1 |\mathrm{H}\rangle_2 \rightarrow \frac{1}{\sqrt{2}} |\mathrm{H}\rangle_3 , \tag{3.1}$$

$$|\mathrm{D}\rangle_1 |\mathrm{V}\rangle_2 = \frac{1}{\sqrt{2}} |\mathrm{H}\rangle_1 |\mathrm{V}\rangle_2 + \frac{1}{\sqrt{2}} |\mathrm{V}\rangle_1 |\mathrm{V}\rangle_2 \rightarrow \frac{1}{\sqrt{2}} |\mathrm{V}\rangle_3 , \tag{3.2}$$

$$\begin{aligned} |\mathrm{D}\rangle_1 |\mathrm{D}\rangle_2 = \frac{1}{2} |\mathrm{H}\rangle_1 |\mathrm{H}\rangle_2 + \frac{1}{2} |\mathrm{H}\rangle_1 |\mathrm{V}\rangle_2 + \frac{1}{2} |\mathrm{V}\rangle_1 |\mathrm{H}\rangle_2 + \frac{1}{2} |\mathrm{V}\rangle_1 |\mathrm{V}\rangle_2 \\ \rightarrow \frac{1}{2} |\mathrm{H}\rangle_3 + \frac{1}{2} |\mathrm{V}\rangle_3 = \frac{1}{\sqrt{2}} |\mathrm{D}\rangle_3 , \end{aligned} \tag{3.3}$$

$$\begin{aligned} |\mathrm{D}\rangle_1 |\mathrm{A}\rangle_2 = \frac{1}{2} |\mathrm{H}\rangle_1 |\mathrm{H}\rangle_2 - \frac{1}{2} |\mathrm{H}\rangle_1 |\mathrm{V}\rangle_2 + \frac{1}{2} |\mathrm{V}\rangle_1 |\mathrm{H}\rangle_2 - \frac{1}{2} |\mathrm{V}\rangle_1 |\mathrm{V}\rangle_2 \\ \rightarrow \frac{1}{2} |\mathrm{H}\rangle_3 - \frac{1}{2} |\mathrm{V}\rangle_3 = \frac{1}{\sqrt{2}} |\mathrm{A}\rangle_3 . \end{aligned} \tag{3.4}$$

This up-conversion method allows us to obtain short pulse of the same duration ($\approx$3 ps) and pulse rate (76 MHz) as the 810 nm laser, while setting both the polarization state and the intensity with waveguide modulators at 1550 nm, which are faster and more efficient than modulators in the visible range. The intensity of each pulses, set using the modulators, average 0.5 photons/pulse for the signal states and 0.1 photons/pulse for the decoy states. These were chosen to optimize the secure key rate generation at high loss [126]. One last advantage of using up-conversion is that the shorter coherence time of the continuous-wave 1550 nm laser (compared to the pulsed 800 nm mode-locked laser) insures that the phase of the 532 nm pulses are randomized. This is necessary to ensure security and certain pulse laser, such as the mode-locked 810 nm laser used, have non-random phase difference between pulses which could potentially leak information to an potential eavesdropper. The coherence-time was measured to be $<$6 ns [156], significantly below the $\approx$13 ns between pulses.

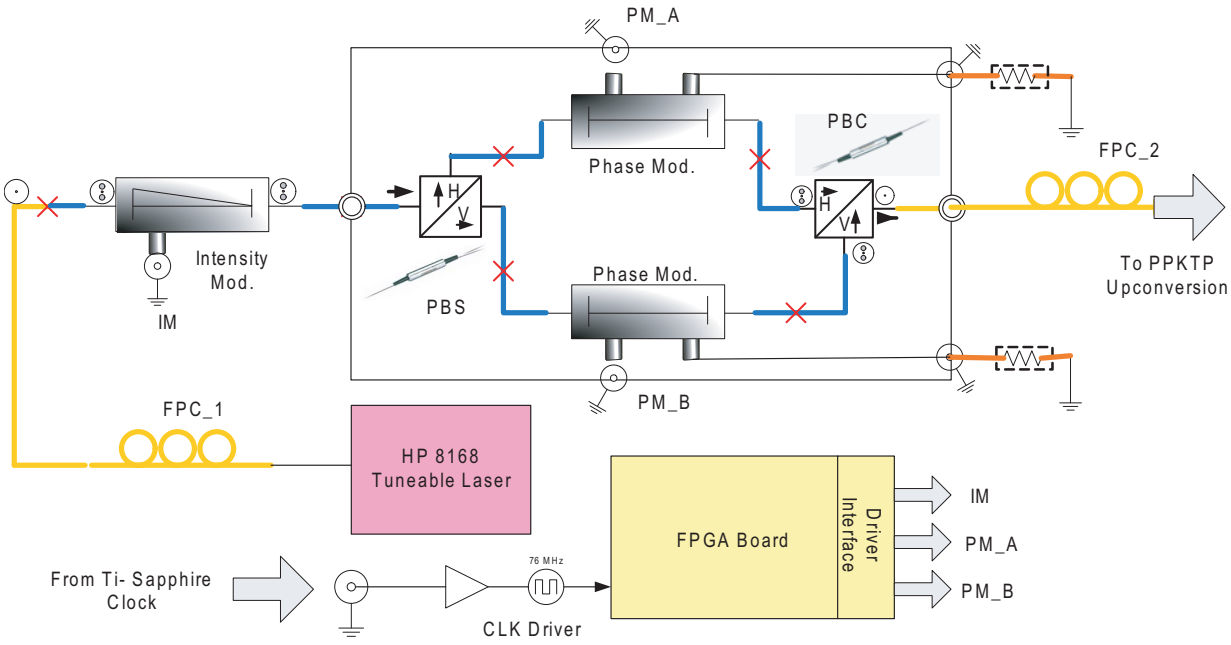

Figure 3.4: Schematic of the telecommunication waveguide intensity and polarization modulator based on a balanced Mach-Zehnder interferometer configuration. Two interferometric arms, each containing an electro-optical phase modulator, are used to control the relative phase between horizontal and vertical polarizations. A polarization controller is then used to rotate the polarizations into the rectilinear polarization basis used for the QKD protocol. Figure reproduced with permission from [159].

3.1.2 Telecommunication waveguide intensity and polarization modulator

The intensity and polarization of the 1550 nm continuous-wave laser is controlled using an intensity modulator followed by two phase modulators in a Mach-Zehnder interferometer configuration. This modulator was initially built by Zhizhong Yan [159] and uses customized off-the-shelf $LiNbO_3$ electro-optical telecommunication waveguide phase and intensity modulators from EOSpace [160]. Figure 3.4 shows a schematic diagram of the modulators. For simplicity, our implementation uses a fixed sequence of randomly chosen states which are repeated instead of a continuous random sequence. The sequence contains 128 states and is composed of 92% signal and 8% decoy states.

The input of the polarization state is set to diagonal with respect to the first beam splitter by using a fiber polarization controller. This ensures that equal beam intensities enter each interferometric arms at the polarization beam splitter. Each interferometric arms contain an electro-optical phase modulator used to control the relative phase between H and V polarizations. The phase difference is set using four different voltage combinations

so that when they recombine at the output polarization beam splitter we obtain either diagonal, antidiagonal, right-handed circular or left-handed circular polarizations. Diagonal and antidiagonal polarizations are defined in Equation (1.1) and (1.2) while right-handed ($|\mathrm{R}\rangle$) and left-handed ($|\mathrm{A}\rangle$) circular polarizations are defined as:

$$|\mathrm{R}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + i\,|\mathrm{V}\rangle), \tag{3.5}$$

$$|\mathrm{L}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle - i\,|\mathrm{V}\rangle). \tag{3.6}$$

After the two paths have recombined, a second fiber polarization controller is used to rotate the polarizations into the rectilinear polarization bases, leaving diagonal and antidiagonal polarizations unchanged while changing right-handed circular and left handed circular polarizations to horizontal and vertical polarizations, respectively. This system is therefore able to produce any of the four polarizations states by adjusting the voltages of the two phase modulators.

Finally, an intensity modulator is used to adjust the intensity for either a signal or a decoy state (controlled by setting the voltage sent to the intensity modulator). The voltage applied to each modulators are set using a field programmable gate array (FPGA) circuit board and a driver interface circuit. The modulation show high stability and switching contrast. The switching speed is currently limited to a few hundreds of MHz by the FPGA and driver interface circuits, with the modulators themselves capable of reaching a switching speed of a few GHz. The switching speed could be increased by upgrading the FPGA and driver interface circuits which are both commercially available in the GHz range [161, 162].

This implementation of the polarization modulation is advantageous because it intrinsically ensures that all distinct polarization states are identical in all other aspect (such as frequency, bandwidth, and intensity), a difficulty in designs incorporating multiple laser diodes [37] or multiple optical amplifiers [163]. Having all non-polarization aspects identical is necessary to ensure security, as any distinguishable characteristic can leak information to a potential eavesdropper. We note that while the intensity of the 1550 nm laser is independent of polarization, the intensity of the up-converted 532 nm can become polarization dependent if the efficiency of the PPKTP crystals is not matched. These efficiency can be manually adjusted by changing the alignment or by changing the polarization of the pulsed 810 nm laser (typically 810 nm).

3.1.3 Quantum channel with variable loss

Once produced, the 532 nm photon pulses are coupled into a single-mode fiber. A fiber splitter is used to sends ≈0.3 % of the photons to a thick-silicon avalanche photodiode (Excelitas SPCM-AQ4C) in order to measure the average photon number per pulse. This enables the average photon number of the signal pulse to be adjusted to the desired 0.5 photons/pulse by adjusting the power of the 1550 nm laser before the modulators, leaving the modulators to automatically set the decoy state to the desired value (0.1 photons/pulse) based on the ratio of the decoy state to the signal state. The fiber splitter sends the remaining photons to a free-space quantum channel consisting of a bare fiber output followed by a 3-inch-diameter lens. The lens is placed on a longitudinal translation stage allowing the loss to be adjusted by varying the position of the lens, making the beam more or less divergent, thus altering the amount of light collected by the receiver. A photo of the quantum channel is shown in Figure 3.5.

3.1.4 Free-space quantum receiver

Detections of the quantum signals are done using a free-space receiver implementing a two-basis passive choice measurement. The receiver was designed to be robust, integrated, and portable, while using commercial technologies, providing an initial design for a quantum receiver on a satellite platform. The frame of the receiver is built using Thorlabs 30 mm and 60 mm cage system [164] supported on an small optical breadboard. Figure 3.6 shows a schematic diagram of the receiver and a photo is shown in Figure 3.7.

Photon signals are collected using a 2-inch diameter lens with a 250 mm focal length. A second lens, of 6.5 mm diameter and 11 mm focus length, is used to collimate the beam. A combination of three wave plates consisting of one half-wave plates (HWP) and two quarter-wave plate (QWP), one before and one after the HWP, are used to compensate any unitary polarization rotations that may have been introduced by the quantum channel.

The passive basis choice is done using a custom-built pentaprism beam splitter, which allows us access to three ports—two of which to be used for quantum measurements (with each port outputting of 47.5% of the signal). The third port (with the remaining 5% of the signal) is currently unused but could potentially serve for beacon detection or as a port for an alternative source in the reverse direction, making it advantageous in a satellite implementation. The output diagram of the pentaprism are shown in Figure 3.6. The effect of the pentaprism on the polarization was tested and no significant degradation to the measured polarization was measured.

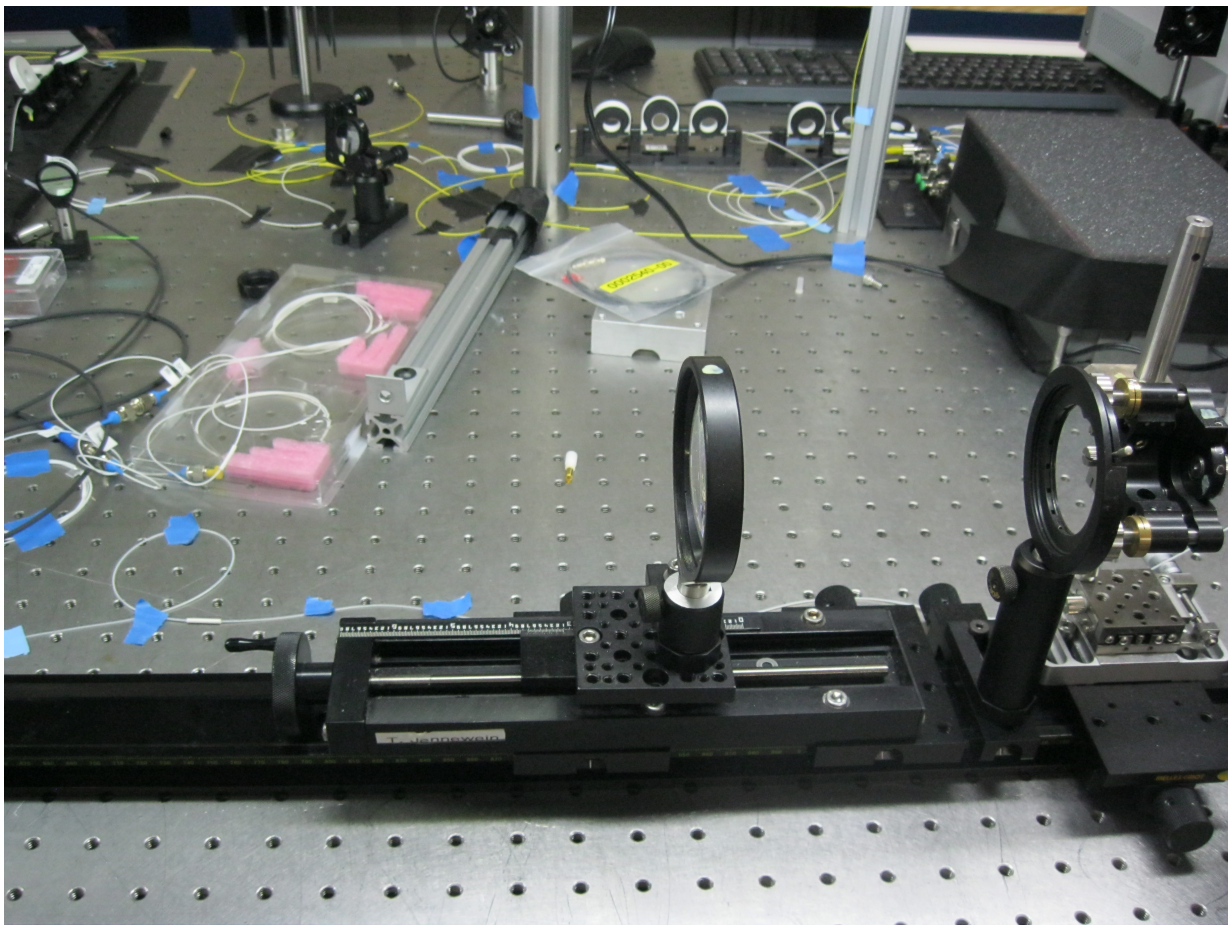

Figure 3.5: Photo of the quantum channel. The 3-inch lens allows the divergence of the beam to be adjusted, thereby modifying the loss of the channel.

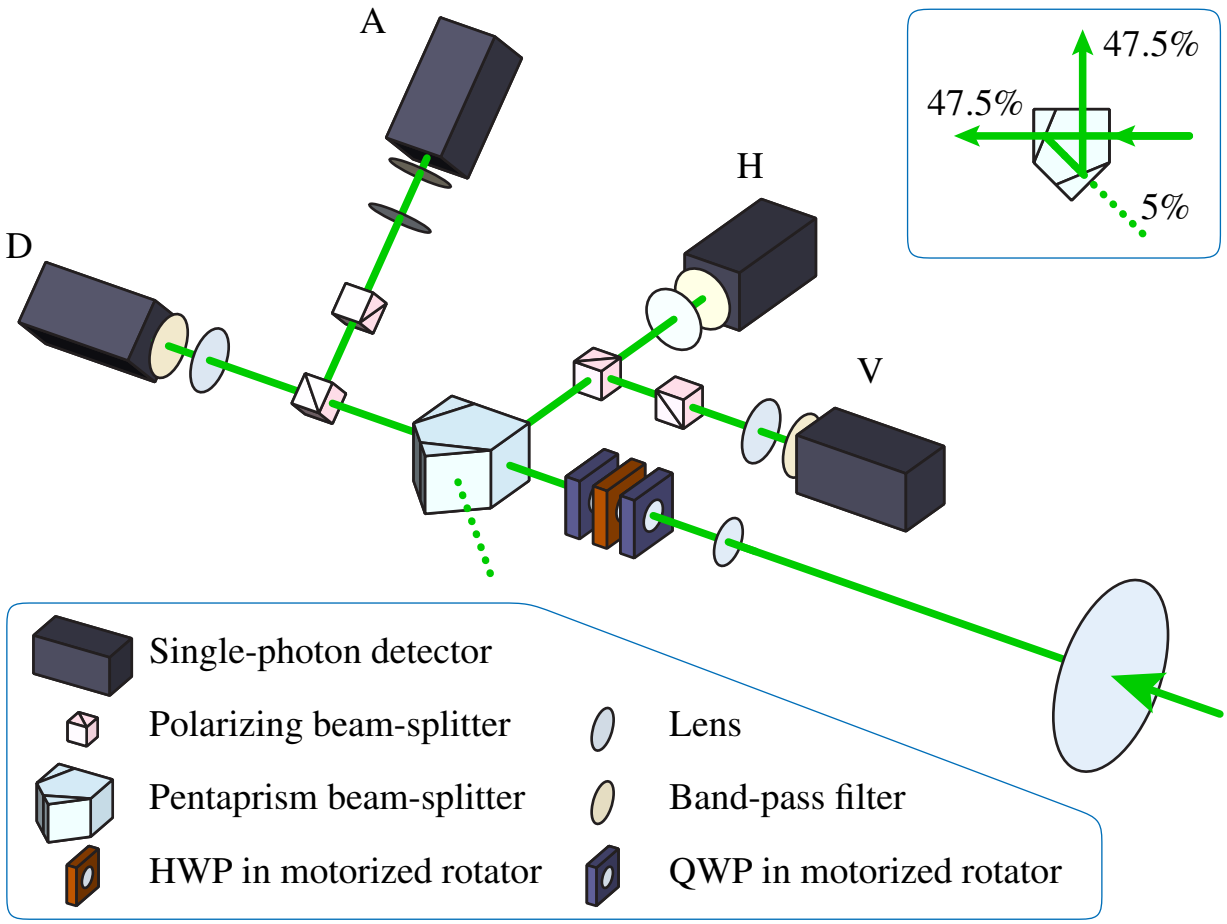

Figure 3.6: Schematic of the quantum receiver. Photon signals are captured by a 2-inch lens and measured in one of two orthogonal bases. Three motorized rotating wave plates are used to correct any unwanted polarization rotations in the quantum channel.

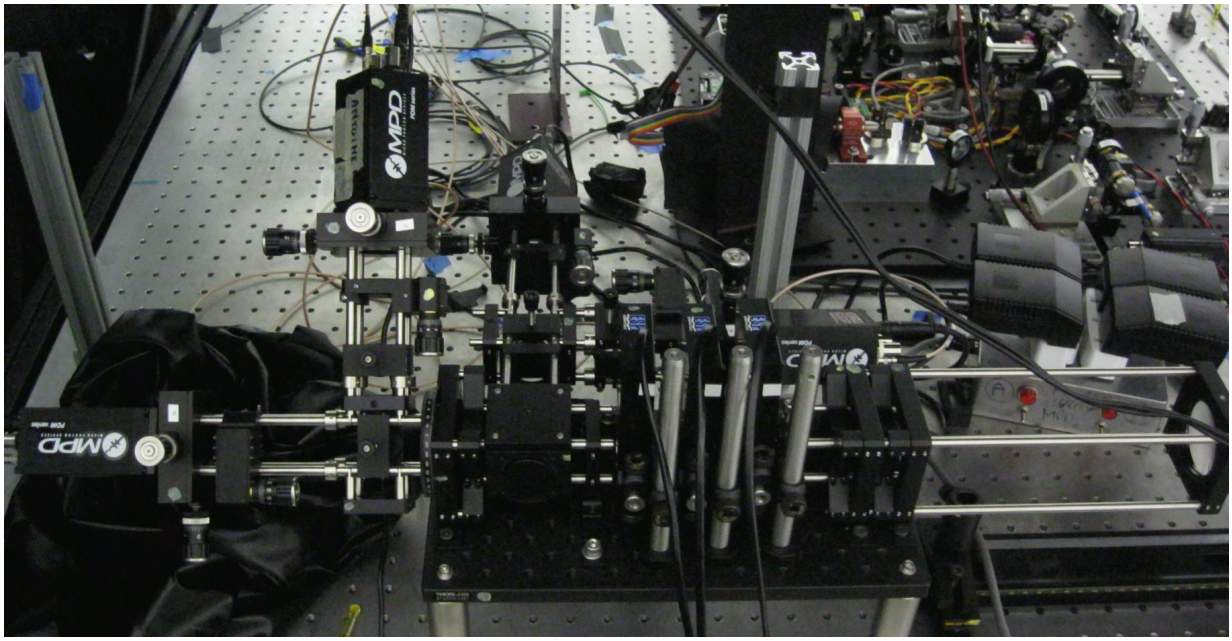

Figure 3.7: Photo of the quantum receiver. Thorlabs cage system is used as the frame of the receiver which is mounted on a small 6-inch by 12-inch breadboard.

In each of the two used ports, the polarization measurement is performed using a 5 mm polarizing beam splitter cube. The reflected port is used for measurements in the H/V basis while the transmitted port is used for the D/A basis. The assembly in the transmitted port is rotated 45°. This was done in order to perform the measurement in the D/A basis with the same polarizing beam splitter cube (which transmits horizontal and reflects vertical polarizations). The 45° rotation of the polarizing beam splitter cube causes diagonal polarization to be transmitted while the antidiagonal polarization is reflected. An additional polarizing beam splitter cube, rotated 90° so as to transmit vertical polarization (antidiagonal in the case of the rotated assembly in the transmitted port), is added in each reflection ports of the measurement polarizing beam splitter cubes. This is done to suppress noise as the reflected port of the polarizing beam splitter cubes have lower polarization visibility than the transmitted port ($\geq$99% visibility in the reflected port compared to $\geq$99.9% visibility in the transmitted port).

The detection is performed using four silicon avalanche photodiodes from Micro Photon Devices [82]. These detectors feature good detection efficiency ($\approx$50 %), low dark counts ($\approx$20 cps) and low jitter ($\leq$50 ps). Photons are focused onto the 50 μm active area of the detectors with 1-inch diameter, 60 mm focal length lenses (one before each detector). Each detector is attached to an X-Y translation stage for fine positional adjustment. Finally, a 2 nm band-pass filter is placed in front of each detectors to suppress background noise.

3.1.5 Automated polarization alignment

Our system uses optical fiber both to transmit the unconverted 532 nm signal from the source to the quantum channel, and to transmit the modulated 1550 nm laser. A common problem with optical fibers is that they do not preserve the polarization state. An optical fiber will modify the polarization states by applying a unitary rotation to state. Furthermore, temperature drift and mechanical stress on the fiber will cause the unitary induced by the fiber to change, causing polarization drift over time. The unitary can be compensated either in free-space, using wave plates, or in directly in the fiber, by manually inducing mechanical stress on the fiber to change the unitary to the identity. Both approaches can be tedious if done manually, particularly when trying to align multiple polarization states simultaneously. To overcome this difficulty, we designed and implemented a polarization compensation software that performs quantum state tomography [165] and calculates the optimal compensation to restore the polarization states, which is implemented using free-space wave plates located at the receiver.

A set of three wave plates are included in the quantum receiver, two quarter-wave plates (QWP) on either side of a half-wave plate (HWP), which can be used to correct any unitary polarization misalignment between the source and the receiver. A custom software (written by Brendon Higgins) is used to characterize the polarization misalignment and calculates the position of the wave plates required to compensate it. The wave plates, which are mounted in motorized rotation stages, are then automatically adjusted accordingly. A largely similar strategy has been implemented in the context of QKD previously utilizing an independent strong laser signal [166]. The scheme we explore here differs in that we wish to use the quantum signals themselves.

The minimum complete set of measurements requires only four outcomes, in the three basis, to be measured (such as horizontal, vertical, diagonal and right-handed circular polarizations). Four measurement in the rectilinear bases (i.e. horizontal, vertical, diagonal and antidiagonal polarizations) do not form a complete set, because no circular polarization component is represented. At least two non-orthogonal input polarization states are required for complete characterization. There are an infinite set of rotations that may take a single input polarization state to the one that is ultimately measured, and thus the characterization of the unitary using only one input state cannot be well defined. Both of these input states can all be in the rectilinear bases (such as horizontal and diagonal polarizations), provided they neither be equal nor orthogonal. For our characterization, all four rectilinear bases states are used as input, allowing the source operation to remain unchanged.

The characterization of the unknown unitary polarization rotation is done by first accumulating statistics in the rectilinear bases (horizontal, vertical, diagonal and antidiagonal polarizations), using the quantum signal and single-photon detectors while the three wave plates are in their optical axis positions (no effect on rectilinear states). After sufficient statistics are accumulated, the last QWP is rotated by 45° to allow measurements in the circular basis (right-handed and left-handed circular polarizations). The measurement in all six polarization states are then used to characterize the unitary. These six outcomes form an overcomplete set, i.e. they are more than is strictly necessary, however within experimental contexts this overcompleteness aids statistical robustness of the characterization. Because all information on the detections must be revealed, any counts obtained during this characterization process are insecure and thus not used for key generation.

Once enough statistics have been accumulated, the software performs quantum state tomography [165] to determine the measured states after the unitary. From this, the operation needed to return these states to the desired ones is computed and implemented using the wave plates. This operation should, in theory, be the inverse of the unitary.

The performance of the polarization compensation software was theoretically predicted using a Monte Carlo type test which calculates the visibility degradation after the compensation. The test randomly generated a unitary operation and simulated the compensation based on a certain number of received signal and received background counts. The program then applied the compensation and calculated the remaining reduction in polarization visibility (with 0 being no reduction and 1 reducing the polarization visibility to 0%). This was performed with 20000 randomly generated unitary (uniformly distributed), for various values of received signal and received background counts. An example of the results of these simulations is shown in Figure 3.8. This shows that polarization visibilities of at least 99% (10^{-2} or less in visibility reduction) can be achieved with less than a thousand received signal photons. In addition, the compensation is robust against background counts as high as the signal, far beyond the maximum noise level for QKD.

3.1.6 Data collection and time-tagging

Data is collected using two time-tagger units [167] (see Figure 3.9), one collecting the signals from the intensity and polarization modulators and the other collecting the signals from the single-photon detectors of the quantum receiver. These units use a field programmable gate array board, and time-stamp the signal with a precision of 78 ps. The two units are synchronized using a GPS receiver providing a 1 Hz signal, used to identify the start of the current second, and a 10 MHz signal, used to stabilize the internal clock of the time-tagger.

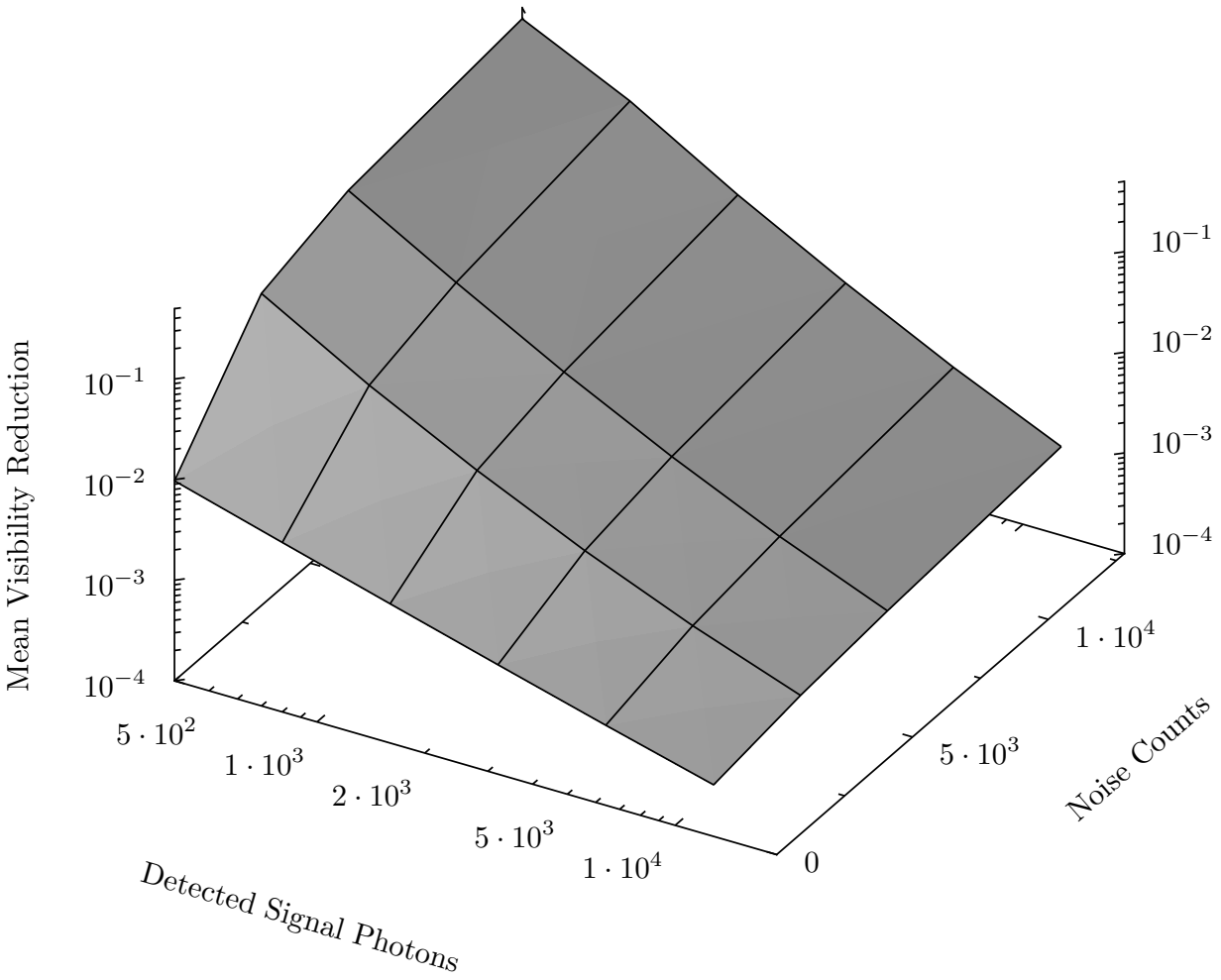

Figure 3.8: Theoretically predicted polarization visibility reduction remaining after applying the automated polarization compensation algorithm. A few thousand received signal is sufficient for good characterization and compensation even when the background counts are as high as the signal. In a typical satellite uplink (see Figure 2.26 and 2.27), this would correspond to less than 0.1% of the counts received in an upper quartile pass.

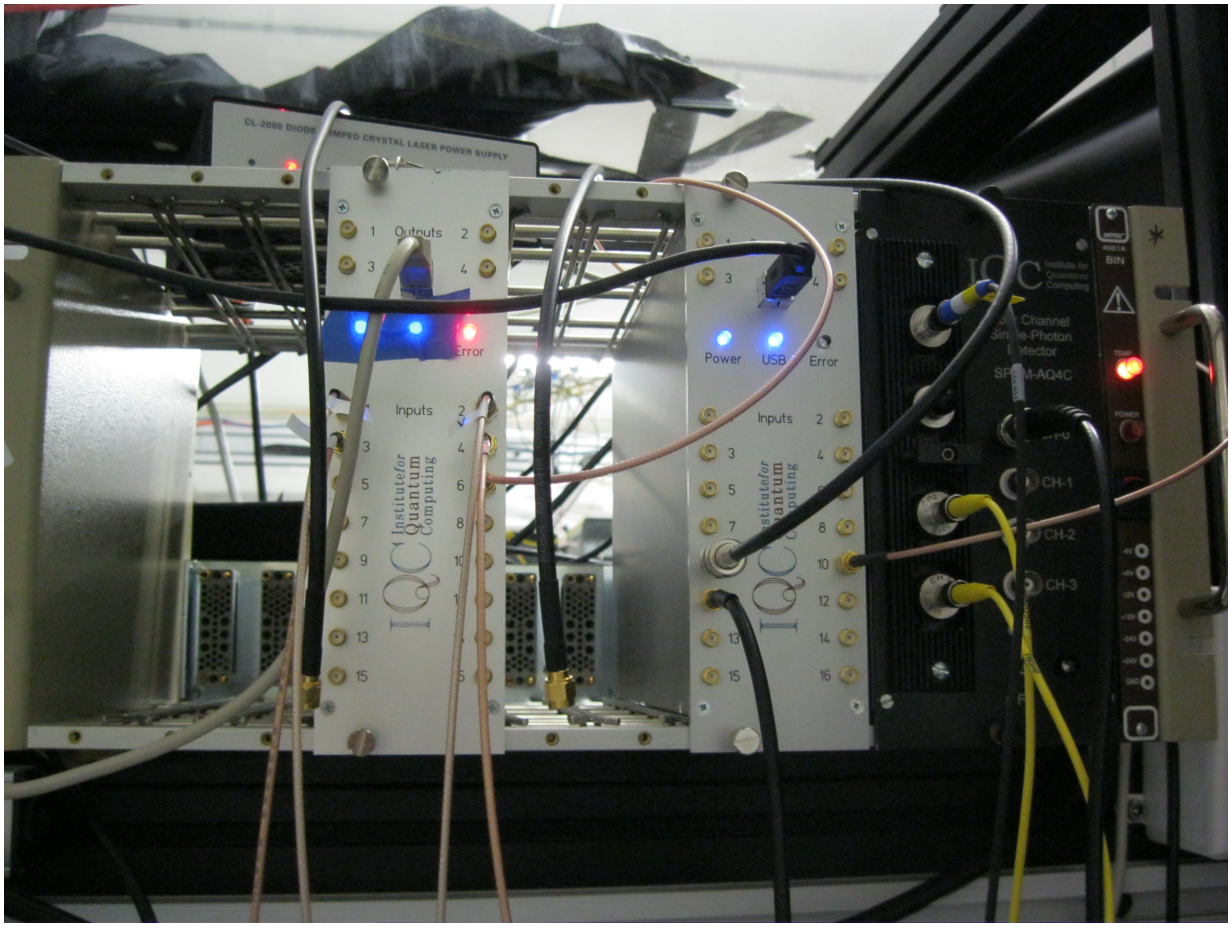

Figure 3.9: Photo of the Time-tagger units used for data collection.

The data is sent to two x86-64 computers which are connected together using a local-area network, where the data can be analyzed to extract secure key. Alternatively, a low power Freescale IMX53 ARM board [168] can be connected to the computer at the receiver and used to perform the processing required for the QKD protocol, thus simulating the limited processing power of the satellite.

3.2 QKD software for limited computational resources

The analysis of the quantum signals and the QKD protocols necessary to extract secure keys are implemented using custom software designed to operate with the limitations of a satellite receiver platform. Computationally intensive tasks are, as much as possible, performed at the transmitter (Alice) which would be located on the ground, allowing for greater computational power. This ensures that the receiver platform (Bob) can operate efficiently

despite limited computational resources. In addition, the amount of classical communication is reduced to a minimum to operate in the limited communication rates available for a small satellite platform. This software was written in C# by Nikolay Gigov [169]. An overview of the software design is shown in Figure 3.10.

The time-stamp of the counts collected at Bob are sent, along with the basis they were measured in, to Alice by using the local-area network. For a small fraction of the counts (≈5%), the measured state is also sent. These revealed states are used to estimate the quantum bit error ratio (QBER). Alice performs the timing analysis by minimizing the QBER of the revealed counts. The positions of the counts where the basis matched are then communicated to Bob which discards the rest of the counts. A one-way error correction algorithm, based on low-density parity-check codes [170], is used to correct the errors in the key. Alice performs the more computationally intensive decoding algorithm while Bob only runs a linear algorithm to compute his syndromes. Finally, privacy amplification is performed using a Toeplitz-matrix-based [171] routine suitable for low-power hardware implementation.

Both the error correction and the privacy amplification procedures are done offline (i.e. after the quantum signals are exchanged). In a satellite implementation, it can be done either at the end of the quantum transmission or during a later pass, possibly using a different ground station that does not require any quantum capabilities.

Bob's software consists of a driving control environment and an embedded processing component. The driving control environment is responsible for loading the time-tagger operating system drivers, configuring and reading out the time-taggers, and displaying live statistics. The embedded processing component uses a efficient C program to perform all the processing required at Bob. The driving control environment is executed on a x86-64 desktop computer while the embedded processing component can be executed either on the same computer or on a low-power ARM board.

3.2.1 Timing analysis

The first task of the software is to match Bob's received counts with the counts sent by Alice. A few factors make this process challenging. The initial 1 Hz signal of the GPS, which is used to signal the start of each second, is only accurate to 100 ns. In addition, the internal clock of each time taggers may drift, and require a 10 MHz signal from the GPS to help align the internal clocks of each time tagger. Lastly, our data acquisition hardware is not capable of operating at the high pulse rate of the laser source (76 MHz). This limitation is a fundamental memory and bandwidth limitation due to our device

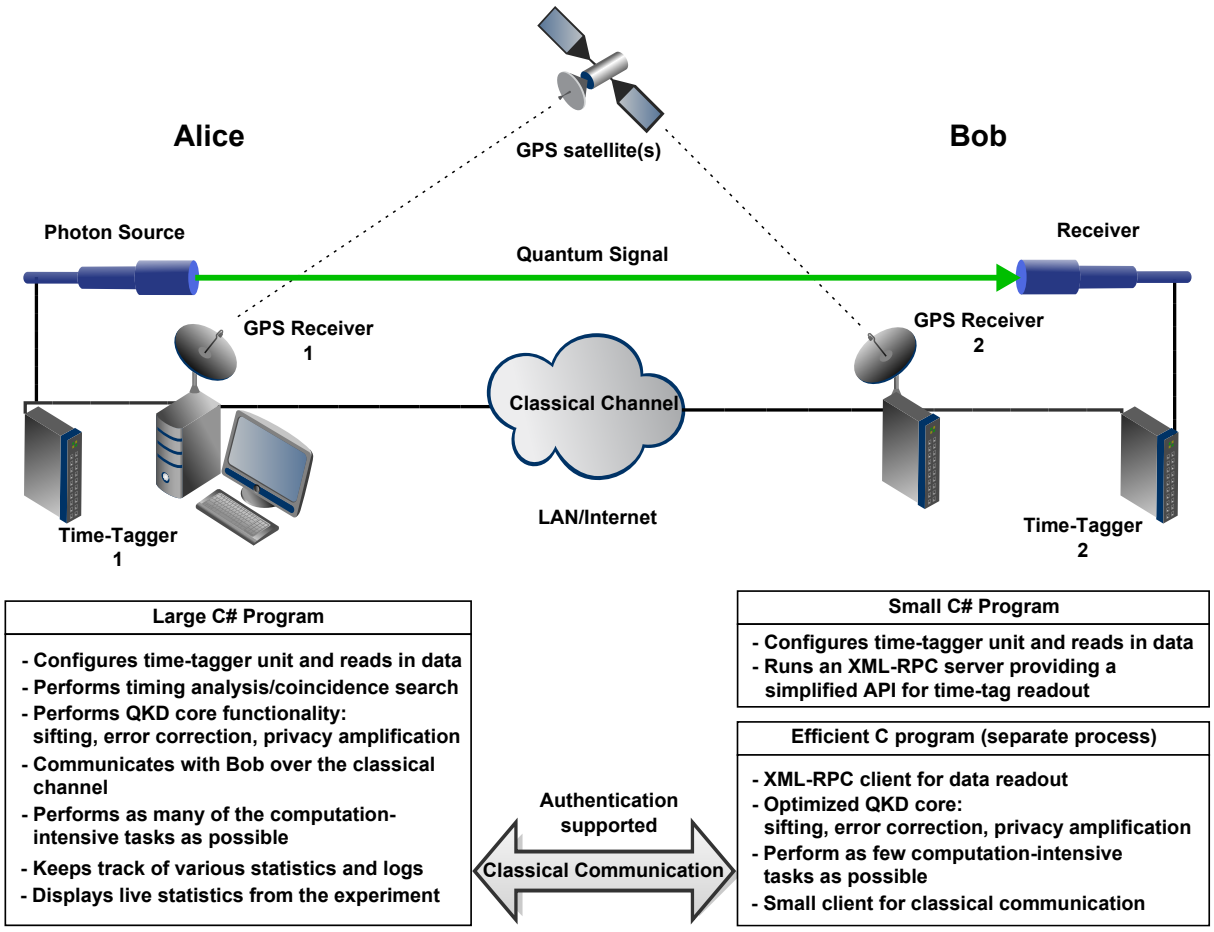

Figure 3.10: Overview of the software design. Alice's software consists of an integrated solution written in C# and is designed to perform as much of the computationally intensive operations as possible. Bob's software is designed to run on modest low-power hardware and consists of a small C# layer and an efficient C program that performs the necessary portions of the QKD protocol at the receiver side. Figure reproduced with permission from [169].

recording a time-stamp for each counts. It is thus necessary to reduce the information load by only time-tagging a subset of the laser's output pulse signals. This requires the software to interpolate the time-stamps of the signal pulses by assuming that the laser's period is stable over several microseconds.

The timing analysis process, performed at Alice, begins with an initial synchronization using the timing information from both time-tagger and the known optical an electronic delay between the time the pulses are sent and received (measure before the experiment). An histogram-based optimizing coincidence search is then performed based on the count rates. This is done to identify the signal peaks. The highest count rate for each laser period is identified, after which the coincidence search identifies the correct one based on QBER estimate from a fraction of received counts revealed by Bob ($\approx$5%). The software does this search by calculating the QBER for each identified peaks to find the minimum QBER, thus finding the likeliest delay. This approach is valid because any delays other than the correct one would produce random correlations, leading to a QBER approaching 50%. If the delay is off by a multiple of the laser period, the high QBER would be caused by the randomness of the sequence, whose period (a few microseconds) is much greater than the uncertainty in the initial synchronization. Figure 3.11 shows the user interface at Alice which includes the histogram showing the location of the optimal delay, yielding an average QBER of 3.33%.

Once the counts are successfully matching, Alice identifies which of Bob's counts where in the correct basis and sends this information to Bob (publicly). All counts where the basis did not match are discarded and both parties are left with what is called the sifted key.

3.2.2 Error correction

The sifted key will contain some errors due to background noise, dark counts, and imperfection in the source and receiver alignments. To reconcile Alice and Bob's key we perform error correction using low-density parity-check codes [170]. These codes require low communication overhead and are inherently asymmetric in therms of computational complexity (i.e. Alice can perform most of the computation). These advantages make these codes highly suitable for satellite-based QKD.

Alice begins by preparing an irregular parity-check matrix based on the QBER estimate obtained during timing analysis. This is done using a modified progressive-edge growth software [172, 173] and employs known optimal degree distribution profiles [125, 174]. This

Figure 3.11: User interface at Alice showing the histogram-based optimizing coincidence search. The light blue area shows the counts captured with the optimal delay for the current second. This optimal is determined by idetifying the signal peaks by finding the maximum count rates in each laser period, and then moving the delay across the peaks and optimizing the QBER. The width of the capture counts (light blue are) is determined by the coincidence window.

matrix is then transmitted to Bob, in a compact form, where an efficient linear algorithm is used to compute a syndrome from the sifted key. The syndrome is a vector defined by

$$s = Mx(mod(2)), \tag{3.7}$$

where s is the syndrome, M is the parity-check matrix and x is Bob's sifted key. For long sifted keys (typically 100000 bits or more), the sifted key is divided in blocks and the same parity-check matrix is used to determine the syndrome for each block, thus reducing computational time and communication.

The syndromes of each blocks are sent to Alice where it is used, along with the parity-check matrix an the estimate of the QBER, to reconcile Alice's sifted key with Bob's. This is accomplished using *belief propagation*, an iterative message passing decoding algorithm, also known as the sum-product algorithm [175, 176]. Our sum-product LDPC decoder is written in C# and is based on that found in [177].

The reconciliation step may fail if the number of rows of the parity-check matrix is too small. If this happens, the key block can either be discarded or the algorithm can be retried using an augmented parity-check matrix containing all the rows of the previous matrix, similar to the "nested" LDPC codes proposed in [178]. In a satellite mission, the choice can be based on the availability of the classical communication channel. Our implementation exhibits a 2% failure rate with typical efficiencies (η_{EC}) around 1.2.

3.2.3 Privacy amplification

Once the sifted key has been successfully error corrected, privacy amplification is used to reduce the amount of information that may have leaked to an eavesdropper. To ensure security, all error in the key (observed by the QBER estimate) are assumed to be caused by an eavesdropper. The QBER estimate can thus give us an estimate of the amount of information that may have leaked to an eavesdropper. In addition, all parity information revealed during the error correction step are public and this information must also be removed from the final key.

The privacy amplification process uses a *two-universal hash function* [9, 179] applied to the sifted key to produce a provably secure key with reduced length L. This process is a symmetric operation that needs to be performed by both Alice and Bob. The computational complexity and the amount of classical communication required depend on the choice of hash function.

Our implementation employs the Toeplitz matrix [179, 180] construction implemented using a linear feedback shift register. A Toeplitz matrix is a two-universal hash function [171] that has constant descending left-to-right diagonal elements. An $L \times N$ Toeplitz matrix can be written as

$$T_{\mathbf{r}} = \begin{bmatrix} r_L & r_{L+1} & \cdots & & & & \cdots & r_{N+L-1} \\ r_{L-1} & r_L & r_{L+1} & \cdots & & & \cdots & r_{N+L-2} \\ \vdots & & \ddots & & & & & \vdots \\ r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & \cdots & r_{N+1} \\ r_1 & r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & r_N \end{bmatrix}. \tag{3.8}$$

A Toeplitz matrix $T_{\mathbf{r}}$ is completely defined by the $(N + L - 1)$-bit vector $\mathbf{r} = (r_1, r_2, \ldots, r_{N+L-1})$, making its storage and transmission requirements considerably reduced. These requirements can be further reduced by employing a $L \times N$ matrix of the form $U_{\mathbf{r}} = (I_L | T_{\mathbf{r}})$, i.e. a concatenation of an L-dimensional identity matrix I_L and an $L \times (N - L)$ Toeplitz matrix $T_{\mathbf{r}}$:

$$U_{\mathbf{r}} = \begin{bmatrix} 1 & 0 & \cdots & 0 & r_L & r_{L+1} & \cdots & & & \cdots & r_{N-1} \\ 0 & 1 & \cdots & 0 & r_{L-1} & r_L & r_{L+1} & \cdots & & \cdots & r_{N-2} \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & & & & \vdots \\ 0 & & 0 \cdots & 0 & r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & r_{N-L+1} \\ 0 & 0 & \cdots & 1 & r_1 & r_2 & \cdots & r_{L-1} & r_L & r_{L+1} & \cdots & r_{N-L} \end{bmatrix}. \tag{3.9}$$

This $U_{\mathbf{r}} = (I_L | T_{\mathbf{r}})$ matrix is also a two-universal Toeplitz matrix, but requires only $N - 1$ bits to define [181, 182].

Alice generates such a matrix by constructing a random binary string $\mathbf{r} = (r_1, r_2, \ldots, r_{N-1})$ of length $N - 1$, and then transmits $\mathbf{r}$ to Bob over the classical channel. She and Bob then use $\mathbf{r}$ and a linear feedback shift register to effect the application of the Toeplitz matrix $U_{\mathbf{r}}$, computing the final secure key.

The identity portion of each row of $U_{\mathbf{r}}$ uses no space and can be accounted for with a simple AND operation. We represent $T_{\mathbf{r}}$ as an $(N - L)$-bit logical linear feedback shift register. Initially, the linear feedback shift register contains the last $N - L$ bits of $\mathbf{r}$, $(r_L, r_{L+1}, \ldots, r_{N-1})$. The remaining bits from $\mathbf{r}$ are used as input for the LFSR. In this way, we conserve memory by never needing to store full matrices.

The logical LFSR is broken up into multiple 32-bit LFSR blocks, each of which is designed to fit inside a register on a processing unit. The register size of 32 bits is chosen for the support of multiple platforms, including our low-power ARM test board. 64-bit

platforms are also available, and with single instruction, multiple data (SIMD) extensions, the register can be as large as 128 bits.

The number of column in the Toeplitz matrix (N) is determined by the length of the sifted key block on which the privacy amplification is applied to, while the number of row (L) corresponds to the length of the final secure key. L is calculate using QKD security proofs to determine what length of key can be obtained while ensuring security. We use Equation (2.31) in combination with the measure background contribution (in the form of the vacuum yield Y_0) to obtain a better key rate while maintaining security [126].

3.2.4 Vacuum yield

The key rate equation presented in Chapter 2 (Equation (2.31)) assumed all noise was caused by an eavesdropper. In an experimental implementation we can measure the level of noise received by the system during the QKD exchange, allowing us to place a better bound on the possible contribution of an eavesdropper to the QBER. To assure security, it is important that this measure be done during the QKD exchange, and monitored throughout, instead of being characterized separately, as an eavesdropper may manipulate the characterization.

The measured noise is implemented using the vacuum yield (Y_0), defined as the cumulative probability of detector dark counts and background noise within the coincidence window. This parameter is measured by using the timing analysis to find the peaks and then adding an offset to move between the peaks. This offset gives an estimate of the background and dark count rates. The vacuum yield is then simply the measured count rate in this offset, divided by the pulse repetition rate (76 MHz), and multiplied by the ratio of the QKD coincidence window to the coincidence window of the background estimate (typically 3 ns).

We note that this approach is insecure, as an eavesdropper could manipulate the background counts between pulses by injecting additional light. Proper measurement of the vacuum yield would require a source that can produce true vacuum pulses (no signal light), which our current system is incapable of producing. These vacuum pulses could be obtained by using a laser that can be momentarily switched off (or a triggered pulsed laser where one can skip a pulse by not triggering), or by using a intensity modulator capable of high intensity contrast to approximate a vacuum pulse.

For our experimental implementation, all parameters used to determine the final key rate are measured quantities. The lower bound, give by Equation (2.31), can then be used

as an exact equation:

$$R = q\frac{N_\mu}{N_\mu + N_\nu}\{-Q_\mu \eta_{\text{EC}} H_2(E_\mu) + Q_1^L \left[1 - H_2(E_1^U)\right] - Q_\mu \Delta / N_\mu\}. \tag{3.10}$$

where, as previous, q is a basis reconciliation factor (1/2 for BB84), N_μ and N_ν are the signal and decoy detections respectively and Q_μ is the gain for signal states (the gain is calculated as the ratio of the number of photons received by Bob to the number of pulses sent by Alice). η_{EC} is the efficiency parameter of the error correction algorithm, H_2 is the binary entropy function, E_μ is the QBER estimate for signal states, and Q_1^L and E_1^U are the lower bound of the gain and the upper bound of the QBER for single-photon pulses. Δ is a security parameter as defined in Equation (2.30).

The lower bound of the gain for single-photon pulses (Q_1^L) can be calculated using an improved version of Equation (2.28) which includes the measure of noise [126]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \tag{3.11}$$

where $\mu = 0.5$ and $\nu = 0.1$ are the average photon number for signal and decoy states respectively and Q_ν is the gain for decoy states.

The upper bound on the QBER for single-photon pulses (E_1^{U}), given by Equation (2.29), can also be improved using the vacuum yield term [126]:

$$E_1^{\text{U},\mu} = \frac{E_\mu Q_\mu}{Q_1^L} - \frac{E_0^\mu Y_0}{Q_1^L e^\mu}, \tag{3.12}$$

where E_ν is the QBER estimate for decoy states, and E_0^μ is the measured vacuum error rate for the signal states. There also exist another upper bound for E_1^{U} [183]:

$$E_1^{\text{U},\nu} = \frac{E_\nu Q_\nu \text{e}^\nu - E_0^\nu Y_0}{\nu Q_1^L} \mu e^{-\mu}, \tag{3.13}$$

E_0^μ is the measured vacuum error rate for the decoy states. Since both upper bounds are valid, one can use the smallest of the two to get the best upper bound in all cases:

$$E_1^{\text{U}} = \min\left\{E_1^{\text{U},\mu},\ E_1^{\text{U},\nu}\right\}. \tag{3.14}$$

3.2.5 Overhead and performance

One of the concerns in satellite communication is the limited power availability, computational processing speed, on-board memory, and communication speed with the ground [184].

It is therefore crucial that our QKD software performs as efficiently as possible. To verify this we characterized the computational processing time, memory usage and communication requirements of our software. In addition, our software was implemented on a low-power embedded system to show its capability to function on a system with limited resources and power availability. The characterization of the software was performed by Nikolay Gigov [169].

Unlike the transfer of the optical quantum signals, which must be transfered during the limited flyby time of the satellite, the classical communication can be performed either in parallel with the optical link or at a later time, using a ground station with a radio frequency link (but not necessarily with optical capabilities). In the case where the classical transfer occurs in parallel with the optical link, the processing time and communication bandwidth will be the limiting factor. Using a separate ground station for the classical communication (or combining some classical communication at the original ground station with classical communication at a second one) would alleviate this processing and communication bandwidth requirement. The main concern with using such an approach is memory restrictions on the satellite.

If the classical communication occurs after the optical link, the satellite will be required to store all time-tags accumulated during the optical link, along with the measurement basis and result. In addition, the satellite must also store the LDPC matrix used for error correction and the privacy amplification Toeplitz matrix shift register.

In contrast, real-time classical communication would allow most of these tags to be filtered through sifting and temporal filtering, while reducing the amount of data of the remaining tags by removing the need for exact time-stamps (since the time-tags are already matched) and measurement basis (obsolete after sifting). The error correction step is more efficient when performed after the transfer of optical quantum signal because is efficiency increases with large sifter key size. This is because the sum-product algorithm [170] used in the error correction operates optimally on blocks as larger as possible [169]. If the classical communication where to be done in real-time, the error correction and privacy amplification could be performed at the end of the satellite flyby, when the elevation angle of the satellite is too low to allow quantum signal to be exchanged (due to high loss), but still allowing radio frequency communication (which is more robust to loss due to the higher signal intensity).

For our implementation, the block size for the error correction was artificially limited to 600000. This artificial limit was implemented because longer block sizes require more processing time, especially in terms of creating the error correction matrix. There are no block size limit to the privacy amplification, which can be implemented efficiently and the

memory required is minimal. Having no limit on the block size on the privacy amplification is important because the finite-size effects should be based on the block size used in privacy amplification, meaning a limit would require the finite-size statistics to be applied on the block size limit rather than the full key size (or the smallest of the two), leading to worst results.

Memory requirements

The time-tags produced by our current time-tagging hardware have a size of up to 64 bits. This can be reduced significantly to allow reduced memory requirement and reduced classical communication traffic, but at the cost of additional computational steps. One of the simplest way to achieve this is to group the time-tags in 1 s chucks and only store the full information of the first time-tag, truncating the other tags to only the sub second information. The 1 s grouping was chosen because our GPS receiver outputs a data packet once every seconds (the GPS data is required for initial synchronization). We can thus group the time-tags with the GPS data for each 1 s intervals. This truncation of time-tags reduces the size of each tags (except the first) to 40 bits. The measurement basis and result are included in these 40 bits time-tags.

The error correction requires a M by N sparse parity check matrix to be applied to a N bits block of sifted key to produce the syndrome vector of size M. We can deduce an estimate of the size of the LDPC matrix, based on the channel QBER (E_μ), by applying Shannon's channel coding theorem [185] to the binary symmetric channel [186]. Using this approach, we obtain an estimated matrix size of [187]

$$M = N\eta_{\mathrm{EC}} H_2(E_\mu), \tag{3.15}$$

giving us a matrix size that varies based on the size on the block N, the estimated error correction efficiency (η_{EC}), and the estimate of the QBER. If the decoding step fails one can simply retry with a larger matrix (rather than discard the block of sifted key), allowing to still extract secure key. The new matrix must consists of the original matrix with additional lines appended to it. Because of the linear relationship between the number of line M and the error correction efficiency η_{EC}, a larger matrix will imply a worst error correction efficiency (higher η_{EC}).

Both the LDPC matrix and syndrome vector must be stored. For typical block sizes, error correction efficiencies and QBER, the total memory requirements for this is on the order of 100 bits per sifted bit. For privacy amplification, Bob only needs to store a random

binary sting of, at most, the same length as the sifted key. The total memory requirement is thus 40 bits per time tags and an additional ≈101 bits per sifted bits.

The total raw key length for the best pass of an uplink with a 300 MHz WCP source (calculated in Section 2.5) is ≈300 kbits, with the sifted key being, at most, half of this value. Therefore the expected maximum memory usage during a single pass is ≈27 Mbits, or ≈3.4 Mbytes. In a downlink, the expected raw key length is ≈1.6 Mbits, leading to a maximum memory usage of ≈18 Mbytes. These are well within the feasible realm of memory capacities for space qualified technologies, with some recent space missions, such as the mars rovers, having memory capacities as high as 256 MBytes [188].

Computational requirements

The computational resource requirements were tested on an inexpensive (≈ $150), low-power (2 W) Freescale i.MX53 QSB single-board computer which used a single-core 1 GHz ARM processor with 1 GB of volatile RAM [168]. The requirements were estimated by accumulating 300 s of data at a receiver detection rate of ≈150 kHz. Each one second chuck of data was then truncated to various detection rates within the expected range of detection rates of satellite QKD (based on the raw key rates calculated in Section 2.5). The full QKD protocol is then implemented on the data subsets at these various raw key rates.

The memory and CPU usage on the embedded processing system is shown in Table 3.1. The processing time was found to scale quadratically due to the quadratic scaling of the matrix multiplication process in the privacy amplification, while all other post-processing steps scaled linearly. These processing times represent worst case scenario as the lowest testes raw key rate, 10 kHz (corresponding to a total of 3 Mbit for the 300 s), is still more than the expected raw key length of the best pass in a satellite downlink when using a 300 MHz source rate (≈1.6 Mbits), and almost an order of magnitude more than the expected maximum raw key length in an uplink (≈300 kbits).

Table 3.1: Measured performance of the satellite-side QKD process running on a Freescale i.MX53 embedded ARM board processing 300 seconds of QKD data."OS" is the time taken by operating system facilities invoked by the QKD process. The processing time was found to scale quadratically with the raw-key rate—a least-squares quadratic fit to the data gives a coefficient of determination $R^2 = 0.9995$. The processing time, OS overhead and memory usage of the satellite-side QKD process have been measured with the Linux *time* command.

Raw key rate [Hz]	**Sifted key rate [Hz]**	**QBER [%]**	**Processing time [sec]**	**OS [sec]**	**RAM used [Mbyte]**
10 000	3538	4.4	46.7	14.4	25.98
20 000	7186	4.8	65.4	16.2	43.06
30 000	10 586	4.6	86.7	18.3	59.11
40 000	13 833	4.9	115.9	18.4	75.63
50 000	17 512	5.0	157.1	21.5	93.74
60 000	21 145	4.9	206.1	21.8	110.30
70 000	24 552	4.8	257.7	23.5	125.38
80 000	28 276	4.7	323.5	24.6	141.92
90 000	32 489	4.8	408.3	26.6	158.44
100 000	35 527	5.1	481.9	29.2	175.04

3.3 Results of the high loss QKD demonstration

3.3.1 Stability and polarization compensation

The stability of the high loss QKD system was tested by measuring the QBER for ≈6 h. The results, shown in Figure 3.12, show that the system was, on average, stable for 1 h before significant increase to the QBER occured. However, the duration of the stability varied greatly, from as little as 0.5 h to over 2.5 h. The drift is mostly due to temperature drifts which affect the polarization in the fibers going from the modulators to the up-conversion source, and from the up-conversion source to the quantum channel.

The automated polarization compensation was used when the QBER began to significantly increase (at ≈2.1 h and ≈3.3 h). In both instances, the QBER was returned to it optimal value, showing its effectiveness. This also shows that the QBER drift is due to polarization misalignment rather than optical misalignment (which the automated polarization compensation system cannot compensate). No forms of alignment, other than the automated polarization compensation, were performed on any part of the system during the measurement.

3.3.2 Fixed loss results

The experiment was performed for losses ranging from 29 dB to 56 dB. 5% of the sifted detections (chosen randomly) were compared to estimate the QBER. These compared detections are discarded from the final key to maintain security. The measured QBER, raw key rate and background count rate are shown in Figure 3.13.

The measured signal QBER ranged from 1.97% to 8.12%. The QBER at lower losses was limited by the intrinsic QBER of the source (which varied aroun 2–3%). At higher losses, the QBER increased due to lower signal to noise ratio. The raw key rate varied between 37336 bits/s at 29.5 dB and 35.3 bits/s at 56 dB, while the background count rate varied between 1–140 cps. Both raw key rate and background count rate are based on the counts within the coincidence window, which was reduced at higher loss to maximize the secure extraction. The coincidence window was adjusting based on the loss following Table 3.2. This coincidence window adjustment accounts for a large portion of the increase in background count rate at lower loss, with the rest of the increase being due to signals from the 1550 nm laser and some continuous wave component remaining in the pulsed 810 nm laser.

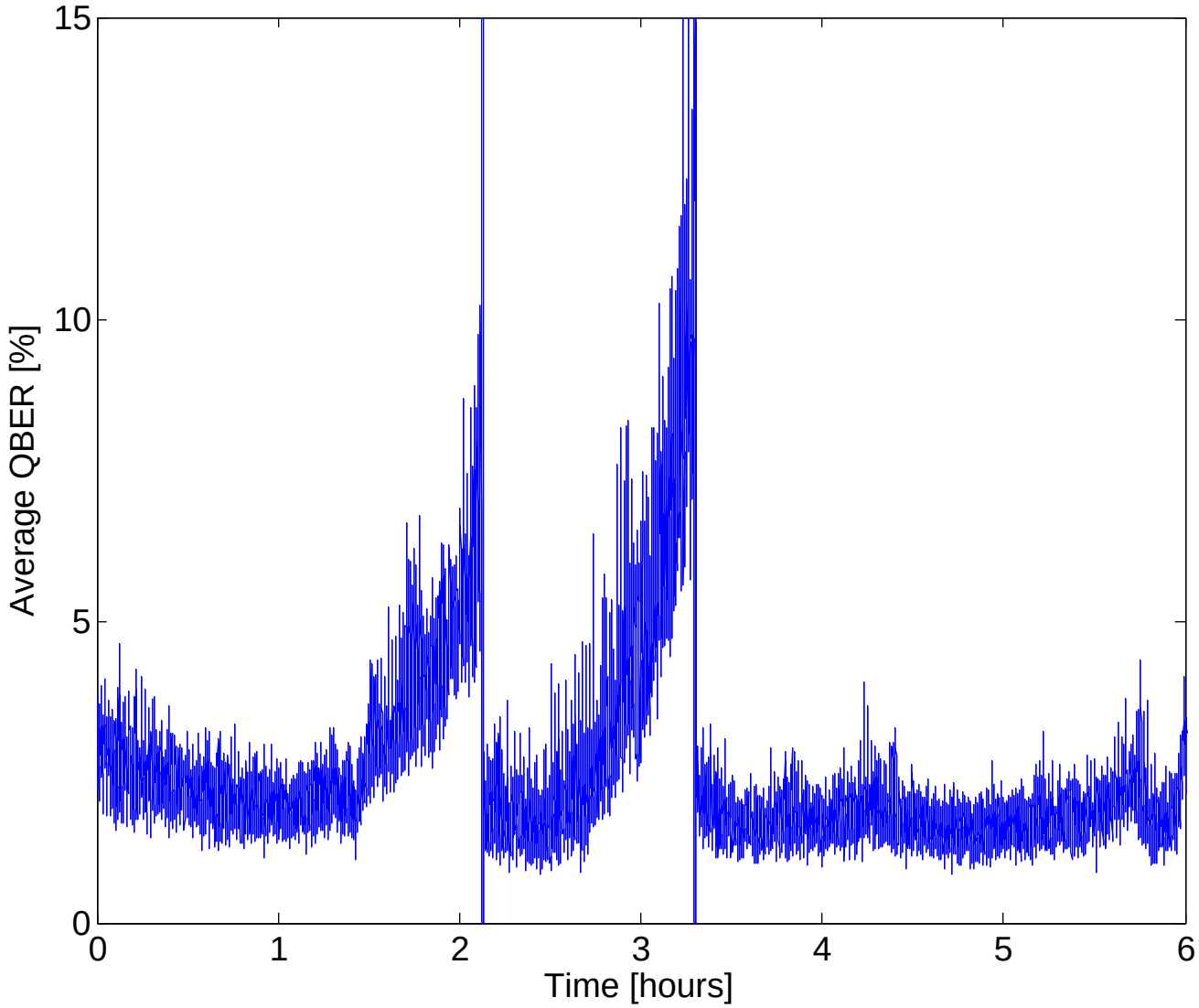

Figure 3.12: Stability of the QBER over time in the high loss QKD system. The system was shown to be stable over an average of ≈1 h. The automated polarization compensation system was used at ≈2.1 h and ≈3.3 h, returning the QBER to its optimal value.

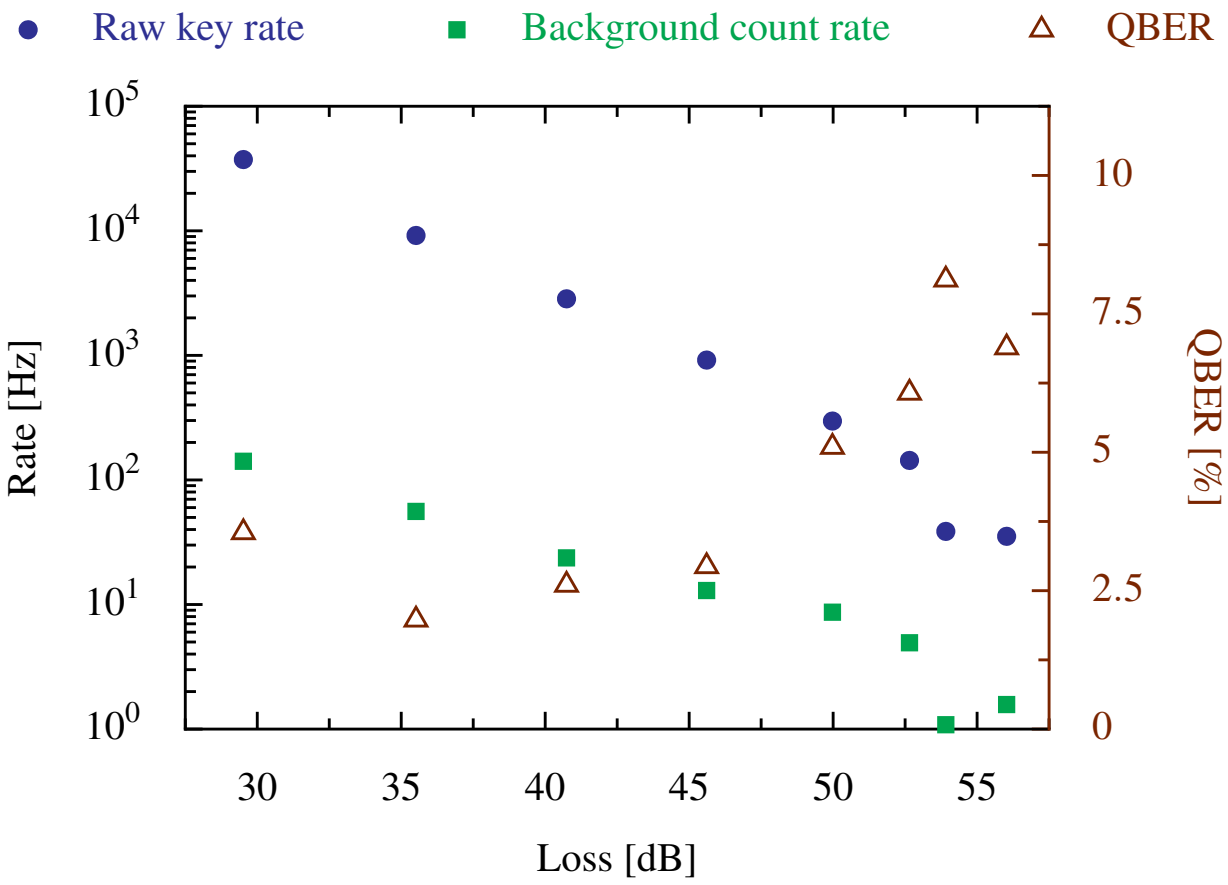

Figure 3.13: Raw key rate, background detection rate and QBER obtained in different loss regimes. The raw key and background rates include only detections that fall within the coincidence window. The background rate (the product of the vacuum yield Y_0 and the pulsed laser frequency, 76 MHz) is determined by measuring the counts received between laser pulses. At lower loss, the background term is dominated by signal from the 1550 nm laser and some continuous wave component remaining in the pulsed 810 nm laser. Since these background signals are produced by the source, they are reduced (along with the raw key rate) as the loss is increased. Variations in QBER between runs are mainly due to temperature fluctuations that affected the birefringence of the optical fiber and the performance of the 1550 nm modulators.

Table 3.2: Coincidence window used for the different losses. The coincidence window is chosen to maximize the secure key rate. At low losses the coincidence window is larger to increase the raw key rate. As the loss increases the increased signal-to-noise ratio is partially compensated by reducing the coincidence window, thus reducing the background counts (which is evenly distributed in time) at the cost of reducing,to a lesser degree, the ray key rate (which has a distribution that is closer to a Gaussian). For comparison, the period between to pulses is 13 ns. The width of the signal peak (typically ≈1 ns) is determined by the combined contributions of the laser pulse width (≈3 ps, negligible), the drift in the repetition rate of the pulsed laser (typically a few 100s of ps), the detector timing jitter (≈50 ps), the electronic jitter in the detector (adding ≈200 ps to the detector jitter), the timing accuracy of the time-tagger (156.25 ps) and the delay of the four detectors compared to each other (typically aligned withing 100–200 ps).

Loss [dB]	**<25**	**25–29**	**29–40**	**40–45**	**45–52**	**52–53**	**53–54**	**>54**
Coincidence window [ns]	1.5	1.3	1.2	1.1	1	0.6	0.4	0.2

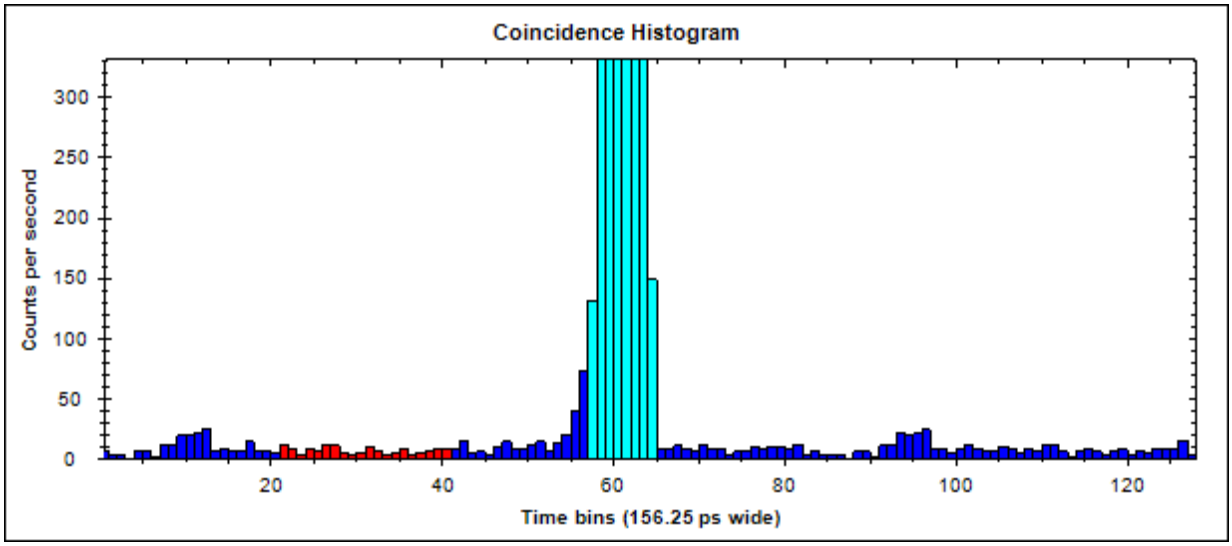

Figure 3.14: Example of the location of the background coincidence window (shown in red). The location of the background coincidence window is a constant time offset from the signal coincidence window (shown in light blue) and was chosen to avoid the regions of increased rates (the small peaks that are visible next to the background coincidence window). These regions of increase are rates likely due to optical ghosting effects, which are correlated to the source and therefore should not be counted as background.

The background count rate is measured by measuring the background between the pulses using a 3 ns coincidence window. An example of the background window location is shown (in red) in Figure 3.14. The 3 ns width was chosen to ensure an accurate estimate of the background. The location is chosen to avoid the regions of increased rates between the peaks. These regions of increased rates are likely due to optical ghosting, where light is reflected from one optical surface (meant to transmit), propagates backward, and is reflected from a second optical surface (also meant to transmit). This results in optical signals from the signal states but with a temporal delay. Since these are correlated with the signal they should not be attributed to background contributions. The background rate of the 3 ns background window is adjusted to the coincidence window used in the experiment and divided by the number of pulse to obtain the vacuum yield (Y_0).

The measured QKD parameters, needed for Equation (2.31), Equation (3.10), Equation (3.11), Equation 3.12, Equation 3.13 and Equation 3.12, are shown in Table 3.4. The experimental data was recorded over periods of ≈300–600 s. For 29.5–45.6 dB, the experimental data was sufficient to extract secure keys in both the asymptotic limit and while accounting for finite-size statistical fluctuations. For 50 dB and 52.7 dB, the duration of the experiment was artificially increased to allow secure key extraction under finite-size

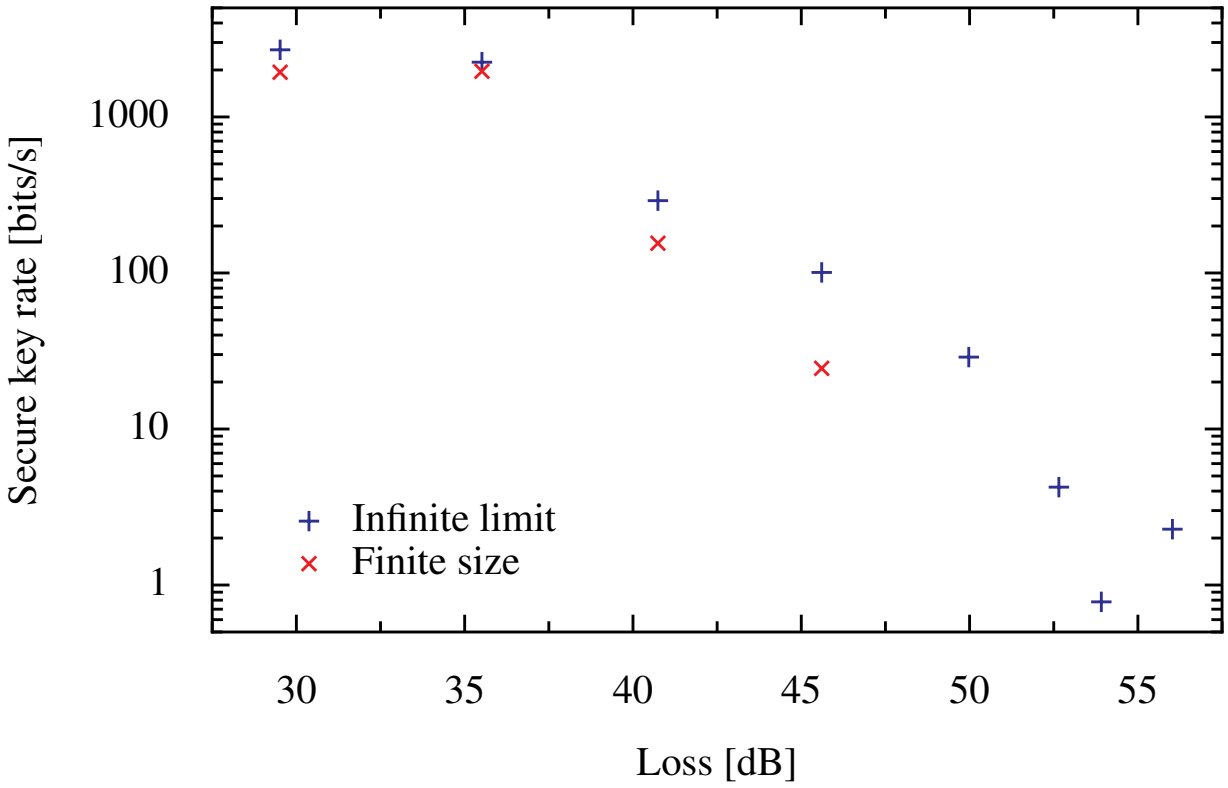

Figure 3.15: Secure key rate (lower bound) obtained in different loss regimes. At low loss the detection rate at the receiver is sufficiently high for the finite-size results to converge with the infinite limit. At high loss we were unable to extract secure key with finite-size statistics using the 300-600 s of experimental data.

statistics. This was done by appending the existing data at the specific loss and appending it to itself until the data was sufficiently long to allow secure key. For 53.9 dB and 56 dB, secure key was only extracted in the asymptotic limit as the duration necessary to extract secure key with finite-size statistics was deemed impractical.

Full error correction and privacy amplification were implemented in our experimental results. The error correction achieved efficiencies of 1.1–1.4, with better efficiencies at higher QBER. This is in line with other studies that have found better achievable error correction efficiencies at higher QBER [189]. After error correction, privacy amplification reduced the probability of an insecure key to $\epsilon = 10^{-9}$. The extracted secure key rate, both for the asymptotic limit and finite-size statistics, are shown in Figure 3.15. The secure key with finite size statistics for 50 dB and 52.6 dB are not included because they require data to be acquired over a longer duration that was actually performed, and thus are based on the assumption that similar quality signals can be exchange over long periods.

Table 3.3: Experimentally measured QKD parameters during the fixed loss demonstrations. The parameters corresponds to those in Equation (2.31), Equation (3.10), Equation (3.11), Equation 3.12, Equation 3.13 and Equation 3.12. For losses of 50 dB and 52.7 dB we had to increase the duration to allow secure key extraction while accounting for finite-size statistics. This was done artificially using data taken at the given loss over a duration of ≈600 s and appending it to itself (i.e. 3030 s of data is obtained by combining 5 sets of the original 606 s of data). At 53.6 dB and 56 dB the system was no longer capable of extracting any secure key while accounting for finite-size statistics. The finite-size statistics is based on a worst case statistical fluctuation of 10 standard deviations.

Parameter	**Measured value**							
Loss [dB]	**29.5**	**35.5**	**40.7**	**45.6**	**50.0**	**52.7**	**53.9**	**56**
Duration [s]	288	606	599	593	5×606	300×682	301	315
μ	0.506	0.490	0.506	0.502	0.441	0.504	0.466	0.466
ν	0.0397	0.0422	0.0519	0.0633	0.0424	0.0489	0.0461	0.0475
E_μ [%]	3.55	1.97	2.60	2.94	5.09	6.07	8.12	6.89
E_ν [%]	39.3	13.0	19.3	7.73	12.7	14.8	22.2	21.8
E_0^μ [%]	50.8	51.9	50.4	50.6	50.3	50.4	50.6	50.6
E_0^ν [%]	42.0	38.0	49.3	44.7	47.2	47.1	47.7	47.5
Q_μ [$\times 10^{-6}$]	536	132	40.8	13.2	4.26	2.06	0.554	0.506
Q_ν [$\times 10^{-7}$]	469	154	44.3	18.9	5.61	2.61	0.853	0.853
Q_1 [$\times 10^{-6}$]	345	107	23.9	8.24	3.04	1.23	0.468	0.414
Q_1^L [$\times 10^{-6}$]	331	101	21.5	6.56	2.60	1.19	0	0
E_1 [%]	5.35	2.21	4.04	4.06	4.50	4.98	8.64	6.82
E_1^U [%]	5.69	2.42	4.78	5.40	7.40	6.49	0	0
Y_0 [$\times 10^{-7}$]	18.7	7.39	3.13	1.71	1.15	0.652	0.143	0.208
η_{EC}	1.4	1.5	1.4	1.35	1.15	1.115	1.1	1.1
Raw rate [bits/s]	37336	9178	2845	917	297	144	38.6	35.3
Sifted rate [bits/s]	18910	3688	1411	459	147	71.2	19.0	17.4
Secure rate [bits/s] (asymptotic)	2681	2233	289	100	28.8	4.22	0.774	2.26
Secure rate [bits/s] (finite-size)	1926	1954	155	24.4	0.430	0.240	0	0

Our system is able to extract secure key at up to 56 dB in the asymptotic limit (extracting 2.26 bits/s) and up to 45.6 dB with finite size statistics on 600 s of experimental data (extracting 24.4 bits/s). These results compare well to a previous high loss demonstration [59] that achieved secure key in the asymptotic limit at 57 dB of loss without performing any post-processing and using only one manually changeable measurement basis (reducing dark counts and elimination double clicks between bases).

3.3.3 Simulating the loss of satellite passes

We further showed the capability of our system to function in the demanding loss regime of a satellite uplink by simulated the varying loss of satellite passes. The varying loss was obtained by moving the lens of the quantum channel during a 45 min experimental run. The initial position of the lens provided a loss of ≈65 dB. The loss was the progressively lowered to ≈30 dB over the course of 20 min, and then increased back to ≈65 dB over the following 25 min. The measured loss during the experiment is shown in Figure 3.16.

Each side of the loss curve (split at the lowest loss point) is then fitted with two cubic curves. These fits are used to match the experimental loss to the average loss of a satellite uplink during a pass. The loss (calculated in Chapter 2) is from a 600 km low Earth orbit satellite uplink using a 785 nm wavelength, 25 cm transmitter, 30 cm receiver and 2 μrad pointing error, and assumes a rural (5 km vis.) sea-level atmosphere. Both the best and upper quartile passes are experimentally simulated.

For each passes, the theoretical losses of each 1 s of the pass is matched to a 1 s point on the curve fits of the varying loss by progressively scanning from the the center (lowest loss) to either edges. Each theoretical point is matched with the closest loss point on the fitted curve that exceeds the theoretical loss. If the closest fitted point is already matched to another theoretical point, the next higher fitted loss point is used instead.

This method ensures that the interpolated loss points are both unique and strictly greater than the theoretical loss points. By matching the loss points using curve fits we ensure that the data samples are not biased by the fluctuations in the measured losses. Figure 3.17 and 3.18 show the theoretically predicted losses, the curve fit value, and the experimentally measured loss, of teach 1 s points of the passes. The estimated QBER is also shown, along with a 95% central credible interval (shaded region).

The measured losses closely match the theoretical predictions while maintaining realistic fluctuations. The QBER fluctuates more at higher loss due to the reduced sample size. This reduction in sample size is due in part to the reduction in received signals (due to the

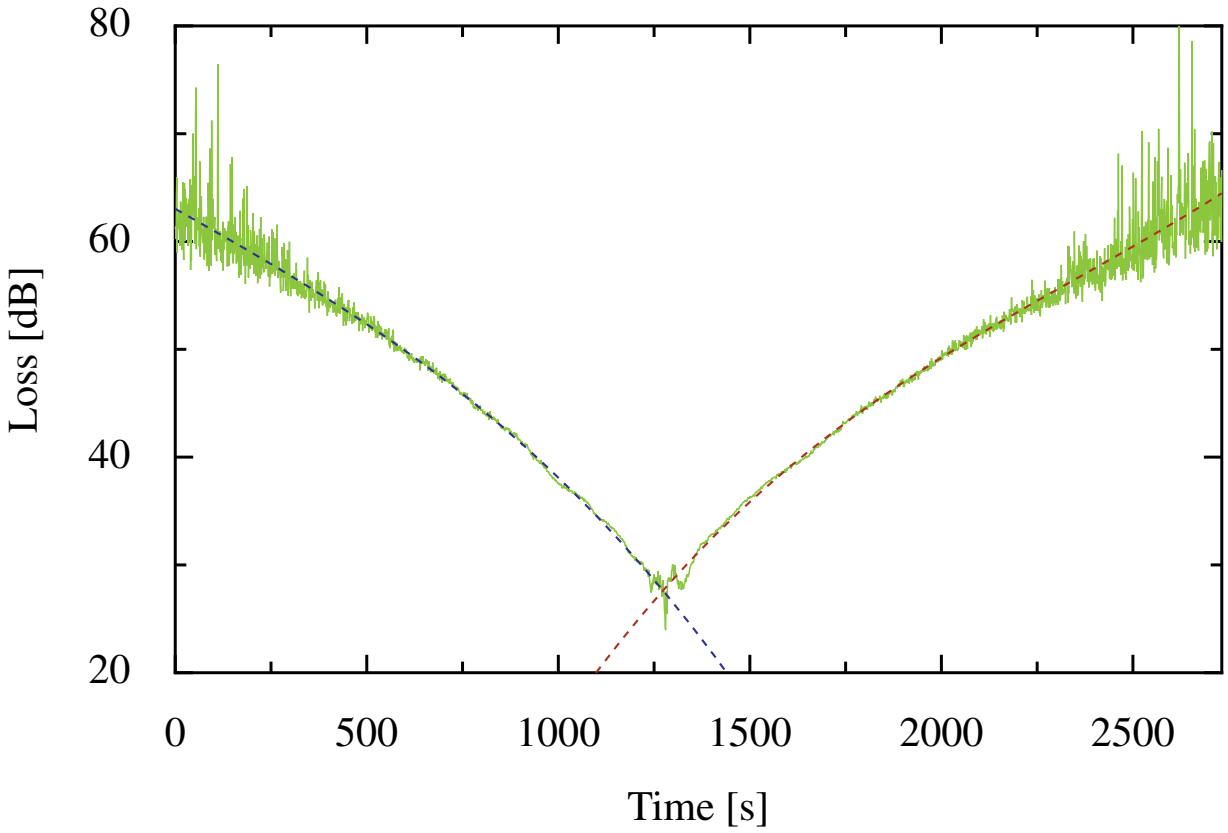

Figure 3.16: Experimentally measured loss over the 45 min data collection used to simulate the varying loss of a satellite pass. The data is fitted with two cubic curves that are then used to match the experimental data with the theoretical average loss of a satellite pass, without being biased by experimental loss fluctuations.

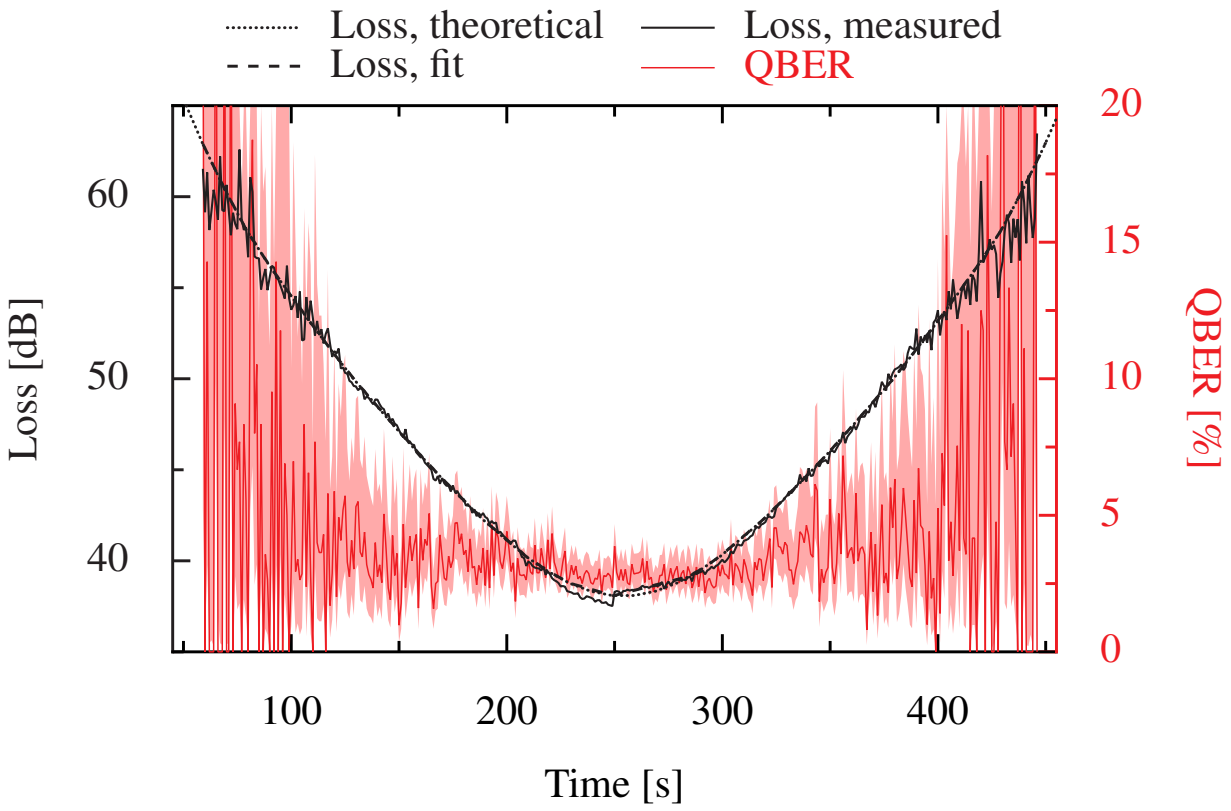

Figure 3.17: Theoretically predicted losses of the best satellite pass, the matched fit losses, and the corresponding measured losses and QBER. The QBER includes a 95% credible interval (shaded region). The theoretical loss is based on an uplink with a 600 km circular Sun-synchronous low Earth orbit satellite at a wavelength of 785 nm, with a receiver diameter of 30 cm, a 2 μrad pointing error and a rural sea-level atmosphere.

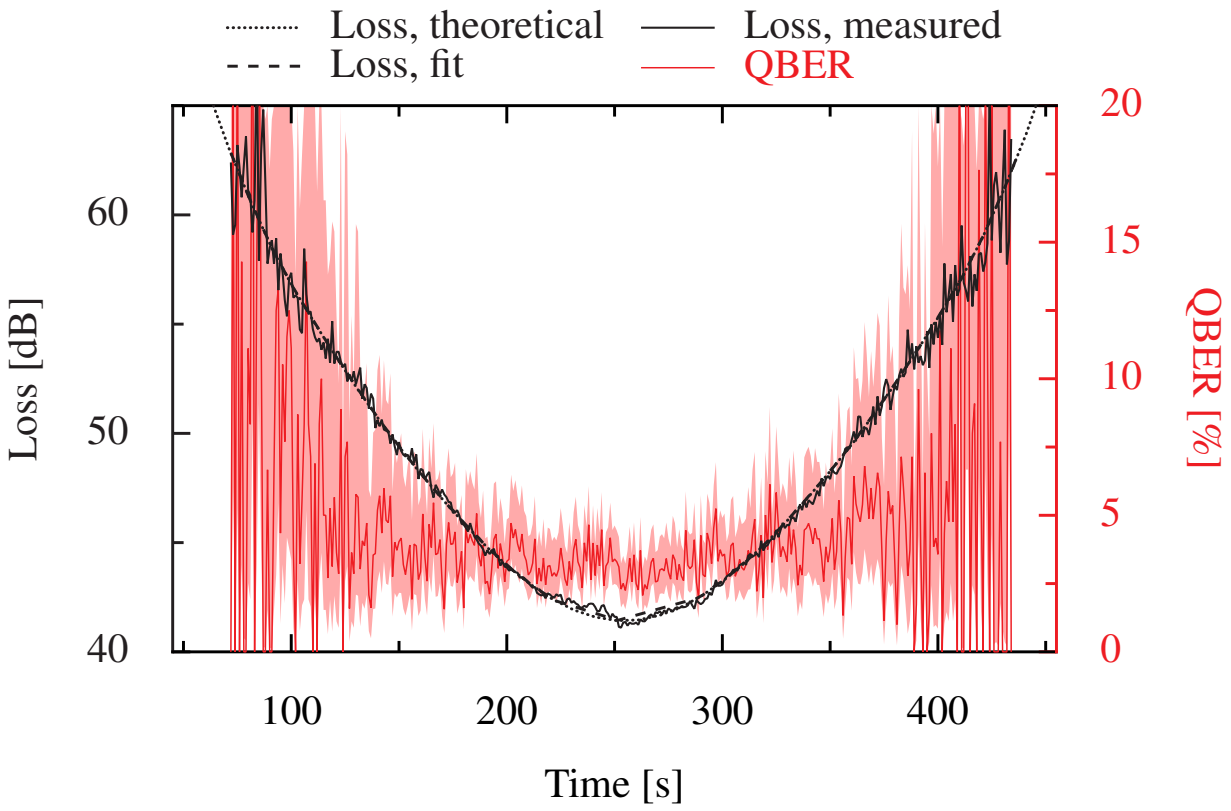

Figure 3.18: Theoretically predicted losses of the upper quartile satellite pass, the matched fit losses, and the corresponding measured losses and QBERs. The QBER includes a 95% credible interval (shaded region). The theoretical loss is based on an uplink with a 600 km circular Sun-synchronous low Earth orbit satellite at a wavelength of 785 nm, with a receiver diameter of 30 cm, a 2 μrad pointing error and a rural sea-level atmosphere.

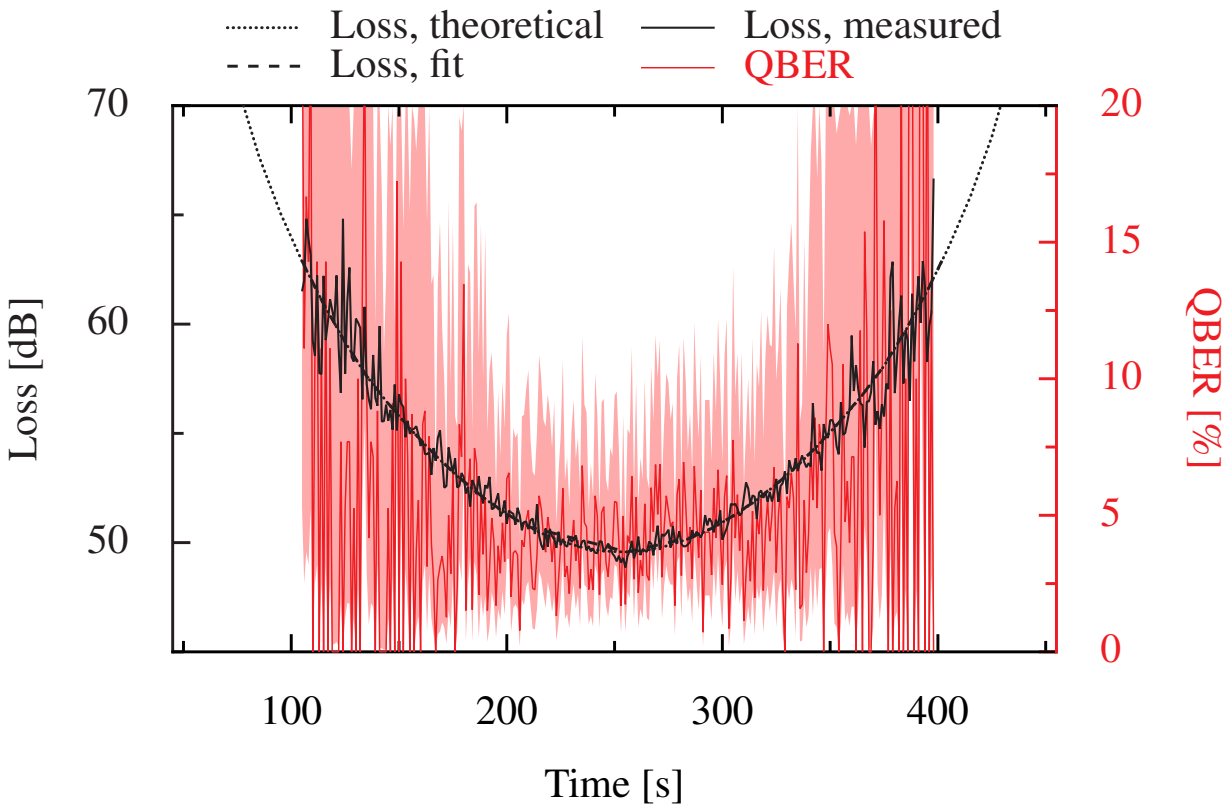

Figure 3.19: Theoretically predicted losses of the upper quartile satellite pass, the matched fit losses, and the corresponding measured losses and QBERs. The QBER includes a 95% credible interval (shaded region). The theoretical loss is based on an uplink with a 600 km circular Sun-synchronous low Earth orbit satellite at a wavelength of 785 nm, with a receiver diameter of 30 cm, a 2 μrad pointing error and a rural sea-level atmosphere.

high loss), and in part to the reduced coincidence window at high losses (see Table 3.2) which temporally filters out more of the detections at high loss. The instances where the measured QBER was zero had low sample sizes of only 66 cps or less (averaging 16.1 cps), sometimes as low as only 1 cps. Since the average QBER is around 4%, the average 16.1 cps have (statistically) 51.8% chance of producing 0% QBER. The confidence in the QBER measurement is quantified by the credible interval (shaded region).

The credible interval is obtained using Bayesian statistics [190, 191], given the binomial distribution of the measurement results (each measured counts will yield either the expected or unexpected polarization result) and assuming a uniform prior distribution over the range of 0–1 (the possible values of QBER). The credible confidence interval is obtained by computing the inverse of the beta cumulative distribution function, with the beta cumulative distribution function given by

$$p = \frac{1}{\beta(a,b)} \int_0^x t^{(a-1)}(1-t)^{(b-1)}, \tag{3.16}$$

with $p = (1 \pm c)/2$ (where c is the desired confidence, 0.95 in our case), $a = 1 + N_E$ (where N_E is the number of counts giving the expected polarization result), $b = 1 + N_U$ (where N_U is the number of counts giving the unexpected polarization result), and $\beta(a, b)$ is the beta function. Taking the inverse will yield x which corresponds to the value at the confidence point (maximum value for $p = (1 + c)/2$ and minimum value at $p = (1 - c)/2$).

Performing full post post-processing on these data sets we were able to extract 8578 bits out of the best pass while accounting for finite-size statistics. Both the upper quartile and median passes required multiple passes to extract secure key with finite-size statistics. The upper quartile produced 349 bits of secret key out of 2 passes while the median pass produced 765 bits out of 35 passes. This shows that passes with insufficient statistics to produced a key do not need to be discarded, but can instead be kept and added to a later pass to create a larger key. In addition, the success of 2 upper quartile passes strongly suggest that a system with twice the source rate (152 MHz instead of 76 MHz) would be sufficient to extract secure key from a single upper quartile pass (as it would produce as much statistics from a single pass as our system does with two). The QKD parameters extracted from the passes are shown in Table 3.4

This demonstration of secure key extraction from simulated satellite passes (with finite-size statistics), as well as the demonstration of secure key extraction from up to 56 dB (asymptotically), shows that QKD can be successfully performed in the demanding regime of a satellite uplink. Our system is capable of performing all post processing steps, including full error correction and privacy amplification, with reduced computational resources at the receiver. These achievements are important milestones towards satellite QKD.

Table 3.4: Experimentally measured QKD parameters of the experimentally simulated passes. The parameters corresponds to those in Equation (2.31), Equation (3.10), Equation (3.11), Equation 3.12, Equation 3.13 and Equation 3.12. The best pass was able to produce 8578 bits of secure key while accounting for finite-size statistics. Both the upper quartile and median passes required multiple passes (2 and 35 respectively) to extract any secure key while accounting for finite-size statistics (resulting in a total of 349 bits and 765 bits total secure key respectively). The finite-size statistics is based on a worst case statistical fluctuation of 10 standard deviations.

Parameter	**Best pass**	**Upper quartile pass**	**Median pass**
Duration [s]	388	363	294
μ	0.506	0.506	0.514
ν	0.0576	0.0574	0.0581
E_μ [%]	3.04	3.42	4.35
E_ν [%]	13.9	14.6	16.3
E_0^μ [%]	50.7	50.6	50.7
E_0^ν [%]	45.3	45.6	44.6
Q_μ [$\times 10^{-6}$]	24.3	12.4	2.51
Q_ν [$\times 10^{-7}$]	28.9	15.3	3.44
Q_1 [$\times 10^{-6}$]	14.2	7.36	1.46
Q_1^L [$\times 10^{-6}$]	11.9	6.15	1.31
E_1 [%]	4.83	5.25	6.09
E_1^U [%]	6.27	6.85	7.17
Y_0 [$\times 10^{-7}$]	1.70	1.24	0.671
η_{EC}	1.28	1.24	1.15
Raw key [bits/pass]	656746	314371	51444
Sifted key [bits/pass]	326823	155318	25253
Number of passes needed for finite-size	1	2	35
Secure key [bits/pass] (finite-size)	8578	174.5	21.86

Chapter 4

QKD using a diffusive screen

Light scattered by a diffusive material has been extensively studied in the context of classical imaging [192–200]. In the context of quantum applications, single-photons, encoded in polarization, were recently used to show secure imaging of an object [201]. The polarization encoding allows the user to detect if the image was altered, much in the same way as QKD allows the detection of an eavesdropper. This technique therefore allows secure imaging where the system is able to detect if the photons producing the image were tampered with.

In this chapter we explore the concept of using a diffusive screen to enable multi-user QKD. A QKD source is pointed at a diffusive screen which scatters the light in a large angle (either in transmission of reflection) while maintaining the polarization states. A quantum receiver is then used to capture light and extract a secure key. In the future, such a diffusive screen could be used to create QKD hot-spots where users could exchange, with little or no pointing required, a secure key using a mobile quantum receiver device, ideally embedded in devices such as mobile phones or portable computers. This would allow these devices to accumulate keys when in range of these hot spots which can then be used to secure online activities (such as online banking, shopping, etc.). This approach could be used to implement a wireless quantum key distribution system to complement fiber based quantum networks [202–207]. While the technology is still far from providing the necessary efficiency for such a hot-spot, a proof of concept demonstration is currently possible.

In the first part of this chapter, Section 4.1, we describe the characteristics of the diffusive screens. Section 4.2 then explores the improvements needed to our quantum receiver in order to make this experiment possible. Finally, Section 4.3 briefly discusses the future plans for performing this proof of concept demonstration.

Author contributions

Thomas Jennwein and Brendon Higgins conceived the experiment and provided advice. I designed and built the transmitter and redesigned and modified quantum receiver. I performed the characterizations and analyzed the data.

4.1 Diffusive screens characteristics

To enable polarization-based QKD using a diffusive screen, we need a screen that preserves the polarization state of the diffused photons. Three screens were tested to determine their potential for QKD: one transmissive screen and two reflective screens [208]. The screens were mounted on a rotation stage to allow control over the angle of measurement (see Figure 4.1).

A set of three wave plates (two quarter-wave plates on either side of a half-wave plate) is placed before the screen and is used to compensate any polarization misalignment from the source to the screen using an automated polarization alignment software (see Section 3.1.5). This assumes polarization is maintained by both the screen and free space propagation, a reasonable assumption since the screen should preserve the polarization state, and free space propagation has negligible effects on the polarization [68]. Placing the wave plates before the screen instead of in the quantum receiver (as in Section 3.1.4) allows us to compact the receiver, reducing the loss from non-collimated beams (as is the case for the divergent light diffused by the screens).

4.1.1 Loss of the diffusive screen

After hitting the screen, the light is diffused (either in transmission or reflection) over a large angle. For a 1 mm collimated beam, the diffused light is visibly granulated by the screen (see Figure 4.2). This effect is caused by the granularity of the screen itself, causing a granular diffusion when the incoming beam is of similar size as the granularity of the screen. The granularity of the screen, shown in Figure 4.3, is on the order of 0.1-1 mm. The granular effect increases if the beam is more tightly focused (an thus smaller) (Figure 4.4), and decreases when the beam is defocused (Figure 4.5).

To determine the feasibility of the experiment, we measured the angular distribution of the intensity. The intensity, shown in figure 4.6, was measured 30 cm after the screens with a 1 mm collimated input beam at normal incidence. The angular intensity distribution is

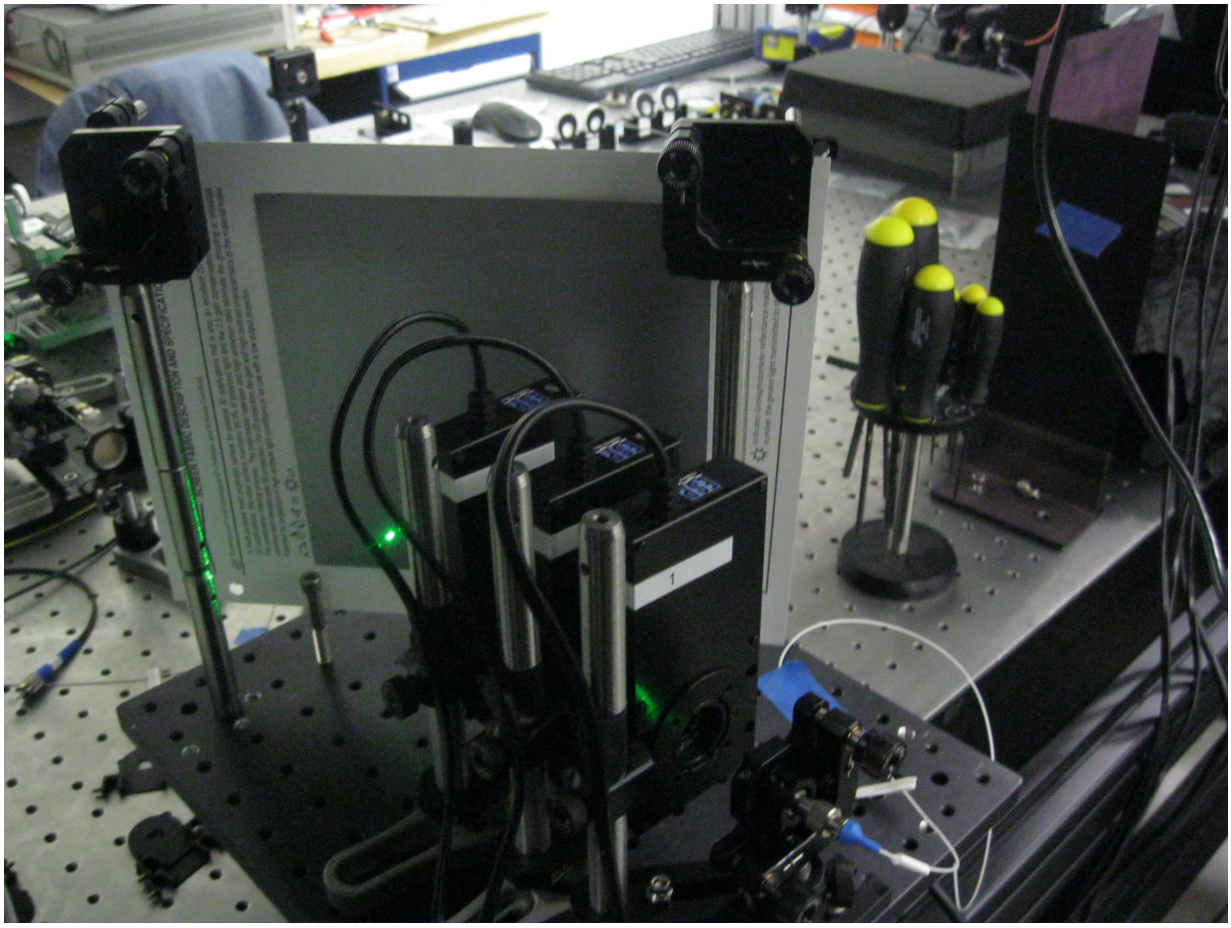

Figure 4.1: Transmitter for QKD with a diffusive screen (here a reflective diffusive screen). The breadboard is mounted on a rotation stage to adjust the measurement angle and three wave plates are used to automatically correct polarization misalignment.

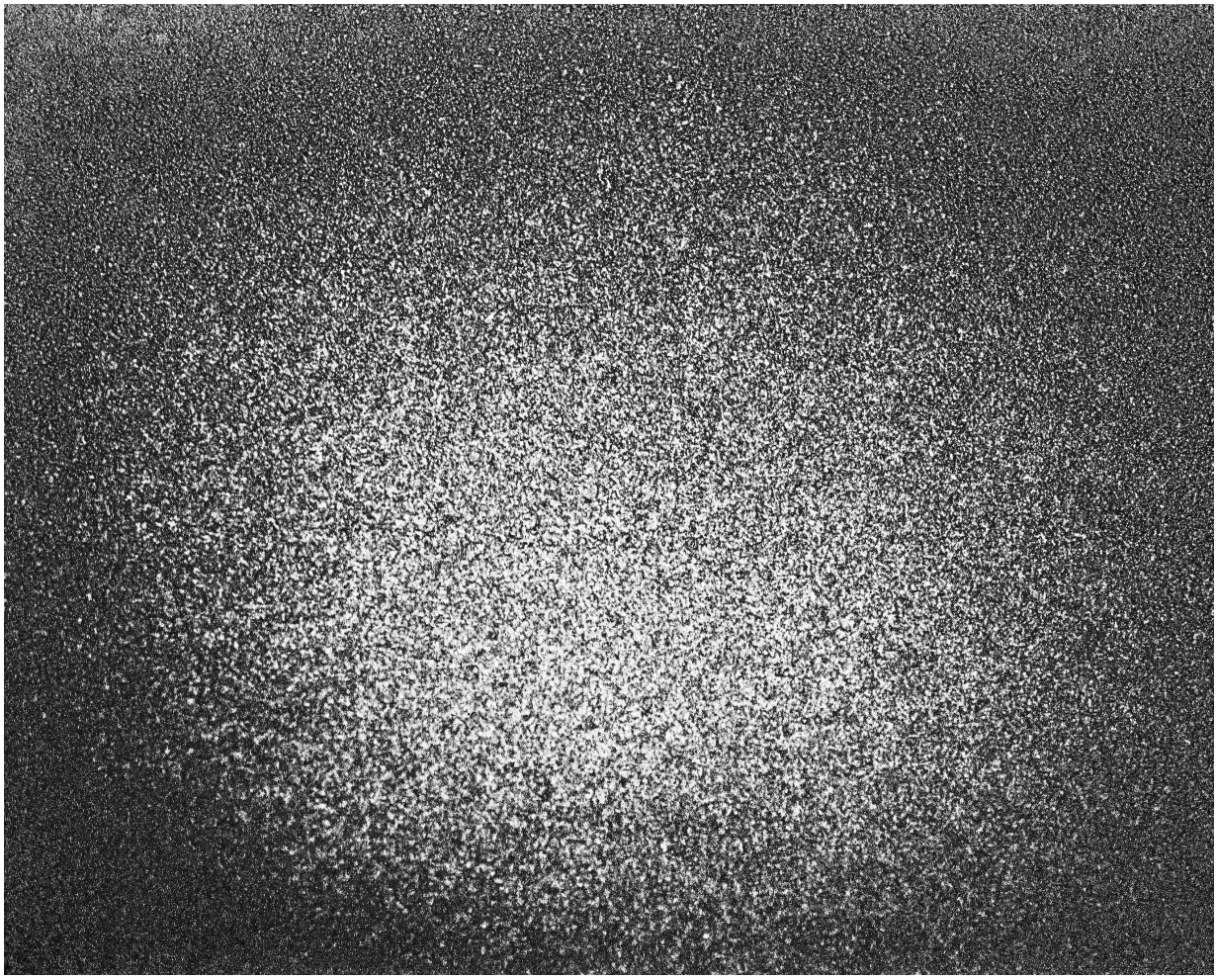

Figure 4.2: Photo of the light 30 cm after a (reflective) diffusive screen. The beam being diffused is a 1 mm collimated beam. Granularity on the order of 0.1 mm can be seen in the diffusion. The image in the photo is ≈20 cm in width.

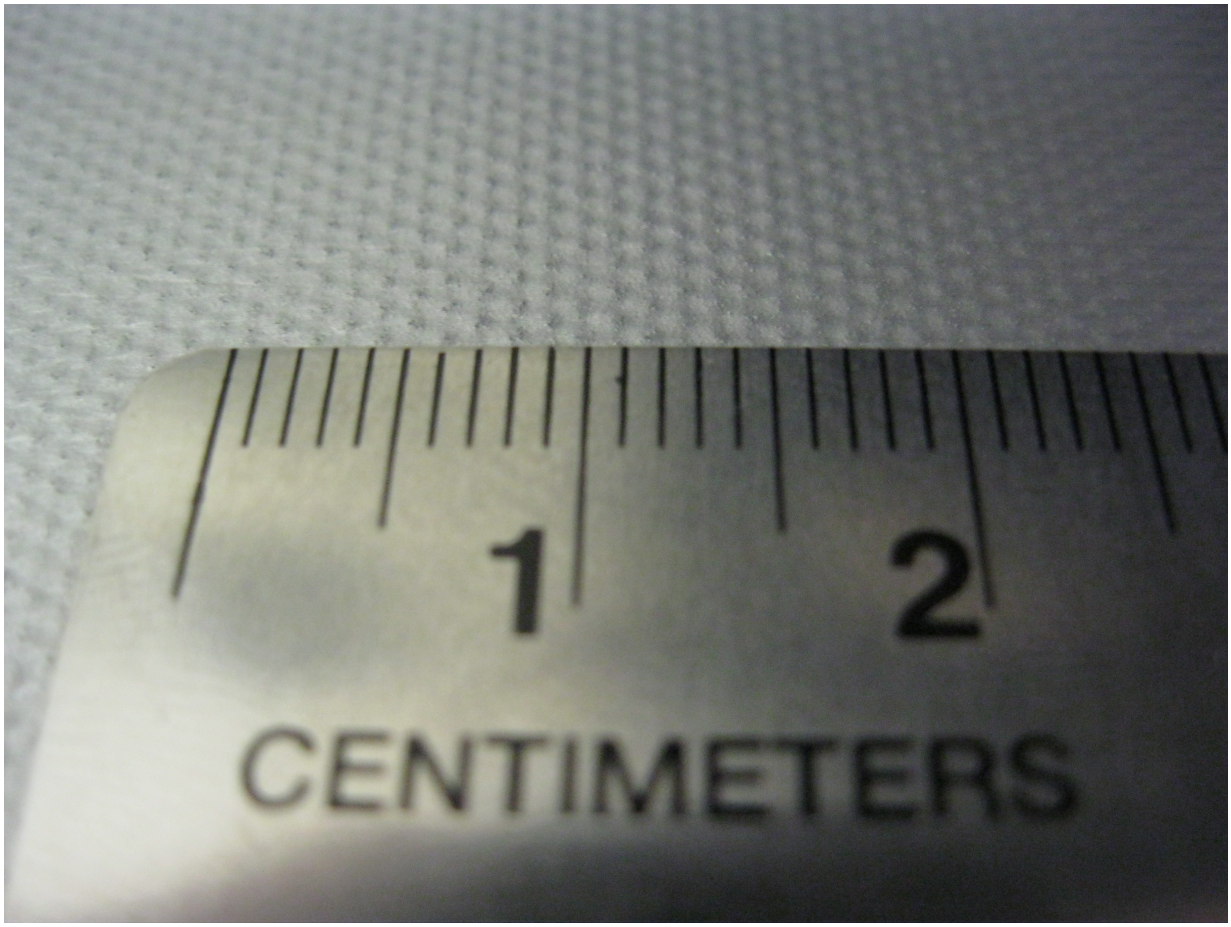

Figure 4.3: Photo of the reflective diffusive screen showing its granularity to be on the order of 1 mm. Smaller granularity on the order of 0.1 mm can also be seen. The other diffusive screens do not show the larger granularity but still have the smaller granularity on the order of 0.1 mm. All screens show similar granularity in the diffusion, suggesting the smaller granularity dominate the effect.

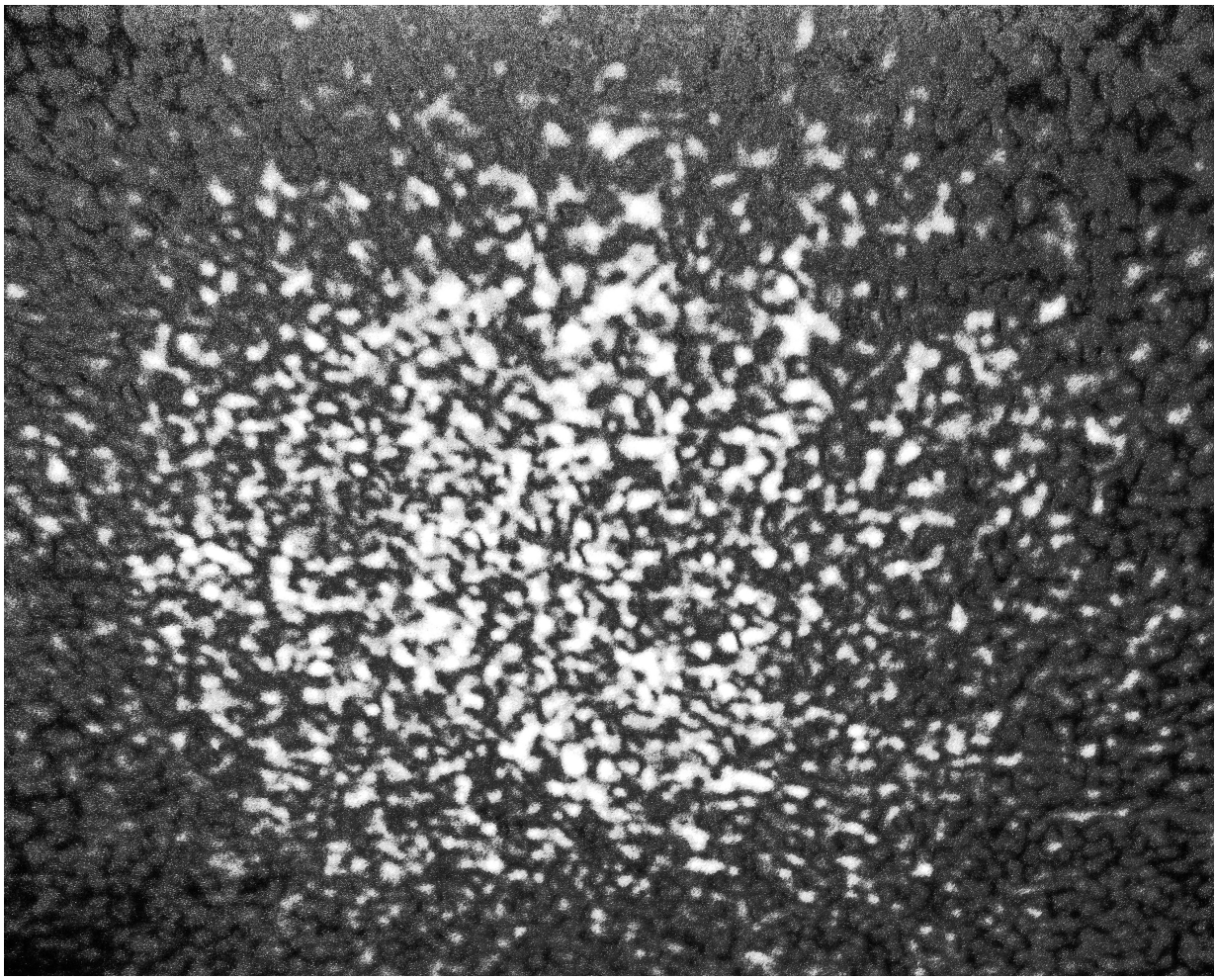

Figure 4.4: Photo of the light 30 cm after a (reflective) diffusive screen when the input beam is focused on the screen. The input beam is focused to ≈0.1 mm by a 5 cm lens, creating a large amount of granularity (on the order of 1 mm) in the diffusion. The image in the photo is ≈20 cm in width.

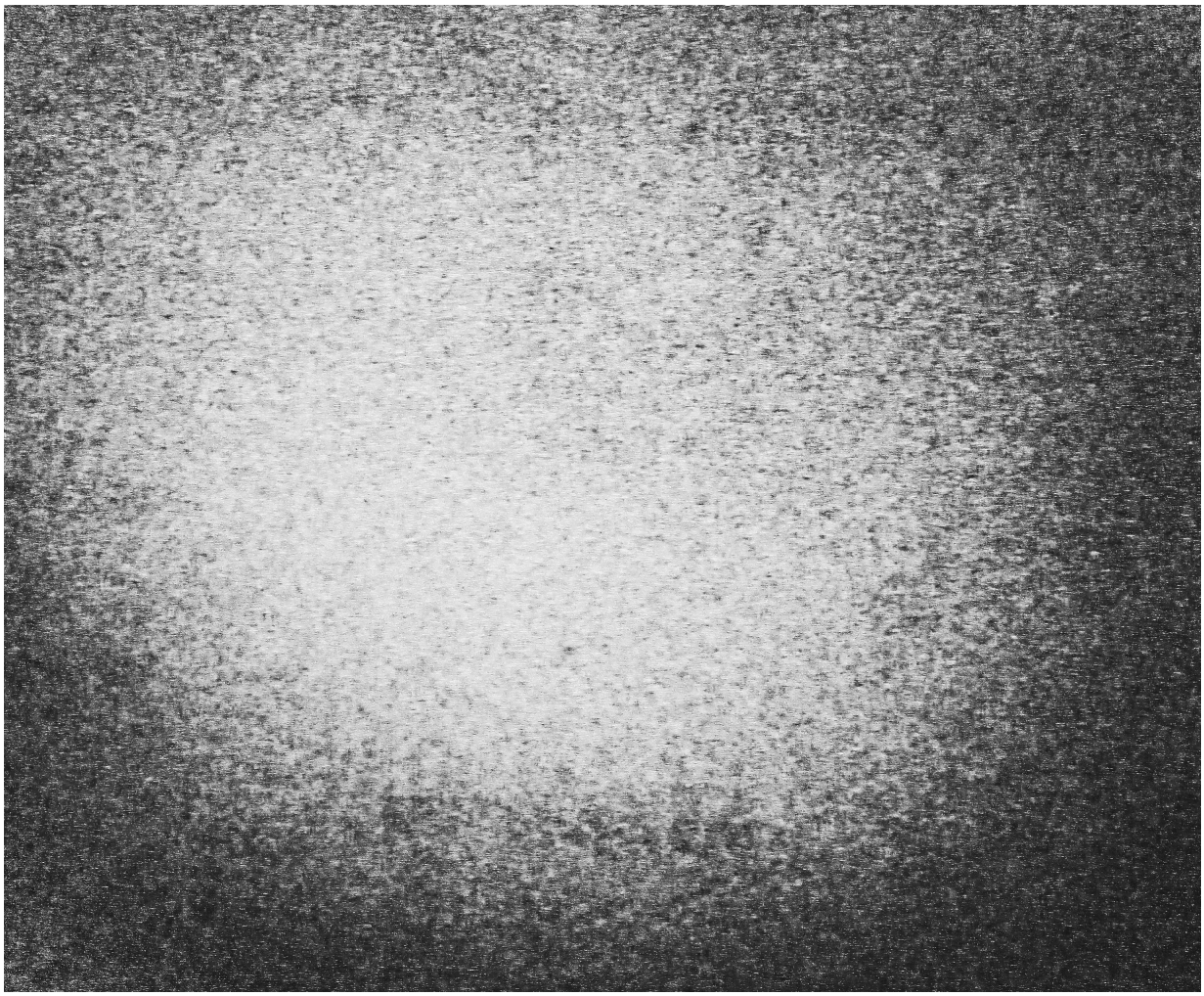

Figure 4.5: Photo of the light 30 cm after a (reflective) diffusive screen when the input beam is larger (and divergent) on the screen. The input beam is ≈1 cm when hitting the screen. Some fine granularity, on the order of 0.01 mm, can still be seen. The image in the photo is ≈20 cm in width.

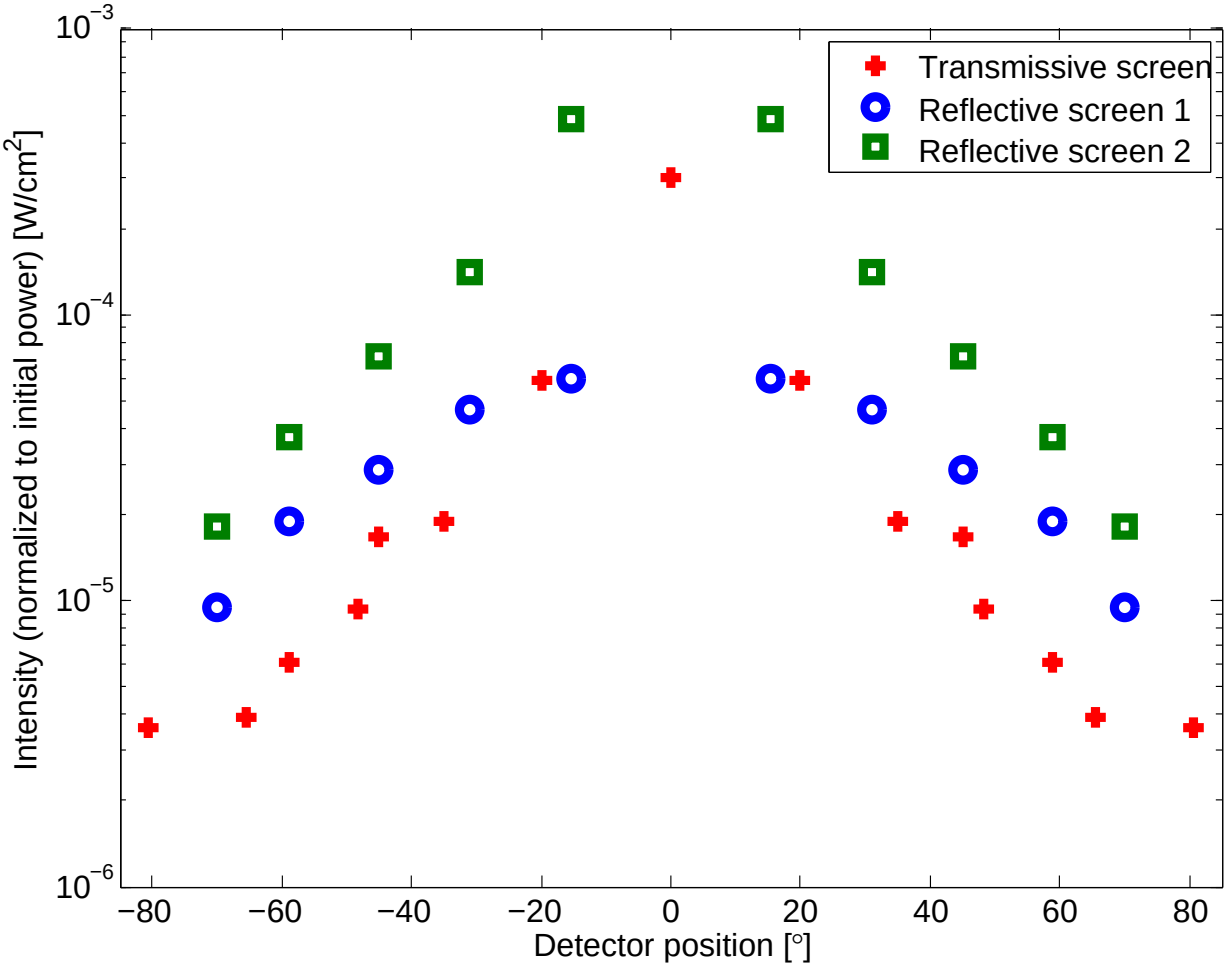

Figure 4.6: Intensity profile of the diffusive screens at 30 cm. The measurement for the reflective screens begins at 15.4° because it could not be measured at normal incidence (0°). The second reflective screen offers significantly less attenuation than the other two screens.

shown to have a Gaussian profile. The power meter used had an active detection area of 9.7 mm by 9.7 mm [164], much larger than the 0.1 mm granularity.

The input lens of our receiver (Section 3.1.4) is 2-inch in diameter, leading to an area of 20.4 cm^2. The power received, given if first order by the measured intensity multiplied by the ratio of the areas (20.4/0.94≈26), should therefore vary between $\approx 8 \times 10^{-3}$ W and $\approx 5 \times 10^{-5}$ W, or 21–43 dB of attenuation. This is well withing the capabilities of our high loss QKD system (Section 3.1) was shown to be capable of operation at over 50 dB of loss (Section 3.3).

Since the intensity decreases quadratically with distance, the near normal incidence diffusion of the best reflective screen should remain below 50 dB at up to 8.5 m. This

makes the concept of QKD with a diffusive screen theoretically possible with our system when considering only loss limits, as our system (described in Chapter 3) is capable of operation at up to 56 dB in the asymptotic limit and up to 50 dB with finite size statistics.

4.1.2 Visibility of the diffusive screen

Another important consideration in the feasibility of QKD using a diffusive screen is the effect of the screen on the polarization state. This effect is characterized using the polarization visibility (Equation (2.24)). This was measured by sending polarized light, either $|H\rangle$, $|V\rangle$, $|D\rangle$ or $|A\rangle$, and measuring the power received after diffusion in both the original polarization and its orthogonal polarization. This was done for all four input states.

The average polarization visibility for each screen is shown in Table 4.1. All screens exhibit a significant drop in polarization visibility when measured at a large angle, limiting their use for QKD to less than 45°. In addition, the first reflective screen suffers from poor polarization visibility even at near 0°. This poor visibility, combined with the screen's higher attenuation, makes the first reflective screen unsuitable for QKD. The other two screens both show good polarization visibility near (or at) 0°. The lower visibility of the second reflective screen can be attributed to the non-zero angle (15.4°) where it was measured.

In addition to measuring the intensity of the diffused light for the initial and the orthogonal polarizations, we also measure the intensity of the polarizations in the other basis (i.e. $|D\rangle$ and $|A\rangle$ for inputs $|H\rangle$ or $|V\rangle$; $|H\rangle$ and $|V\rangle$ for inputs $|D\rangle$ or $|A\rangle$). We found that, for all screens and angles, the intensities were approximately the same in both of the two polarizations regardless of the input states. This suggests that the screen depolarizes light at larger angle, rather than applying an unitary to the state, i.e. the change is not a simple rotation around the Bloch sphere [140]. While this does not rule out a transformation of the polarization towards right-handed and left-handed circular polarizations, such a transformation would be non-unitary as the non-orthogonal basis remains balance in all input cases. Any unitary that would transform the input polarization $|H\rangle$ or $|V\rangle$ while maintaining $|D\rangle$ and $|A\rangle$ balanced would not keep $|H\rangle$ and $|V\rangle$ balanced when the input state is $|D\rangle$ or $|A\rangle$. Since the transformation cannot be a unitary, there no way to compensate the effect of the screen using our automated polarization alignment (Section 3.1.5).

Table 4.1: Diffusive screen visibility at 0° and 45° with a transmissive screen and for 15.4° and 45° with a reflective screens. The initial visibility without screen is also included (only at 0° because the is no diffusion to send light at 45°)

	Average polarization visibility near 0° [%]	**Average polarization visibility at** 45° [%]
No screen	96.0	NA
Transmissive screen	95.1	86.2
Reflective screen 1	88.8	66.1
Reflective screen 2	93.3	82.9

4.2 QKD receiver requirements

While the loss and polarization visibilities of the screen is theoretically sufficient for our system, the receiver design shown in Section 3.1.4 proved to be unsuitable for non collimated light input. In addition, degradation of the detectors caused an increase in dark counts, leaving us unable to perform the experiment without significant improvements to our receiver.

4.2.1 Optical components and alignment

Our original quantum receiver (Section 3.1.4) consisted of a 2-inch input lens with a 250 mm focus followed by a 6.5 mm lens with a 11 mm focus to collimate the beam inside the receiver. Using geometrical optics [209] one can determine, to first order approximation, the distance needed between the two lenses to leave a collimated beam after the second lens:

$$d = \frac{f_1 s_0}{s_0 - f_1} + f2 \tag{4.1}$$

where d is the distance between the two lenses required to colimate the beams, s_0 is the object distance (distance from the first lens to the focal point of the object), and f_1 and f_2 are the focal length of the first and second lens respectively. Because the size of the beam when hitting the diffusive screen is much smaller than the size of the lens, we can approximate the screen as a point source. The object distance s_0 is then the distance between the screen and the first lens. When using a collimated input beam, the object distance tends to infinity. The distance required between the lenses (d) is then simply be the sum of the two focus lengths (261 mm).

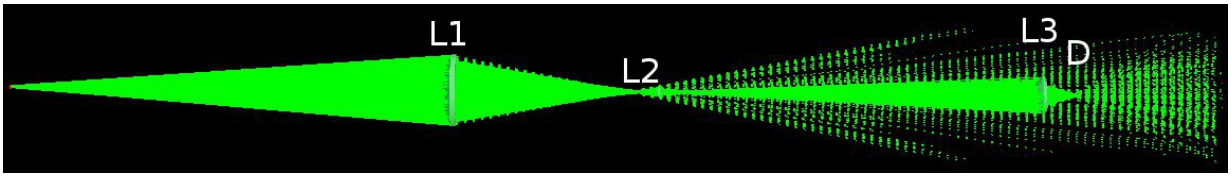

Figure 4.7: Theoretical propagation of the light from the diffusive screen in the modified quantum receiver using a 100 mm focal length input lens (L1). Even with the improvements to the receiver, the theoretically predicted intensity reaching the 50 μm detector (D) active area is only ≈30% of the light captured by the input lens. The screen is located 30 cm from the input lens and the spot size on the screen is 1 mm. L2 has a 11 mm focal length and L3 has a 30 mm focal length.

Using Equation (4.1), we find that when the screen is at 30 cm from the input lens, the distance between the lenses should be 1511 mm, far beyond any reasonable length. To reduce this distance it was necessary to change the input lens of the receiver. A 100 mm focal length lens would require a much more modest 161 mm of separation. The quantum receiver was further improved by replacing the 60 mm focal length lenses, used to focus the incoming light onto the detectors, with 30 mm focal length lenses. This shorter focus lens helps maximize the amount of light reaching the 50 μm detector active area by focusing to roughly half the size that was possible with the 60 mm lens. In addition, the 5 mm polarizing beam splitters cubes were replaced with 10 mm cubes, reducing the possibility of stray light being detected without having passed through the polarizing beam splitters.

The theoretical performance of the system can be estimated more accurately using a ray tracing software [210]. Figure 4.7 shows the predicted performance of the modified receiver, revealing that much of the light still misses the active area of the detector. The optimal performance was obtained with a lens separation (d) of 15 cm, where ≈30% of the light captured by the input lens reaches the active area of the detector. Combined with the measured intensity profile of the diffusive screens (Figure 4.6), the theoretical attenuation at 30 cm from the screen should vary from ≈27–50 dB. Factoring in the detector efficiency of ≈50% and a conservative optical transmission of 50%, we are left with a minimum attenuation of ≈33 dB.

When the modifications were implemented, we found the minimum attenuation (using the reflective screen with an angle near 0°) to be closer to 42–45 dB. This may be due to imperfect optics and limited alignment precision. We also found better results when the input beam was more tightly focused on the screen, thus better approximating a point source, despite the increase in granularity. At 1 m this yields a minimum attenuation of 52–55 dB, at the limit of our QKD system (which able to extract key at up to 56 dB in

the asymptotic case) .

4.2.2 Detector

A crucial factor in enabling high loss QKD is to have very low background noise. This not only requires good background shielding but also detectors with low dark counts. Our free space detectors originally had very low dark counts (5–20 Hz). Unfortunately, these detectors degraded over time, reaching dark counts closer to 50 Hz when the diffusive screen QKD experiment was attempted. This significantly reduced the high loss capabilities of our system. The increased dark counts resulted in a total noise increase of approximately a factor 2, reducing the signal to noise ratio by half. Since the maximum attenuation where a QKD system can function is directly proportional to the signal-to-noise ratio (in the asymptotic case), this increase in background reduced the maximum loss capability of our system from 56 dB to 53 dB. This results in a system barely capable of performing QKD at a distance near 1 m, and an angle of 0°.

The reduced capabilities of our system left us only capable of performing the experiment at very low angles and close distances, making the demonstration considerably less interesting. Instead of pursuing the experiment with the limited capabilities of the current system, it was decided to postpone the experiment until new, low dark detectors could be acquired.

4.3 Future steps of the diffusive screen QKD demonstration

Further improvements to the receiver could be obtained by replacing the free space detectors with fiber couplers and using a fiber coupled detector. This would allow better control over background noise and, since most fiber coupled detectors function with 100 μm core fiber, could increase the area of the collected light by a factor 4. In addition, using a fiber coupler would allow us to significantly reduce the distance between the second lens (used to collimate the beam) and the fiber coupler. Alternatively, it may be more beneficial to add an extra lens between the collimating lens and the fiber coupler to help collect the light. While these improvements could render QKD with a diffusive screen feasible, the reduced visibility at high angles will limit the range of the diffusive screen to withing 45° unless a better diffuser is found.

Due to time constraints, we were unable to implement all of these necessary improvements, leaving us unable to complete the proof of concept demonstration. These improve-

ments are still planned to be implemented, and we expect to perform this demonstration in the near future. This demonstration is expected to be performed in collaboration with Elena Anisimova, a PhD student working on new single-photon detectors with ultra-low dark counts.

Chapter 5

QKD with a moving receiver platform

In this chapter we discuss an experimental demonstration of QKD using a moving receiver platform. Similar experiments where recently performed demonstrating QKD using a moving transmitter platform [54, 55, 211, 212]. In line with our goal of a satellite QKD uplink, we designed and implemented our own system capable tracking a moving QKD receiver and performing a successful key exchange while the receiver is moving at an angular speed similar to a low Earth orbit satellite.

The experimental components of our system are detailed in Section 5.1. Section 5.2 discusses the experimental conditions of the experiment. The results are then presented and discussed in Section 5.3. Finally, Section 5.4 presents the future improvements planned for the system.

Author contributions

Brendon Higgins improved the pointing at tracking software and integrated the automated polarization compensation system with the QKD software to allow active polarization compensation. Catherine Holloway developed the initial pointing at tracking software. Nikolay Gigov developed the QKD software. Thomas Jenewein and Brendon Higgins provided advice on the various parts of the experiment. I designed and built the transmitter and the receiver platforms. I aligned the optical systems. Thomas Jennewein, Brendon Higgins, Catherine Holloway, Christopher Pugh, Sarah Kaiser, Miles Cranmer, Christian Barna, Sasha Chuchin, Jennifer Fernic and I performed the experiment. I analyzed the results and performed the theoretical modeling of the intrinsic QBER of the source. Thomas Jennewein and I designed the new high rate QKD source that will be built in the near future to improve the system.

5.1 Experimental components

5.1.1 Pointing and tracking system

Our pointing system consists of two 80mm diameter RV Series Rotation Stage from Newport [213]. These offer full 360° of travel range, fast rotation speed (20°/s), and good positioning accuracy ($\leq 0.02°$). The motors are mounted using custom-built adapters, with one motor turned 90°. Both the transmitter and the receiver are mounted on such systems, allowing them to be pointed towards each other. A custom-built counterweight is added to ensure the weight is balanced on the motor's axis. Each motors can function with up to 91.8 kg when horizontal (axis of rotation is vertical) and up to 45.9 kg when vertical (horizontal axis of rotation).

Figure 5.1 shows the pointing system with our quantum receiver mounted to it. The horizontal motor, at the bottom, allowed us to set the azimuthal angle while the vertical motor sets the elevation angle. The motors are controlled using a XPS Series Motion Controllers [213] at the transmitter (which also controls three wave plates used for polarization alignment, see Section 5.1.3), and a more compact ESP301 Motor Controller [213] at the receiver.

The tracking system uses a Complementary metal-oxide-semiconductor (CMOS) camera measuring the position offset of incoming beacon lasers at 850 nm. This position information is then used to adjust the pointing to match the incoming direction of the beacon lasers. One camera and three lasers are mounted together on both the transmitter and on the receiver, using a custom-built holder, as shown in Figure 5.2. The camera has a field of view of 4.73° in one axis and 5.91° in the other axis, and an accuracy of 0.0046°/pixels. This accuracy, along with the positioning accuracy of the motors ($\leq 0.02°$), are the limiting factor in the total pointing accuracy of the system.

Both the transmitter and the receiver are also equipped with an accelerometer and gyroscope which can be used to determine the heading and motion of the system. At the moment, the pointing software reads and record the data from the accelerometer and gyroscope but does not make use of it. In a future improvement one could use of this data to implement an initial acquisition system (before the beacon lasers are acquired by the camera).

The motor positions are controlled by a custom tracking software (written in C#) initially written by Catherine Holloway and improved by Brendon Higgins. The software uses the position offset measured by the camera, based on the center of mass of the beacon laser's spot, to calculate the angular deviation of the spot and its angular speed. This

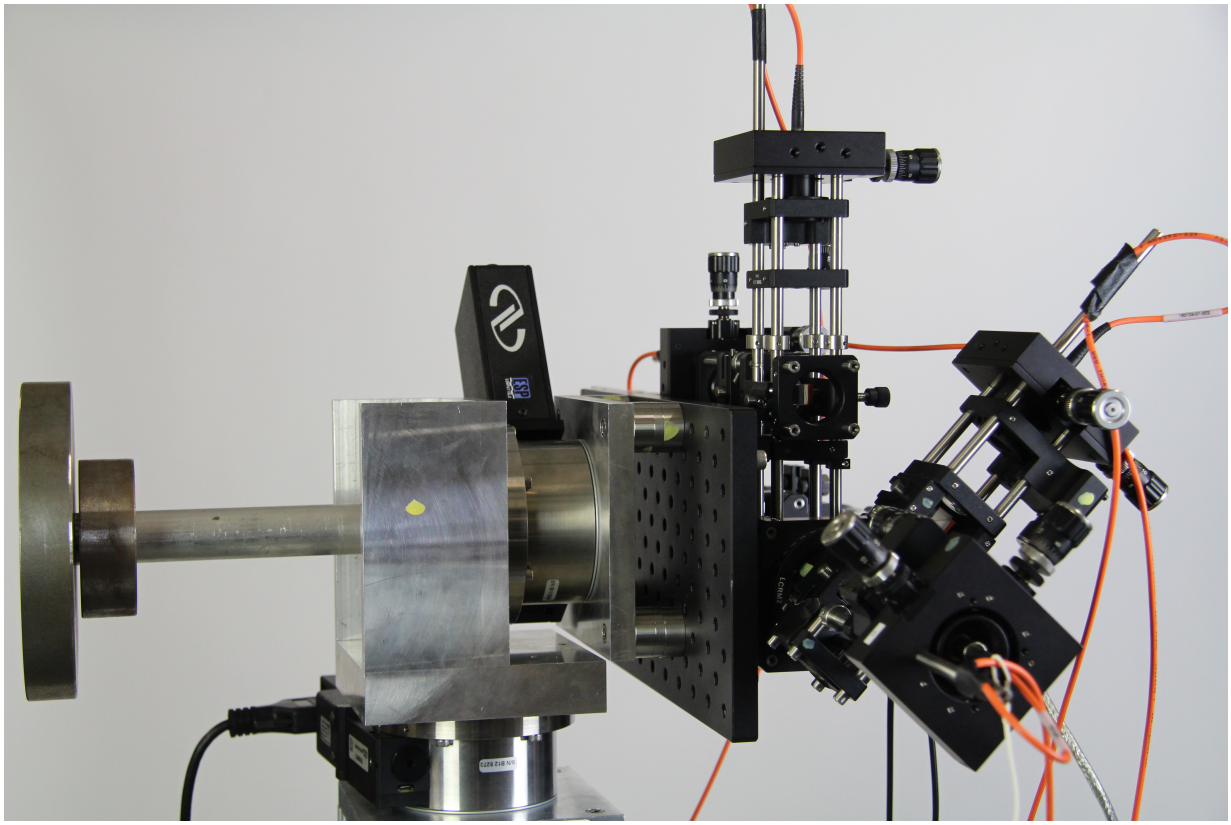

Figure 5.1: Photo of the pointing system with the quantum receiver mounted to it. The motors allow us full range of motion for the pointing direction of the telescope. A custom-built counterweight is used to balance the weight on the motors, ensuring proper performance of the motors.

Figure 5.2: Photo of the camera and beacon laser system used for tracking. Three lasers are used for extra power and for redundancy should one fail during the experiment. Both the transmitter and receiver are equipped with this camera and laser system, allowing each camera to track the other's lasers. The camera has a field of view of 4.73° in one axis (1024 pixels) and 5.91° in the other axis (1280 pixels), corresponding to an accuracy of 0.0046°/pixels.

approach allowed for smooth, continuous motion, which is better for the motors, and more appropriate for pointing with moving targets.

The spot velocity estimation uses the change in offset compared to the last frame, taking into account the motor velocity, to estimate the angular speed. The velocities of the motors are then set to match the angular speed of the spot plus a corrective velocity to correct the spot offset. As the deviation of the spot is reduced the corrective velocity is also reduced until the spot matches the desired position and the motor velocity matches the angular speed of the spot. Both the spot velocity estimation and spot deviation correction use an exponentially decaying weighting factor on its previous estimates to smooth out the change and thus wash out the high frequency jitter. The system can operate at up to 25 Hz, limited by the frame rate of the camera. On the receiver, the system is limited to 12 Hz due to limitations of the software interface with the ESP301 Motor Controller.

The user interface is shown in Figure 5.3. From this user interface one can select the camera, adjust the gain, the exposure time, and the minimum threshold for a pixel to be considered (values below the threshold are assume to be background count by the program; this threshold helps reduce the background interference when centering the spot from the beacon lasers). The optimal position of the spot on the camera may not be at the center due to imperfect collinearity of the beacon and camera compared to the quantum signal. This is compensated by adjusting the X and Y offset which determine where on the camera the spot will be centered. The user interface also allows one to input an initial tip and tilt guess for initial acquisition.

Our pointing software is capable of achieving pointing accuracies on the order of 0.01°.

5.1.2 Receiver platform

The original quantum receiver (Section 3.1.4) had a very narrow field of view of ≈0.04 mrad, or 0.002°. Because this narrow field of view is significantly smaller than the pointing accuracy of our system (on the order of 0.01°) it was necessary to modify the receiver to increase the field of view. We used a ray tracing software [210] to determine how these modifications would affect our receiver. From this we found we could increase the field of view by using an input lens (L1) with a tighter focus, and using a lens with a tighter focus for the last lens (L4). We also found that adding an extra lens (L3) between the collimating lens (L2) and the last lens (L4) would help collect light.

Our modified receiver design, shown in Figure 5.4, consists of a 2-inch diameter input lens with a 100 mm focal length (L1) followed by a 6.5 mm diameter, 11 mm focal length

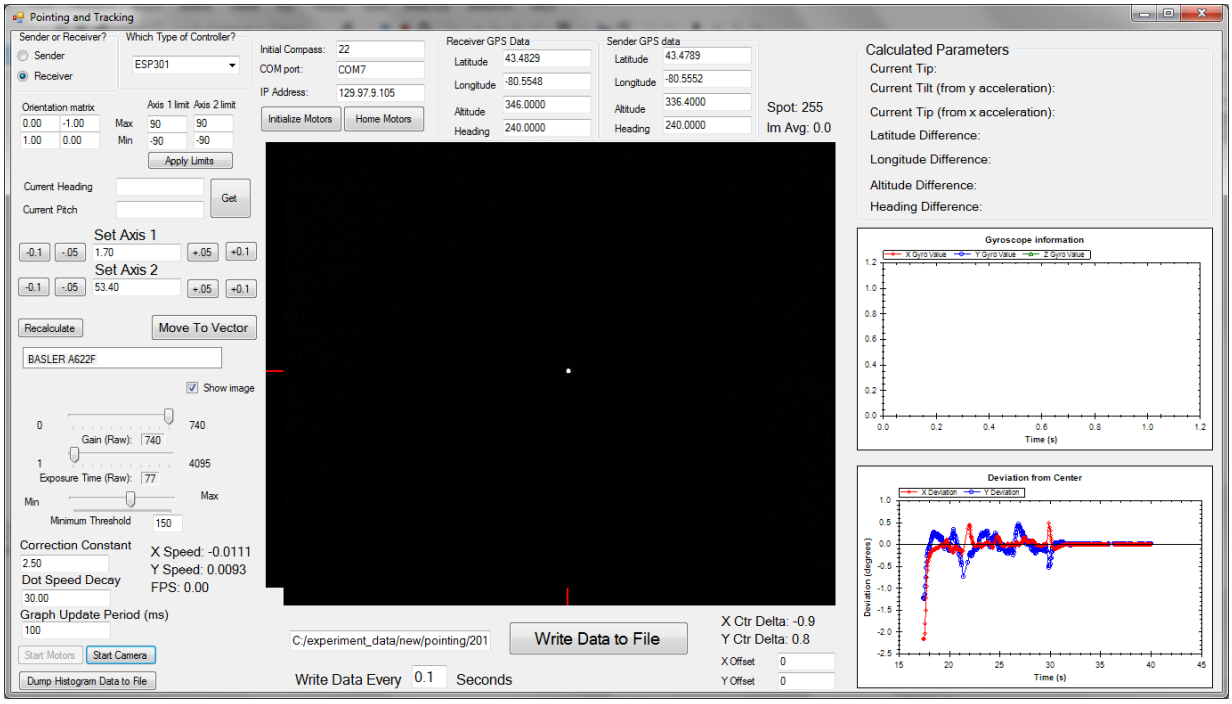

Figure 5.3: Pointing system user interface. The program measures the position of the spot seen on the camera and sets the motors velocity based on the angular velocity and position offset of the spot.

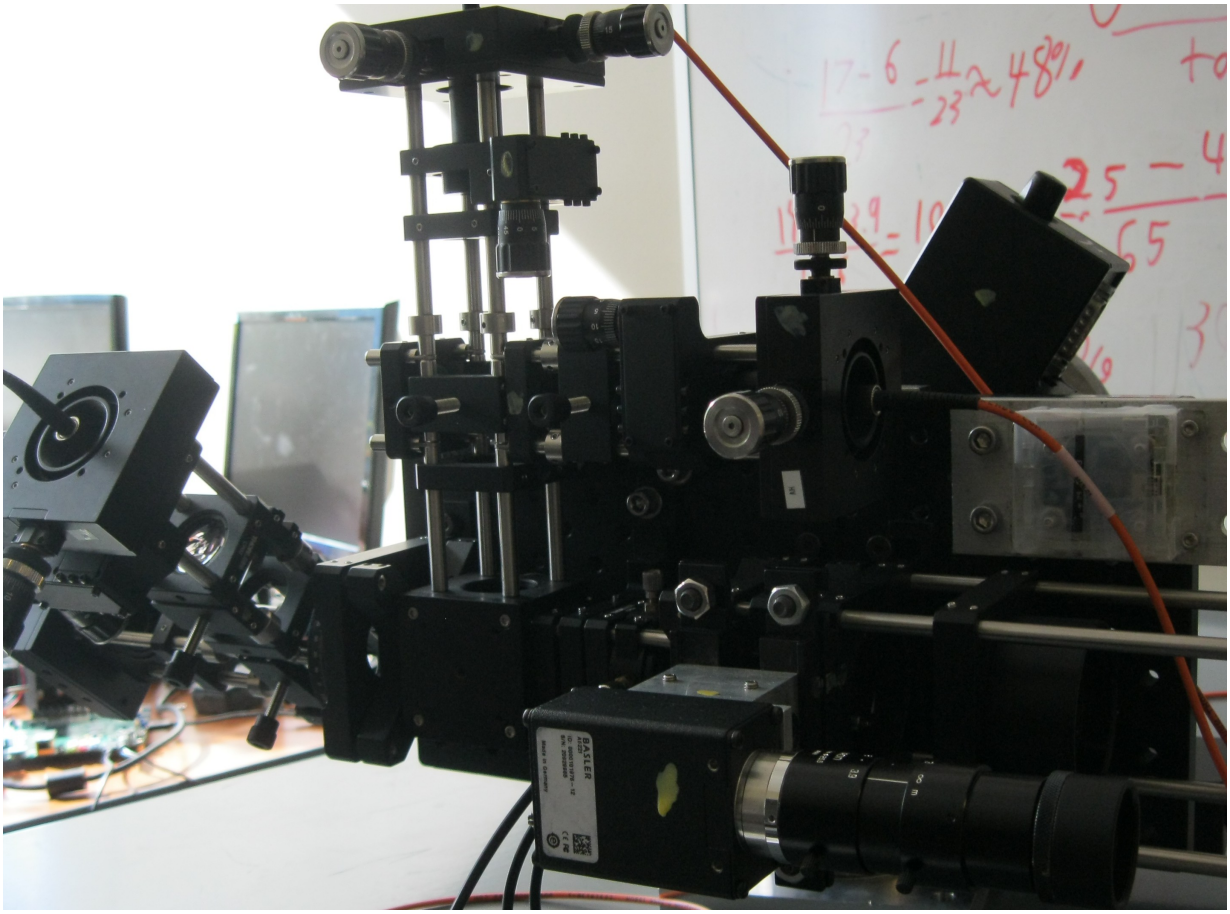

Figure 5.4: Photo of the modified receiver. A 2-inch diameter, 100 mm focal length lens collects light which is collimated by a 6.5 mm diameter, 11 mm focal length lens. A combination of a 1-inch diameter, 60 mm focal length lens and a 12.5 mm diameter, 10 mm focal length lens are used to couple light into each of the four multimode fibers.

lens (L2) place immediately before a custom pentaprism beam-splitter (unmodified from the original design).The distance between the first two lenses is 123 mm, slightly more than the sum of their focal length (111 mm). The three wave-plates from the original design were moved to the transmitter, allowing the receiver to be more compact. The 532 nm filters (2 nm bandwidth) that were originally before the detectors were removed, and two were placed before the pentaprism along with two shortpass filters with a cut-on (high transmission) range of 400 nm to 700 nm.

The 5 mm polarizing beam splitter was replaced with 10 mm versions, an improvement originally made to facilitate the demonstration of QKD with a diffusive screen (Chapter 4). The four 1-inch diameter, 60 mm focal length lenses (L3), originally used to focus light on the active area of the detectors, are now used to gather light for a 12.5 mm diameter,

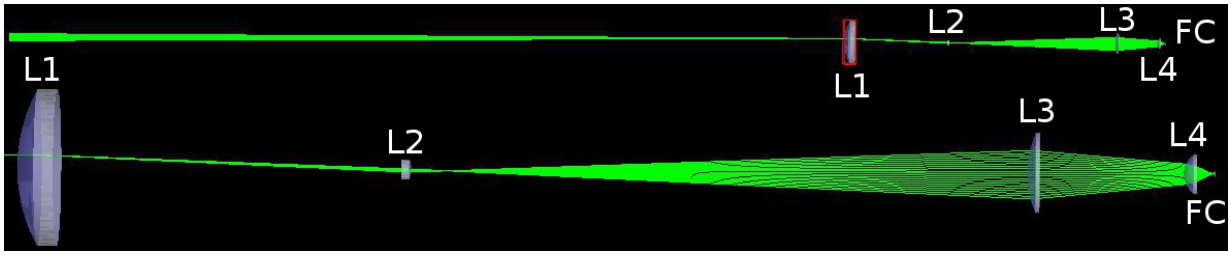

Figure 5.5: Theoretical propagation of the light with pointing mismatch in the modified quantum receiver. The top image includes the source and the bottom image is a zoomed view of the receiver. By improving the receiver design we are able to increase the theoretical field of view by a full order of magnitude. Focal lengths are 100 mm (L1), 11 mm (L2), 60 mm (L3) and 10 mm (L4). The fiber couplers are marked as FC.

10 mm focal length lens (L4). These 10 mm focal length lenses (one in each of the four arms) are used to focus light into 105 μm multimode fibers which carry the light into four fiber coupled detectors. This fiber coupling allows us to increase the field of view, by having a 105 μm core rather than a 50 μm active area, while helping to reduce background counts. The detector system is a fiber coupled 4-channel photon counting card (SPCM-AQ4C) from Excelitas Technologies [83]. These detectors have a 180 μm active area, a detection efficiency of $\approx$48% at 532 nm, and an average dark count rate of 500 cps. While these detectors do have a significantly higher dark count rate, their ability to function with a 105 μm multimode fiber enables an greater field of view of the receiver, reducing the loss from pointing as well as the number of dropouts expected by our system. In addition, the lower losses and higher background counts expected by this demonstration reduces the importance of low dark counts compared to the high loss demonstration.

Figure 5.5 shows the theoretical light propagation in the final version of the quantum receiver. Light from a source, placed 1 m from the input lens, is focused on the input lens and propagated up to the detector active area. The pointing mismatch from the receiver is obtained by having a non-zero width to the source. The rays further from the center of the source are received with pointing errors of $\arcsin(L/d)$, where L is the distance from the center of the source to where the ray originates from, and d is the distance from the source to the input lens. To simulate the pointing mismatch of the transmitter, we translate the focus point of the rays away from the center of the input lens. This creates a transmitter pointing error of $\arcsin(l/d)$, where l is the distance from the center of the input lens where the light is focused. The field of view of the modified quantum receiver was measured to be $\approx$0.4 mrad, or 0.02°, a full order of magnitude greater than the original.

The receiver is mounted in the rear cargo area of a pickup truck (see Figure 5.6). To

help reduce vibrations, we use a suspension system consisting of an inner tube placed under the bottom breadboard, and bungee cords to hold the breadboard down. Four screws are also attached to the optical breadboard to ensure the quantum receiver is secured on the truck. These screws maintain the horizontal position of the receiver while allowing it to freely move vertically by ≈10 cm. Beyond this range the screw head will either be stopped by the wooden base, or the breadboard itself will come in contact with the base. This vertical movement allows the suspension system to stabilize the receiver while providing a "hard stop" should the suspension system break.

5.1.3 Transmitter system

The QKD source used for this experiment is the same as described in Section 3.1.1, except with a different 810 nm pump laser. The titanium sapphire laser used in the original source was not available and a different titanium sapphire laser, with 50 fs pulses (compared to 3 ps in the original titanium sapphire laser), was used instead. The light produced by the source is sent to the transmitter using a single-mode fiber.

Our free-space transmitter (Figure 5.7), which was designed and built during the course of this project, consists of a bare fiber on a five-axis fiber positioner and is collimated to a ≈1 cm beam using a 1-inch diameter, 30 mm focal length lens. A customized chopper wheel (Figure 5.8), where six polarization films have been added, was used to characterize the polarization drift in the fiber from the lab to the transmitter. Each of the six polarization films measure one of 6 polarizations: horizontal, vertical, diagonal, anti-diagonal, right-handed circular and left-handed circular. In addition, some of the closed slots of the chopper have been removed to maximize the light transmitted.

The chopper is followed by at beam splitter reflecting 10% of the input light to a fiber coupler, and a multimode fiber is used to send the light to a single-photon detector (one channel of another SPCM-AQ4C 4-channel photon counting card from Excelitas Technologies [83]). The same automated polarization alignment software described in Section 3.1.5 is used determine the required compensation. The compensation is then implemented using a set of three wave plates (two quarter-wave plates on either sides of a half-wave plate).

Since the chopper wheel is placed in the path of the beam, it will effectively reduce the source frequency by half due to the wheel's duty cycle (half of the slots are either closed or contain a polarizer). This is different from additional loss as the signal-to-noise ratio in the signals from the open slots remain the same as the signal-to-noise ratio if the chopper was not present. A future improvement would be to move the chopper in the reflected path of

Figure 5.6: Photo of the moving receiver platform. The receiver system is mounted on a wooden platform using bungee cords and an inner tube which act as a suspension system to reduce vibrations. The wooden platform is attached to the truck using bungee cords at all four corners, acting as an additional suspension system in the horizontal plane (the weight of the platform, ≈50 kg, and its low center of mass prevent any significant vertical movement relative to the truck bed).

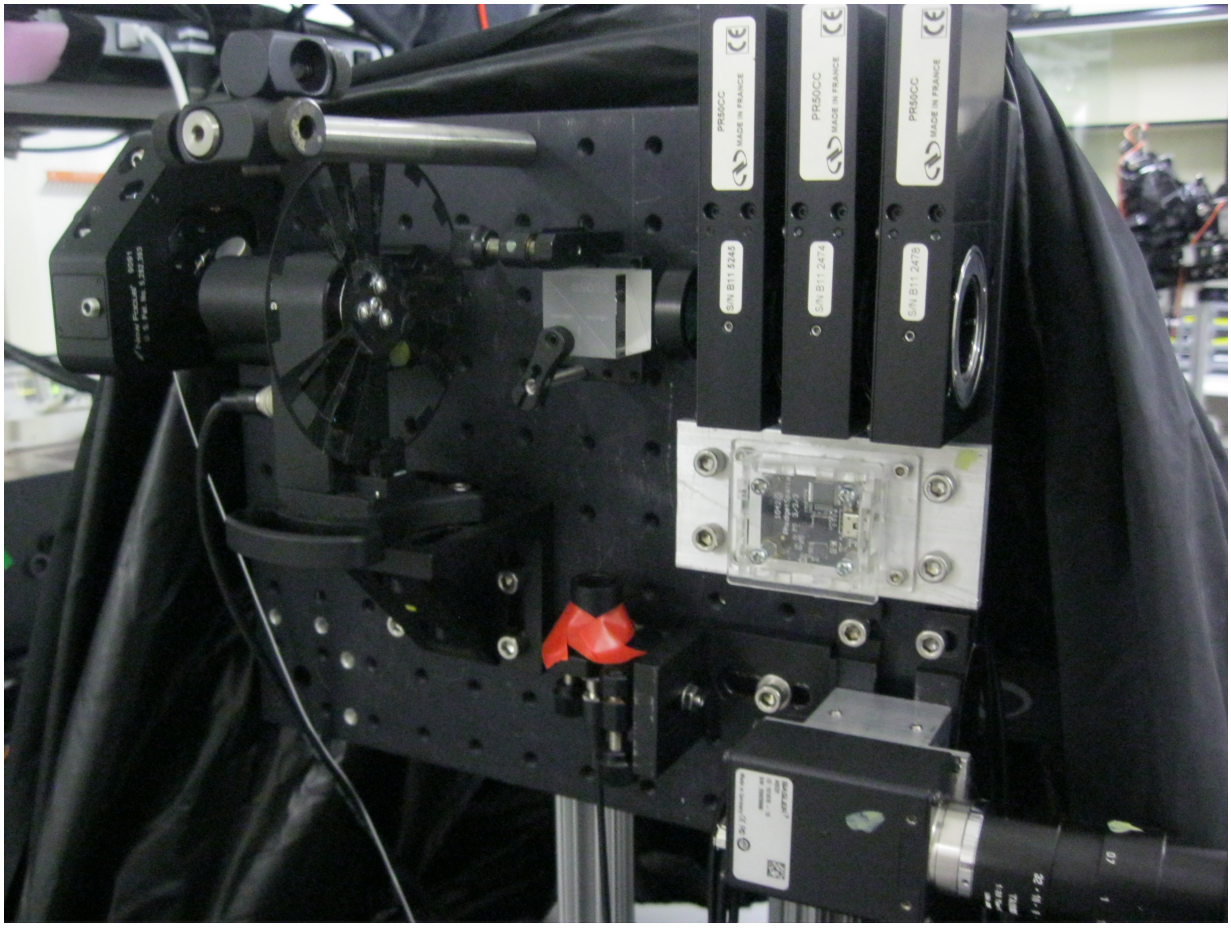

Figure 5.7: Photo of the transmitter. Light coming out of a bare fiber is collimated using a 1-inch, 3 mm lens. A modified chopper wheel is used to characterize the polarization drift and a set of three wave plates is used to compensate the drift.

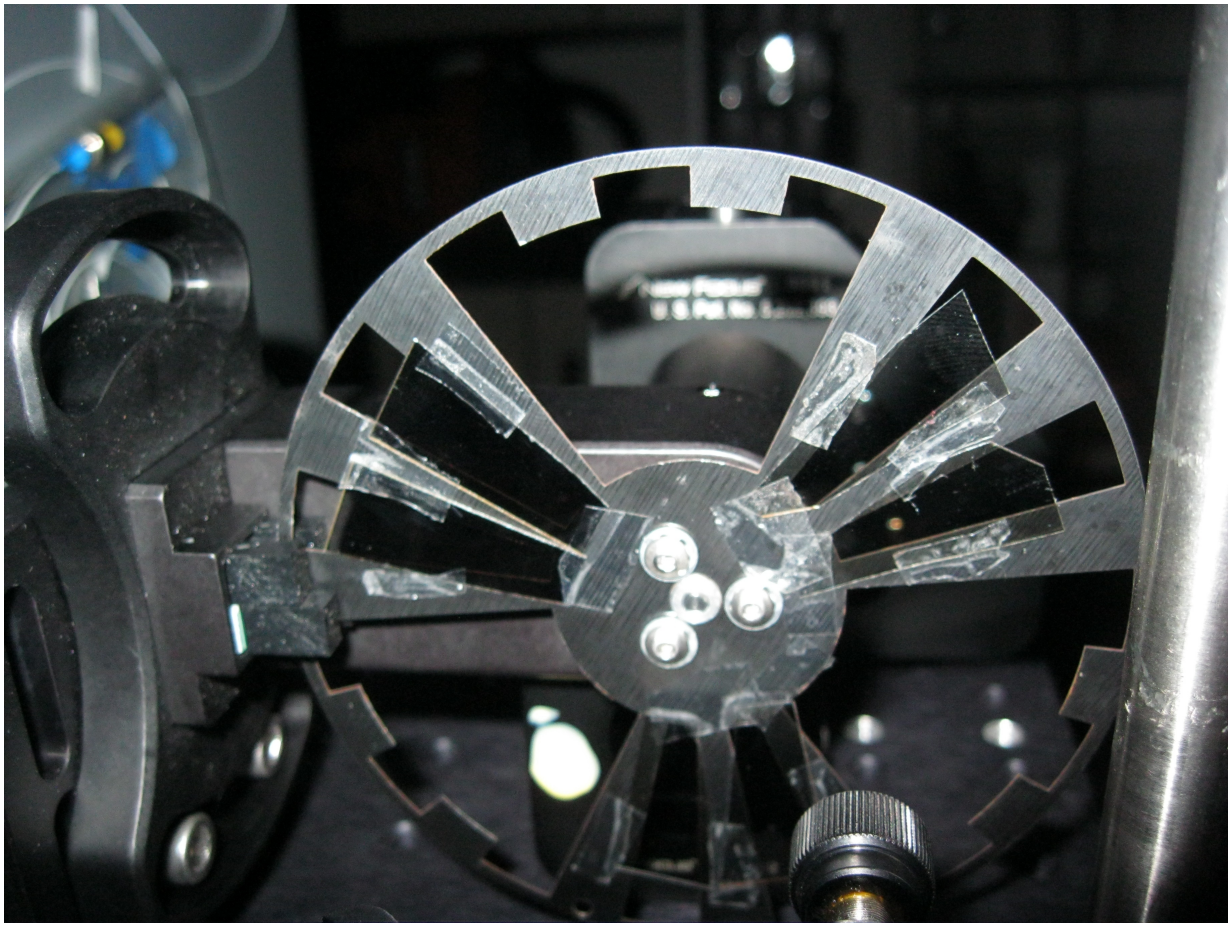

Figure 5.8: Photo of the modified optical chopper wheel. Polarizers have been placed in Six of the open slots for characterization and six closed slots have been removed to maximize the duty cycle, allowing more signals to be transmitted intact. The final duty cycle is 50%, effectively reducing the source frequency by half.

the 10% reflective beam splitter. This would require characterization of the phase change induced by the reflection, an additional complication to the polarization compensation.

The transmitter is mounted on a second set of rotation stages and includes its own set of camera and beacon lasers. The assembly is mounted in a dome on the roof of the University of Waterloo Research Advancement Center 1 (Figure 5.9).

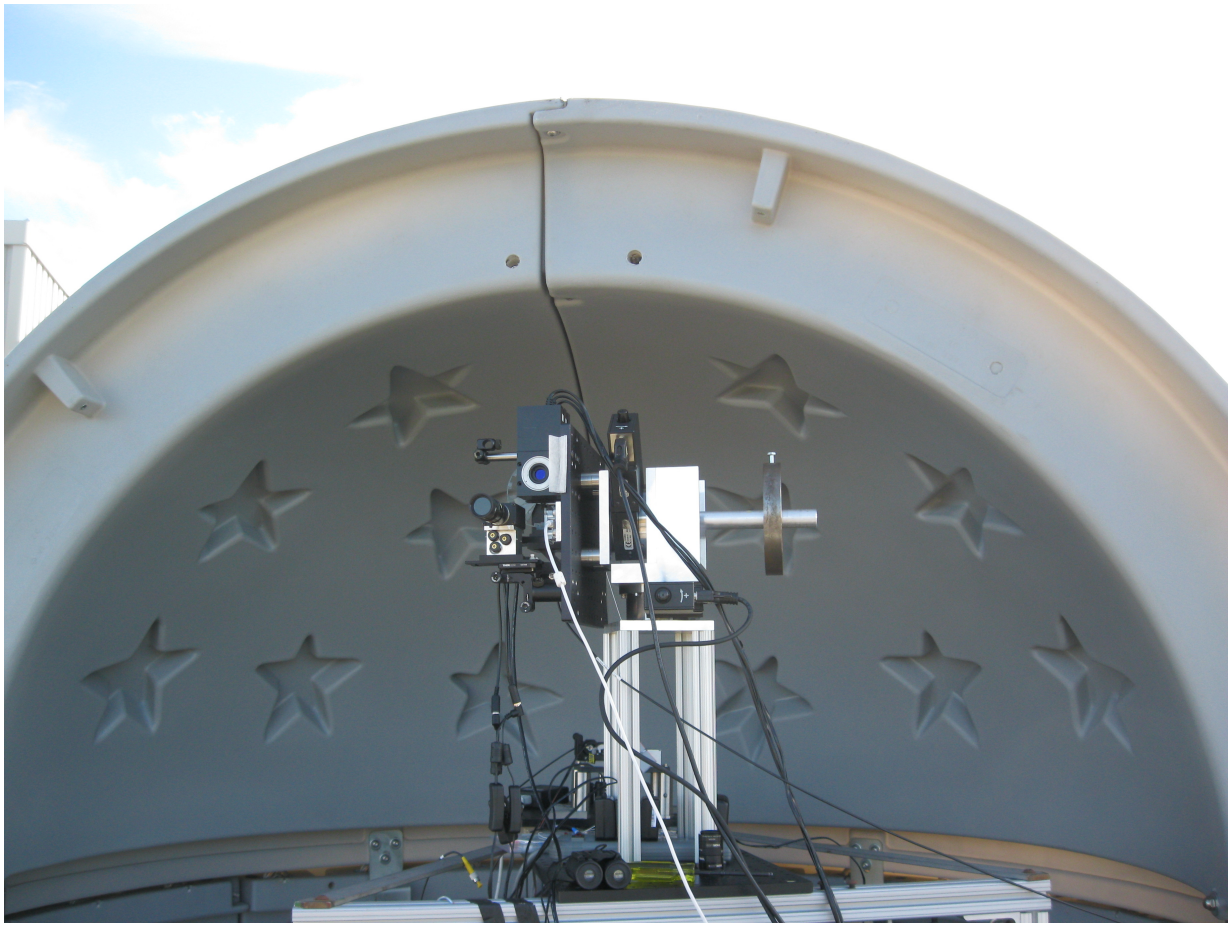

Figure 5.9: Photo of the transmitter station. The transmitter system is mounted on an aluminum frame in an astronomy dome. The frame is not attached to the floor but bags of rocks are used at the bottom of the frame to increase stability and reduce vibrations.

5.2 Experimental conditions

During the experiment, the truck drove along Westmount road, approximately 650 m from the dome at the roof of the Research Advancement Center 1 where the transmitter was located (Figure 5.10). The spot at the receiver (Figure 5.11) was approximately 12 cm in diameter (FWHM). The truck was driven at speeds of ≈20 km/h and ≈30 km/h, leading to theoretical angular speeds of 0.45°/s and 0.68°/s. The measured angular speeds were 0.5°/s and 0.75°/s, suggesting actual speeds of 22 km/h and 33 km/h. In comparison, a LEO satellite will have a maximum angular speed of ≈ 0.7°/s (when near zenith). Therefore the ≈30 km/h test corresponds to the worst case angular speed of a LEO satellite. Both experimental tests where performed during the same night (June 21th 2014) under clear sky and with a measured average temperature of 17.3°C an no measured winds, with the 20 km/h test performed around 2:15 am and the 30 km/h test performed around 2:45 am.

The initial link was established at rest, at the earliest point in the road that allowed a line-of-sight between the transmitter and the receiver. From there, the motors were stopped and the truck was moved to an earlier point in the road (with no line-of-sight to the transmitter). The motors were then turned on and the truck was accelerated from rest to its desired speed while the transmitter was out-of-sight. Since no beacon could be seen during this time, all signals registered by the camera were below the noise level resulting in no motor movement from the pointing. Once a line-of-sight was established, and the beacon acquired by the camera, the pointing system began adjusting the motors and tracking the signal.

The total test duration, including acquisition was approximately 20 s at 20 km/h and 10 s at 30 km/h. For both tests the aquisition time was approximately 5 s. However, the 20 km/s test was less constant than the 30 km/h test, resulting in bigger dropouts of 2–3 s. In contrast, the more stable 30 km/h test had only short sub-second dropouts. As a result, quantum signals were visible for approximately 10 s and 5 s for 20 km/h and 30 km/h respectively.

5.2.1 Analysis of the link loss

Data from an initial static test (used for characterization), where the motors were running but the truck was stationary, yielded an intrinsic total loss of 27 dB (including channel, receiver optics and detector efficiency). Using our link analysis, the estimated size of the beam at the receiver (≈12 cm), and the pointing accuracy or our motors (measured to be ≈ 0.01° during the static test), we calculate a diffraction loss contribution of ≈12 dB and

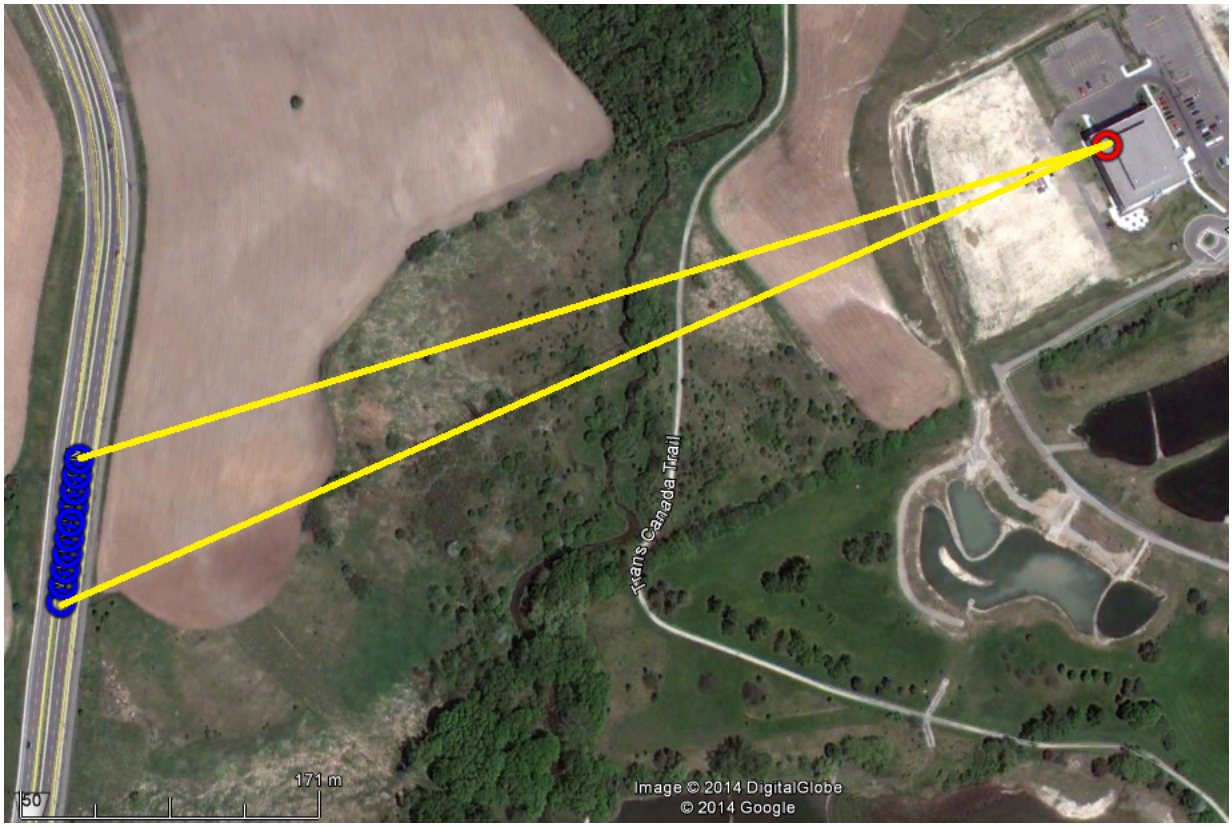

Figure 5.10: Map showing the location of the dome (red) and the part of the road the truck was driven on (blue) during the moving receiver tests. The yellow lines represent the cone in which the line-of-sight was possible. The distance from the dome to the truck is ≈650 m and the length of the road traveled during the test was ≈100 m. This map was generated using Google Earth [214]

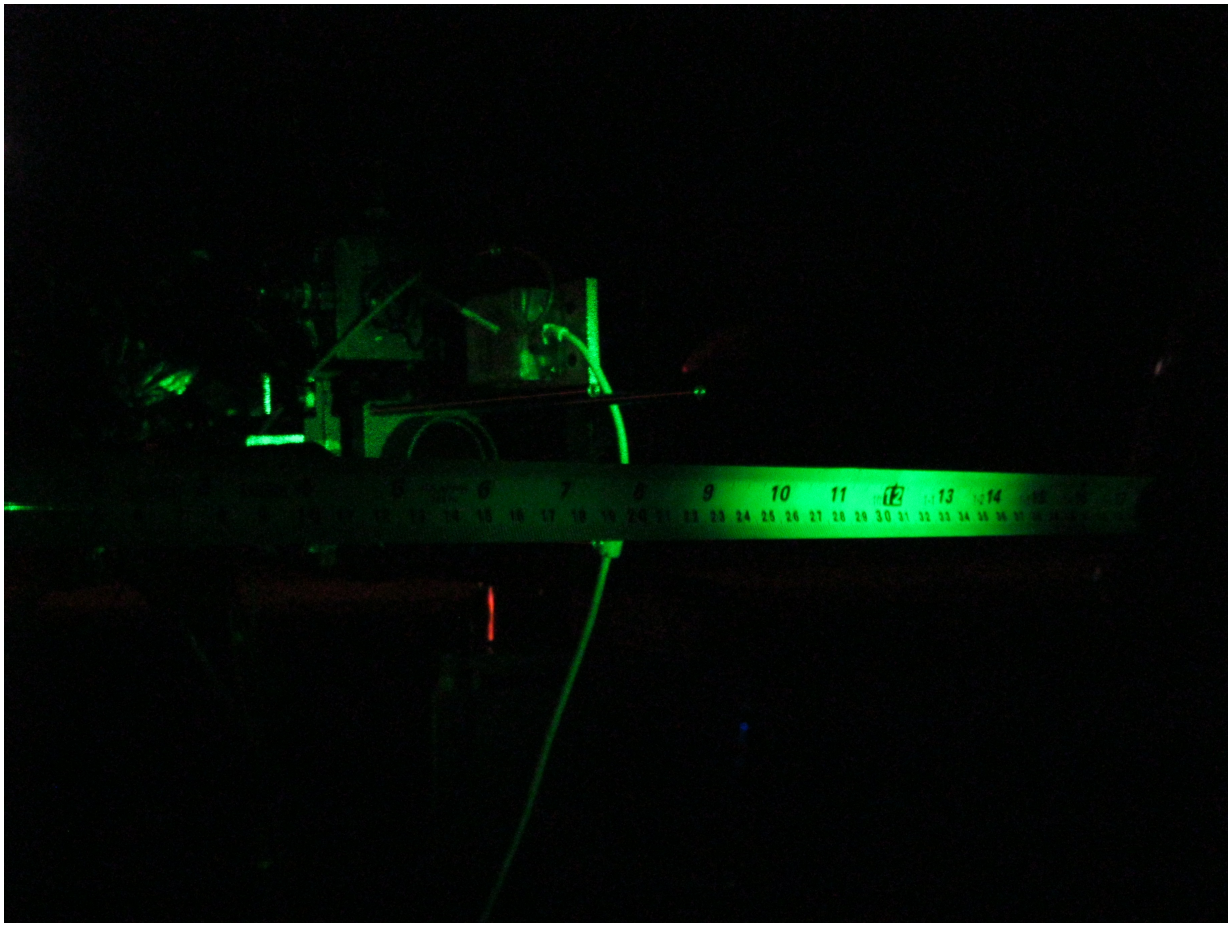

Figure 5.11: Photo of the alignment beam spot at the receiver on Westmount (distance of ≈650m). The spot size was approximately 12 cm in diameter (FWHM), over twice the size of the input lens of the receiver telescope (2-inch)

an additional ≈7 dB of average loss from the average beam broadening due to atmospheric turbulence and transmitter pointing error. The detector efficiency also contribute an additional ≈3 dB. This leaves 5 dB of loss to be attributed to atmospheric transmittance and optical losses in the receiver.

During preliminary tests in the lab, we aligned the transmitter and receiver over a distance of ≈1 m and measured a total loss of ≈5 dB. Over this short distance diffraction and atmospheric turbulence was negligible, leading to a spot size on the receiver of ≈1 cm (same size as the beam at the output of the transmitter). Since this spot size is much smaller than our receiver aperture (1-inch), we will essentially have no geometric losses. In addition, the motors were inactive and the pointing was manually aligned to an accuracy on the order of $< 0.001°$, over an order of magnitude better than our motor's accuracy, and much better than the field of view of the receiver. Therefore, loss from pointing error will also be essentially zero. Finally, atmospheric transmission will also have no significant contribution over such a short distance. Therefore the measured ≈5dB of loss measured can all be attributed to detector efficiency (3 dB) and optical losses in the receiver.

The 2 dB of optical losses measured in the lab can be attributed to two main causes, imperfect coupling efficiency (misalignment) and optical components (including reflectivity, absorption, etc.). The optical components contribution comes from reflectivity of the optics (typically around 0.5% per optical components, giving a total of ≈4%), the imperfect transmission of the filters (totaling a loss of ≈7%), a 5% loss at the pentaprism beam-splitter (due to the third port containing 5% of the input light), and reflectivity of the detector window (measured to be 2.5%). This leads to a total transmission of ≈82%, roughly 0.8 dB of loss.

The coupling losses come from coupling from free-space into the multimode fibers and from the coupling efficiency of the multi-mode fibers to the detectors. This coupling efficiency in the fiber is determined by the spacial overlap on the input beam on the fiber core, while the coupling efficiency to the detector is determined by the overlap of the beam at the output of the fiber with the detector active area. By replacing the multimode fiber with a single-mode fiber and adjusting the position of the fiber in the receiver, we were able to measure the the spot size hitting the fiber core to be on the order of 25 μm. This would allow a coupling efficiency near unity (assuming a Gaussian beam distribution). This suggest the other 1 dB of loss to be attributed to the coupling efficiency of the fiber to the detectors (≈80% coupling).

In the 650 m test, additional optical losses would be incurred due to reduced coupling efficiency into the multimode fibers, due to the lower pointing accuracy causing the beam to be off-center compared to the fiber core, aberration of the beam at the edge of the lenses,

and other imperfections in the optics. The field of view of the receiver was measured to be 0.02°, which corresponds to a drop in power of one standard deviation (60% in one dimension, 37% in two dimension). At a deviation of 0.01° (our pointing accuracy), the power would drop to 88% for each dimensions, totaling 78% (1.1 dB). We note that this is just a rough calculation to estimate the coupling efficiency in order to determine if the losses measured are reasonable. This rough method should not be considered exact.

The total loss due to atmospheric turbulence and optical losses at 650 m was measured to be ≈5 dB. Using the lab measurement we can account for 2 dB caused by optical losses. The previous rough calculation of the extra coupling loss due to pointing error of the receiver allows us to account for an additional 1 dB. This leaves only ≈2 dB of loss which would be caused by atmospheric transmittance, aberration of the beam at the edge of the lenses and other imperfections in the optics.

The predicted atmospheric transmission losses after 650 m for a rural (5 km visibility) sea-level rural atmosphere, modeled using MODTRAN [80], is 1.5 dB, leaving 0.5 dB to be attributed to aberration of the beam at the edge of the lenses and other imperfections in the optics.

While the truck was moving, we measured an additional 11 dB of loss on average, increasing our total average loss to 38 dB. This extra loss was caused by the additional vibrations of the receiver while the truck was moving, which effectively reduced pointing accuracy of the receiver to a measured value of ≈0.04°. Applying our previous rough analysis of the coupling efficiency drop due to pointing error leads to a power drop to 13% in each dimension, totaling 2% in both dimensions (17 dB). Since the initial drop in the static test was 1.1 dB, this rough calculation predicts additional coupling efficiency loss of 15.9 dB compared to the static test, sufficient to explain the measured 11 dB of additional loss. The various loss contributions are summarized in Table 5.1.

Based on this loss, and the results of the high loss demonstration (Chapter 3, where we demonstrated QKD at up to 56 dB in the asymptotic limit), our system should be able to perform QKD at up to an additional 18 dB of loss. If we where to increase the distance without changing any part of the system, the extra losses would be due to geometric losses (quadratic scaling when the beam waist is already much larger than the receiving telescope) and atmospheric transmittance (exponential scaling), giving an additional transmission loss of

$$-10\log_{10}((\frac{650}{x})^2) + 1.5\frac{x-650}{650}, \tag{5.1}$$

where x is the new distance in meters. For an additional loss of 18 dB, the distance would be $x \approx 2865$ m. At this distance, the total geometric loss would be 31.9 dB and the

Table 5.1: Summary of the loss contributions during a static and a moving test. Losses from coupling efficiency was measured in the lab and and lens aberration and imperfect optics are based on the measurement in the static test. All other values are theoretical predicted using our link analysis and the specifications of the components. The total theoretical loss shows that the measured losses are reasonable. The lower measured loss in the moving test can be explained by the inaccuracy in the calculation of the loss contribution from the receiver pointing error.

Loss contributor	**Loss in the static test [dB]**	**Loss in the moving test [dB]**
Diffraction	12	12
Turbulence and transmitter pointing	19	19
Total Geometric	19	19
Receiver pointing	1	17
Atmospheric transmission	1.5	1.5
Lens aberration and imperfect optics	0.5	0.5
Optical losses	1	1
Coupling efficiency to the detector	1	1
Detector efficiency	3	3
Total	27	43
Measured	27	38

atmospheric transmission would be 6.6 dB. Our system should therefore have a maximum operable distance of around 2.9 km, limited mainly by geometric effects. We note that the increased detector dark counts (≈500 cps instead of ≈10cps), as well as the increased background counts, further limit the maximum loss tolerable by our system. Since the total background and dark counts are ≈10 times greater than in the high loss demonstration, the signal must also be ≈10 times greater to maintain the signal to noise ratio. This reduces the maximum loss tolerable by our system to 46 dB (assuming the same intrinsic QBER as the high loss demonstration), giving a maximum distance of around 1.35 km.

5.3 Results of the moving receiver demonstration

5.3.1 Performance of the pointing system

In both the 20 km/h and 30 km/h tests the truck accelerated to the desired speed before the beacon was acquired by the camera. Once the beacon was acquired the pointing system began tracking the link. In both cases the beacon was first acquired by the receiver camera. Once the pointing system aligned the receiver, the transmitter camera also acquired the receiver's beacon and, allowing for the link to be established.

The reason the transmitter acquired the beacon laser later is because the precise heading of the truck (and thus the precise direction the receiver was pointing towards) was hard to replicate. Therefore, when the truck passed its initial calibration position (where the link was initially established while the truck was static), the receiver's beacon would point in a different position than it was during the calibration and miss the transmitter. In contrast, the transmitter remained static, thus maintaining a constant pointing direction and allowing its beacon to still hit the receiver as it passed. Once the receiver acquired the transmitter's beacon and aligned to it, its beacon once again became visible at the transmitter.

Pointing during the 20 km/h moving receiver test

In our first test the truck was driven at ≈20 km/h. The beacon spot deviation during the test is shown in Figure 5.12. During the first 3 s of the test, only the receiver's camera had acquired a beacon signal. Once the transmitter's camera also acquired beacon signal the spot deviation stabilized. After ≈6 s, the spot stabilized to an average deviation of 0.005° in the transmitter camera (Alice) and 0.04° in the receiver camera (Bob).

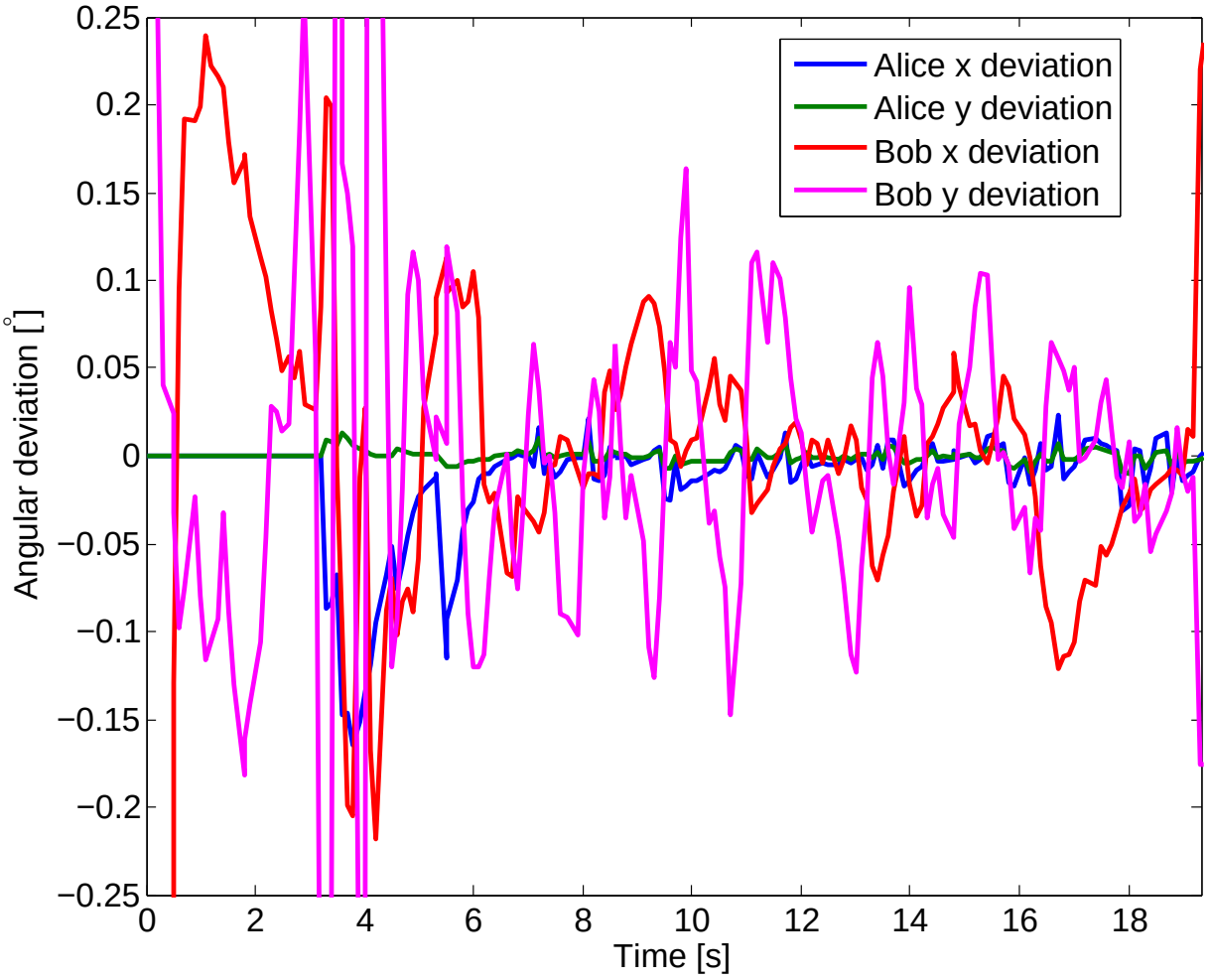

Figure 5.12: Beacon angular deviation measured by the camera during the 20 km/h test. The receiver (Bob) shows an increased variation compared to the transmitter (Alice) which is caused by additional jitter from the truck. The increased deviation in the x-axis (along the direction of motion of the truck) suggest that the speed of the truck was not constant, causing additional pointing error.

The lower accuracy of the receiver can be attributed to vibrations at the receiver while the truck was moving, causing additional jitter in the pointing direction of the receiver. Since the position of the spot in the camera depends on the origin position of the beacon relative to the pointing direction of the camera, the change in pointing direction of the receiver due to jitter would directly affect the deviation of the spot on the receiver camera. At the transmitter, the change in pointing direction of the receiver would only slightly change the origin of the beacon, resulting in negligible deviation. The transmitter is also affected by jitter from the aluminum frame (as it dissipates the angular momentum created by the motors), however this jitter is much smaller than those caused by the truck, allowing a more accurate pointing. We note that if the transmitter and receiver where swapped, with the transmitter on the truck, the transmitter pointing would be reduced in the same way as with the receiver. This would result in worst performance as the reduced transmitter pointing would reduce the likelihood of the beam spot hitting the receiver, causing more drop outs. In contrast, a lower pointing accuracy at the receiver causes lower efficiency coupling, which increases loss, but rarely complete drop outs.

At both the transmitter and the receiver, the deviation was significantly worse in the x-axis (along the direction of motion of the truck) compared to the y-axis (orthogonal to the direction of motion). This is not due to the increased speed along the y-axis but rather to the difficulty in maintaining a constant speed while driving. Our pointing system calculates the average speed and implements it along with a correction factor, therefore it should not be negatively affected by a faster constant speed. A non-constant speed would however cause additional pointing error. In addition, the aluminum frame at the dome will induce more jitter in the horizontal plane compared to the vertical plane (the frame, which is not secured to the floor, is light enough to experience small sways from side-to-side but will not move vertically). Therefore the frame will induce more jitter in the x-axis compared to the y-axis when dissipating the angular momentum created by the motors.

Figure 5.13 shows the speed of the motors during the test. Once again the transmitter's camera only acquire the beacon 3 s after the initial acquisition by the receiver. After stabilization (at ≈6 s), the motors settle to a more constant angular speed to match the angular speed of the truck. This is best seen at the transmitter (Alice) where the motors settle to an angular speed of 0.53°/s in the x-axis and 0.008°/s in the y-axis.

At the receiver (Bob), the angular speed averaged 0.50°/s in the x-axis and 0.018°/s in the y-axis. The angular speed at the receiver has more variations than the angular speed at the transmitter because of the additional jitter of the truck. The average x-axis angular speed is slightly lower than the average at the transmitter because it only included the

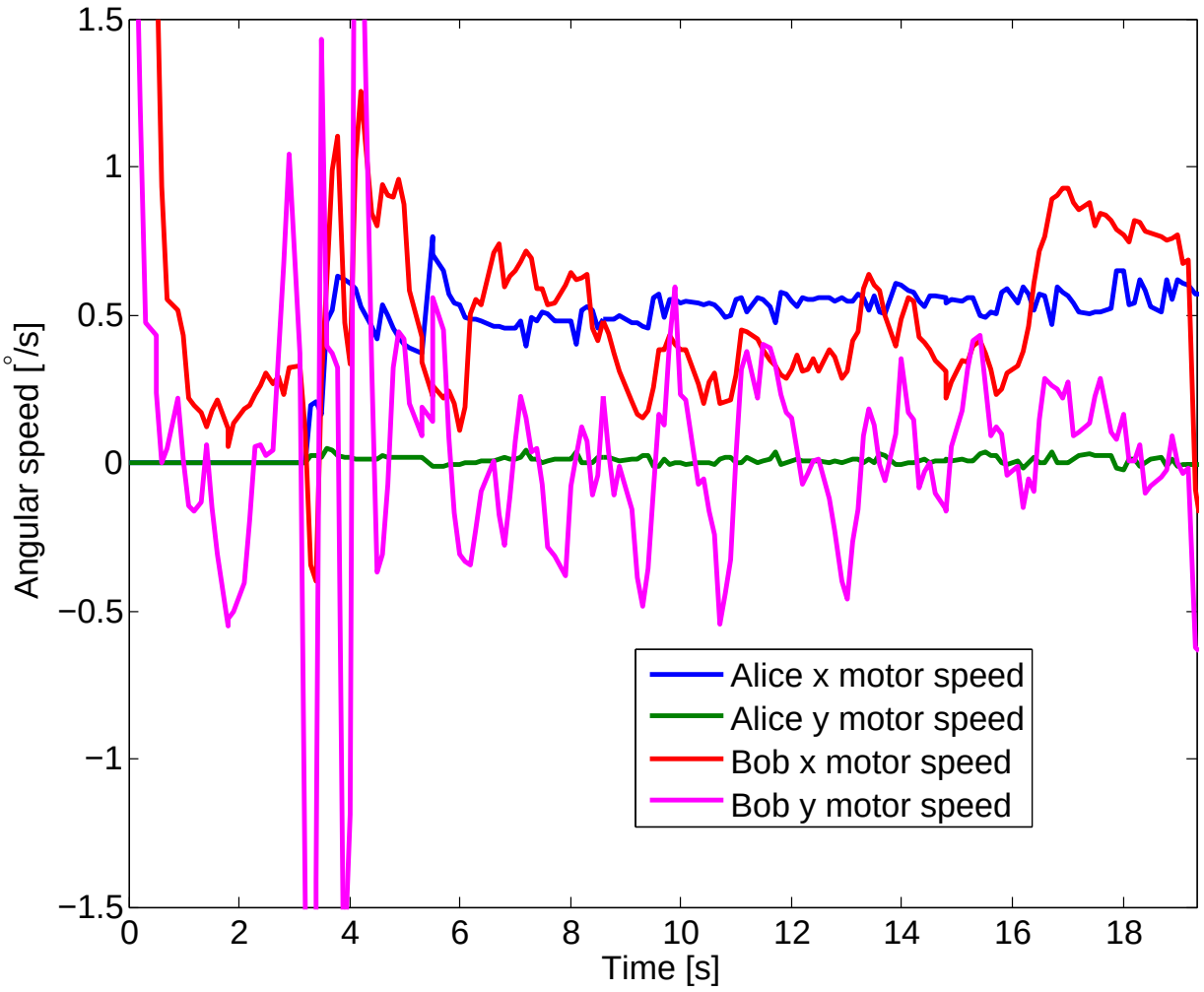

Figure 5.13: Angular speed of the motors during the 20 km/h test. As was the case for the spot deviation, the motor speeds at the transmitter (Alice) show less variation than the motor speed at the receiver (Bob) due the the latter being negatively impacted by the extra jitter of the truck. The x-axis angular speed at the receiver slowly increases during the test, showing that the truck was accelerating.

speed when the link was acquired (from ≈6 s to ≈19 s), thereby ignoring the region of higher angular speed at 4–6 s that occurred before the link acquisition.

The x-axis angular speed at the transmitter shows a clear increase during the test, from 0.45°/s at 7 s to 0.62°/s at 19 s. This is due to the increasing speed of truck, which was measured by the GPS receiver (Figure 5.14). This change in speed of the truck is what caused the additional pointing error in the x-axis seen in Figure 5.12. The GPS receiver also measured the heading of the truck, showing an average heading of ≈ 9° E of N with small variation of ≈ 5° over the course of the test.

The measured angular speed of 0.53°/s corresponds to the angular speed of a 600 km altitude LEO satellite at 60° of elevation from the horizon, with the range 0.45–0.62°/s corresponding to 55–70° from the horizon. From Section 2.1 (specifically Figure 2.2), over 75% of passes never reach an elevation angle above 55°. Only approximately 11% of passes ever reach an elevation angle above 70° from the horizon. Therefore the 20 km/h test is sufficient to represent the angular speed of almost 90% of passes.

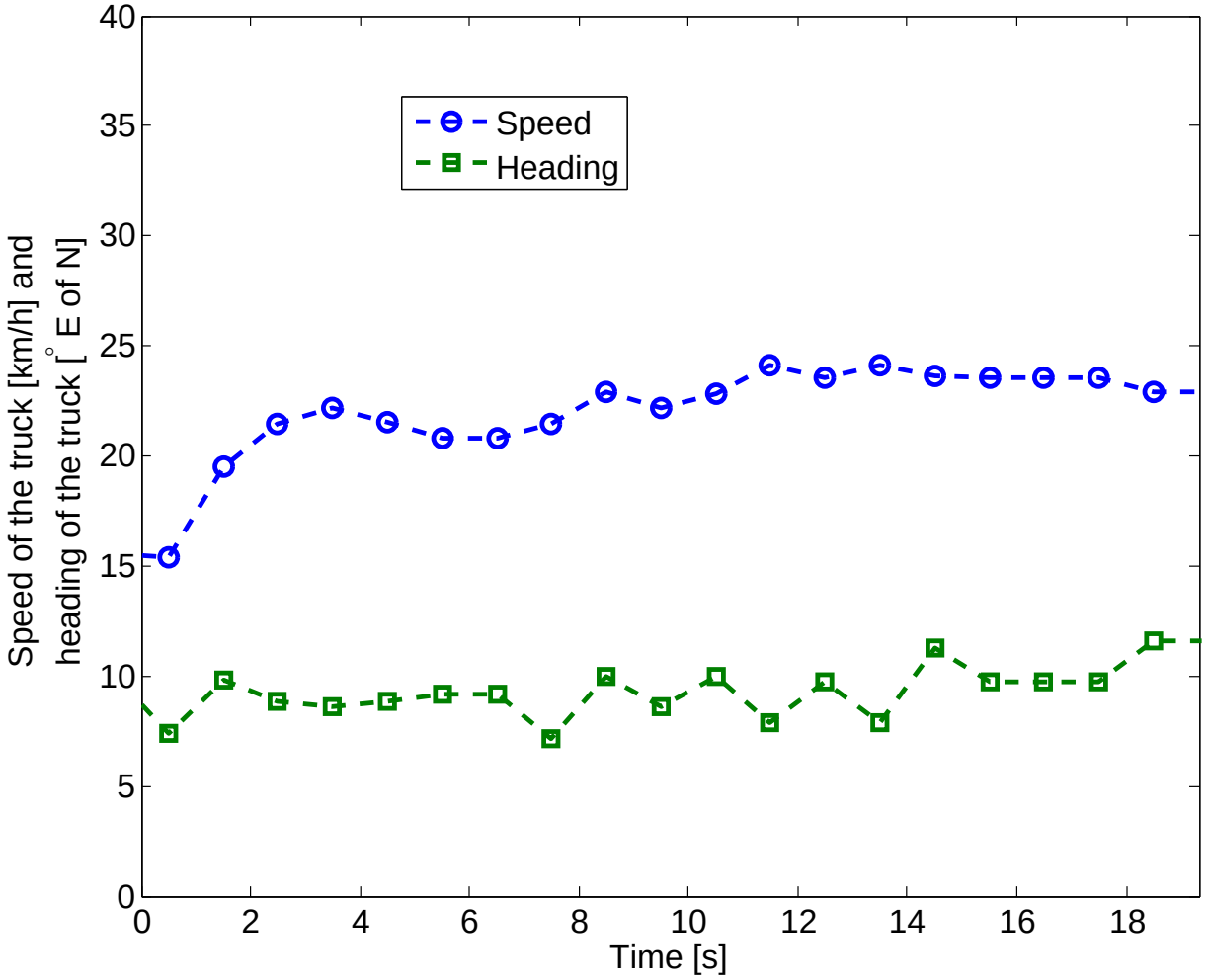

Figure 5.14: Speed, in km/h, and heading, in degree East (E) of North (N), of the truck measured by the GPS during the 20 km/h test. The measured speed increases during the test, showing that the increase in the angular speed of the transmitter motor was due to increased speed of the truck. The heading of the truck varied between 7° and 12° E of N and averaged $\approx 9°$ E of N.

Pointing during the 30 km/h moving receiver test

For the second test, the truck was driven at ≈30 km/h to better represent the maximum angular of a LEO satellite (0.7°/s when near zenith). Figure 5.15 shows the beacon spot deviation during the test. Once again the receiver's camera was the first to acquire a beacon signal. However, the transmitter's camera acquired its signal sooner (around 1.5 s) compared to the 20 km/h test (3 s), allowing for an earlier stabilization (after 3.5 s). The stabilization time was also shorter (2 s instead of 3 s). This difference in acquisition time may be the result of a more stable link (suggesting a more constant speed) and the random nature of the jitter from the truck (which may have moved the beacon towards the transmitter sooner).

The average deviation during the test (from ≈3.5 s to ≈9 s) was 0.005° in the transmitter camera (Alice) and 0.06° in the receiver camera (Bob). Comparing with the 20 km/h test (Figure 5.13), one can see that the amplitude of the deviations at the receiver increased due to the higher speed of the truck, causing higher amplitude jitter and thus higher average deviation. The deviation at the transmitter, for which the effect of the jitter from the truck is negligible, did not change significantly compared to the 20 km/h test.

Another difference between the two tests is that the deviation at the receiver is similar in both axis (both averaging to 0.06°). This suggests the speed of the truck was almost constant during the test. In contrast, the x-axis deviation the transmitter still showed a significantly greater deviation than the y-axis (averaging 0.007° compared to 0.003°). This extra deviation is caused by the jitter in the aluminum frame which can sway from side-to-side but not move up and down, creating more jitter in the x-axis. As stated previously, this jitter is caused by the angular momentum created by the motor which is dissipated by the frame.

The angular speed of the motors is shown in figure 5.16. Once the beacon was acquired by the transmitter, at around 1.5 s, the angular speed quickly settled to an average angular speed of 0.75°/s in the x-axis and 0.012°/s in the y-axis. The receiver averaged angular speeds of 0.7°/s in the x-axis and 0.013°/s in the y-axis. Once again, the extra variation in the receiver is due to the jitter from the truck, and the average angular speed in the x-axis is lowered because the average ignores the higher angular speed of the motor before the test fully stabilized (at ≈3.5 s).

The x-axis angular speed at the transmitter shows an almost constant speed during the test. Upon closer inspection one can find that the speed was still increasing, but at a much slower rate than the 20 km/h test. The angular speed increase of the 30 km/h was ≈ 0.03°/s (compared to ≈ 0.17°/s during the 20 km/h test). The speed measured by the

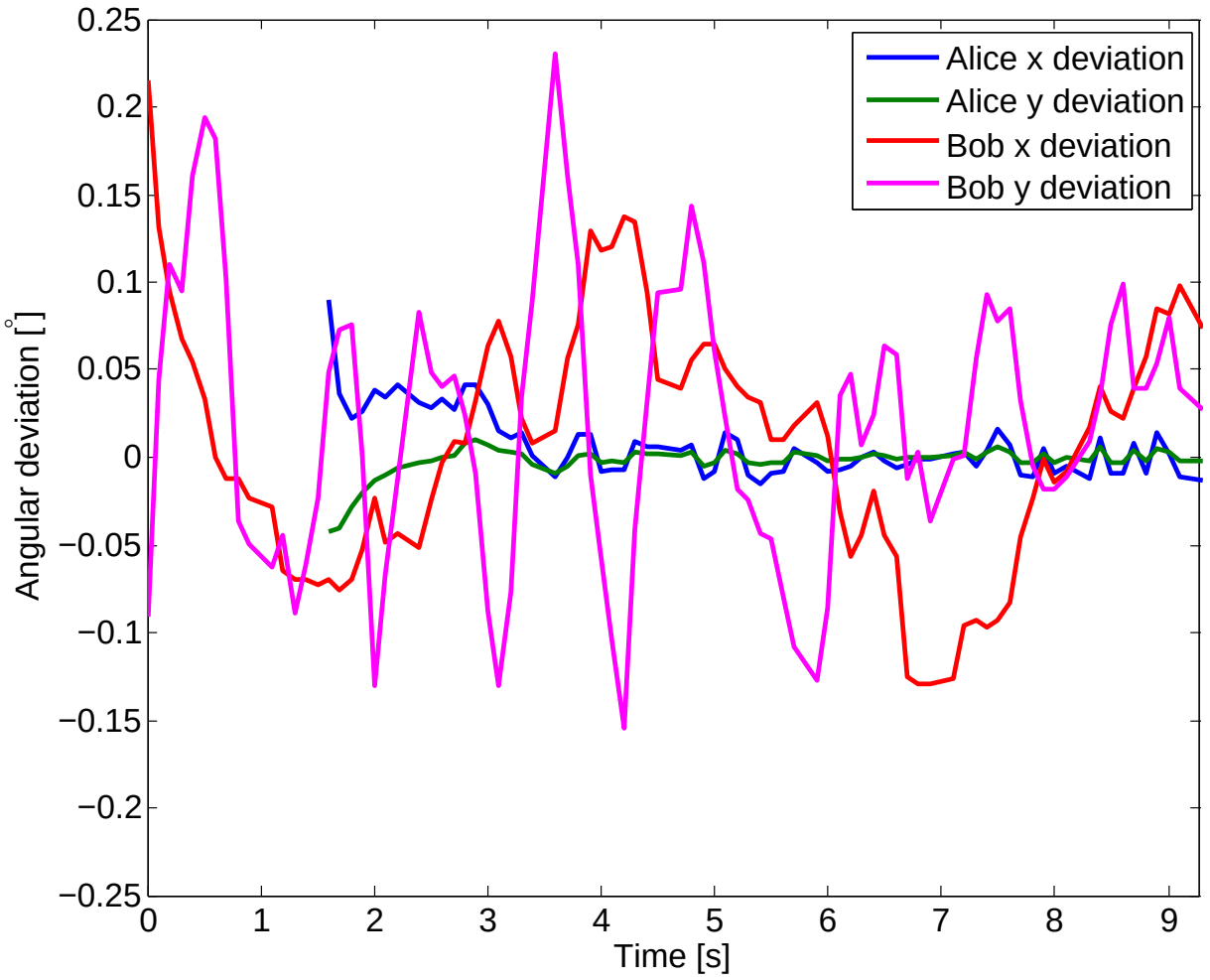

Figure 5.15: Beacon angular deviation measured by the camera during the 30 km/h test. Once again the increase in variation at the receiver (Bob) can be attributed to the jitter produced by the truck. The average deviation in the x-axis at the receiver is the same as the average deviation in the y-axis, suggesting a more constant angular speed. The transmitter (Alice) however still show increased deviation in the x-axis, caused by the jitter in the frame, since it can more easily move in the horizontal plane compared to the vertical plane.

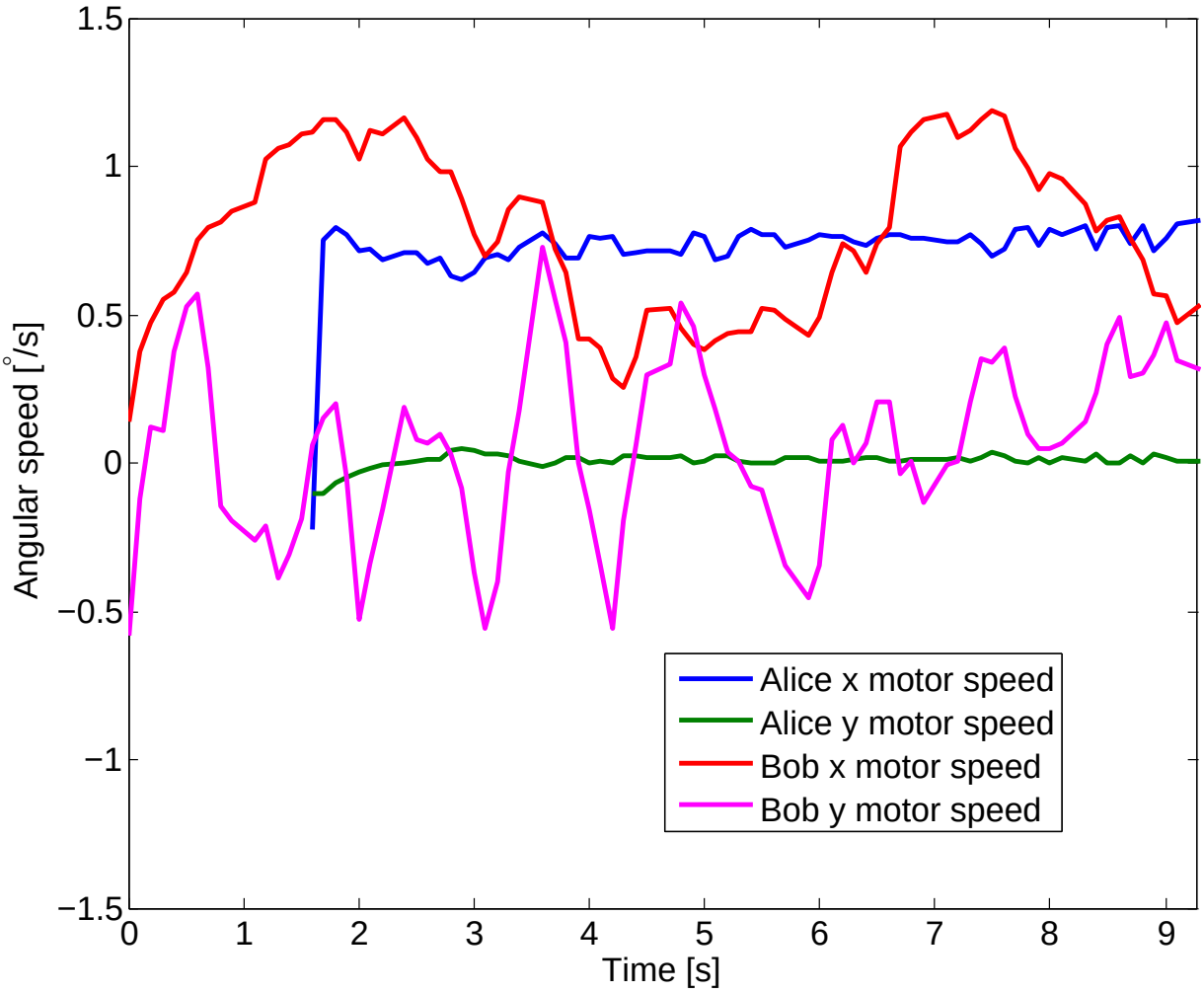

Figure 5.16: Angular speed of the motors during the 30 km/h test. The higher variation at the receiver (Bob) is again due to the jitter of the truck. Unlike the 20 km/h test, the x-axis angular speed at the transmitter (Alice) shows a more constant speed with only a small increase of $\approx 0.03°/s$ during the test.

GPS receiver (Figure 5.17) also showed a very constant speed with a small increase. This more constant speed is reflected in the beacon spot deviation at the receiver (Figure 5.15) which showed no significant difference between its x-axis deviation (along the direction of motion of the truck) and its y-axis deviation (orthogonal to the direction of motion). Once again, the heading of the truck had only a small variation ($\approx 3°$), with an average heading of $\approx 10°$ E of N.

The measured angular speed of $0.75°/s$ is greater than the maximum angular speed of a 600 km altitude LEO satellite ($\approx 0.7°/s$ at zenith). The 30 km/h test thus represents a pointing and tracking situation that is worst than any part of a LEO satellite pass.

5.3.2 Performance of the polarization compensation system

Before being transmitted by our receiver telescope, the quantum signal, which originates in our lab on the first floor of the Research advancement center 1, must travel trough ≈70 m of fiber. This fiber will introduce a unitary change, based on the thermal and physical stress along the fiber, which will cause a misalignment of the polarization states. In addition, the fiber connecting to the transmitter is exposed to the outside environment and will move as the transmitter is rotated, causing the unitary to change during the tests. These change to the polarization states are compensated using a polarization characterization and compensation system where the measurement is performed using a chopper wheel and the compensation is implemented using a set of three wave plates.

Lab demonstration of the polarization compensation system

Using the polarization characterization we can monitor the polarization states after traveling through the fiber and estimate the quality of the polarization states after the compensation. During initial test in the lab (Figure 5.18), the polarization compensation system was shown to be capable of compensating random polarization change in ≈3–5 s. The polarization change was simulated by randomly moving a fiber-based polarization controller.

Since the update period of the polarization compensation system is only 1 Hz, 3–5 s corresponds to only 3–5 steps. This however is not the speed limit of the polarization compensation system. The speed of the compensation is determined by a cost factor that limits how far the wave plates will move. This cost factor is a user given value of the relative weight of the movement distance of the wave plates (in degree) compared to the expected gain in polarization visibility. A high cost factor will reduce the speed of the compensation, leading to more stable yet potentially less optimal polarization compensation. If the

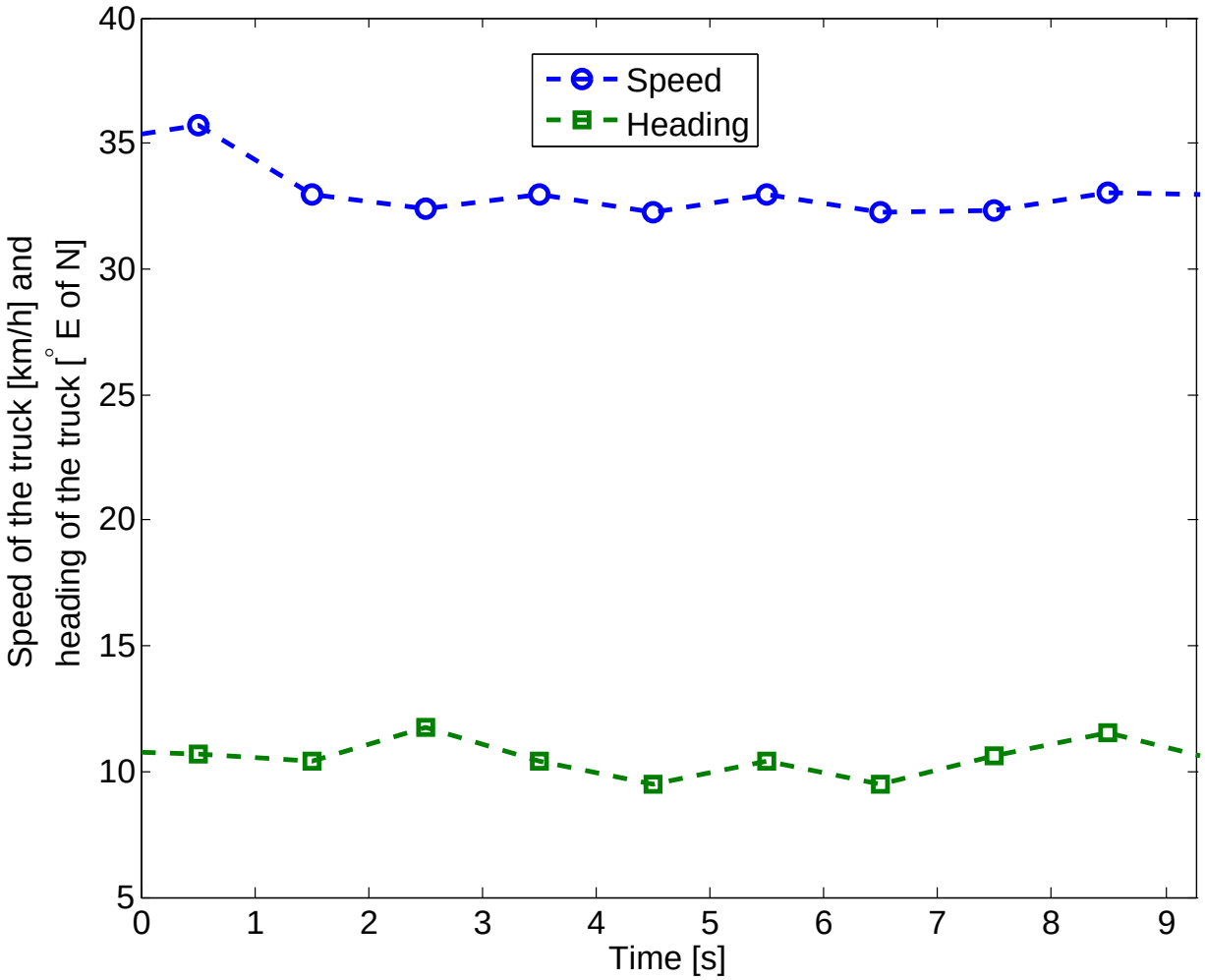

Figure 5.17: Speed, in km/h, and heading, in degree East (E) of North (N), of the truck measured by the GPS during the 30 km/h test. The measured speed was vary stable during the test, with a slightly higher speed at the beginning, before the link acquisition. The heading of the truck varied between 9° and 12° E of N and averaged $\approx 10°$ E of N.

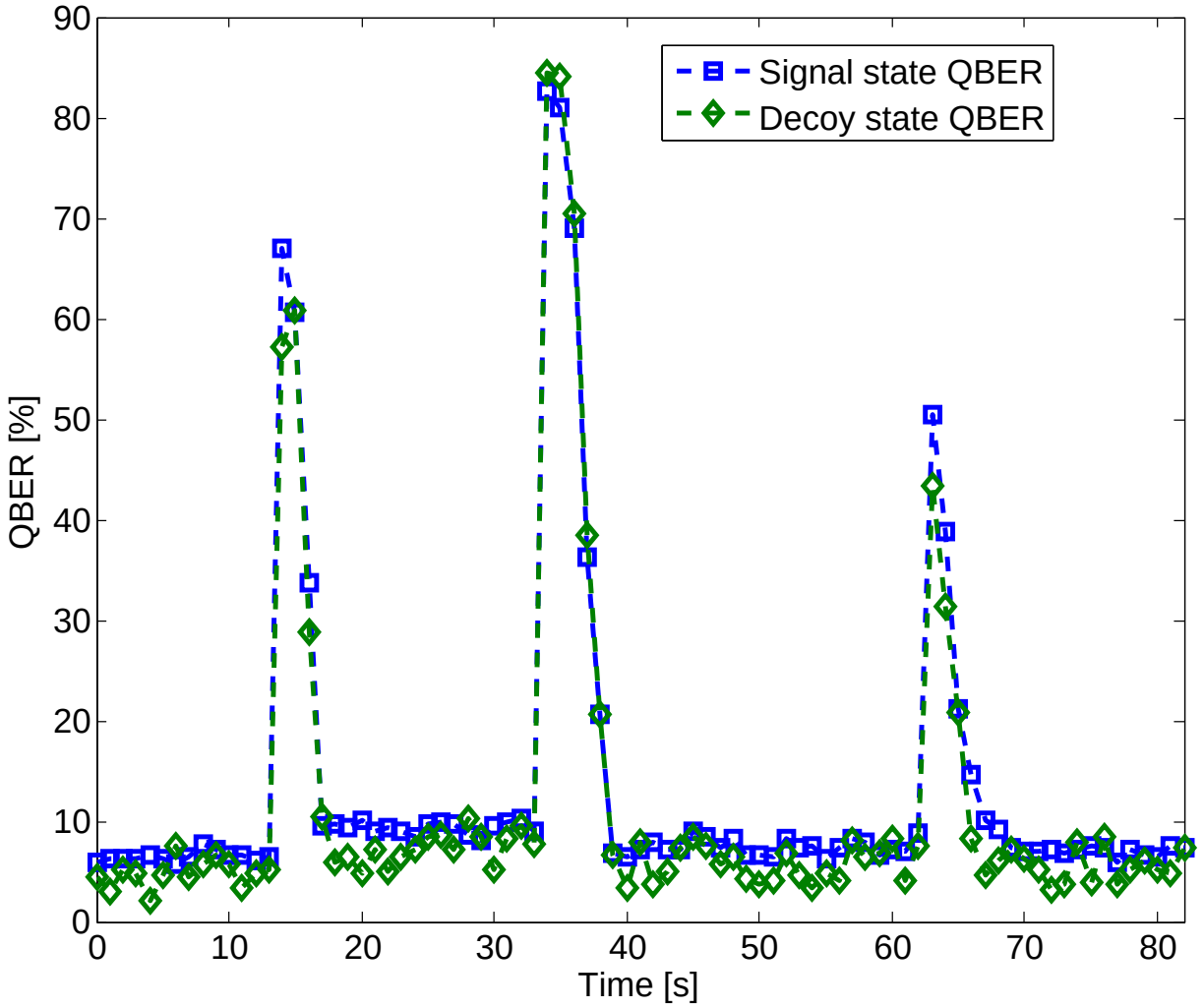

Figure 5.18: Measured post compensation QBER in the lab. The change in polarization was produced by randomly moving a fiber-based polarization controller. After the change, the polarization compensation system requires only ≈3–5 s to compensates the change. The minimum QBER value is limited by the source.

cost factor is too high may lead to a slower polarization compensation than the drift it's trying to compensate, resulting (over time) in a drop in the visibility of the compensated polarization. However a cost factor too low will cause high instantaneous movement of the wave plates which will reduce the stability of the polarization at the output. In extreme cases the new wave plate setting may be further than the per second speed of the wave plate's rotation stage (20°/s), reducing the update of the polarization compensation as it waits for the motion to finish. Lower cost factors (which could compensate the polarization change faster than 3–5 s) had visibly lower stability when there were no polarization drift.

In the moving tests, the polarization drift is expected to be slow, and therefore is not well represented by a large instantaneous change. The cost factor that produced the lab result of 3–5 s compensation was chosen because it allowed for a reasonably fast compensation without significant impact on the stability when there were no polarization drift.

Performance of the polarization compensation system during the tests

Because the characterization is performed using the same timing analysis as the QKD software, where the proper peak is chosen based on its QBER, an initial rough alignment had to be performed manually using fiber-based polarization controller located in the lab. This alignment allowed us to achieve an initial QBER at the transmitter of ≈10%. This alignment is insufficient to properly perform QKD yet it is sufficient to ensure the proper peaks will be easily discernible by the software compared to the the other peaks which only have random correlations with the expected states (averaging 50% QBER). From there the polarization compensation can return the state to its original polarization produced in the lab.

The QBER measured at the transmitter before compensation and the predicted QBER after compensation are shown in Figure 5.19 for the 20 km/h test, and in Figure 5.20 for the 30 km/h test. In both tests, the pre-compensation QBER was measured around 10–12% and the post-compensation QBER was predicted to be around 6–7%. The pre-compensation QBER also shows an increase during the tests (more so in the 30 km/h test), while the post compensation QBER is, on average, constant.

In both tests, the pre-compensation and post-compensation QBER show a correlated variation on the order of 2%. This correlation is mainly due to variation in purity of the polarization states at the source. In addition, noise from background and dark counts will also result in variation of the measured an predicted QBER.

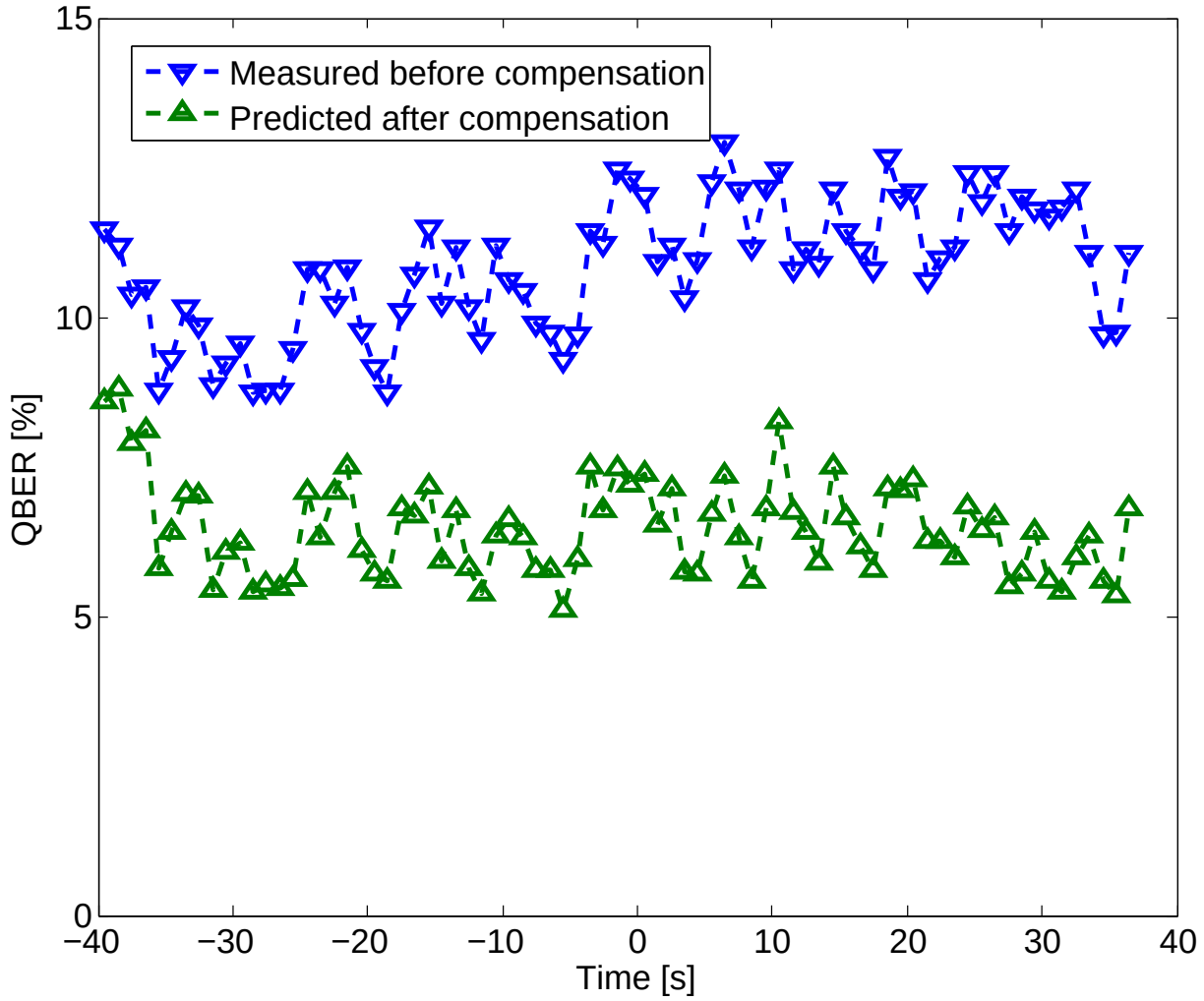

Figure 5.19: Measured pre-compensation and predicted post-compensation QBER at the transmitter during the 20 km/h test. The polarization compensation system corrects the unitary induced by the fiber and returns the polarization states to its intrinsic QBER of ≈6–7% (limited by the quality of the source in the lab).

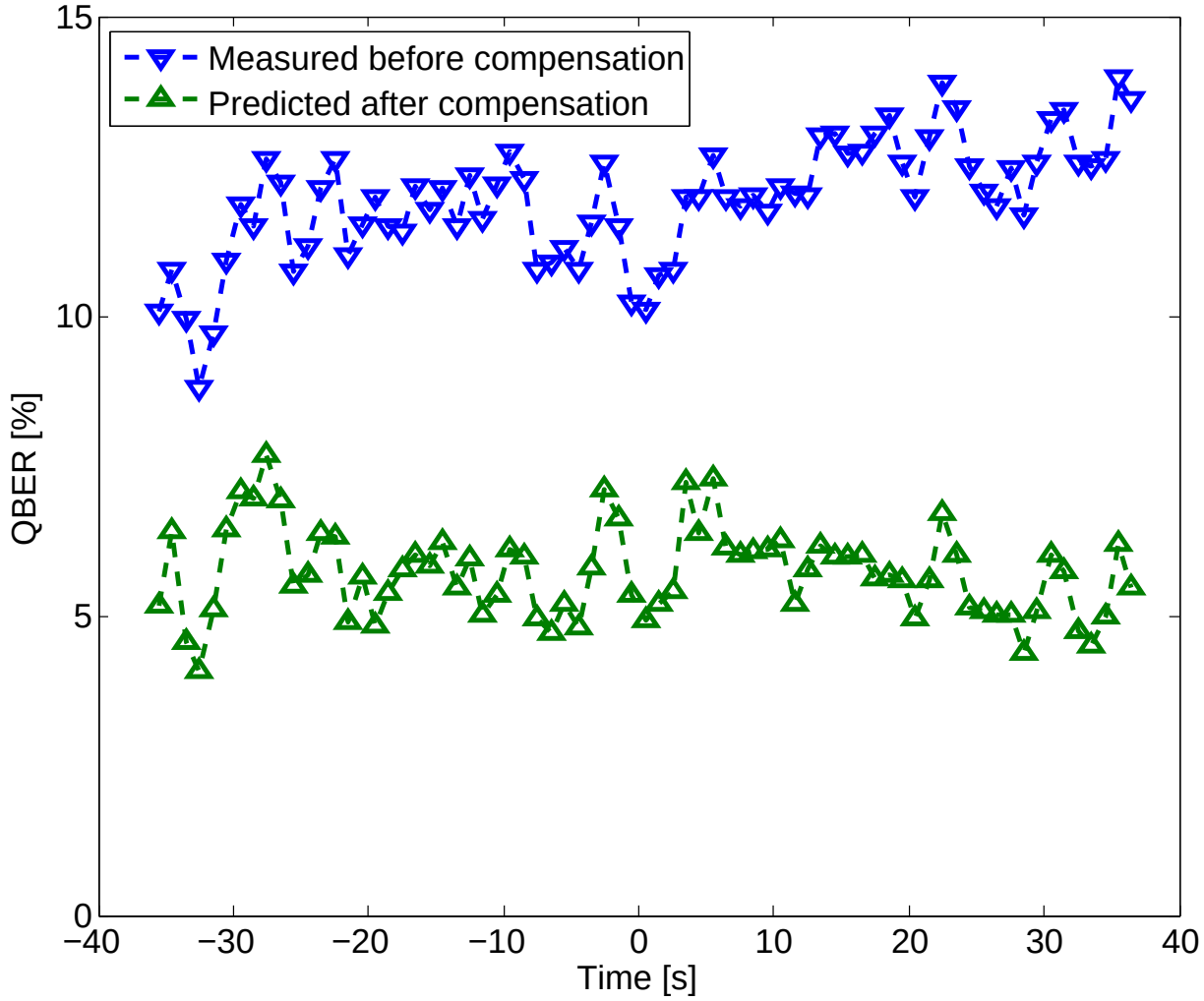

Figure 5.20: Measured pre-compensation and predicted post-compensation QBER at the transmitter during the 30 km/h test. Once again the polarization compensation system corrects the unitary induced by the fiber and returns the polarization states to its intrinsic QBER of ≈6% (limited by the quality of the source in the lab).

5.3.3 Analysis of the intrinsic QBER of the WCP QKD source

The post-compensation QBER is limited by the quality of the source in the lab. A possible cause is an imperfect overlap between the two crystals, which in turn is due to the short pulse duration and large bandwidth of the titanium sapphire laser used as 810 nm pump. The titanium sapphire laser used had a short pulse duration of ≈50 fs, giving it a Fourier limited bandwidth of ≈20 nm. Using filters, the bandwidth was reduced to ≈2 nm, giving a Fourier limited pulse duration of ≈500 fs. In comparison, the titanium sapphire laser used in the high loss QKD demonstration (Chapter 3) had a pulse duration of ≈3 ps and a bandwidth of <1 nm.

The shorter pulse duration can causes the up-converted 532 nm beam in each of the two crystals to be more sensitive to temporal mismatch, causing a bad temporal overlap between the two beams. In addition, the increased spectral width allows for mismatch in the up-converted spectra of the two crystals, which have non-identical up-conversion efficiency curves as a function of spectrum. A shorter spectrum reduces the allowed spectrum of up-conversion, making is easier to match the efficiency curve more closely. Together, both of these effect reduce the overlap of the up-converted beams, limiting the quality of the states that are produced from a combination of the two crystals (such as the diagonal state, which is produced by equal overlapping of the two output beams with a phase of +1). Any imperfect overlap and imbalance will affect the states in a non-unitary way, preventing the polarization compensation from reversing their effect (since wave plates can only be used to implement unitary transformations).

The modulators may also cause increased intrinsic QBER, either by applying the wrong phase to the states or due to an imbalance in power between the two arms of the interferometer. An imbalance will limit the quality of the states in a similar way as an imbalance in the efficiency of the crystals, and is therefore also not unitary and thus cannot be reversed by the polarization compensation system. Since each states is determined by their respective phases, any deviation from the intended phase in the modulators will change the state and cause additional QBER. Such deviations would affect the states on an individual basis and therefore cannot be undone using the polarization compensation (except in the case of a single constant deviation for all phases).

Polarization states predicted by the polarization compensation system

We can visualize the polarization states by using a Bloch sphere representation [140]. Figure 5.21 (Figure 5.22) shows the projection of the state onto the equator of the Bloch

sphere during one second of the 20 km/h (30 km/h) test. The equator of the Bloch sphere represents the linear polarizations (diagonal is 0°, vertical is 90°, antidiagonal is 180° and horizontal is 270°), allowing us to easily visualize polarizations states compared to their intended polarizations. Even after compensation, three of the four predicted polarization states in the 20 km/h test, and two of the four states in the 30 km/h, show a length of much less than one. This is due in part to the states having a non-zero contribution in the axis orthogonal to the equator (which corresponds to right-handed and left-handed circular polarizations), and in part to non-perfect purity of the states.

A pure state is any state that can be represented by a state vector [17]. In contrast, states that are not pure states (called mixed state) can only be described by a set of two or more state vectors with a probability distribution for each state vector. For example, the diagonal state is a pure state that can be described as $|\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle + |\mathrm{V}\rangle)$. However, a mixed state composed of equal part $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ cannot be represented as a single vector combination of $|\mathrm{H}\rangle$ and $|\mathrm{V}\rangle$ but must instead be seen as having equal probability (50%) of being either $|\mathrm{H}\rangle$ or $|\mathrm{V}\rangle$, never a combination.

Table 5.2 shows the purity (measure of how pure a state is) and fidelity (measure of the overlap between the measured state and the theoretical state) of the post-compensation polarization states. Each of the four intended polarizations states (horizontal, vertical, diagonal and antidiagonal) are pure states, yet the average purity for all four state during the tests where 0.91 in the 20 km/h test and 0.92 in the 30 km/h test, indicating that the states were partially mixed (all non-mixed states should have a purity of one). The decrease in purity can be caused by imperfect overlap of the up-converted beams of the two crystals, and can also be caused by background contributions. The background contribution would affect all four polarization states equally (on average), yet in both tests the average purity of the antidiagonal state (≈0.99% in both tests) and the purity of the horizontal state (≈96% in the 20 km/h test and ≈0.99% in the 30 km/h test) are much higher than the purity of the diagonal (≈89% in both tests) and vertical (≈78% in both tests) states. This implies that the background can only have a small contribution in the degradation of the purity for the diagonal and vertical states, with the rest of the contribution being due to the imperfect overlap of the up-converted beams of the two crystals.

The polarization states are also visibly skewed towards ≈ 135°. This could be caused by the polarization compensation not fully compensating the unitary in the fibers, an imbalance in the efficiency of the two crystals, and imbalance in the transmission of the two arms of the modulators, or a deviation from the intended phases applied by the modulators. To identify the cause we model these effects and optimize the parameters to replicate the states observed. This analysis is done using a density matrix representation [17].

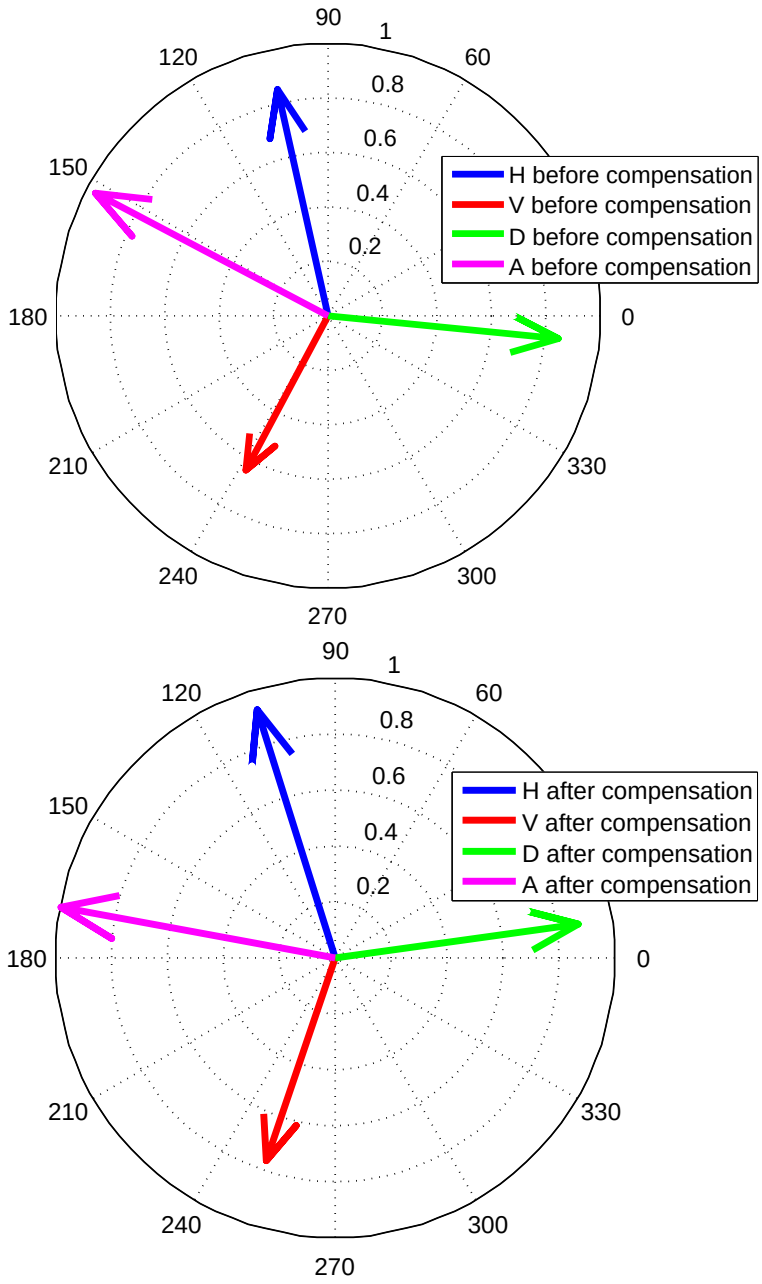

Figure 5.21: Measured pre-compensation (top) and predicted post-compensation (bottom) polarization states projected on the equator of the Bloch sphere. Even after compensation the four states do not match the theoretical distribution (90° from each other) and are instead skewed towards $\approx 135°$. This can be caused by an imbalance in the total up-conversion efficiency of the crystals. In addition, the length of three of the two vectors are less than unity due to the non-perfect purity of the states which is can be caused by imperfect overlap of the up-converted beams from the two crystals.

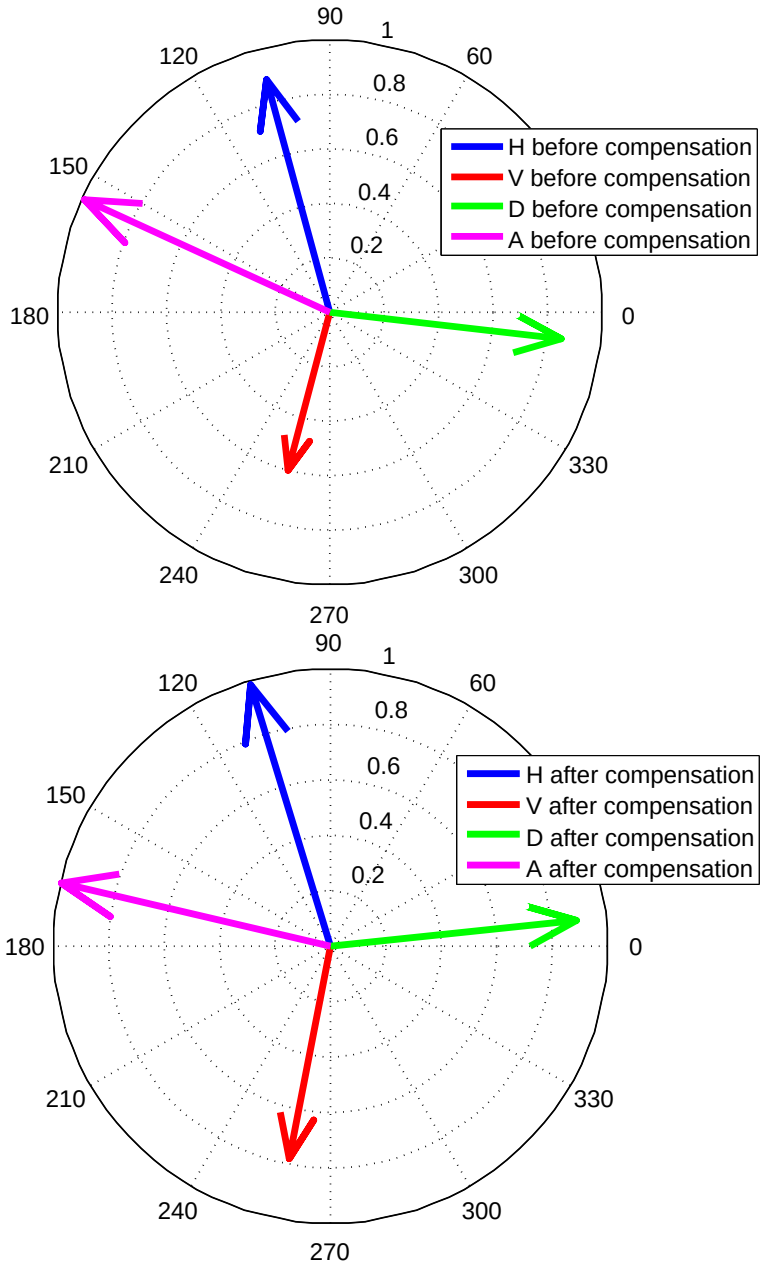

Figure 5.22: Measured pre-compensation (top) and predicted post-compensation (bottom) polarization states during the 30 km/h test projected on the equator of the Bloch sphere. Once again the states are skewed towards $\approx 135°$, possibly due to the imbalance in the total up-conversion efficiency of the crystal. The length of the vector are slightly closer to unity than in the 20 km/h, which may suggest a slightly better overlap of the up-converted beams from the two crystals, or better signal-to-noise ratio at the transmitter during the 30 km/h test.

Table 5.2: Purity and fidelity of the the predicted state post-compensation polarization states. Both the purity and fidelity of the 30 km/h test are better than those for the 20 km/h test, suggesting a lower intrinsic QBER of the source.

	20 km/h test		**30 km/h test**	
Expected state	**Purity**	**Fidelity**	**Purity**	**Fidelity**
$\|H\rangle$	0.9566	0.9601	0.9952	0.9839
$\|V\rangle$	0.7832	0.8659	0.7867	0.8705
$\|D\rangle$	0.8927	0.9347	0.8900	0.9337
$\|A\rangle$	0.9927	0.9807	0.9960	0.9835
Average	0.9063	0.9354	0.9170	0.9429

Theoretical model of polarization effects from the source

The input state at the modulator interferometer is the diagonal state ($|D\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)$), which can be represented with the density matrix [140]

$$\rho_D = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}. \tag{5.2}$$

The phase modulators will apply a phase difference between the two arms of the interferometer. Since we cannot measure global phases, we can model the phase modulators as applying a phase to the vertical ($|V\rangle$) component of the state only. This phase can be modeled using the unitary [140]

$$U_{\text{phase}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}, \tag{5.3}$$

where ϕ is the phase being applied for each states. The theoretical phases are $\pi/2$ for $|H\rangle$, $-\pi/2$ for $|V\rangle$, 0 for$|D\rangle$, and π for$|A\rangle$).

The imbalance in the two arms of the modulator will cause one of the two components of the state (either the $|H\rangle$ component or the $|V\rangle$ component) to be greater than the other. For a general state, this effect will cause the transformation

$$U_{\text{mod}}(\alpha\,|H\rangle + \beta\,|V\rangle) = N_{\text{factor}}(\alpha\cos\theta_{\text{mod}}\,|H\rangle + \beta\sin\theta_{\text{mod}}\,|V\rangle), \tag{5.4}$$

implying

$$U_{\text{mod}} = N_{\text{factor}} \begin{bmatrix} \cos\theta_{\text{mod}} & 0 \\ 0 & \sin\theta_{\text{mod}} \end{bmatrix}. \tag{5.5}$$

N_{factor} is a normalization factor which is determined by the normalization condition

$$\alpha^2 \cos^2 \theta_{\text{mod}} + \beta^2 \sin^2 \theta_{\text{mod}} = 1, \tag{5.6}$$

which depends on the amplitudes α and β of the state it's acting upon. This unusual normalization condition arises because the imbalance process is not unitary. It can be seen as loss acting independently on each arms of the interferometer, giving a probability of the photon state being loss. To maintain normalization we must post-select on having a photon state exit the interferometer, leading to the above normalization condition.

After the interferometer, the state is rotated to transform the right-handed and left-handed circular polarizations to horizontal and vertical polarizations. The rotation matrix performing this transformation is given by

$$R = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}. \tag{5.7}$$

The state then travels through fibers to the up-conversion source. This fiber will induce an unknown unitary on the state. All unitary rotations of the polarization state are part of the special unitary group $SU(2)$ [215] and can be written as

$$U_a = \begin{bmatrix} \cos(\theta_a) e^{i\phi_a} & -\sin(\theta_a) e^{-i\psi_a} \\ \sin(\theta_a) e^{i\psi_a} & \cos(\theta_a) e^{-i\phi_a} \end{bmatrix}. \tag{5.8}$$

During the up-conversion, the efficiency of the crystals may be unbalanced, leading to a similar effect as the imbalance in the modulator. The transformation can be modeled in the same way:

$$U_{\text{cryst}} = N_{\text{factor}} \begin{bmatrix} \cos \theta_{\text{cryst}} & 0 \\ 0 & \sin \theta_{\text{cryst}} \end{bmatrix}, \tag{5.9}$$

with the normalization condition

$$\alpha^2 \cos^2 \theta_{\text{cryst}} + \beta^2 \sin^2 \theta_{\text{cryst}} = 1. \tag{5.10}$$

Finally, the state will be rotated by the unitary of the fiber going to the roof and by the polarization compensation system (using the wave plates). The polarization compensation system attempts to return the state to the correct orientations by calculating the wave plate positions that will maximize the fidelity of the states. Because some of the effects describe above are not unitary rotation, the polarization compensation will attempt to rotated the states to the closest match it can find. Therefore, the polarization compensation will not only compensate the unitary of the fiber to the roof but also the other polarization degrading effect.

Table 5.3: Fidelity of the modeled state with the predicted state (from the polarization compensation system) at the output of the transmitter. Our model found good agreement with most of the polarization states except the vertical state, where the fidelity was only 88% and 89% for the 20 km/h and 30 km/h test, respectively.

Expected state	**Fidelity for the 20 km/h test [%]**	**Fidelity for the 30 km/h test [%]**
$\|H\rangle$	96.37	99.31
$\|V\rangle$	88.16	89.12
$\|D\rangle$	94.19	94.73
$\|A\rangle$	99.85	100.00
Average	94.64	95.79

We can model both the unitary of the fiber to the roof and the unitary applied by the polarization compensation system with a single $SU(2)$ matrix:

$$U_b = \begin{bmatrix} \cos(\theta_b)e^{i\phi_b} & -\sin(\theta_b)e^{-i\psi_b} \\ \sin(\theta_b)e^{i\psi_b} & \cos(\theta_b)e^{-i\phi_b} \end{bmatrix}. \tag{5.11}$$

The final state at the output of the transmitter is then given by

$$U_b U_{\text{cryst}} U_a R U_{\text{mod}} U_{\text{phase}} \rho_D U'_{\text{phase}} U'_{\text{mod}} R' U'_a U'_{\text{cryst}} U'_b \tag{5.12}$$

where $'$ denotes the conjugate transpose of the matrix.

Applying the theoretical model of polarization effects of the source

We applied our model by optimizing the parameters to maximize the fidelity of our modeled polarization states at the transmitter with the predicted states from the polarization compensation system. We found average fidelities of 95% and 96% for the 20 km/h and 30 km/h test respectively (Table 5.3). In both cases, the fidelity of the vertical state ($|V\rangle$) was the limiting factor, with 88% for the 20 km/h test and 89% fidelity for the 30 km/h test respectively. For all other states the fidelity was above 94%, reaching as high as 100% for the the antidiagonal state ($|A\rangle$). The optimized parameters are listed in Table 5.4.

Only two of the four of the phases applied by the modulators showed significant deviation form the desired values (ϕ_V and ϕ_D), while the other two (ϕ_H and ϕ_A) showed only

Table 5.4: Optimized parameters used to model the state at the output of the transmitter. Two of the phases (ϕ_V and ϕ_D) showed a significant deviation from the desired values which would result in non-unitary degradation of the polarization states, which cannot be corrected by the polarization compensation system. In addition, the crystals showed a significant imbalance (θ_{cryst}) which would also result in a non-unitary degradation of the polarizations states. While the unknown unitary from the modulator to the crystals (θ_a, ϕ_a and ψ_a) and the unknown unitary from the crystals to the output of the transmitter (θ_a, ϕ_a and ψ_a) both showed significant deviations, both of these are unitary and can therefore, in principle, be compensated by the polarization compensation system.

Parameter	**Desired value for minimum intrinsic QBER**	**Value for the 20 km/h test**	**Value for the 30 km/h test**
ϕ_H	1.5708	1.5708	1.5953
ϕ_V	-1.5708	-1.5217	-1.4603
ϕ_D	0	-0.1104	-0.1227
ϕ_A	3.1416	3.1661	3.0802
θ_{mod}	0.7854	0.7977	0.7977
θ_a	0	-2.0494	1.1045
ϕ_a	0	-0.0491	0.0245
ψ_a	0	3.1416	3.0925
θ_{cryst}	0.7854	0.9940	0.9695
θ_b	0	1.0917	1.1024
ϕ_b	0	-3.1054	3.1170
ψ_b	0	-3.1209	-3.1907

small deviation. The states that showed higher deviations in the modulator phases are also the one that showed the lowest fidelity during the experiment (Table 5.2), suggesting that a large part of the reduced fidelity of these two states may have been caused by the phase. The modulator's interferometer showed little imbalance (θ_{mod}), suggesting it did not have a significant impact on the intrinsic QBER. However, the balance in the crystals (θ_{cryst}) showed a significant deviation from the desired value, resulting in efficiencies of ≈30% in one crystals and ≈70% in the other, a ratio of 2.3. This would significantly affect the intrinsic QBER of the source. These effects (modulator phases, imbalance in the modulator interferometer and imbalance in the efficiency of the crystal) are non-unitary and therefore cannot be compensated by the polarization compensation system.

In principle, both the unknown unitary from the modulator to the crystals (θ_a, ϕ_a and ψ_a) and the unknown unitary from the crystals to the output of the transmitter (θ_a, ϕ_a and ψ_a) can be compensated by the polarization compensation system (as they are unitary transformations). Therefore, while their values deviate significantly from the desired values it would not directly contribute to the degradation in the intrinsic QBER of the source.

It is of interest to point out the high variation in the angle θ_a of the unknown unitary from the modulator to the crystals, the only parameter that showed a large change between the two tests. This change corresponds to 3.1535, of 1.0039π. Because $\phi_a \approx 0$ and $\psi_a \approx \pi$, the unitary will be:

$$U_a \approx \begin{bmatrix} \cos(\theta_a)e^0 & -\sin(\theta_a)e^{-i\pi} \\ \sin(\theta_a)e^{i\pi} & \cos(\theta_a)e^0 \end{bmatrix} = \begin{bmatrix} \cos(\theta_a) & \sin(\theta_a) \\ -\sin(\theta_a) & \cos(\theta_a) \end{bmatrix}, \tag{5.13}$$

for the 20 km/h test and

$$U_a \approx \begin{bmatrix} \cos(\theta_a+\pi)e^0 & -\sin(\theta_a+\pi)e^{-i\pi} \\ \sin(\theta_a+\pi)e^{i\pi} & \cos(\theta_a+\pi)e^0 \end{bmatrix} = \begin{bmatrix} -\cos(\theta_a) & -\sin(\theta_a) \\ \sin(\theta_a) & -\cos(\theta_a) \end{bmatrix}, \tag{5.14}$$

for the 30km/h test. Therefore both unitaries are equivalent up to a global phase π.

Finally, the deviation of the parameters in the unknown unitary from the crystals to the output of the transmitter (θ_a, ϕ_a and ψ_a) are likely caused by the polarization compensation system which attempts to correct the polarization states to maximize fidelity. Since the fidelity is affected by processes beyond the unitary from the fiber to the dome, the polarization compensation system will not compensate this last unitary but will instead try to compensate all effects as best it can.

This can be visualized by calculating the polarization states after the crystals, projecting it on the equator of the Bloch sphere and comparing it with the state after the

polarization compensation system (Figure 5.23 and 5.24). The polarization states after the crystals is calculated by applying the inverse of the unitary from the crystals to the output of the transmitter (calculated by our model) to the predicted polarization state after the transmitter. This shows how compensating only the unitary in the fiber to the dome would result is significantly worst fidelity.

The largest non-unitary deviation occurs at the efficiency imbalance of the crystals, suggesting is was the main limitation in the intrinsic QBER of the source. In addition, imperfect overlap of the crystals (which was not modeled) would reduce purity. Applying The calculated unknown unitary from the modulator to the crystals in reverse to the polarization axis at the crystals (horizontal and vertical), we find that the axis of the crystals is rotated by $\approx 35^\circ$ on the equator of the Bloch sphere. This would bring the axis of the crystals from $90^\circ/270^\circ$ (H/V) to $125^\circ/305^\circ$, in close agreement with the observed 135° from Figure 5.21 and 5.22 (which is also affected by the individual phases at the modulator).

More stable optical alignment, along with a longer pulse duration and shorter bandwidth, would be required to return the QKD source to a better intrinsic QBER (the titanium sapphire laser used in the high loss QKD demonstration allowed for an intrinsic QBER of $\approx$2%). However the new titanium sapphire laser is designed to produce femtosecond pulses and cannot generate longer pulses. In addition, increasing the pulse duration by using additional spectral filtering reduces the power available for up-conversion, limiting the average photon number of our pulses to less than our desired $\mu = 0.5$. This not only decreases the signal-to-noise at the receiver (which in turns increases the QBER), but also reduces the signal-to-noise ratio at the polarization compensation system, limiting the compensation quality during the test. We therefore had no choice but to perform the experiment with the current intrinsic source as no other pulsed pump laser was available.

This theoretical modeling of the intrinsic QBER of the source was performed after the test and time constraints prevented us from performing the experiment again. A more rudimentary version of this analysis has been implemented as part of the polarization compensation system so that the performance of source can be better characterize in future experiment.

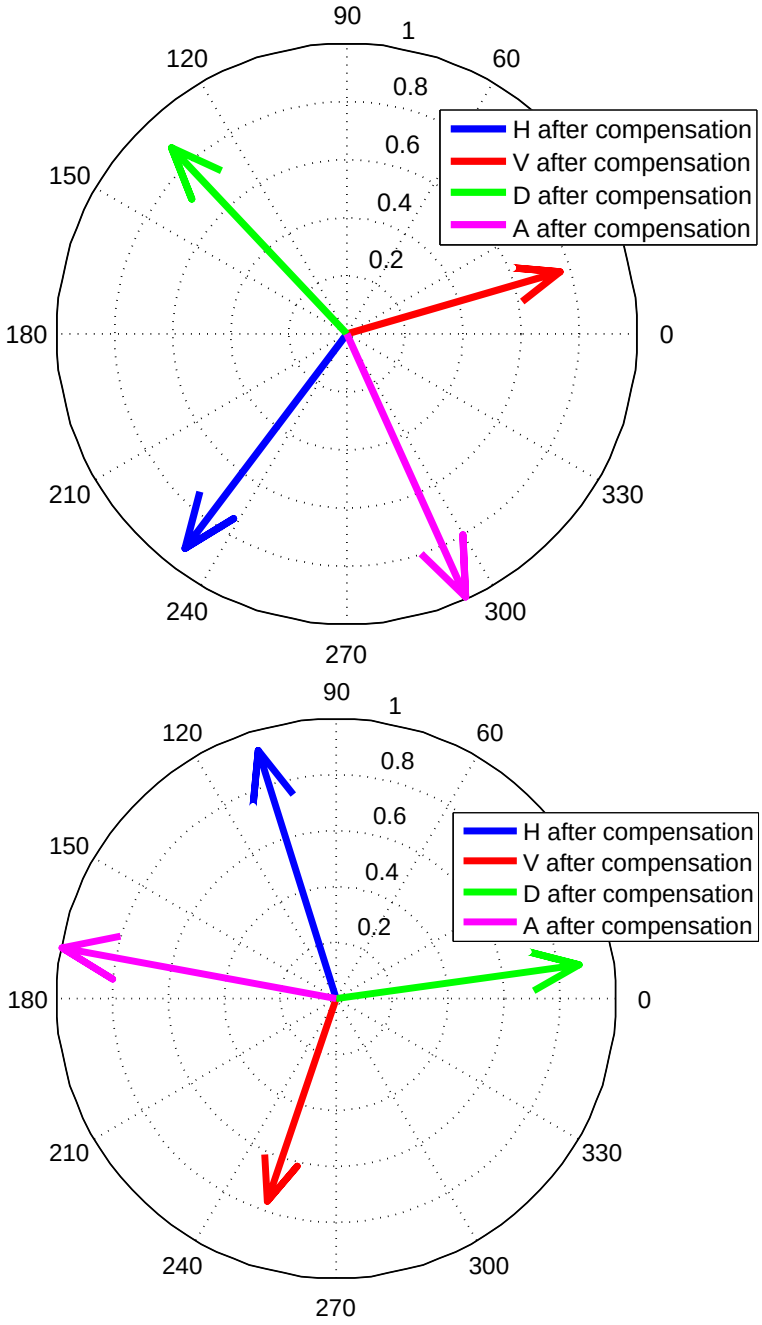

Figure 5.23: Modeled polarization states at the output of the crystals (top) and Post-compensation polarization states predicted by the polarization compensation system at the transmitter (bottom) during the 20 km/h test projected on the equator of the Bloch sphere. The polarization compensation system is capable of improving the fidelity of the states by compensating based on fidelity with the initial states rather than simply compensating the unitary of the fiber to the dome (which would result in the same polarization states at the transmitter as the ones at the output of the crystals).

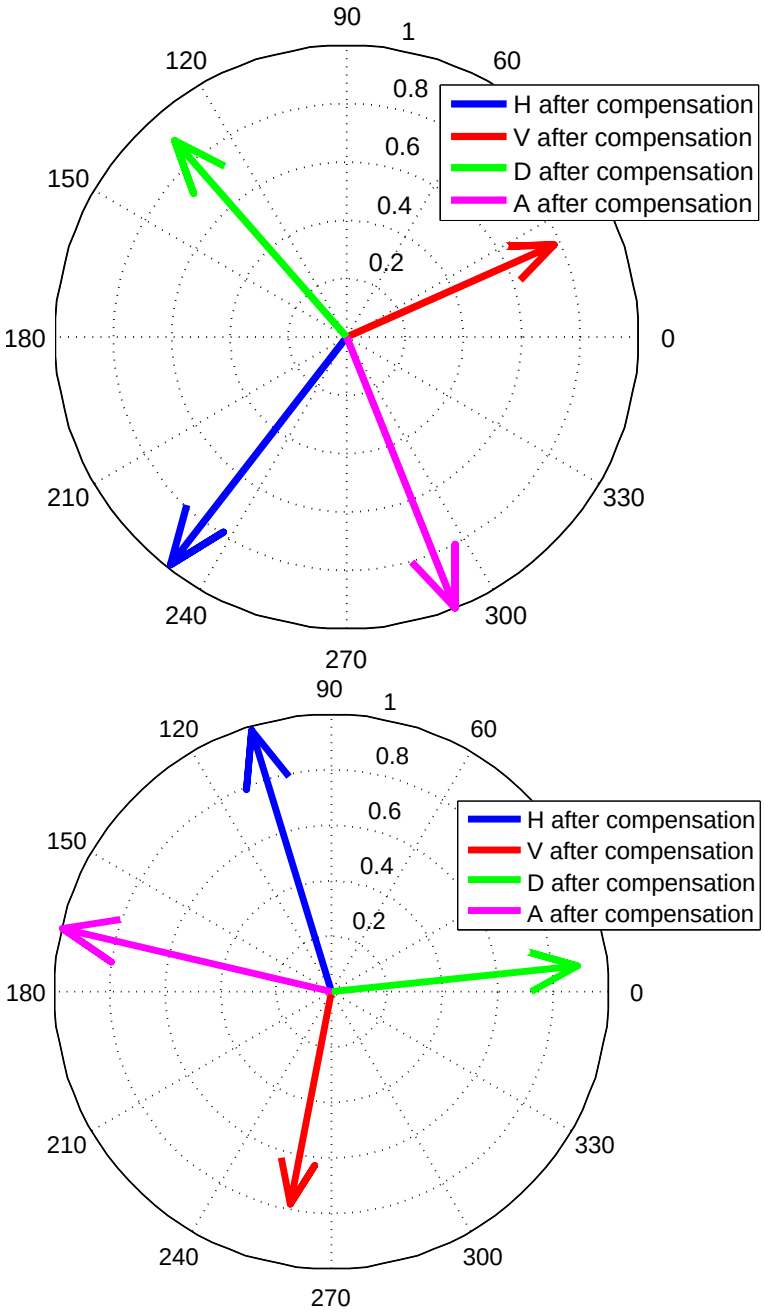

Figure 5.24: Post-compensation polarization states predicted by the polarization compensation system (top) and modeled post-compensation polarization states (bottom) during the 30 km/h test projected on the equator of the Bloch sphere. Once again the fidelity of the states at the transmitter is improved by having the polarization compensation system maximize the fidelity of the states with the initial states rather than simply compensating the unitary of the fiber to the dome.

5.3.4 Performance of the full system

Full system during 20 km/h moving receiver test

The measured QBER and count rates measured at the receiver during the 20 km/h test is shown in Figure 5.25. For the first 6 s (before the link stabilized) there were no significant quantum signals recorded by the receiver, leading to high QBER (≈40%). While this QBER is below the typical average background QBER, one must remember that the QKD software determines the correct peak by minimizing QBER. In this case there were no real peaks and so the program optimized on the area of background counts with the lowest QBER.

The average background counts measured at the receiver during this acquisition period was ≈1500 cps, and the timing widow used was 1 ns. Since the period of the source is 12.5 ns, this implies that the average count rate after time filtering was only ≈120 cps, half of which are discarded during sifting. The signal pulses represent 92% of the pulses, while the decoy pulses represent 8% of the pulses. Therefore an average of only 55 cps are attributed to signals and 5 cps to decoys. These low count rates are what allows the program (which identifies the correct signal peak based on minimum QBER) to post select on QBER than strongly deviate from the expected 50% (especially with the decoy QBER).

Once the link stabilizes the receiver begins to receive quantum signal counts. The average count rate from the quantum signals was around 30000 cps, with a maximum count rate of 45000 cps and short drop outs at ≈9–10 s and at ≈16–17 s. As the count rate rises the QBER also drops because it is no longer based on noise. Peaks can also be seen on the user interface (Figure 5.26), showing the time correlation of the quantum signals.

A comparison of the predicted QBER at the transmitter after compensation (as seen in Figure 5.19) with the measured signal QBER at the receiver (E_μ in Figure 5.25) is shown in Figure 5.27. The measured QBER drops to a value very close to the predicting QBER, indicating that the link's contribution to the total QBER is significantly less than the intrinsic QBER. The QBER's increase in the link is due to transmitter and receiver misalignment and background counts.

Full system during 30 km/h moving receiver test

Figure 5.28 shows the measured QBER and count rates in the 30 km/h test. Similarly to the 20 km/h test, there were no significant quantum signal recorded by the receiver until the link stabilized at ≈4 s. The below average signal QBER is again due to the software

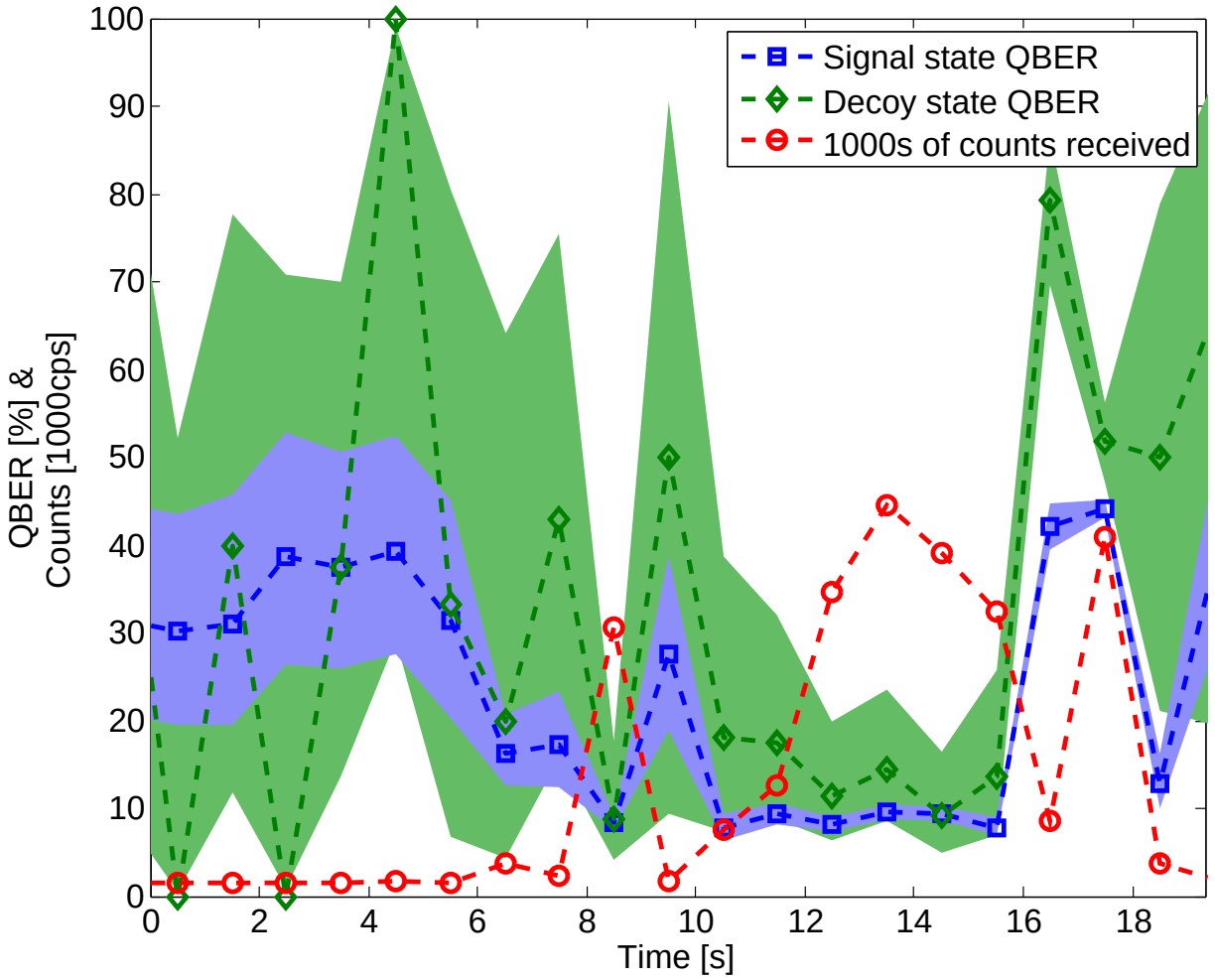

Figure 5.25: QBER and count rate measured at the receiver during the 20 km/h test. The shaded regions around the QBERs corresponds to a 95% central credible interval (described in Section 3.3.3). The QBER drops when the count rate increases at 7–15 s. Outside of this range the QBER is based on noise. The decoy state QBER has higher fluctuations compared to the signal QBER because it is based on a very small number of counts (on the order of 5 cps). The 100% decoy QBER measured at ≈5 s occurred when only 2 decoy counts were measured (both happened to be orthogonal to the intended polarization).

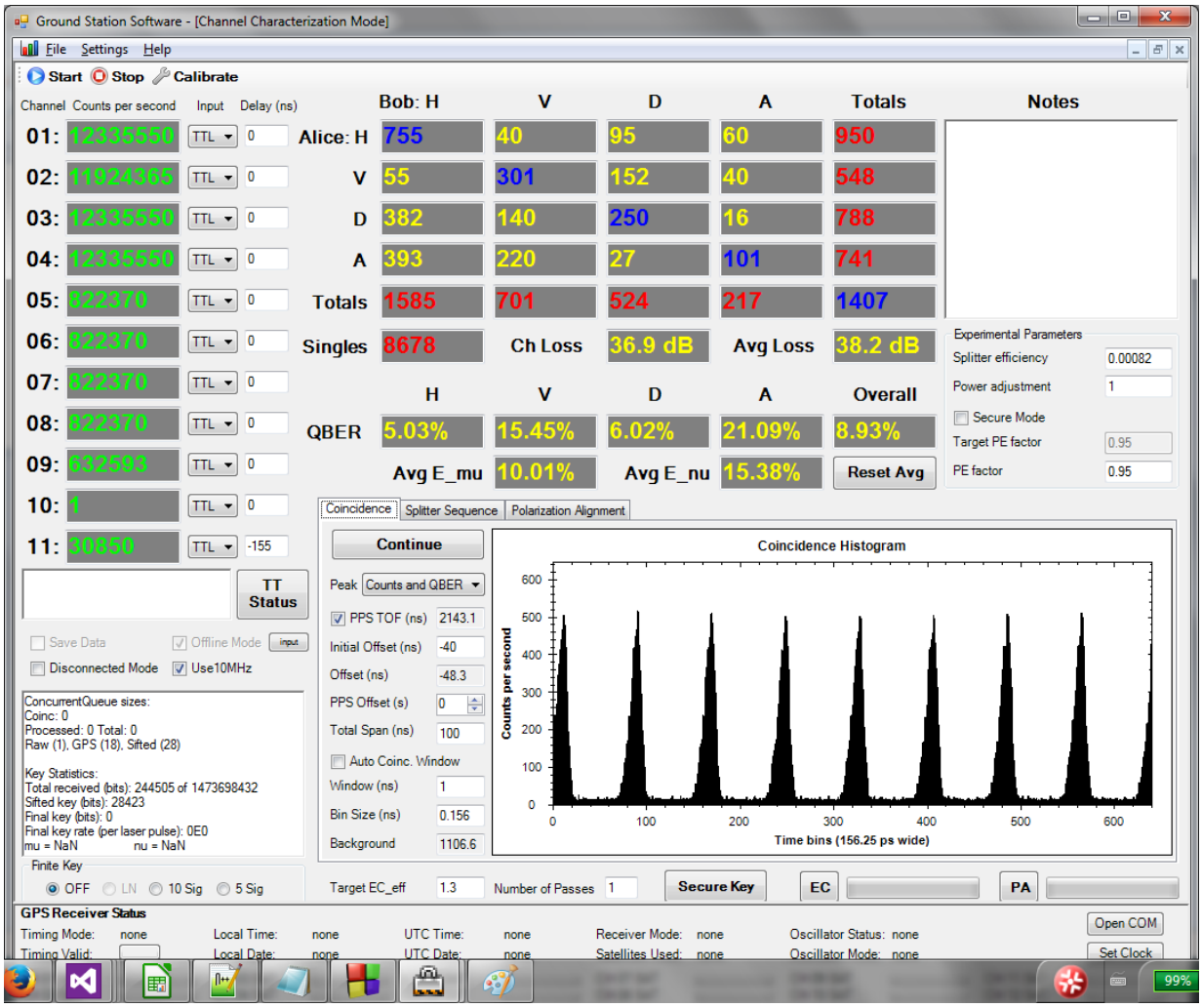

Figure 5.26: Snapshot of the user interface showing quantum signal peaks during 1 s of the 20 km/h test. The background level can also be seen at the base of the peaks. Once again the width of the signal peak is determined by the combined contributions of the laser pulse width (≈50 fs, negligible), the drift in the repetition rate of the pulsed laser (typically a few 100s of ps), the detector timing jitter (≈600 ps, includes detector electronics), the timing accuracy of the time-tagger (156.25 ps) and the delay of the four detectors compared to each other (typically aligned within 100–200 ps).

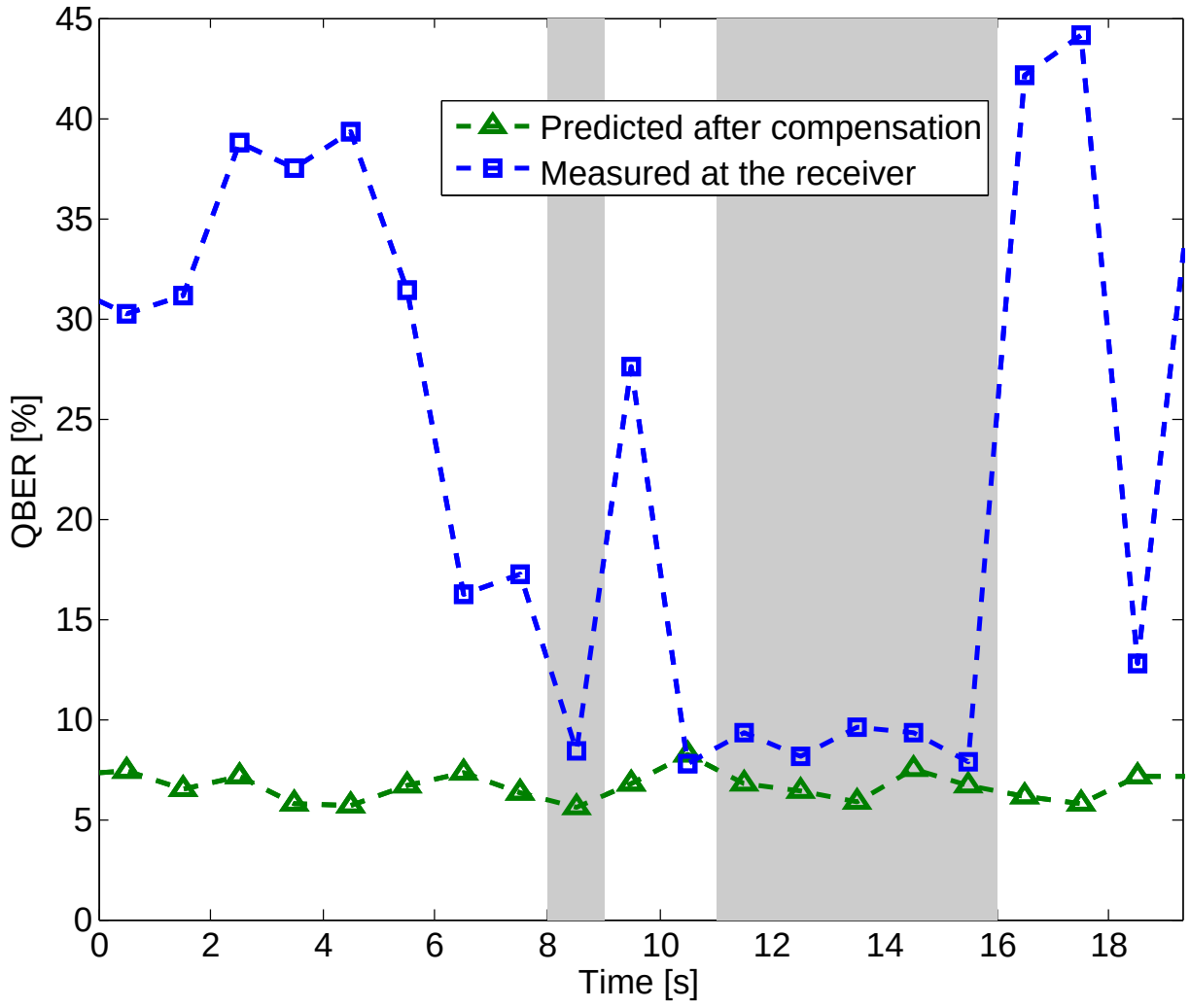

Figure 5.27: Comparison of the predicted QBER at the transmitter after compensation with the measured QBER at the receiver during 20 km/h test. Once the link is stabilized the measured QBER reduces to a value only slightly higher than the predicted QBER at the transmitter, showing that there is minimal QBER increase due to the link. The higher QBER at ≈9.5 s is due to a drop of the received counts (see Figure 5.25). Shaded area represents points where the number of signal counts at the receiver exceeded 10000.

minimizing on the QBER. One difference with the 20 km/h test is that the decoy QBER remains high during the link acquisition time. However, the total decoy counts during that time was only 7 counts, averaging less than 2 cps. Therefore the decoy states did not significantly affect the QBER minimization. It is therefore not unreasonable for the decoy states to have high QBER in this region given the high statistical uncertainty and the fact that they did not significantly affect the QBER minimization.

After stabilization, the quantum signals increased the count rate a the receiver to up to 70000 cps. In contrast to the 20 km/h test, the 30 km/h test did not experience any drop outs. Drop outs are a random effect caused by pointing error (mainly the transmitter's pointing error), and therefore do not always occur. As with the 20 km/h test, the QBER dropped as the count rates increased beyond the noise level. Figure 5.29 shows the time correlated peaks from the quantum signals, confirming that the higher count rate is not based on noise.

Figure 5.30 shows a comparison of the predicted QBER at the transmitter after compensation (as seen in Figure 5.20) with the measured signal QBER at the receiver (E_μ in Figure 5.28). Once again the measured QBER is only slightly higher than the predicting QBER, indicating that the link's contribution to the total QBER is significantly less than the intrinsic QBER.

Time-of-flight correction

A first order time-of-flight correction was implemented to compensate the change in the time delay of the received counts while the truck was moving. This time-of-flight correction used the GPS coordinate to calculate the change in the transmission path length between two seconds, and implemented a linear correction on the time-tags in the seconds. Therefore, the accuracy of the time-of-flight correction is reduced when the change in transmission path length deviates from a constant. The time-of-flight extracted from the GPS is shown in Figure 5.31. The change in the time-of-flight is very close to being linear, suggesting that our model is sufficient to compensate it's effect.

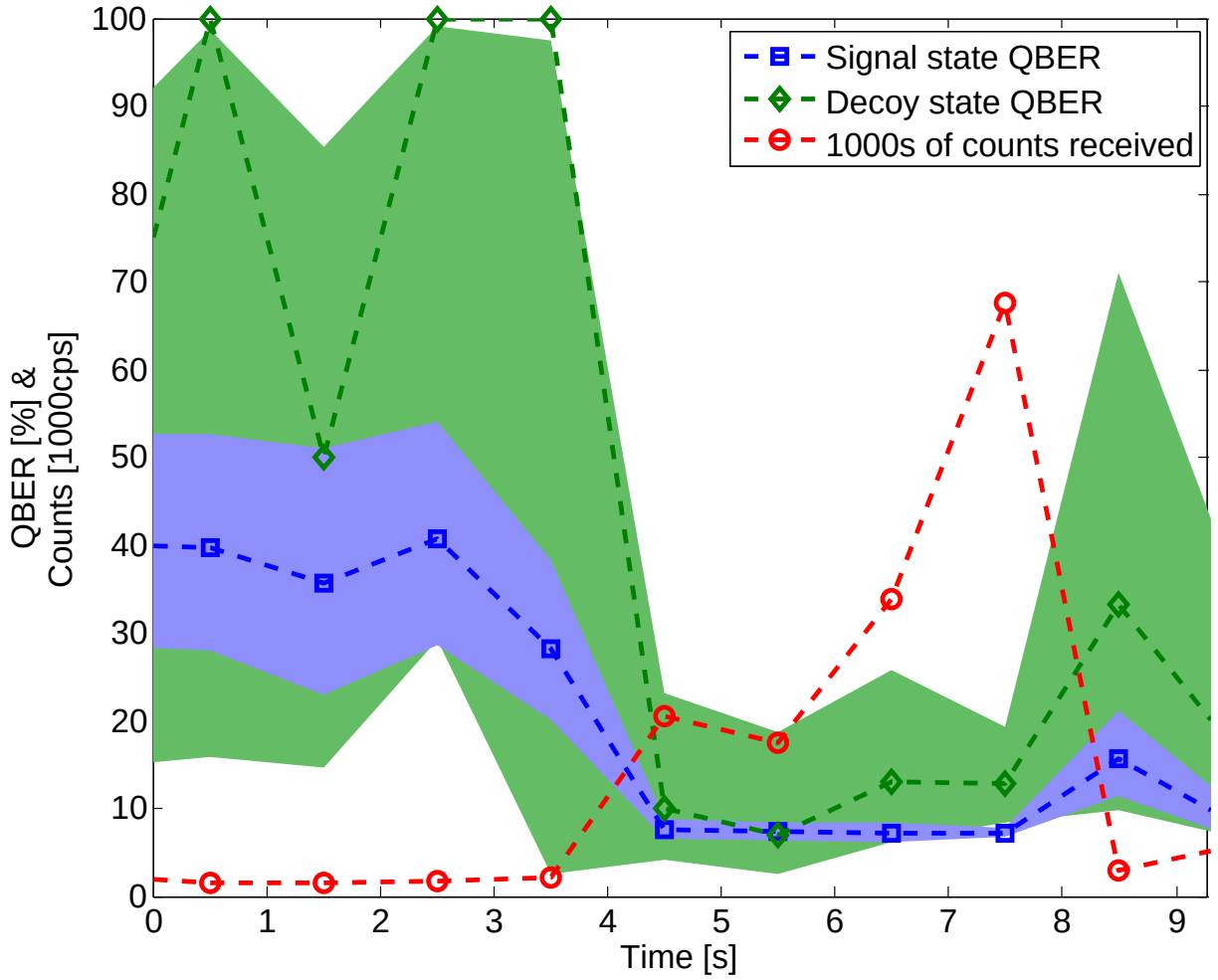

Figure 5.28: QBER and count rate measured at the receiver during the 30 km/h test. The shaded regions around the QBERs corresponds to a 95% central credible interval (described in Section 3.3.3). Once again the QBER drops when the count rate increases at 4–8 s, while being based on noise outside of this region. The high QBER of the decoy states near the beginning is due to the high statistical fluctuation of the measurement which is based on an average decoy count rate of less than 2 cps.

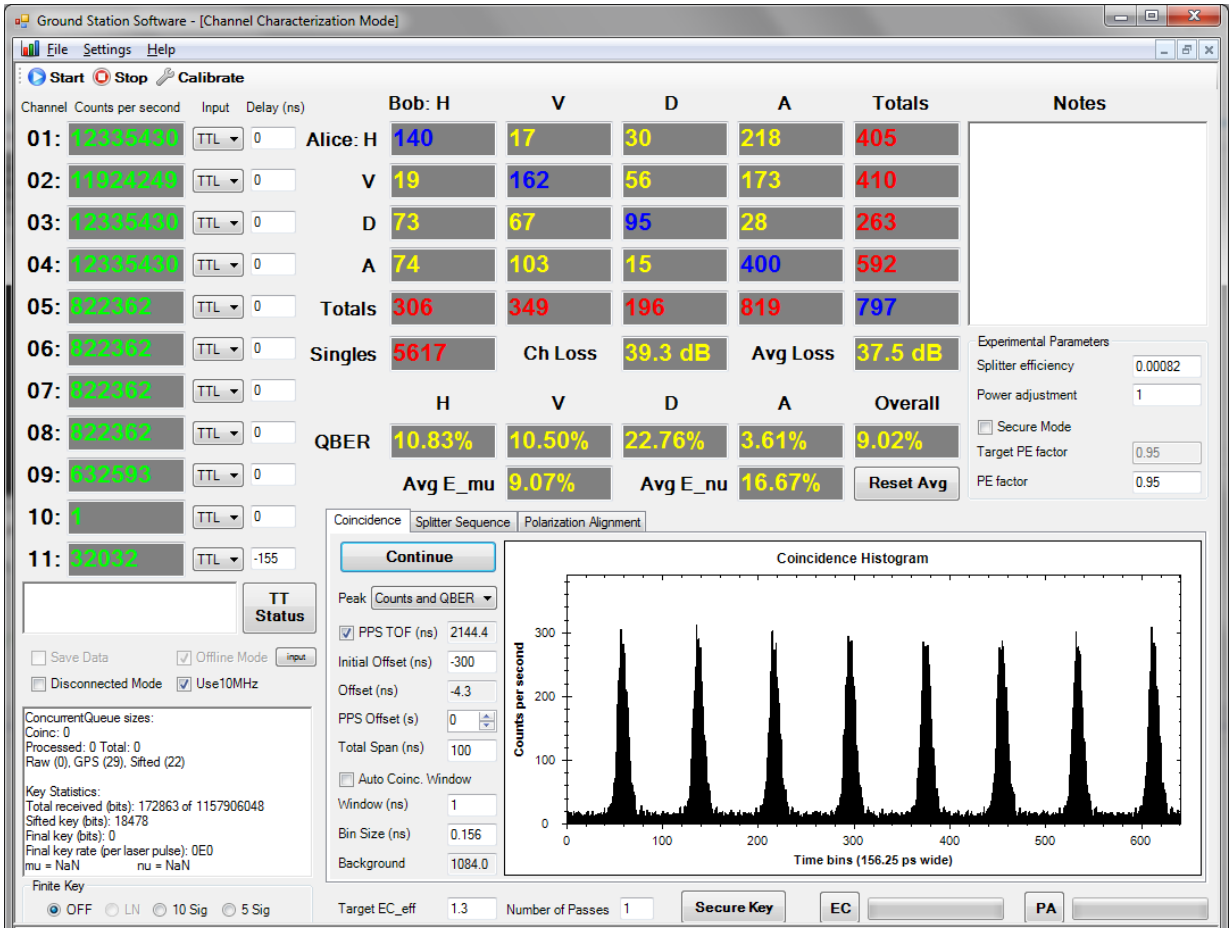

Figure 5.29: Snapshot of the user interface showing quantum signal peaks during 1 s of the 30 km/h test. Once again the background level can be seen at the base of the peaks.

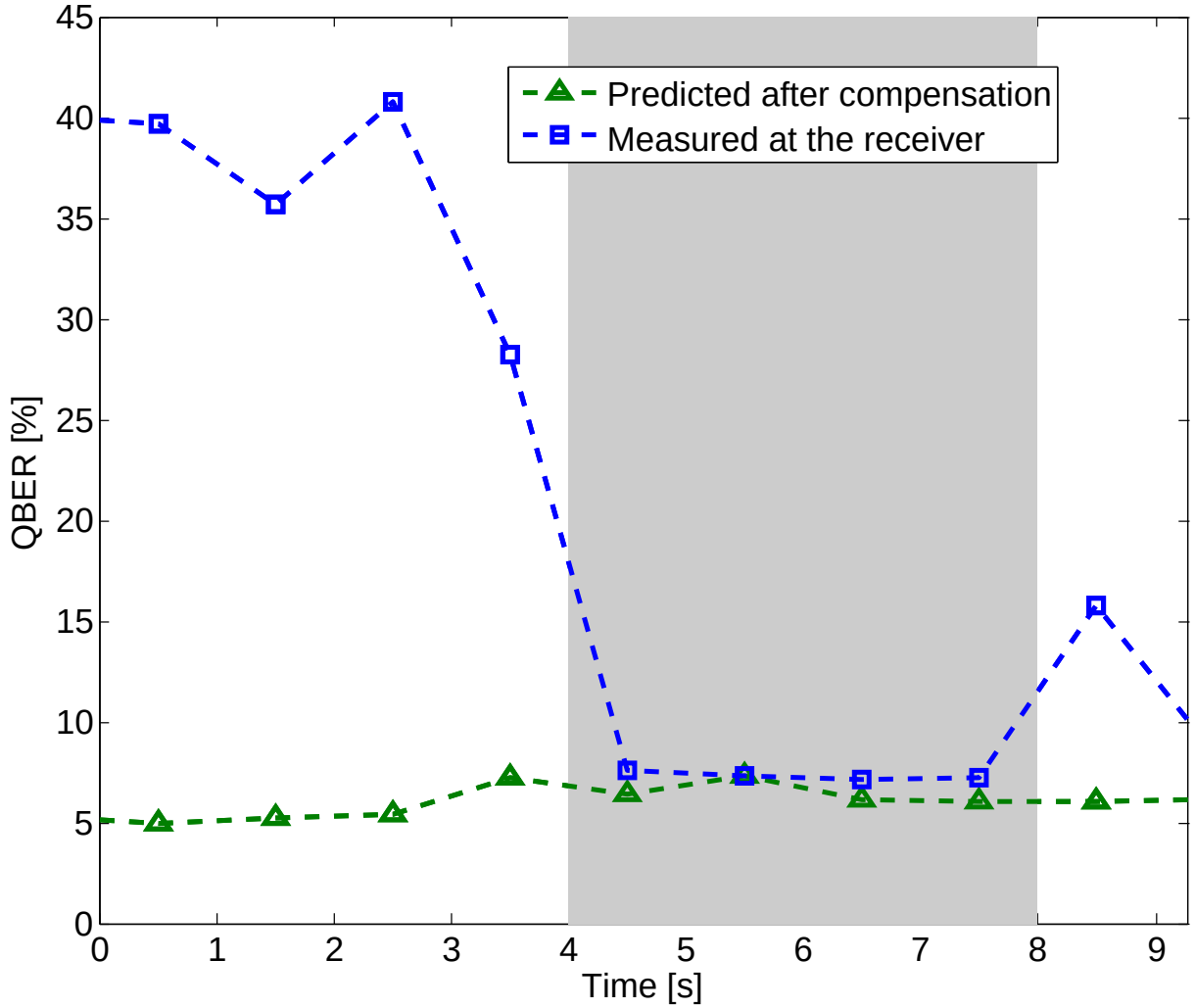

Figure 5.30: Comparison of the predicted QBER at the transmitter after compensation with the measured QBER at the receiver during 30 km/h test. The measured QBER after link stabilization is once again only slightly higher than the predicted QBER at the transmitter, showing that there is minimal QBER increase due to the link. Shaded area represents points where the number of signal counts at the receiver exceeded 10000.

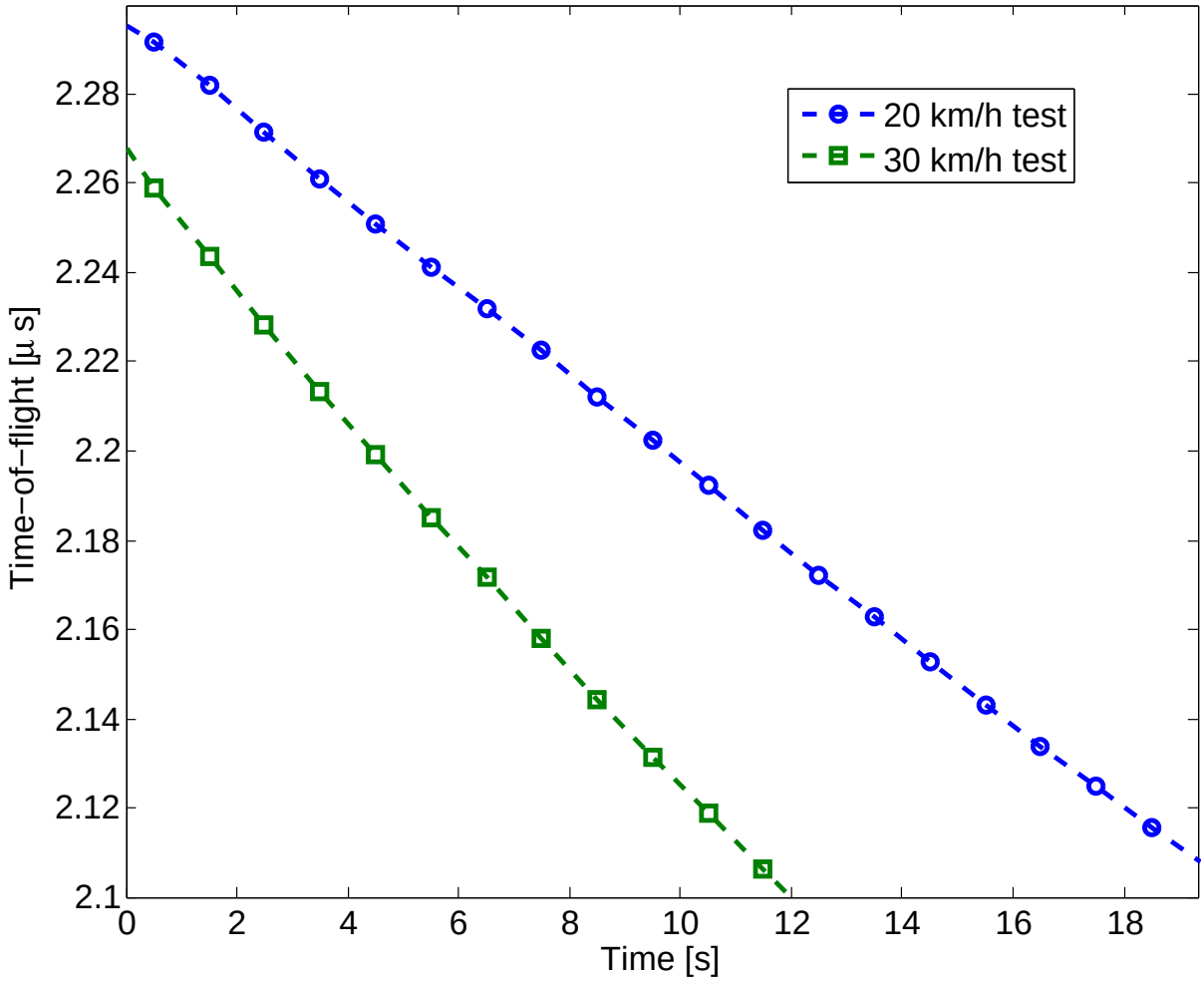

Figure 5.31: Time of flight from the dome to the receiver based on the GPS coordinates. The time-of-flight changes almost linearly and can therefore be compensated using our first order linear time-of-flight correction.

Table 5.5 shows the experimentally measured QKD parameters during the moving receiver tests. The parameters shown are the same used in Equation 3.10 and Equation 3.11. The data is post selected on seconds with count rates exceeding 10000 counts to remove data where the received counts were mostly noise. In addition, the last two seconds of the 30 km/h test (out of 4 s) were also removed because they produced wider peak (around 10 ns width compared to the typical 1 ns). This post-selection does not break security because it is based on count rates and timing information but not on the measurement outcome(1 s worth) [72]. These peaks may be the result of an instability in the pulsing frequency of the titanium Sapphire laser, or from an inaccurate timing information from the GPS.

In both tests, the QBER seen at the receiver when receiving quantum signals was around 8–9%. From polarization compensation (Section 5.3.2), the theoretically predicted QBER was already 5-6% due to limitations of the source. The additional 1–3% QBER seen at the receiver can be attributed to the higher background counts, as well as minor polarization misalignments at the transmitter and at the receiver.

Our protocol was able to extract a small amount of secret key in the asymptotic limit (7.8 bits in the 20 km/h test and 73.5 bits for the 30 km/h test). The reason these key length are so small is because our protocol is optimized for low QBER (in the range of 2–5%). Our protocol is therefore not able to reach the theoretical limit for 4-states BB84 protocols. The maximum QBER known to allow BB84 when using true single photons is 11% for on-way post-processing [216] and 20% for two way post-processing [217] (note that these are not proven limit, higher QBER may be possible). Since WCP source does not use true single photons, the limit is even lower. From Equation (2.27), the asymptotic rate is $q\{-Q_\mu \eta_{\mathrm{EC}} H_2(E_\mu) + Q_1 [1 - H_2(E_1)]\}$. For $\mu = 0.5$, and with with perfect error correction and no background QBER ($E_\mu = E_1$), the QBER where the rate becomes negative (and therefore no key can be extracted) is 9%.

Recently, it has been shown that key extraction can be improved by using noisy pre-processing, where one introduces noise in the system to reduce the amount of information shared with an eavesdropper, thus reducing the required privacy amplification at the cost of increasing error correction. This noise can be added after the transmission by randomly flipping bits in the sifted key. In our case, the intrinsic QBER of the source provides this noise, and by characterizing this intrinsic QBER we can bound the minimum error ratio of an eavesdropper, allowing better key generation [218, 219]. Because our system already characterizes the intrinsic QBER of the source (using the polarization compensation sys-

Table 5.5: Experimentally measured QKD parameters during the moving receiver runs. The parameters are based on the seconds where the received counts exceeded 10000 (shaded areas in Figure 5.27 and Figure 5.30), with the exception of the last two seconds of the 30 km/h test which where removed because they produced much wider peaks than was expected. The parameters corresponds to those in Equation (2.31), Equation (3.10) and Equation (3.11). The average loss differs from the average measured loss in Table 5.1 because we post-selected on seconds with >10000 counts.

Parameter	**20 km/h test**	**30 km/h test**
Duration	6 s	2 s
μ	0.480	0.495
ν	0.112	0.118
E_μ [%]	9.12	8.03
E_ν [%]	9.77	7.78
E_0^μ [%]	49.9	50.0
E_0^ν [%]	50.0	50.0
Q_μ	1.03×10^{-4}	1.02×10^{-4}
Q_ν	2.67×10^{-5}	2.83×10^{-5}
Q_1	5.32×10^{-5}	6.71×10^{-5}
E_1 [%]	0.64	4.86
Y_0	5.57×10^{-6}	2.39×10^{-6}
Average loss [dB]	32.1	33.6
η_{EC}	1.1	1.1
Raw key rate	5047 bits/s	4994 bits/s
Sifted key rate	2537 bits/s	2491 bits/s
Secure key rate (asymptotic)	16 bits/s	64 bits/s
Secure key bit-string	000001000011110000000010100000001	101111011111011100000010011000100000001111001010100100101110011010000001000101100100000001011010010001000100101101000000100110

tem), such a method could be used the extract a higher key rate despite the high intrinsic QBER.

Modifying our protocol to allow it to function at higher QBER would require a significant change to our QKD software and would likely result in lower performance at lower QBER (as these protocols are typically optimized for high QBER). Instead it was decided to focus our effort on designing and building a new source capable of lower intrinsic QBER.

Despite successfully extracting secret key in the asymptotic limit, we were unable to extract any secure key when including finite-size statistics. Extracting key with finite size effect would require longer link duration (our link was only 4 s compared to 200 s for a typical satellite pass) or the combination of several links.

5.4 Future improvements to the system

5.4.1 New QKD source

As was stated previously, the moving receiver tests were only able to produce extract secure key from in the asymptotic limit due to high intrinsic QBER of our current QKD source. To overcome this, a new QKD source has been designed. To avoid any issue of imperfect overlap between up-converted beams, the new source will directly modulate the polarization state of a pulsed laser source. In addition, the new source will operate at 785 nm, closer to the optimal wavelength for a satellite uplink (see Section 2.5.1).

The modulation system will be similar to the telecom waveguide intensity and polarization modulator described in Section 3.1.2. An intensity modulator will be used to control the average photon number of both signal and decoy states, while two phase modulators, in a Mach-Zehnder interferometer configuration, will control the polarization state. The modulators will be off-the-shelf $LiNbO_3$ electro-optical modulators designed to operate at 785 nm [160]. The lower wavelength allows us to use the modulators directly on a pulsed laser with the desired final wavelength. The planned laser will have a repetition of 40 MHz.

A further improvement to the source will increase the repetition rate by replacing the 785 nm laser by an up-conversion source that combines a high rate 1550 nm laser, capable of 500 MHz repetition rate, with a 1590 nm laser to produce high rate 785 nm pulses. The approach of using an up-conversion source was chosen because of the availability of higher rate sources at 1550 nm compared to 785 nm.

The pulsed 1550 nm laser is an electronically triggered laser from ID Quantique [32], while the 1590 nm laser is a wavelength tunable continuous wave laser from EMCORE [220],

allowing us to adjust the wavelength of the up-converted beam. The up-conversion will be achieved using a single type-I periodically poled lithium niobate (PPLN) crystal from HC Photonics [221]. Since only one crystal is used, only a single up-converted beam will be produced, removing any up-conversion overlap concern. The up-converted beam will then be directly modulated to the desired state.

5.4.2 Additional improvements

In addition to a new source, new telescopes with larger aperture size and a fine pointing system are currently being designed. The larger aperture size will reduce diffraction losses while the fine pointing system will reduce the loss from pointing error and eliminate dropouts. These improvements will not only improve the links to the truck but are necessary to extend to longer distances.

Chapter 6

Conclusions and outlook

This work has demonstrated the feasibility of using a low Earth orbit satellite for quantum key distribution (QKD). In Chapter 2, a detailed theoretical modeling showed the capability of both uplink and downlink scenarios in producing secure keys. The downlink was shown to perform significantly better than the uplink making it the preferred option for high rate QKD. However, the uplink was shown to benefit from a simpler design and relaxed satellite pointing requirements, while allowing more scientific freedom by having access to the source, which is located on the ground, enabling a far greater range of quantum experiments. These advantages make the uplink ideal for scientific demonstrations using low complexity satellite QKD systems, where high key rate is less crucial.

We used our model to resolve important design considerations such as operating wavelength, telescope designs, pointing requirements, specific orbits and ground station location. We found the optimal wavelength to be near 785 nm for an uplink, allowing the production of up to 2 Mbit with reasonable telescope sizes and currently available technology. We also showed that such system could be used to perform fundamental experiments such as Bell tests and teleportation at distances on the order of 1000 km, far beyond what can be reached on ground with current technology.

The demanding high loss regime of a satellite uplink was explored in Chapter 3 by experimentally performing full QKD, including all post processing steps, at losses beyond 50 dB. Our system was shown capable of extracting secure keys at up to 56 dB of losses in the asymptotic limit, and at up to 45 dB with finite-size statistics on 10 min of data. We also showed secure key extraction with simulated satellite passes that replicate the losses and short durations expected of a satellite uplink. We were able to extract 8578 bits of secure key, while including finite-size statistics, from a simulated best pass. In addition, we were able to extract 349 bits of secure key (with finite-size statistics) from the combination

of 2 upper quartile passes. This suggests that our system would be able to extract secure key from a single upper quartile pass if the source rate was increased by a factor 2 (from 76 MHz to 152 MHz).

In Chapter 4, we investigated the feasibility of using light scattered on a diffusive screen to perform QKD. While this concept showed promising results, degradation in our detectors reduced the high loss capabilities of our system to ≈53 dB. This limited our system to performing the experiment at distances of less than 1 m and angles near 0°. Future work with better detectors will be necessary to fully demonstrate the viability QKD with a diffusive screen.

Finally, Chapter 5 detailed a custom built pointing system that was used to exchange quantum signals to a truck moving at angular speeds of up to $0.75°/s$, exceeding the maximum expected angular speed in a low Earth orbit satellite pass ($0.7°/s$). This required the design and construction of a transmitter and a quantum receiver with pointing capabilities, as well as the design and implementation of an active polarization compensation system. The limitations of the QKD source, which showed an intrinsic QBER of 5–6%, prevented the extraction of a secure key when including finite-size statistics. Yet our system was still shown capable of producing secure key in the asymptotic limit (up to 73.5 bits when the receiver was moving at an angular speed of 0.75°). In addition, we showed that our system was capable of tracking the moving receiver sufficiently well to exchange quantum signals at raw key rates of 20–70 kbits/s without the need of a fine pointing mechanism.

Several steps are still necessary to fully enable satellite QKD. First, the QKD system must be modified to a wavelength better suited for satellite QKD. This requires changes to the source as well as both the transmitter and the receiver. The changes are currently being performed, with the final system planed for a wavelength of 785 nm, an optimal wavelength for a satellite QKD uplink.

A crucial step will be the creation of a new source capable of both low intrinsic QBER and a higher source rate. Plans are currently underway to construct a 785 nm source capable of reaching a 500 MHz repetition rate by combining a high rate 1550 nm pulsed laser and a wavelength tunable 1590 nm continuous laser trough up-conversion (Section 5.4.1). The new source would use only one up-conversion crystal, removing the need to perfectly match two output beams to create superposition. The up-converted beam would then be directly modulated to create the desired quantum states.

For true key security, the QKD sequence will need to be changed to a fully random sequence instead of the current repeating pseudo-random sequence. This will require a quantum random number generator and better driving electronics of the modulator. True

vacuum pulses must also be added to the sequence to replace the current insecure method of measuring the background between the signal peaks. These vacuum peaks will be added in the next generation 500 MHz QKD source (while still using a repeating pseudo-random sequence).

An entangled source will also be needed in order to increase the range of quantum experiments to a satellite. This is necessary to perform, among other experiments, a long distance Bell test to the satellite. For this purpose, an entangled source is currently being constructed with one of the produced photons near 785 nm. Modifications to the QKD software are also planned to allow key extraction using an entanglement-based QKD scheme.

By moving the chopper wheel (Section 5.1.3) to the reflected path of the beam splitter one could double the rate of transmitted signal pulses (as the chopper either blocks or polarizes half of the pulses). In addition, the chopper wheel could be modified with additional polarizers, doubling the number of signals used in estimating the unitary that the polarization compensation system needs to compensate. Moving the chopper wheel would require characterization of the unitary produced in the reflection at the beam-splitter. The contribution from this unitary would then have to be removed (through the software) when determining the optimal wave plate settings to compensate the unitary of the fiber.

The position data of the transmitter and receiver, provided by the GPS, and the orientation data, provided by the gyroscope, could be used to implement initial acquisition. This would allow a rough pointing of the telescopes, sufficient for acquisition of the beacon lasers, at which point the coarse pointing would take over and align the telescopes to allow transfer of quantum signals.

Finally, the addition of a fine pointing system will be crucial in both the transmitter and receiver to allow longer distance transmission to a moving receiver. The current system has shown to be sufficient in terms of tracking speed, but the low pointing accuracy is too lossy to function at long distances. The addition of such a fine pointing system is already underway.

Future plans are to perform QKD at longer distances to a moving receiver platform such as a boat, where the tracking speed is more relaxed but finer pointing accuracy is crucial. QKD to either a high altitude balloon, allowing longer distances and atmospheric losses similar to a satellite, or to a plane, allowing both longer distances similar to a boat and high angular speeds similar to the truck, are currently being evaluated.

The work presented here achieved important milestones necessary to implement satellite QKD. We showed the theoretical feasibility and performance of satellite QKD and

experimentally overcame important challenges. We demonstrated QKD at high losses and showed the ability of exchanging quantum signals to a moving platform traveling at greater angular speeds than a low Earth orbit satellite.

Appendix A

Loss estimation program

Here we show the MATLAB code used to estimate the loss.

A.1 Main loss code

```
%note: units are always SI units
clear;

%%%%%Main parameter inputs
dorbit=600e3;       %Orbit distance from the Earth
Gaperture=0.5;      %Diameter of the ground telescope
Saperture=0.3;      %Diameter of the satellite telescope
P_error=2e-6;       %Pointing error in rad
lambda=785e-9;      %Wavelenght
detector=[0.59];        %Detector efficiency
optical_components=0.5;     %Loss from the optical components (3dB)
A=1.7e-14;      %Cn(0)^2 for sea level atmosphere
v=21;       %Average rms wind speed for sea level atmosphere
Tmirror=0;              %Diameter of the secondary mirror in a ...
    Cassegrain design at the transmitter (this secondary mirror is ...
    assumed to be circular and at the center of the beam)
Rmirror=0;              %Diameter of the secondary mirror in a ...
    Cassegrain design at the receiver (this secondary mirror is ...
    assumed to be circular and at the center of the beam)

%%%%%Definition of the type of scenario
entangled=1;        %WCP source is 0, entangled source is 1
```

```
19 up=1;           %Downlink if up==0, uplink if up==1
20
21 %%%%%Assignment of the transmitter and receiver
22 if(up==0)
23     Raperture=Gaperture;        %Diameter of the receiving apperture
24     Taperture=Saperture;         %Diameter of the transmitting apperture
25 elseif(up==1)
26     Raperture=Saperture;        %Diameter of the receiving apperture
27     Taperture=Gaperture;         %Diameter of the transmitting apperture
28 end
29
30 %%%%%Assignement of the beam waist
31 if(entangled==0)
32     w=Taperture;        %Optimal FWHM for a faint laser
33     norm_factor=4*log(2)/(pi*w*w*(exp(-log(2)*Tmirror*Tmirror/(w*w))-...
34         exp(-log(2)*Taperture*Taperture/(w*w))));       %Normalising ...
              factor so that the total power output of the transmitting ...
              aperture is 1 W
35 elseif(entangled==1)
36     w=Taperture/2;      %Optimal FWHM for an entangled source
37     norm_factor=4*log(2)/(pi*w*w);      %Normalising factor so that ...
          the total power output of the entangled source is 1 W
38 end
39
40 %%%%%Optional parameters (affect accuracy and speed of the simulation)
41 R=6.37e6;       %Earth's radius (average)
42 points_transmitter=50;      %Point evaluated at the transmitting ...
      apperture (in each dimension)
43 dxo=Taperture/points_transmitter;           %Discretization of the x ...
      axis of the transmitting apperture
44 dyo=Taperture/points_transmitter;           %Discretization of the y ...
      axis of the transmitting apperture
45 dx=1e-2;        %Discretization of the x axis of the receiving apperture
46 points_receiver=5000;       %Point evaluated at the receiving apperture
47 %%note: the distance evaluated (from the center of the receiver) is ...
      points_receiver*dx, thus this value must be ≥ to Raperture/2, the ...
      default values, 5000*1e-2 give a maximum receiver size of 100 ...
      meters in diameter
48
49 %%%%%%%loading the atmospheric transmittance: the file contains a 2D ...
      matrix of atmospheric transmittance (named atmosphere in the file) ...
      as a function of wavelength and angle. The file also contains a ...
      vector of the wavelength (named ALambda).
50 load (sprintf('atmosphere(rural-5km)'))
```

```
51 angleT=80:-1:0;     %By default the angle is not specified in the ...
       file. Change this line if using an updated file with a different ...
       angle vector.
52 %%This file is generated using MODTRAN.
53
54 trans=0;        %Transmittance as a function of angle for the chosen ...
       wavelength
55 dLambda=5e-9;       %Uncertainty in wavelenght
56 for i=(lambda-dLambda):5e-11:(lambda+dLambda)
57     trans=trans+interp1(Alambda*1e-6,atmosphere,i)/(1+2*dLambda/5e-11); ...
              %Transmittance vs angle including uncertainty
58 end
59 %%Alternatively, trans can be manually specified
60
61 %%%%%%%loading the orbit data: the file contains vectors for range ...
       (distance between the ground and the satellite) and elevation ...
       (elevation angle of the satellite from the horizon).
62 load (sprintf('Ranges_ottawa-d=%gkm',dorbit/1000),'range','elevation')
63 %%This file is generated using STK from AGI.
64 %%Alternatively, each vectors can be manually specified or the ...
       elevation vector alone can be specified and range will be ...
       automatically calculated
65 theta=90-elevation;     %Converts the elevation as angle from zenith ...
       (this is what the code was designed to use)
66  range=range/1000;       %Converts the range to m (the file specifies ...
        in km)
67
68 %%%%%Initial definitions
69 Intensity=zeros(10*(points_receiver-2),1);      %Radial intensity ...
       distribution at the receiver (assumes circular symmetry)
70 w_t=zeros(numel(theta),1);      %Width of the distribution at the ...
       receiver from atmospheric turbulence
71 loss_diff=zeros(numel(theta),1);        %loss from diffraction only
72 loss_turbulence=zeros(numel(theta),1);      %loss from diffraction + ...
       pointing + turbulence
73 loss_transmittance=zeros(numel(theta),1);       %loss from ...
       diffraction + pointing + turbulence + atmospheric transmittance
74 loss_optical=zeros(numel(theta),1);     %total loss (diffraction + ...
       pointing + turbulence + atmospheric transmittance + detector ...
       efficiency and optical loss)
75
76 %%%%%Calculation of the Width of the distribution from turbulence ...
       (only accounted for in uplink)
77 if(up==1)
```

```
78      for i=1:numel(theta)
79
80          if(range(i)>0)      %check if range exists, otherwise calculate
81      d=range(i)      %distance from the earth to the satellite
82          else
83      d=-R*cos(pi*theta(i)/180)+sqrt((R*cos(pi*theta(i)/180))^2+...
84                  dorbit^2+2*R*dorbit);        %distance from the earth ...
                       to the satellite
85          end
86
87          z=0:50:d;       %Points of the ingration (default all points ...
               from the ground to the satellite using a discretization of ...
               50 meters between points)
88          H=-R+sqrt(R^2+z.^2+2*R*z.*cos(pi*theta(i)/180));        ...
               %Height (from grund) for each point of the integration
89          Cn2=0.00594*(v/27)^2*(H*1e-5).^10.*exp(-H/1000)+...
90              2.7e-16*exp(-H/1500)+A*exp(-H/100);     %calculation of ...
                   the refractive index structure constant at each point ...
                   of the integration
91          I=trapz(z,Cn2.*(1-z/d).^(5/3));     %Integration over the ...
               path (this is the integral that appears in the calculation ...
               of the transverse coherence length)
92          w2(i)=sqrt(2)*2*d/((2*pi/lambda)*((1.46/(cos(pi*theta(i)/180))*...
93              (2*pi/lambda).^2*I).^-(3/5)));      %Width of the ...
                   distribution at the receiver from atmospheric turbulence
94
95      end
96  end
97
98  for i=1:numel(theta)
99
100         if(range(i)>0)      %check if range exists, otherwise calculate
101     d(i)=range(i)       %distance from the earth to the satellite
102         else
103     d(i)=-R*cos(pi*theta(i)/180)+sqrt((R*cos(pi*theta(i)/180))^2+...
104                 dorbit^2+2*R*dorbit);         %distance from the earth ...
                       to the satellite
105         end
106
107 error=sin(P_error)*d(i);            %Pointing error in distance at ...
       the receiving aperture
108
109 A=zeros(points_receiver,1);         %Field at one point at the ...
       receiving apperture
```

```
I=zeros(points_receiver,1);          %Intensity at one point at the ...
    receiving apperture
kc=zeros(points_receiver,1);         %Position at the receiving ...
    receiving apperture
kc2=zeros(10*(points_receiver-1),1);         %Position at the ...
    receiving receiving apperture

for k=1:points_receiver              %Rayleigh-Sommerfeld diffraction
    kc(k)=(k-1)*dx;     %Vector of the radial distance from the ...
        center of the receiver

%Calulation of the contribution to the field from each point in the ...
    transmitting aperture
    for h=-(((Taperture/2)/dxo)):(((Taperture/2)/dxo))
        limit=sqrt(abs(((Taperture/2)^2-h^2*dxo^2)))/dyo;
        for j=-limit:limit
            if(sqrt(h*h*dxo*dxo+j*j*dyo*dyo)>=(Tmirror/2))
            A(k)=A(k)+dxo*dyo*sqrt(exp(-((h*h*dxo*dxo+j*j*dyo*dyo)/...
                (w*w))*4*log(2.0)))*exp(2i*pi*sqrt(d(i)^2+...
                (kc(k)-h*dxo)^2+(j*dyo)^2)/lambda)/(d(i)^2+...
                (kc(k)-h*dxo)^2+(j*dyo)^2);
            end
        end
    end

    I(k) = norm_factor*d(i)*d(i)*abs(A(k))^2/(lambda*lambda);        ...
        %Radial intensity distribution at the receiver (assumes ...
        circular symmetry)
end

%%%%%Increase the number of points in the intensity distribution to ...
    improver the accuracy of the receiver power calculation
for l=1:10*(points_receiver-2)
    kc2(l)=(l-1)*dx/10;
    Intensity(l)=interp1((1:points_receiver),I,1+l/10);     %Radial ...
        intensity distribution at the receiver (assumes circular ...
        symmetry) with increased number of points
end

%%%%%Integrate over the receiver to find the received power when only ...
    considering diffraction
power=0;        %received power
for l=1:10*(points_receiver-2)
```

```
142     if(kc2(l)<(Raperture/2))        %Must be inside the receiver ...
            diameter to contribute
143         if(kc2(l)>(Rmirror/2))          %must be outside the ...
                obstructed area of the secondary mirror to contribute
144             power=power+(Intensity(l)+Intensity(l+1))*pi*...
145                 (2*kc2(l+1)-dx/10)*dx/20;       %received power
146         end
147     end
148 end
149
150 loss_diff(i)=-10*log10(power);      %loss from diffraction only
151
152 %%%%%Performs a 2D convolution of the diffracted profile with the ...
        pointing error and atmospheric turbulence distributions.
153 I=convolution(I,error,w2(i),Raperture,points_receiver,dx);
154
155 %%%%%Increase the number of points in the intensity distribution to ...
        improver the accuracy of the receiver power calculation
156 for l=1:10*(points_receiver-2)
157     kc2(l)=(l-1)*dx/10;
158     Intensity(l)=interp1((1:points_receiver),I,1+l/10);     %Radial ...
            intensity distribution at the receiver (assumes circular ...
            symmetry) with increased number of points
159 end
160
161 %%%%%Integrate over the receiver to find the received power when ...
        considering all geometric losses
162 power=0;        %received power
163 for l=1:10*(points_receiver-2)
164     if(kc2(l)<(Raperture/2))        %Must be inside the receiver ...
            diameter to contribute
165         if(kc2(l)>(Rmirror/2))          %must be outside the ...
                obstructed area of the secondary mirror to contribute
166             power=power+(Intensity(l)+Intensity(l+1))*pi*...
167                 (2*kc2(l+1)-dx/10)*dx/20;       %received power
168         end
169     end
170 end
171
172 loss_turbulence(i)=-10*log10(power);        %loss from diffraction + ...
        pointing + turbulence
173
174 %%%%%Adding the loss from atmospheric transmittance
```

```
175 if(theta(i)<80)     %The current file does not contain data past 80 ...
       degrees from zenith
176     transmittance=interp1(angleT,trans,theta(i));          ...
           %Transmittance of the atmosphere at the current angle
177 else
178     transmittance=interp1(angleT,trans,79.9);       %The value at 80 ...
           for the atmosphere(rural-5km) is 0 which would generate a loss ...
           value of infinity. Interpolating at value at 79.9 prevents ...
           this problems. (Note that a value of 0 at 80 is unphysical and ...
           happened because the atmospheric transmission was rounded off ...
           at 0 when the file was generated)
179 end
180
181 loss_transmittance(i)=-10*log10(transmittance*power);       %loss ...
       from diffraction + pointing + turbulence + atmospheric transmittance
182
183 loss_optical(i)=-10*log10(optical_components*detector*transmittance*power); ...
           %total loss (diffraction + pointing + turbulence + atmospheric ...
       transmittance + detector efficiency and optical loss)
184 end
```

A.2 2D convolution code

```
1  function meanI=convolution(I,error,w2,Raperture,points_receiver,dx)
2
3  %%%%%Because both distributions are Gaussian they can be combined ...
       into a Gaussian of width sqrt((2*error)^2+w2^2). (error is a ...
       standard deviation a therefore equal to half the beam width)
4  if(((2*error)^2+w2^2)>0)        %Verifies that the total distribution ...
       from pointing error and atmospheric turbulence is non-zero
5  dtheta=2*pi/100;
6  meanI=zeros(points_receiver,1);         %Average Intensity at one ...
       point at the receiving apperture (with pointing error and turbulence)
7  for h=1:1:1+Raperture/dx        %Points of the intensity profile at ...
       the receiver that are evaluated (there is no received power from ...
       the intensity outside the telescope, this reduces the time of the ...
       function)
8      j=(1:1:points_receiver)';       %Radial points integrated over
9      q=0:dtheta:(2*pi-dtheta);       %Angular points integrated over
10     r0=sqrt((((j-1).^2+(h-1)^2).*dx^2)*ones(1,numel(q))-...
11         2.*(j-1).*(h-1).*dx*dx*cos(q));
```

```
12      sigma_r0=2*dtheta*exp(-2*((r0/sqrt((2*error)^2+w2^2)).^2))./...
13          (pi*((2*error)^2+w2^2));
14      meanI(h)=sum((j-1).*sum(sigma_r0,2).*I)*dx*dx;          %Average ...
            Intensity at one point at the receiving apperture (with ...
            pointing error and turbulence)
15  %%Note: to understand how the convolution is done see equation 82 and ...
        83 of "Operational and convolution properties of two-dimensional ...
        Fourier transforms in polar coordinates" by Natalie Baddour
16  end
17
18  else
19      meanI=I;        %If the total distribution from pointing error ...
            and atmospheric turbulence is zero the beam profile is unchanged
20  end
21
22  end
```

Appendix B

Background counts estimation program

Here we show the MATLAB code used to estimate the background counts. This code is a modified version of a program written by Bassam Helou.

B.1 Downlink background code

```
clear;

Detector_number=4;      %Number of detectors used at the receiver ...
    (typically 4 for QKD)
%%Note: some experiments require a different number of detectors.
D_dark=Detector_number*20;      %Summed dark counts in all detectors ...
    per seconds.

%%%%%Main parameter inputs (in SI)
dorbit=600e3;       %Orbit distance from the Earth
FOV=50e-6;      %Field of View of the receiver
lambda=670e-9;      %Wavelenght
Raperture=0.5;      %Diameter of the ground telescope
Filter=1e-9;        %Bandwidth of the filter
detector=[0.65];        %Detector efficiency
optical_components=0.5;     %Loss from the optical components (3dB)
artSkyBright=19.21;     %artificial sky brightness for our location
moon_phase=0.5;     %Phase of the moon

%natural sky brightness based on wavelength and moon phase
if(moon_phase==1)
```

```
    if(lambda<500)
       natural_sky_brightness=17.5;
    elseif(lambda≥500&&lambda<600)
        natural_sky_brightness=17;
    elseif(lambda≥600&&lambda<720)
        natural_sky_brightness=16.8;
    elseif(lambda≥720)
        natural_sky_brightness=16;
    end
elseif(moon_phase==0.5)
    if(lambda<500)
        natural_sky_brightness=20;
    elseif(lambda≥500&&lambda<600)
        natural_sky_brightness=19.5;
    elseif(lambda≥600&&lambda<720)
        natural_sky_brightness=19.2;
    elseif(lambda≥720)
        natural_sky_brightness=18.4;
    end
end

%%%%%%%loading the atmospheric transmittance: the file contains a 2D ...
    matrix of atmospheric transmittance (named atmosphere in the file) ...
    as a function of wavelength and angle. The file also contains a ...
    vector of the wavelength (named ALambda).
load (sprintf('atmosphere(rural-5km)'))
angleT=80:-1:0;     %By default the angle is not specified in the ...
    file. Change this line if using an updated file with a different ...
    angle vector.
%%This file is generated using MODTRAN.

trans=0;        %Transmittance as a function of angle for the chosen ...
    wavelength
dLambda=5e-9;       %Uncertainty in wavelenght
for i=(lambda-dLambda):5e-11:(lambda+dLambda)
    trans=trans+interp1(Alambda*1e-6,atmosphere,i)/(1+2*dLambda/5e-11); ...
            %Transmittance vs angle including uncertainty
end
%%Alternatively, trans can be manually specified

%%%%%%%loading the orbit data: the file contains vectors for range ...
    (distance between the ground and the satellite) and elevation ...
    (elevation angle of the satellite from the horizon).
load (sprintf('Ranges_ottawa-d=%gkm',dorbit/1000),'range','elevation')
```

```
55 %%This file is generated using STK from AGI.
56 %%Alternatively, the elevation vector can be specified (range is not ...
       used for the downlink background calculation)
57
58 for i=1:numel(elevation)
59
60 receiver = struct('FOV', FOV, 'wavelength', lambda, ...
       'telescopeRadius', Raperture*100, ...
61 'filterBandpass', Filter*1e-9, 'setupEfficiency', ...
       detector(k)*optical_components,...
62 'artSkyBright', artSkyBright, 'natSkyBright', natSkyBright,...
63 'observElevation', elevation(i),'trans', trans);
64
65 %background counts calculations using modified version of Bassam's code
66 backgroundCountsDown(i) = calcDownlinkBackground(receiver)+D_dark;    ...
       %in photon/sec
67
68 end
```

```
1  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
2  %Description:
3  %calcDownlinkBackground calculates the estimated number of background ...
       counts a
4  %ground station will receive per second.
5  %Input:
6  %    1. receiver(strucutre): The receiver's parameters are entered in
7  %    receiver
8  %       The required entries in the structure are:
9  %            The following 8 arguments parameterize the telescope
10 %            a) 'FOV': The field of view of the receiver (in rad).
11 %            b) 'wavelength': The wavelength photons are emitted at.
12 %            c) 'telescopeRadius': The receiver's radius in cm.
13 %            d) 'filterBandpass': approximately the area under of the ...
       curve
14 %                of the receiver's filter bandwith (in nm).
15 %            e) 'setupEfficiency': the optical efficiency of the setup
16 %                multiplied by the detector efficiency (format 0.a).
17 %            f) 'observElevation': The receiver's observation elevation
18 %            angle. In other words, this is the angle from the horizon ...
       in degrees.
19 %            The following three parameters specify the night sky ...
       brightness:
```

```
20 %           g) 'artSkyBright'(the artificial night sky brightness): ...
       The brightness of the
21 %              night sky (in mag) due to lights emitted by human ...
       actvities.
22 %              (in mag)
23 %           h) 'natSkyBright'(the natural night sky brightness): The ...
       brightness of the
24 %              night sky (in mag) due to natural sources such as the ...
       moon.
25 %              (in mag)
26
27 %Output:
28 %       backgroundCounts: The estimated number of background counts ...
       that are
29 %       detected by the receiver. (photons/s)
30
31
32 function backgroundCounts = calcDownlinkBackground(receiver)
33
34 %refernce counts at the astronomical band containing receiver.wavelength
35 refCountsAtWav = obtainReferenceCount(receiver.wavelength);
36 %refernce counts at the V band containing receiver.wavelength
37 refCountsVband = obtainReferenceCount(550);
38 %Calculate the total night sky brightness
39 transStruct = struct('wavelength', receiver.wavelength, 'angle', ...
       90-receiver.observElevation,'trans', receiver.trans);
40 extinctionCoeff = getTransmission(transStruct);
41 correctedNatSkyBright = ...
       receiver.natSkyBright-log10(extinctionCoeff)/(0.4);
42 % totalBright = log(10^(-0.4*receiver.artSkyBright) + ...
43 %     10^(-0.4*correctedNatSkyBright))/log(10^(-0.4));
44 %FOV area in arcsec^2
45 FOVarea = pi*(receiver.FOV*206264)^2;
46 %telescope area in cm^2
47 telescopeArea = pi*receiver.telescopeRadius^2;
48
49 backgroundCounts = FOVarea*telescopeArea*receiver.setupEfficiency*...
50     receiver.filterBandpass*(refCountsAtWav*10^(-0.4*correctedNatSkyBright) ...
          + ...
51     refCountsVband*10^(-0.4*receiver.artSkyBright));
52
53 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
54 % Since the apparent magnitude is a relative measure, one needs the
55 % photon flux at a certain magnitude to compute the photon flux at a
```

```
% different magnitude.
% This function takes in a wavelength (in nm), determines which
% astronomical band it is closest to, and then output the number of
% reference counts (in ph cm-2 s-1 nm-1) at 0 magnitude.
function refCounts = obtainReferenceCount(wavelength)

%Data format: Wavelength, ΔWavelength, reference number of counts
data = [360     40      7650; ...
        440     80      14845; ...
        550     90      10386; ...
        640     150     5801; ...
        790     150     3883; ...
        1260    200     1954; ...
        1600    370     1015; ...
        2220    500     447; ...
        3400    700     139; ...
        5000    1200    53];

numData = size(data, 1);

%first if the wavelengh is less than what the data gives approximates ...
    it to
%the first band
if (wavelength < data(1,1))
    refCounts = data(1, 3);
    return;
elseif (wavelength > data(numData,1))
    refCounts = data(numData, 3);
    return;
end

foundBand = false;
ind = 1;
%find which astronomical band the wavelength is closed to
while (foundBand == false)
    currUpBound = data(ind, 1) + data(ind, 2);
    nextLowBound = data(ind+1, 1) - data(ind+1, 2);

    %check if the wavelength is between two bands
    if (wavelength  ≥ data(ind, 1) && wavelength ≤ data(ind+1, 1))
        %wavelength closer to next band center
        if (abs(wavelength-data(ind, 1)) > abs(wavelength-data(ind+1, ...
            1)))
            closerInd = ind + 1;
```

```
98              %should go to upper band but first make sure it is within
99              %ΔWavelength
100             if (wavelength  < nextLowBound)
101                 if (wavelength ≤ currUpBound) %is it within current band
102                     closerInd = ind;
103                 %if not it is closest to which band boundary?
104                 elseif (abs(wavelength-nextLowBound) > ...
105                         abs(wavelength-currUpBound))
106                     closerInd = ind;
107                 end
108             end
109         else %closer to current band
110             closerInd = ind;
111             % make sure it is within ΔWavelength
112             if (wavelength  > currUpBound)
113                 if (wavelength ≥ nextLowBound) %is it within next band
114                     closerInd = ind + 1;
115                 %if not it is closest to which band boundary?
116                 elseif (abs(wavelength-nextLowBound) < ...
117                         abs(wavelength-currUpBound))
118                     closerInd = ind + 1;
119                 end
120             end
121         end
122
123         foundBand = true;
124     end
125
126     ind = ind+1;
127 end
128
129 refCounts = data(closerInd, 3);
```

B.2 Uplink background code

```
1 clear;
2 Detector_number=4;      %Number of detectors used at the receiver ...
     (typically 4 for QKD)
3 %%Note: some experiments require a different number of detectors.
4 D_dark=Detector_number*20;      %Summed dark counts in all detectors ...
     per seconds.
```

```
5
6  %%%%%Main parameter inputs (in SI)
7  dorbit=600e3;       %Orbit distance from the Earth
8  FOV=50e-6;      %Field of View of the receiver
9  lambda=785e-9;      %Wavelenght
10 Raperture=0.3;      %Diameter of the ground telescope
11 Filter=1e-9;        %Bandwidth of the filter
12 StarBright=23.5;         %Starlight contribution in magnitude (23.5 ...
       for starlight+airglow, 24.5 for only starlight)
13 detector=[0.59];        %Detector efficiency
14 optical_components=0.5;     %Loss from the optical components (3dB)
15 latitude=45.31;     %Latitude coordinate of the used location (20km ...
       outside of Ottawa)
16 longitude=-75.5;        %Longitude coordinate of the used location ...
       (20km outside of Ottawa)
17 moon_phase=0.5;     %Phase of the moon
18 moonElevation=45;       %Elevation angle of the moon from zenith
19 earthAlbedo=0.3;        %Earth albedo ate the ground station (the ...
       average Earth albedo is 0.3)
20
21 %%%%%%%loading the atmospheric transmittance: the file contains a 2D ...
       matrix of atmospheric transmittance (named atmosphere in the file) ...
       as a function of wavelength and angle. The file also contains a ...
       vector of the wavelength (named ALambda).
22 load (sprintf('atmosphere(rural-5km)'))
23 angleT=80:-1:0;     %By default the angle is not specified in the ...
       file. Change this line if using an updated file with a different ...
       angle vector.
24 %%This file is generated using MODTRAN.
25
26 trans=0;        %Transmittance as a function of angle for the chosen ...
       wavelength
27 dLambda=5e-9;       %Uncertainty in wavelenght
28 for i=(lambda-dLambda):5e-11:(lambda+dLambda)
29     trans=trans+interp1(Alambda*1e-6,atmosphere,i)/(1+2*dLambda/5e-11); ...
               %Transmittance vs angle including uncertainty
30 end
31 %%Alternatively, trans can be manually specified
32
33 %%%%%%%loading the orbit data: the file contains vectors for range ...
       (distance between the ground and the satellite), elevation ...
       (elevation angle of the satellite from the horizon) and azimuth angle.
34 load (sprintf('Ranges_ottawa-d=%gkm',dorbit/1000),'range','elevation',...
35     'azimuth')
```

```
%%This file is generated using STK from AGI.
%%Alternatively, each vectors can be manually specified or the ...
    elevation vector alone can be specified and range calculated by ...
    giving the orbit altitude in sat.heightSat (see below)

 for i=1:numel(elevation)

sat = struct('FOV', FOV, 'rot', azimuth(i), 'elev', ...
    elevation(i)*pi/180, 'latitude', latitude, ...
'longitude', longitude, 'wavelength',lambda*1e9, 'telescopeRadius', ...
    100,...
'filterBandpass', Filter*1e-9, 'earthAlbedo', earthAlbedo, ...
    'moonIlluminated', moon_phase,...
'setupEfficiency',detector(k)*optical_components, 'moonElevation', ...
    moonElevation,'trans', trans);
%%Note: the speceified telescopeRadius in 100 (1m) to save ...
    calculation time, a correction to the actual receiver size is done ...
    after the initial calculation. This is especially useful when ...
    evaluating different receiver diameter by adding an extra ...
    for(Rapperture=[input desired values in this vector]) around the ...
    correction.

%Choose a method to specify the altitude of the satellite
%sat.heightSat = dorbit;        %Orbit altitude, must be specified if ...
    range is not
sat.distanceFromGrndStn = range(i)/1000;        %distance from ground ...
    to satellite (more accurate with the orbit analysis)


imgInfo='C:\Users...\images\world_avg.tif\world_avg_dat.tif';       ...
    %Loads the image of the artificial background light
%%Important: you must have this file on your computer and specify the ...
    complete path.

%%%%%background counts using modified version of Bassam's code
[backgroundCountsUp_temp(i), additionalInfo] = ...
    calcBackgroundCnts(sat, imgInfo);

%%%%%Extra fuction calculation the background contribution from ...
    starlight and airglow. The contribution in only relevant when all ...
    other contributions are very small. contributes around ...
    4photons/s/nm/cm/mrad^2, meaning a 30cm receiver with a 50microrad ...
    field of view and 1nm filter would see around 0.3photons/s.
```

```
receiver = struct('FOV', FOV, 'wavelength', lambda, ...
    'telescopeRadius', 100, ...
'filterBandpass', filter*1e9, 'setupEfficiency', ...
    detector*optical_components,...
'StarBright', StarBright, 'observElevation', 90-theta(i));

backgroundCountsUp_temp(i)=backgroundCountsUp_temp(i)+UplinkStarBackground(receiver);
      %in photon/sec

%%%%%Correction to the actual receiver size
%%This is where one would start a for(Rapperture=[input desired ...
    values in this vector]) loop

cosTerm = (dist*cos(angle*pi/180));
    height_sat = (-R+sqrt(R^2+dist^2+2*R*cosTerm)); %based on cosine law

    solid_angle_ratio=2*pi*((sqrt(Raperture^2+height_sat^2)...
    -height_sat)/sqrt(Raperture^2+height_sat^2));       %ratio of the ...
        solid angle with the actual Raperture compared to a ...
        telescopeRadius of 1m

    backgroundCountsUp(m)=backgroundCountsUp_temp(i)*solid_angle_ratio...
    +D_dark;        %corrected background count

%%End of a for(Rapperture=[input desired values in this vector] loop

end
```

```
%Description:
%calcBackgroundCnts calculates the estimated number of background ...
    counts a
%satellite will receive per second.
%Input:
%   1. sat(strucutre): The satellite's parameters are entered in sat
%      The required entries in the structure are:
%           The following 8 arguments parameterize the receiver
%           a) 'FOV': The field of view of the receiver (in rad).
%           b) 'wavelength': The wavelength photons are emitted at.
%           c) 'telescopeRadius': The receiver's radius in cm.
%           d) 'filterBandpass': approximately the area under of the ...
    curve
%               of the receiver's filter bandwith (in nm).
%           e) 'setupEfficiency': the optical efficiency of the setup
```

```
14 %                multiplied by the detector efficiency (format 0.a).
15 %           The following two parameters fix the ground station's ...
   location:
16 %           f) 'latitude': The latitude of the ground station's location
17 %               (in degrees).
18 %           g) 'longitude': The longitude of the ground station's ...
   location
19 %               (in degrees).
20 %           The following 3 parameters fix the satellite's position:
21 %           You have two options in specifying the altitude of the
22 %           satellite:
23 %           h1) 'distanceFromGrndStn': The distance of the satellite from
24 %           the ground station in km.
25 %           If distanceFromGrndStn is not specified then you have to ...
   input:
26 %           h1) 'heightSat': The satellite's orbit is assumed to be a ...
   circle
27 %               and (heightSat+radiusEarth) is the radius of the ...
   orbit (in
28 %               km).
29 %           The meaning of the next two parameters is:
30 %           Imagine that the axis connecting, the center of the
31 %           earth and the ground station, is the z axis. In addition, the
32 %           ground station is the origin. The line tangent to earth and
33 %           that lies on the plane defined by the constant longitude ...
   circle
34 %           'longitude' (and that points south) is the x axis. We now ...
   have a
35 %           coordinate system. As in a spherical coordinate system, ...
   let the
36 %           inclination angle be the angle from the z axis and let the
37 %           azimuthal angle be the angle from the x axis. Then 'elev' is
38 %           the inclination (elevation) angle and 'rot' the azimuthal
39 %           angle. An alternative way of obtaining the x, y, z axes ...
   is to
40 %           start with a normal earth coordinate system: z is (0 0 ...
   1), y (0
41 %           1 0), x is (1 0 0). Next using the rotation matrices rotate
42 %           each axis first by (90-lat) around the y axis and then ...
   long around
43 %           the z axis. (lat, long) are the the latitude and ...
   longitude of
44 %           the ground stations. In fact, the above rotations would ...
   (0 0
```

```
45 %           radius earth) to the coordinates of the ground station.
46 %           i) 'elev': See description above (in rad) from the horizon
47 %           j) 'rot': See description above (in rad)
48 %           Other parameters:
49 %           k) 'earthAlbedo': quantifies how strongly the surface ...
       near the
50 %               ground station reflects light (format: 0.a).
51 %           l) 'moonIlluminated': The proportion of the moon that is
52 %               illuminated (format: 0.a).
53 %           m) 'moonElevation': The angle the moon is at as measured from
54 %               the zenith (i.e. looking up) (in degrees)
55 %    2. imgInfo (structure or filename): If a filename then the path of
56 %       the image that can be downloaded from
57 %       http://www.ngdc.noaa.gov/dmsp/download_rad_cal_96-97.html ...
       (the high
58 %       resolution image is expected.
59 %       As a structure here is what is expected:
60 %       a) 'R': The referencing matrix of the image.
61 %       b) 'imgFilename': The path of the image containing the data
62 %       c) 'heightImg': The height of the image
63 %       d) 'widthImg': The width of the image
64 %
65 %Output:
66 %    1. backgroundCounts: The estimated number of background counts ...
       that are
67 %       detected by the receiver. (photons/s)
68 %    The next 4 outputs are useful for plotting:
69 %    2. additionalInfo (structure) Contains additional information ...
       about the
70 %       background counts. The fields of the structure are:
71 %       a) 'fluxlessCtns': Background counts emitted due to human
72 %       activities divided by the photon flux of light emitted by ...
       man. The
73 %       units are cm^2*arcsec^2*um (so you have to provide the flux in
74 %       ph/cm^2/arcsec^2/um)
75 %       b) 'albedolessCnts': Background counts due to the moon ...
       divided by
76 %       the earth's albedo.
77 %    3. X (m*n matrix): nightime lights emitted by humans data.
78 %    4. R (3*2 matrix): Referencing matrix for X
79 %    5. intersLine2D (m*2 matrix;): Points in (longitude, latitude) format
80 %       that lie on the boundary of the intersection of the surface ...
       of the
81 %       earth with the satellite's FOV cone.
```

```
82
83 function [backgroundCounts, additionalInfo, X, R, intersLine2D] = ...
84     calcBackgroundCnts(sat, imgInfo)
85
86 radiusEarth = 6371; %useful constant
87
88 if (isfield(imgInfo, 'widthImg')) %we have a structure input
89     R = imgInfo.R;
90     imgFilename = imgInfo.imgFilename;
91     heightImg = imgInfo.heightImg;
92     widthImg = imgInfo.widthImg;
93 else
94     %We have a string filename input and so the image is the high res pic
95     %from http://www.ngdc.noaa.gov/dmsp/download_rad_cal_96-97.html
96     R = ...
          [0,-0.00832999963313300;0.00832999963313300,0;-180.004164999817,...
97     90.0041649998166];
98     heightImg = 21600;
99     widthImg = 43200;
100    imgFilename = imgInfo;
101 end
102
103 %If distanceFromGrndStn is specified convert it to height Sat
104 if (isfield(sat, 'distanceFromGrndStn') && (sat.distanceFromGrndStn ≥0))
105    cosTerm = (sat.distanceFromGrndStn*cos(pi/2-sat.elev));
106    sat.heightSat = (-radiusEarth  + ...
          sqrt(radiusEarth^2+sat.distanceFromGrndStn^2+...
107    +2*radiusEarth*cosTerm)); %based on cosine law
108 end
109
110 %there are a lot of numerical computations. INTERSECT_ACCURACY indicates
111 %the allowed error of the numerical computations. Most of the ...
       computations
112 %involves finding the longitude of points with a certain latitude and ...
       that
113 %lie on the boundary of the intersection surface.
114 global INTERSECT_ACCURACY
115 %take the case of satellite with 0 elevation as an estimate of the ...
       size of
116 %the intersection surface. At 0 elecation, the surface has a circle ...
       for its
117 %boundary.
118 approxSurfaceRadius = sat.FOV*sat.heightSat;
119 %convert to latitude range
```

```
120 circEarth = 2*pi*radiusEarth;
121 latitudeRange = approxSurfaceRadius/circEarth*360;
122 INTERSECT_ACCURACY = latitudeRange*1e-3;
123
124 additionalInfo = struct('heightSat', sat.heightSat, 'wavelength', ...
        sat.wavelength, ...
125     'elev', sat.elev);
126
127 %First obtain the number of background counts because of nightime lights
128 %emitted by human activities
129 if (sat.heightSat > 0) %heightSat is an optional parameter
130     %Let S be the surface of intersection of the satellite FOV cone ...
            and earth.
131     %Find points on the boundary of S (intersLine2D) and the area of S.
132     [intersLine2D, areaFOV] = intersectionSurfaceInfo(sat);
133     areaFOV = areaFOV*(1e3)^2; %convert from km^2 to m^2
134
135     additionalInfo.areaFOV = areaFOV;
136
137     % obtain the solid angle from which the telescope on the ...
            satellite can
138     %be seen from Earth; note that the telescope radius is in cm.
139     heightSatInM = sat.heightSat*1e3; %heightSat in meters
140     solidAngle = 1; ...
            %%%%%2*pi*(1-heightSatInM/sqrt((sat.telescopeRadius*1e-2)^2 + ...
            heightSatInM^2));
141
142     %extract a portion of the image so as not to deal with very large
143     %images.
144     distanceFactor = 3;
145     maxDistFromLong = distanceFactor*max(abs(intersLine2D(:, 1) - ...
            sat.longitude));
146     maxDistFromLat = distanceFactor*max(abs(intersLine2D(:, 2) - ...
            sat.latitude));
147     %X contains the subimg data and R is the referecing matrix for R
148     [X, R] = extractSubImg(sat.latitude, sat.longitude, R, ...
            abs(maxDistFromLat), ...
149         abs(maxDistFromLong), imgFilename, heightImg, widthImg);
150
151     %finally obtain the average flux emitted by S. The flux is in ...
            ph/cm^2/s/sr/um
152     avgFlux = obtainAvgFlux(X, R, intersLine2D, sat);
153
154     additionalInfo.artFlux = avgFlux;
```

```
155
156     %The counts from lights emitted by human activities
157     fluxlessCtns = (areaFOV*1e4)*solidAngle*sat.filterBandpass/1000;
158     nightimeCnts = avgFlux*fluxlessCtns; %convert area FOV to cm^2
159 else
160     %extract a portion of the image so as not to deal with very large
161     %images.
162     %want 6 pixels
163     lonDist = 6*abs(R(1,2)); latDist = 6*abs(R(2,1));
164     [X, R] = extractSubImg(sat.latitude, sat.longitude, R, latDist, ...
            lonDist, ...
165          imgFilename, heightImg, widthImg);
166     %Obtain the pixel coordinates of the uplink location
167     [centerLat, centerLong] = latlon2pixs(R, sat.latitude, ...
            sat.longitude);
168
169     %obtain the nightime lights photon flux emitted at the location ...
            of the
170     %ground station. The flux is in ph/cm^2/s/sr/um
171     flux = obtainFlux(X(sCeil(centerLat), sCeil(centerLong)), ...
            sat.wavelength);
172
173     %simplified from the 'nightimeCnts = flux*areaFOV*solidAngle;'
174     %expression above. We use small angle approximation on solidAngle
175     fluxlessCtns = ...
            pi*sat.FOV^2*pi*sat.telescopeRadius^2*sat.filterBandpass/1000;
176     nightimeCnts = flux*fluxlessCtns;
177 end
178 transStruct = struct('wavelength', sat.wavelength, 'angle', ...
        0,'trans', sat.trans);
179 extinctionCoefficient0 = getTransmission(transStruct);
180 transStruct = struct('wavelength', sat.wavelength, 'angle', ...
        90-sat.elev*180/pi,'trans', sat.trans);
181 extinctionCoefficientElev = getTransmission(transStruct);
182 nightimeCnts = nightimeCnts * ...
        extinctionCoefficientElev/extinctionCoefficient0;
183
184 %obtain the background counts due to the moon
185 avgSunTemperature = 5778; %in K
186 planckH = 6.626e-34; %m^2*kg/s;
187 speedLight = 3e8; %m/s
188 boltzmannConstant = 1.381e-23; %m^2*kg*s^-2*K^-1
189 radiusSun = 6.955e8; %in m
190 earthSunDistance = 1.496e11; %in m
```

```
191 solarIrradiance = ...
       2*speedLight/(sat.wavelength*1e-9)^4/(exp(planckH*speedLight/ ...
192      (sat.wavelength*1e-9*boltzmannConstant*avgSunTemperature))-1);
193 solarIrradiance = solarIrradiance/earthSunDistance^2*pi*radiusSun^2/1e9;
194 % solarIrradiance = 4.61e18; %ph/s/nm/m^2 at one astronomical unit
195 solarIrradiance = solarIrradiance/(1e2)^2; %convert to ph/s/nm/cm^2
196 %From Bonato et al., 2009, New J. Phys. 11 045017; with FOV instead ...
       of IFOV
197 if (sat.heightSat > 0)
198     photonsDay = sat.earthAlbedo*solarIrradiance*(areaFOV*1e4)...
199     *solidAngle*sat.filterBandpass/pi;
200 else
201     photonsDay = sat.earthAlbedo*sat.telescopeRadius^2*pi*sat.FOV^2...
202     *solarIrradiance*sat.filterBandpass;
203 end
204 %multiply photonsDay by a constant alpha that quantifies the effect of
205 %sunlight not directly reaching earth but getting first reflected by the
206 %moon.
207 albedoMoon = 0.12;
208 moonRadius = 1737.1; %mean radius in km
209 earthMoonDistance = 384405; %in km and an average
210 alpha = albedoMoon*(moonRadius/earthMoonDistance)^2;
211 photonsNight = alpha*photonsDay; %Bonato et al., 2009, New J. Phys. ...
       11 045017
212 %now add the partial effect of the moon
213 %Below is an approximation of the effect of the proportion of the ...
       moon that
214 %is illuminated on the brightness of the moon. The below formula is based
215 %on data from the references listed in the next paragraph. The ...
       formula was
216 %found using the data and Matlab's cftool (R^2 ¬ 0.9997 which is good ...
       enough
217 %since the data is not perfectly accurate anyway.). Finally, note ...
       that the
218 %data is most accurate for the V astronomical band.
219 %Unofficial reference: http://www.asterism.org/tutorials/tut26-1.htm;
220 %Reference:"Astrophysics of the Solar System" By K D Abbhyankar; sec. 6.3
221 aF =      -15; %F for fitted coefficient
222 bF =       0.2774;
223 cF =       15;
224 magnitudeIncrease = aF*sat.moonIlluminated^bF+cF;
225 photonsNight = photonsNight/2.512^magnitudeIncrease;
226 if (sat.moonIlluminated == 0)    photonsNight = 0; end
227 %now correct for atmospheric extinction of moonlight. The data above
```

```
%assumes that the moon's elevation angle is 0 degrees.
%first calculate the extinction at 0 degrees
transStruct = struct('wavelength', sat.wavelength, 'angle', ...
    sat.moonElevation,'trans', sat.trans);
extinctionCoefficient = getTransmission(transStruct);
photonsNight = photonsNight*extinctionCoefficient/extinctionCoefficient0;
%the reflected moonlight passes through the atmosphere again to reach the
%satellite. The extinction coefficient will be calculated with the
%satellite's elevation angle
photonsNight = photonsNight * extinctionCoefficientElev;

%blackbody radiation background counts
avgTemperature = 293; %in K
N0 = 2*speedLight/(sat.wavelength*1e-9)^4/(exp(planckH*speedLight/ ...
    (sat.wavelength*1e-9*boltzmannConstant*avgTemperature))-1); %in ...
        ph/s/nm/m^2/sr
if (sat.heightSat > 0)
    radiationCounts = N0*areaFOV*solidAngle*sat.filterBandpass;
else
    radiationCounts = ...
        N0*sat.FOV^2*pi^2*(sat.telescopeRadius*1e-2)^2*sat.filterBandpass;
end

%nightimeCnts can be 0 because the ground station location is not ...
    light polluted
if (nightimeCnts == 0)
    backgroundCounts = photonsNight + radiationCounts;
else
    %the light detected from the geotiff of nightime lights already
    %contains blackbody radiation counts
    backgroundCounts = nightimeCnts + photonsNight;
end

%finally take into account the setup efficiency
backgroundCounts = sat.setupEfficiency*backgroundCounts;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%correctForSatRot corrects for the satellite's rotation angle.
%It applies the correct rotation to a location with latitude lat and
%longitude lon. The rotation is around the axis connecting the center of
%the earth and the ground station.
% Input:
%   1. sat (structure): Contains the satellite's information
%   2-3. (lat, lon): The latitude and longitude of some location
```

```
% Output:
%   (rotLat, rotLon): The original rotation rotated
function [rotLat, rotLon] = correctForSatRot(sat, lat, lon)

%The ground station in x,y,z coordinates
locInt = convertEarthCoord(sat.latitude, sat.longitude);

%rotation matrices that take the ground station from (0, 0, 1) to (lat,
%lon)
rotLatM = rotMatrix([0 1 0], pi/2-convertRadians(sat.latitude)); %b|c ...
    (0 0 1) has lat of 90
rotLongM = rotMatrix([0 0 1], convertRadians(sat.longitude));

locationCoord = convertEarthCoord(lat, lon);
%do a rotation with axis rotLongM*rotLatM*[0 0 1]' and center
%locInt
locationCoord = locationCoord-locInt;
rotMtemp = rotMatrix((rotLongM*rotLatM*[0 0 1]')', sat.rot);
locationCoord = rotMtemp*locationCoord';
locationCoord = locInt+locationCoord';

%convert back to (lat, lon) coordinates
[rotLon,rotLat,ignore] = cart2sph(locationCoord(1), locationCoord(2), ...
    locationCoord(3));
rotLat = rotLat*180/pi; %convert to degrees
rotLon = rotLon*180/pi;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Given a point with coordinates (lat, lon) determine if a closed ...
    surface is on
%the left of that point. The closed surface is the intersection of the
%satellite's FOV cone with earth.
%returns -1 if the point is on a boundary stable or unstable point ...
    meaning
%that nothing is to the left or right of the point.
function left = surfaceIsToTheLeft(lat, lon, satellite)

%add a small longitude and check whether the resulting point is ...
    inside the surface

global INTERSECT_ACCURACY;
ΔLon = INTERSECT_ACCURACY*5;
smallestDeltaLon = INTERSECT_ACCURACY/2; %the smallest longitude to ...
    be added
```

```
306 inside = false;
307 while (inside == false && ΔLon > smallestDeltaLon)
308     insideLeft = insideCone(satellite, lat, lon-ΔLon); %add to the left
309     if (insideLeft)
310         left = true;
311     end
312
313     insideRight = insideCone(satellite, lat, lon+ΔLon); %add to the right
314     if (insideRight)
315         left = false;
316     end
317
318     inside = or(insideRight, insideLeft);
319
320     ΔLon = ΔLon/1.5;
321 end
322
323 %most likely point is at a stable/unstable extremum
324 if (ΔLon ≤ smallestDeltaLon)
325     left = -1;
326 end
327
328 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
329 %given a point (lat, lon) on the boundary of the surface intersection of
330 %the FOV cone and earth, estimate the constant latitude=lat intersection
331 %with the boundary.
332 %The estimation is made using points on the boundary (bndryPoints).
333 %the point is inputted by providing its index in the bndryPoints array
334 %the array should be organized such that lon is first and then lat.
335 %sat contains the satellite information
336 function lonEstimate = obtainIntersectionLon(bndryPoints, pointIndex, ...
        sat)
337
338 %retrieve the point's coordinates
339 lon = bndryPoints(pointIndex, 1); lat = bndryPoints(pointIndex, 2);
340
341 %if the point is to the left of the surface need to find two other points
342 %to the right of surface. The points also have to be above and below lat.
343 pointIsLeft = surfaceIsToTheLeft(lat, lon, sat);
344
345 if (pointIsLeft == -1)
346     lonEstimate = lon; %constant lat line only intersects one point ...
            (lat, lon)
347     return;
```

```
348 end
349
350 oppositeSide = not(pointIsLeft);
351 %look for a point above lat and to opposite side of the point
352 foundPoint = false;
353 abovePoint = [0 0];
354 ind = 0;
355 while (foundPoint == false)
356     ind = ind+1;
357
358     index = max(1,  pointIndex-ind);
359     currentPoint = bndryPoints(index,:);
360
361     if (index == 1)
362         abovePoint = currentPoint; foundPoint = true;
363     else
364         isLeft = surfaceIsToTheLeft(currentPoint(2), currentPoint(1), ...
                sat);
365
366         if (isLeft == oppositeSide)
367             abovePoint = currentPoint;
368             foundPoint = true;
369         end
370     end
371 end
372
373 %look for a point below lat and to opposite side of the point
374 numPoints = size(bndryPoints, 1);
375 foundPoint = false;
376 belowPoint = [0 0];
377 ind = 0;
378 while (foundPoint == false)
379     ind = ind+1;
380
381     index = min(numPoints,  pointIndex+ind);
382     currentPoint = bndryPoints(index,:);
383
384     if (index == numPoints)
385         belowPoint = currentPoint; foundPoint = true;
386     else
387         isLeft = surfaceIsToTheLeft(currentPoint(2), currentPoint(1), ...
                sat);
388
389         if (isLeft == oppositeSide)
```

```
390             belowPoint = currentPoint;
391             foundPoint = true;
392         end
393     end
394 end
395 
396 %take care of the case that the above or below point has the same ...
       latitude as lat
397 if (abovePoint(2) == lat)
398     lonEstimate = abovePoint(1);
399 elseif (belowPoint(2) == lat)
400     lonEstimate = belowPoint(1);
401 else
402     %now perform linear interpolation
403     latDiff = abs(abovePoint(2)-belowPoint(2));
404     lonDiff = abovePoint(1)-belowPoint(1);
405     latDiffWithPoint = abs(abovePoint(2)-lat);
406     lonEstimate = abovePoint(1)+lonDiff*(latDiffWithPoint/latDiff);
407 end
408 
409 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
410 %obtainAvgFlux obtains the average flux emitted by a surface.
411 %Input:
412 %   1. X (m*n matrix): The image data.
413 %   2. R: X's referencing matrix.
414 %   3. intersLine2D: Points on the boundary of the surface
415 %   4. sat (structure): The satellite information
416 %Output:
417 %avgFlux: The average flux from the surface in ph/cm^2/s/sr/um
418 function avgFlux = obtainAvgFlux(X, R, intersLine2D, sat)
419 
420 radiusEarth = 6371; %useful constant
421 
422 intersLine2D = sortrows(intersLine2D,-2); %sort by latitude in ...
       decreasing order
423 %go through pixel by pixel and calculate the average emitted flux
424 avgFlux = 0;
425 totalPixelArea = 0;
426 %calculate the latitude, longitude limits
427 minLon = min(intersLine2D(:, 1));
428 maxLon = max(intersLine2D(:, 1));
429 minLat = min(intersLine2D(:, 2));
430 maxLat = max(intersLine2D(:, 2));
431 %convert to pixel coordinates
```

```
[minRow, minCol] = latlon2pixs(R, maxLat, minLon);
[maxRow, maxCol] = latlon2pixs(R, minLat, maxLon);
numPoints = size(intersLine2D, 1);
%the idea is to inspect all pixels in a box defined by minrow, maxrow,
%mincol and maxcol. The search is done row by row. The boundaries of each
%pixel are converted to latitude and longitude and compared to area
%segments extracted from intersLine2D. intersLine2D is sorted in latitude
%decreasing order, so as we traverse each row we do not have look ...
    into all
%of intersLine2D but only at a certain section of intersLine2D ...
    starting at
%intersLine2D.

%first calculate the area segments. This will a bit of extra memory but
%will speed up the computation.
%4 columns: latUp latDown lonLeftBndry lonRightBndry
% ------------- latUp
% ------------- latDown
areaSegments = zeros(numPoints-1, 4);
for ind = 1:1:numPoints-1
    %now obtain the boundaries of the area segement
    areaSegments(ind, 1) = intersLine2D(ind, 2); %latUp
    areaSegments(ind, 2) = intersLine2D(ind+1, 2); %latDown

    if (ind ~= numPoints-1)
        %now get the longitude boundaries of the area segment
        longBndry1 = intersLine2D(ind+1, 1);
        longBndry2 = obtainIntersectionLon(intersLine2D, ind+1, sat);

        areaSegments(ind, 3) = min(longBndry1, longBndry2); %lonLeftBndry
        areaSegments(ind, 4) = max(longBndry1, longBndry2); ...
            %lonRightBndry
    else
        %the last point does not have a good estimate for lonLeftBndry
        %and lonRightBndry so just use the previous ones
        areaSegments(ind, 3) = areaSegments(ind-1, 3);
        areaSegments(ind, 4) = areaSegments(ind-1, 4);
    end
end

startRowInd = 1; %will start looking in intersecLine2D from this index
for row = floor(minRow):1:sCeil(maxRow)
    %row latitude boundaries
    % ------------ upperRowLat
```

```
473     % ------------ lowerRowLat
474     [lowerRowLat, ignore] = pix2latlong(R,row,maxCol);
475     [upperRowLat, ignore] = pix2latlong(R,(row-1),maxCol);
476
477     %make sure we have the correct startRowInd
478     ind = startRowInd;
479     latLowBndry = areaSegments(ind ,2);
480     while (latLowBndry > upperRowLat) %b|c higher lat means lower pixel
481         ind = ind+1;
482         latLowBndry = areaSegments(ind ,2);
483     end
484     startRowInd = ind;
485
486     for col = floor(minCol):1:sCeil(maxCol)
487         %col longitude boundaries
488         [ignore, leftColLon] = pix2latlong(R,row,(col-1));
489         [ignore, rightColLon] = pix2latlong(R,row,col);
490
491         currentPixelArea = 0;
492         %now that we have the latitude and longitude boundaries of the
493         %sides of the pixels, estimate the area of intersection of the
494         %pixel and intersection surface.
495         %there will be some intersection of the area segment with the ...
               pixel
496         %as long as:
497         % ------------------------- area segment lower latitude boundary
498         % --------------------------  pixel lower latitude boundary
499         latLowBndry = intersLine2D(startRowInd+1, 2);
500         ind = startRowInd;
501         while (latLowBndry ≥ lowerRowLat && ind < numPoints)
502
503             %initialize
504             latUpBndry = areaSegments(ind ,1);
505             latLowBndry = areaSegments(ind ,2);
506             lonLeftBndry = areaSegments(ind ,3);
507             lonRightBndry = areaSegments(ind ,4);
508
509             %calculate the intersection of the area segment with the ...
                   pixel
510             latStart = min(latUpBndry, upperRowLat);
511             latEnd = max(latLowBndry, lowerRowLat);
512             %now for the left longitude
513             pixelLongDiff = abs(lonLeftBndry-lonRightBndry);
514             distToTheRight = abs(leftColLon-lonRightBndry);
```

```
515             distToTheLeft = abs(leftColLon-lonLeftBndry);
516             if (distToTheRight ≤ pixelLongDiff && distToTheLeft ≤ ...
                    pixelLongDiff)
517                 latRightItrsc = leftColLon;
518             elseif(distToTheRight > distToTheLeft)
519                 latRightItrsc = lonLeftBndry;
520             else
521                 latRightItrsc = lonRightBndry;
522             end
523             %now for the right longitude
524             distToTheRight = abs(rightColLon-lonRightBndry);
525             distToTheLeft = abs(rightColLon-lonLeftBndry);
526             if (distToTheRight ≤ pixelLongDiff && distToTheLeft ≤ ...
                    pixelLongDiff)
527                 latLeftItrsc = rightColLon;
528             elseif(distToTheRight > distToTheLeft)
529                 latLeftItrsc = lonLeftBndry;
530             else
531                 latLeftItrsc = lonRightBndry;
532             end
533
534             %calculate the intersection area
535             ΔLon = abs(latRightItrsc-latLeftItrsc);
536             area = lonLatArea(latStart, latEnd, ΔLon, radiusEarth);
537             currentPixelArea = currentPixelArea+area;
538
539             %proceed to the next area segment
540             ind = ind+1;
541         end
542
543         flux = obtainFlux(X(row, col), sat.wavelength);
544         avgFlux = avgFlux+currentPixelArea*flux;
545         totalPixelArea = totalPixelArea+currentPixelArea;
546     end
547
548     if (ind≠startRowInd)
549         startRowInd = ind-1;
550     end
551 end
552 avgFlux = avgFlux/totalPixelArea;
553
554 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
555 % intersectionSurfaceInfo returns informations about the surface of
556 % intersection of the satellite's FOV cone and earth.
```

```
% Input:
%   sat (structure): The satellite information
% Output:
%   1. intrscPoints (m*2): Points that lie on the boundary of the ...
    intersection
%   surface. The format is (lon, lat)
%   2. surfaceArea: The area of the surface in km^2
function [intrscPoints, surfaceArea] = intersectionSurfaceInfo(sat)

radiusEarth = 6371; %useful constant

%find the intersection surface boundary by going latitude by latitude and
%using constant longitude lines. We check where these lines intersect the
%intersection surface.
numSteps = 50;
%sat0rot has the same data as satellite but rot is equal to 0
sat0rot = sat; sat0rot.rot = 0;
latUpBound = getLatUpBound(sat0rot, sat.latitude, sat.longitude);
latLowBound = getLatLowBound(sat0rot, sat.latitude, sat.longitude);
ΔLat = (latUpBound-latLowBound)/numSteps;
latitudeIntersects = zeros(numSteps+1, 1);
intrscPoints = zeros(2*numSteps, 2);

%first add the boundary points
latitudeIntersects(1) = sat.longitude;
latitudeIntersects(numSteps+1) = sat.longitude;
latUseDown = latLowBound; latUseUp = latUpBound;
lonLowIntrsct = sat.longitude; lonUpIntrsct = sat.longitude;
if (sat.rot ≠ 0)
    [latUseDown, lonLowIntrsct] = correctForSatRot(sat, latLowBound, ...
        sat.longitude);
    [latUseUp, lonUpIntrsct] = correctForSatRot(sat, latUpBound, ...
        sat.longitude);
end
intrscPoints(1, :) = [lonLowIntrsct latUseDown];
intrscPoints(2*numSteps, :) = [lonUpIntrsct latUseUp];

%add the remaining points
ind = 2;
for lat = latLowBound+ΔLat:ΔLat:latUpBound-ΔLat,

    %we can guess what the longitude will be
    indLat = round((lat-latLowBound)/ΔLat)+1; %the current index to ...
        be used
```

```
597     if (indLat == 2)
598         guess = latitudeIntersects(indLat-1)-sat.longitude;
599         lonUpIntrsct = getLongUpBound(sat0rot, lat, sat.longitude, ...
                guess);
600     else
601         %check if the function is now decreasing, for example if we ...
                have a
602         %circle intersection then the longitude increases at first ...
                but then
603         %decreases
604         increasing = insideCone(sat0rot, lat, ...
                latitudeIntersects(indLat-1));
605         diffLong = ...
                abs(latitudeIntersects(indLat-2)-latitudeIntersects(indLat-1));
606         longInitial = latitudeIntersects(indLat-1);
607         if (increasing == false)
608             lonUpIntrsct = getLongLowBound(sat0rot, lat, longInitial, ...
609                 diffLong);
610         else
611             lonUpIntrsct = getLongUpBound(sat0rot, lat, longInitial, ...
612                 diffLong);
613         end
614     end
615     %can reduce computation time by not finding the below value. By ...
            symmetry
616     lonLowIntrsct = sat.longitude - abs(lonUpIntrsct-sat.longitude);
617
618     latitudeIntersects(indLat) = lonUpIntrsct;
619
620     %if the satellite has a rotation angle then need to correct for it
621     if (sat.rot ~= 0)
622         [latUseUp, lonUpIntrsct] = correctForSatRot(sat, lat, ...
                lonUpIntrsct);
623         [latUseDown, lonLowIntrsct] = correctForSatRot(sat, lat, ...
                lonLowIntrsct);
624     else
625         latUseUp = lat; latUseDown = lat;
626     end
627     intrscPoints(ind, :) = [lonUpIntrsct latUseUp];
628     intrscPoints(ind+1, :) = [lonLowIntrsct latUseDown];
629
630     ind = ind+2;
631 end
632
```

```
633 %now estimate the area of the intersection surface
634 surfaceArea = 0;
635 for ind = 1:1:(size(latitudeIntersects, 1)-1)
636     latStart = latLowBound+(ind-1)*ΔLat;
637     latEnd = latLowBound+ind*ΔLat;
638 
639     minDeltaLon = min(abs(latitudeIntersects(ind)-sat.longitude), ...
640         abs(latitudeIntersects(ind+1)-sat.longitude));
641 
642     surfaceArea = surfaceArea + lonLatArea(latStart, latEnd, ...
            minDeltaLon, radiusEarth);
643     %add the area of right triangle with height ΔLat and width ΔLon
644     ΔLon = abs(latitudeIntersects(ind+1)-latitudeIntersects(ind));
645     surfaceArea = surfaceArea + lonLatArea(latStart, latEnd, ΔLon, ...
            radiusEarth)/2;
646 end
647 surfaceArea = 2*surfaceArea; %in km^2
648 
649 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
650 % insideCone determines if a point is inside the surface of ...
        intersection of
651 % the satellite's FOV cone with the surface of the earth.
652 % Input:
653 %    (lat, lon): Specify the location of the point in (latitude, ...
        longitude)
654 %        coordinates.
655 %    sat (structure): Contains the satellite's information
656 function insideCone = insideCone(sat, lat, lon)
657 
658 radiusEarth = 6371; %useful constant
659 
660 %We will work in a coordinate system where the origin is the location of
661 %interest and the axis of the cone is the z axis.
662 %below is the transformation that takes the axis cone to the appropriate
663 %one (step1 is adding a vector so cone axis is of an appropriate length)
664 %step2: elevation rotation
665 step2ElevM = rotMatrix([0 1 0], (pi/2-sat.elev));
666 %step3: rotation transformation
667 step3RotM = rotMatrix([0 0 1], sat.rot);
668 
669 coordPoint = convertEarthCoord(lat, lon);
670 %apply the necessary transformations to bring it near the the ...
        location of
671 %interest
```

```
672 rotLatM1 = rotMatrix([0 1 0], pi/2-convertRadians(sat.latitude)); ...
      %b|c (0 0 1) has lat of 90
673 rotLongM2 = rotMatrix([0 0 1], convertRadians(sat.longitude));
674 %first apply the the rotations that took the location of
675 %interest to [0 0 0]. The inverse of a rotation is its transpose.
676 coordPoint = rotLatM1'*rotLongM2'*coordPoint';
677 coordPoint = coordPoint -[0 0 radiusEarth]';
678 %then apply the inverse of the transformations that made the axis of the
679 %cone the z axis
680 coordPoint = step2ElevM'*step3RotM'*coordPoint;
681
682 lengthAxis = getLocationSatelliteDistance(sat);
683 %equation of a cone whose vertex is the origin and axis the z axis
684 uprightConeEqu = coordPoint(1).^2+coordPoint(2).^2 - ...
685     tan(sat.FOV)^2*(coordPoint(3)-lengthAxis).^2;
686 %note that inside the cone the coneequ will be say negative and ...
      outside the
687 %opposite sign. This is because of the equation of the cone:
688 %cos(FOV)=((x,y,z).coneAxis/length((x,y,z))).
689 if (uprightConeEqu > 0) insideCone = false; return; end
690
691 intersectEarth = false;
692 %now check if the the point emits light that will intersect earth twice
693 centerCoord = step2ElevM'*step3RotM'*[0 0 -radiusEarth]'; centerCoord ...
      = centerCoord';
694 %check if the line connecting the vertex of the cone and the current
695 %location intersects earth twice
696 vertexCoord = [0 0 lengthAxis];
697 v = coordPoint'-vertexCoord;
698 twoCoeff = norm(v)^2;
699 oneCoeff = 2*(Dot(v, vertexCoord)-Dot(centerCoord, v));
700 zeroCoeff = norm(centerCoord)^2+norm(vertexCoord)^2 - radiusEarth^2 - ...
      2*Dot(centerCoord, vertexCoord);
701 discriminant = oneCoeff^2-4*zeroCoeff*twoCoeff;
702
703 if (discriminant < 0 )
704     intersectEarth = true;
705 elseif (discriminant > 0)
706     sol1 =  (-oneCoeff+sqrt(discriminant))/(2*twoCoeff);
707     point1 = vertexCoord+v*sol1;
708     sol2 =  (-oneCoeff-sqrt(discriminant))/(2*twoCoeff);
709     point2 = vertexCoord+v*sol2;
710
711     %sol2 should be smaller and we expect coordPoint to be close to it,
```

```
712     %i.e. we expect it to be the closer solution to the satellite
713     if (norm(coordPoint'-point2) > norm(coordPoint'-point1))
714         intersectEarth = true;
715     end
716 end
717
718 if (discriminant == 0 || (uprightConeEqu <= 0 && intersectEarth == false))
719     insideCone = true;
720 else
721     insideCone = false;
722 end
723
724 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
725 %get the distance between the location of interest and the satellite.
726 %Input:
727 %   sat(structure): Contains information about the satellite
728 %Output:
729 %   locationSatelliteDistance: The distance in km.
730 function locationSatelliteDistance = getLocationSatelliteDistance(sat)
731
732 radiusEarth = 6371; %useful constant
733
734 locationSatelliteDistance = sqrt(sat.heightSat^2 + ...
735     2*radiusEarth*sat.heightSat + ...
736     -2*radiusEarth*sat.heightSat*cos(pi/2-sat.elev)); %law of cosines
737
738 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
739 %return the rotation matrix with axis [x y z] and angle theta
740 function rotM = rotMatrix(axis, theta)
741
742 iden = eye(3);
743 P = axis'*axis;
744 Q = [0 -axis(3) axis(2); axis(3) 0, -axis(1); -axis(2) axis(1) 0];
745 rotM = P + (iden - P)*cos(theta) + Q*sin(theta);
746
747 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
748 %convertEarthCoord converts to (x, y, z) coordinates with the earth's
749 %center as the origin.
750 %Input:
751 %   lat and lon in degrees
752 %Output:
753 %   [x y z] where each coordinate is in km
754 function earthPoint = convertEarthCoord(lat, lon)
755
```

```
radiusEarth = 6371; %useful constant

incAngle = pi/2-convertRadians(lat);
azimAngle = convertRadians(lon);
earthPoint = radiusEarth * ...
    [sin(incAngle)*cos(azimAngle) sin(incAngle)*sin(azimAngle) ...
       cos(incAngle)];

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%lonLatArea calculates the area of a segment that starts at latStart ...
    (latitude
% start) and ends at latEnd (the end latitude). ΔLon (Δ longitude)
% is the height of the segment.
%We can think of this as a rectangle of width latitude and height ΔLon
%in spherical coordinates (that is why we need the radius).
function area = lonLatArea(latStart, latEnd, ΔLon, radius)

%convert to appropriate spherical coordinates
start = 90-latStart; endL = 90-latEnd;

%This is basically an integration in spherical coordinates.
area = abs(convertRadians(ΔLon) * ...
    (cos(convertRadians(start))-cos(convertRadians(endL)))*radius^2);

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%getLongUpBound gets the longitude intersection of a constant ...
    latitude=lat
%line with the boundary of intersection of the satellite's FOV cone ...
    and the
%surface of the earth. The search begins at (lat, lon) and proceeds ...
    to the
%right.
%Input:
%   1. satellite (structure): Contains the satellite's information
%   2-3. (lat, lon): the search begins at this location
%   4. guess: A guess starting point of how far away from (lat, lon) ...
    should
%       the search begin
function upBoundLong = getLongUpBound(satellite, lat, lon, guess)
%estimate what the longitude boundary would be with a binary search
global INTERSECT_ACCURACY;
if (nargin < 4 || guess == 0) guess = INTERSECT_ACCURACY*1e2; end
upBound = guess; lowBound = 0;

```

```
%The search should stop when we have two points very close to each other,
%and such that one point is inside the cone and the other is not.
valid = xor(insideCone(satellite, lat, lon+upBound), ...
    insideCone(satellite, lat, lon+lowBound));

while (valid == false || (abs(upBound-lowBound) > INTERSECT_ACCURACY))
    inside = insideCone(satellite, lat, lon+upBound);

    if (inside == true)
        temp = upBound;
        upBound = min((upBound+abs(upBound-lowBound)), 360);
        lowBound = temp;
    else
        upBound = (upBound+lowBound)/2;
    end

    valid = xor(inside, insideCone(satellite, lat, lon+lowBound));
end

upBoundLong = lon+(upBound+lowBound)/2;

%Similar to getLongUpBound  but the search is to the left
function lowBoundLong = getLongLowBound(satellite, lat, lon, guess)
global INTERSECT_ACCURACY;
if (nargin < 4 || guess == 0) guess = INTERSECT_ACCURACY*1e2; end
upBound = 0; lowBound = -guess;

valid = xor(insideCone(satellite, lat, lon+upBound), ...
    insideCone(satellite, lat, lon+lowBound));

while (valid == false || (abs(upBound-lowBound) > INTERSECT_ACCURACY))
    inside = insideCone(satellite, lat, lon+lowBound);

    if (inside == true)
        lowBound = (upBound+lowBound)/2;
    else
        temp = lowBound;
        lowBound = max((lowBound-abs(upBound-lowBound)), -360);
        upBound = temp;
    end

    valid = xor(insideCone(satellite, lat, lon+upBound), inside);
end

```

```
838 lowBoundLong = lon+(upBound+lowBound)/2;
839
840 %Similar to getLongUpBound  but now we look for the intersection of a
841 %constant longitude line. We search to the south.
842 function upBoundLat = getLatUpBound(satellite, lat, lon, guess)
843 %estimate what the longitude boundary would be with a binary search
844 global INTERSECT_ACCURACY;
845 if (nargin < 4 || guess == 0) guess = INTERSECT_ACCURACY*1e2; end
846 upBound = guess; lowBound = 0;
847 while abs(upBound-lowBound) > INTERSECT_ACCURACY
848     inside = insideCone(satellite, lat+upBound, lon);
849
850     if (inside == true)
851         temp = upBound;
852         upBound = min((upBound+abs(upBound-lowBound)), 360);
853         lowBound = temp;
854     else
855         upBound = (upBound+lowBound)/2;
856     end
857 end
858
859 upBoundLat = lat+upBound;
860
861 %Similar to getLongUpBound  but now we look for the intersection of a
862 %constant longitude line. We search to the north.
863 function lowBoundLat = getLatLowBound(satellite, lat, lon, guess)
864 global INTERSECT_ACCURACY;
865 if (nargin < 4 || guess == 0) guess = INTERSECT_ACCURACY*1e2; end
866 upBound = 0; lowBound = -guess;
867 while abs(upBound-lowBound) > INTERSECT_ACCURACY
868     inside = insideCone(satellite, lat+lowBound, lon);
869
870     if (inside == true)
871         temp = lowBound;
872         lowBound = max((lowBound-2*abs(upBound-lowBound)), -360);
873         upBound = temp;
874     else
875         lowBound = (upBound+lowBound)/2;
876     end
877 end
878
879 lowBoundLat = lat+lowBound;
880
881 %convert from latitude, longitude to pixel coordinates
```

```
882 function [lat, lon] = pix2latlong(R, row, col)
883
884 [lat, lon] = pix2latlon(R, row+.5, col+.5);
885
886 %convert from degrees to radiant
887 function radians = convertRadians(degrees)
888
889 radians = degrees*pi/180;
```

```
1  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
2  %Description:
3  %UplinkStarBackground calculates the estimated number of background ...
       counts a
4  %satellite will receive per second from starlight and airglow.
5  %Input:
6  %   1. receiver(strucutre): The receiver's parameters are entered in
7  %   receiver
8  %      The required entries in the structure are:
9  %           The following 7 arguments parameterize the telescope
10 %           a) 'FOV': The field of view of the receiver (in rad).
11 %           b) 'wavelength': The wavelength photons are emitted at.
12 %           c) 'telescopeRadius': The receiver's radius in cm.
13 %           d) 'filterBandpass': approximately the area under of the ...
       curve
14 %               of the receiver's filter bandwith (in nm).
15 %           e) 'setupEfficiency': the optical efficiency of the setup
16 %               multiplied by the detector efficiency (format 0.a).
17 %           f) 'observElevation': The receiver's observation elevation
18 %           angle. In other words, this is the angle from the horizon ...
       in degrees.
19 %           The following three parameters specify the night sky ...
       brightness:
20 %           g) 'StarBright'(the star+airglow night sky brightness): ...
       The brightness of the
21 %               night sky (in mag) due to lights emitted by stars and ...
       airglow.
22 %               (in mag)
23
24 %Output:
25 %       backgroundCounts: The estimated number of background counts ...
       that are
26 %       detected by the receiver. (photons/s)
27
```

```
28 function backgroundCounts = UplinkStarBackground(receiver)
29
30 %refernce counts at the astronomical band containing receiver.wavelength
31 refCountsAtWav = obtainReferenceCount(receiver.wavelength);
32 %refernce counts at the V band containing receiver.wavelength
33 refCountsVband = obtainReferenceCount(550);
34 %FOV area in arcsec^2
35 FOVarea = pi*(receiver.FOV*206264)^2;
36 %telescope area in cm^2
37 telescopeArea = pi*receiver.telescopeRadius^2;
38
39 backgroundCounts = FOVarea*telescopeArea*receiver.setupEfficiency*...
40     receiver.filterBandpass*(refCountsAtWav*10^(-0.4*receiver.StarBright));
41
42 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
43 % Since the apparent magnitude is a relative measure, one needs the
44 % photon flux at a certain magnitude to compute the photon flux at a
45 % different magnitude.
46 % This function takes in a wavelength (in nm), determines which
47 % astronomical band it is closest to, and then output the number of
48 % reference counts (in ph cm-2 s-1 nm-1) at 0 magnitude.
49 function refCounts = obtainReferenceCount(wavelength)
50
51 %Data format: Wavelength, ΔWavelength, reference number of counts
52 data = [360     40      7650; ...
53         440     80      14845; ...
54         550     90      10386; ...
55         640     150     5801; ...
56         790     150     3883; ...
57         1260    200     1954; ...
58         1600    370     1015; ...
59         2220    500     447; ...
60         3400    700     139; ...
61         5000    1200    53];
62
63 numData = size(data, 1);
64
65 %first if the wavelengh is less than what the data gives approximates ...
       it to
66 %the first band
67 if (wavelength < data(1,1))
68     refCounts = data(1, 3);
69     return;
70 elseif (wavelength > data(numData,1))
```

```
71      refCounts = data(numData, 3);
72      return;
73  end
74
75  foundBand = false;
76  ind = 1;
77  %find which astronomical band the wavelength is closed to
78  while (foundBand == false)
79      currUpBound = data(ind, 1) + data(ind, 2);
80      nextLowBound = data(ind+1, 1) - data(ind+1, 2);
81
82      %check if the wavelength is between two bands
83      if (wavelength  ≥ data(ind, 1) && wavelength ≤ data(ind+1, 1))
84          %wavelength closer to next band center
85          if (abs(wavelength-data(ind, 1)) > abs(wavelength-data(ind+1, ...
                1)))
86              closerInd = ind + 1;
87              %should go to upper band but first make sure it is within
88              %ΔWavelength
89              if (wavelength  < nextLowBound)
90                  if (wavelength ≤ currUpBound) %is it within current band
91                      closerInd = ind;
92                  %if not it is closest to which band boundary?
93                  elseif (abs(wavelength-nextLowBound) > ...
94                          abs(wavelength-currUpBound))
95                      closerInd = ind;
96                  end
97              end
98          else %closer to current band
99              closerInd = ind;
100             % make sure it is within ΔWavelength
101             if (wavelength  > currUpBound)
102                 if (wavelength ≥ nextLowBound) %is it within next band
103                     closerInd = ind + 1;
104                 %if not it is closest to which band boundary?
105                 elseif (abs(wavelength-nextLowBound) < ...
106                         abs(wavelength-currUpBound))
107                     closerInd = ind + 1;
108                 end
109             end
110         end
111
112         foundBand = true;
113     end
```

```
114
115     ind = ind+1;
116 end
117
118 refCounts = data(closerInd, 3);
119
120 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
121 %calculateExtinction calculates the extinction coefficient at a ...
       wavelength
122 %and elevation angle as measured from the zenith
123 %Input:
124 %   1. wavelength: The wavelength (in nm)
125 %   2. elevAngle: The elevation angle as measured from the zenith  in
126 %   degrees
127 function extinctionCoefficient = calculateExtinction(wavelength, ...
       elevAngle)
128
129 % because at 300 this function peaks and at about 255 becomes negative,
130 % consider the 300 wavelength as an upper bound
131 w = max(300, wavelength);
132
133 %The equation below is a fit of data from "Fundamentals of Astronomy" ...
       by C
134 %Barbieri, Chapter 16.3
135 p1 =     0.03884;
136 p2 =       9.683;
137 p3 =       1.108;
138 p4 =       0.525;
139 q1 =        -294;
140 q2 =      -1.077;
141 q3 =      0.6175;
142 extinction0 = (p1*w.^3 + p2*w.^2 + p3*w + p4) ./ (w.^3 + q1*w.^2 + ...
       q2*w + q3);
143 %as we increase elevAngle the air mass increases. Reference: Kasten, ...
       F., and A. T.
144 %Young. 1989. Revised optical air mass tables and approximation formula.
145 %Applied Optics 28:4735  4 7 3
146 extinctionCoefficient = extinction0/ ...
147     (cos(convertRadians(elevAngle))+0.50572*(96.07995-elevAngle)^-1.6364);
148
149 function radians = convertRadians(degrees)
150
151 radians = degrees*pi/180;
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%extractSubImg extracts a sub image from an image specified by its path.
%Input:
%    (centerLat, centerLon): the center of the subimage
%    R: the referencing matrix of the original image
%    latExtent: the new image will be centered at centerLat and  will ...
    extend
%        latExtent above and below the center.
%    latExtent: the new image will be centered at centerLon and  will ...
    extend
%        lonExtent to the right and left of the center.
%Output:
%    newImgData (m*n matrix): The sub image pixel data
%    Rnew: The referencing matrix.
function [newImgData,Rnew] = extractSubImg(centerLat, centerLon, R, ...
    latExtent, lonExtent, imgPath, heightImg, widthImg)


%make sure not to overwrite anything
ind = 0;
tempPath = sprintf('uplinkEstimationTempFile%06d.tif', ind);
while (exist(tempPath, 'file') == 2 && ind < 2000)
    ind = ind+1;
    tempPath = sprintf('uplinkEstimationTempFile%06d.tif', ind);
end

pixelLongDist = lonExtent/abs(R(1,2));
pixelLatDist = latExtent/abs(R(2,1));
%some small safety factor
pixelLongDist = round(pixelLongDist+1);
pixelLatDist = round(pixelLatDist+1);

%obtain the center pixel coordinates
[centerRow, centerCol] = latlon2pixs(R, centerLat, centerLon);

%start with the right extent of the image
diffCenterPix = ceil(centerCol)-centerCol;
minPixelDist = 2+diffCenterPix; %want at least 2 pixels from the ...
    center pixel
wantedPixedDist = pixelLongDist+diffCenterPix;
if (wantedPixedDist < minPixelDist) wantedPixedDist = minPixelDist; end
lonExtentRight = wantedPixedDist*abs(R(1,2));
maxLon = centerLon+abs(lonExtentRight);
```

```
41
42 %The left extent of the image
43 diffCenterPix = abs(floor(centerCol)-centerCol);
44 minPixelDist = 2+diffCenterPix; %want at least 2 pixels from the ...
       center pixel
45 wantedPixedDist = pixelLongDist+diffCenterPix;
46 if (wantedPixedDist < minPixelDist) wantedPixedDist = minPixelDist; end
47 lonExtentLeft = wantedPixedDist*abs(R(1,2));
48 minLon = centerLon-abs(lonExtentLeft);
49 %The up extent of the image
50 diffCenterPix = abs(floor(centerRow)-centerRow);
51 minPixelDist = 2+diffCenterPix; %want at least 2 pixels from the ...
       center pixel
52 wantedPixedDist = pixelLatDist+diffCenterPix;
53 if (wantedPixedDist < minPixelDist) wantedPixedDist = minPixelDist; end
54 latExtentUp = wantedPixedDist*abs(R(2,1));
55 maxLat = centerLat+abs(latExtentUp);
56 %The up extent of the image
57 diffCenterPix = abs(ceil(centerRow)-centerRow);
58 minPixelDist = 2+diffCenterPix; %want at least 2 pixels from the ...
       center pixel
59 wantedPixedDist = pixelLatDist+diffCenterPix;
60 if (wantedPixedDist < minPixelDist) wantedPixedDist = minPixelDist; end
61 latExtentDown = wantedPixedDist*abs(R(2,1));
62 minLat = centerLat-abs(latExtentDown);
63
64 %convert to pixel coordinates
65 [minRow, minCol] = latlon2pixs(R, maxLat, minLon);
66 [maxRow, maxCol] =latlon2pixs(R, minLat, maxLon);
67 minRow = max(1,  round(minRow)); minCol = max(1,  round(minCol));
68 maxRow = min(heightImg,  round(maxRow)); maxCol = min(widthImg,  ...
       round(maxCol));
69 heightImgNew = maxRow-minRow; widthImgNew = maxCol-minCol;
70 %call gdal translate to obtain a portion of the image. The options
71 %format is like '-srcwin TLcol TLrow width height imageFilename
72 %outputfilename'
73 opts = [' ' num2str(minCol) ' ' num2str(minRow) ' ' ...
       num2str(widthImgNew) ...
74      ' ' num2str(heightImgNew) ' "' imgPath '"' ' ' tempPath];
75 dos(['gdal_translate -srcwin' opts]);
76
77 [newImgData, Rnew, ignore] = geotiffread(tempPath);
78
79 delete(tempPath); %delete the temporary file
```

```
%convert from latitude, longitude coordinates to pixel coordinates
function [row, col] = latlon2pixs(R, lat, lon)

%obtain the center pixel coordinates
[row, col] = latlon2pix(R, lat, lon);
%correct for the way latlon2pix works (the .5)
row = row-.5; col = col-.5;
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%Given the wavelength and pixel value convert the radiance from W/cm^2/sr
%to ph/cm^2/s/sr/um
function photonFlux = obtainFlux(pixelValue, wavelength)

radiance = 1e-10*double(pixelValue).^1.5; %in watts/cm^2/sr/um
%convert to photon flux in ph/cm^2/s/sr
energyPhoton = 6.63e-34*3e8/(wavelength*1e-9);
photonFlux = radiance/energyPhoton;
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%sCeil is a special ceil that behaves like ceil except when number is 0
%if number is 0 it is send to 1
function result = sCeil(number)

if (number == 0)
    result = 1;
else
    result = ceil(number);
end
```

B.3 Additional background calculation functions

```
%transStruct is a structure that contains input information
% It contains the following variables:
%   1.angle: provided in degrees
%   1.wavelength: provided in nm
function transmission = getTransmission(transStruct)

```

```
7  angle = transStruct.angle;
8
9  if(angle>79.9)
10     angle=79.9;
11 end
12 angle2=80:-1:0;
13 transmission=interp1(angle2,transStruct.trans,angle);          ...
       %Transmittance of the atmosphere (trough a perpendicular path)
```

Appendix C

Key generation and performance of fundamental experiments program

Here we show the MATLAB code used to estimate the Key generation and performance of fundamental experiments program. This code was originally written by Evan Meyer-Scott with some simulations modified from programs written Thomas Jennewein. Some additional modifications to the programs were done in collaboration with Evan. Some of these simulations require the quantum optics and computation Toolbox by Sze Tan.

C.1 WCP QKD

C.1.1 Signal visibility and count rate

```
function [rate,  vis]=Visibility_weak(loss1,darks1)

%% Initializations
N=7; %Fock space dimension, N must be minimum of 2
standard_defintions_qo_toolbox;



% 2-channel detectors with active basis choices or 4-channel passive?
detector_channels=4;

% Set some parameters like source rate, coincidence window, average ...
    photon
```

```
% number (for faint lasers); optics and detector efficiency should be in
% loss already

%net source rates (i.e. backcalculated from the singles) gives ...
    approximately
%the epsilon, but for faint lasers, net source rate is the laser rep ...
    rate:
net_source_rates=300e6;
% coinc_window is the  maximal source emission time slots - a ...
    somewhat simple model
% is to take 1/single_photon_coherence (in the limit that the single ...
    photon
% coherence is shorter than the pump coherence)
% But it might be set to the coincidence window for simplification
coinc_window=0.5e-9;
f_source=1/coinc_window;

% Convert loss in dB to loss
var_link1=10.^(-loss1/10);


% Add initial visibility, i.e. polarization misalignment
initial_vis=.98;

    %% Run it
        %Make a coherent state, average photon number mu and nu
        mu=0.5;
        nu=0.1;
    alpha=sqrt(mu);
    alpha_nu=sqrt(nu);
    D = expm(alpha*a'-alpha'*a);
    psi = tensor(D*vacc,vacc);
    D = expm(alpha_nu*a'-alpha_nu'*a);
    psi_nu = tensor(D*vacc,vacc);

    %Use a slightly misaligned HWP to simulate polarization misalignment

    eta=acos(initial_vis)/2;
    H_bs = (tensor(a,a') + tensor(a',a))*eta;
    U_bs = expm(-1i*H_bs);
    psi=U_bs*psi;


```

```
53          % Define loss1&2 for this loop
54          effc_link1=var_link1;
55
56          %if we have 4 detector channel the state must be converted to ...
                a 4 mode
57          %state (|H1,V1,D2,A2>). To do this we use a four mode beam ...
               splitter and
58          %use a half wave plate to convert |H1,V1,H2,V2> to |H1,V1,D2,A2>.
59          if detector_channels==4
60          %50:50 beam-splitter
61          H_bs = (tensor(a,a') + tensor(a',a))*pi/4;
62          U_bs = expm(-1i*H_bs);
63          four_mode_U_bs=permute(tensor(U_bs,U_bs),[1 3 2 4]);
64          %half wave plate at 45
65          HWP=expm(-1i*((tensor(a,a')*exp(1i*pi/2) + ...
               tensor(a',a)*exp(-1i*pi/2))*2*pi/8));
66          four_mode_HWP = tensor(tensor(ida,ida),HWP);
67          psi=four_mode_HWP*(four_mode_U_bs*tensor(psi,vacc,vacc));
68          psi_nu=four_mode_HWP*(four_mode_U_bs*tensor(psi_nu,vacc,vacc));
69          end
70
71              %Define Noise factor for arm1
72              noise_factor1=darks1/f_source;
73              % Create detectors, including fock space N, combined ...
                    losses due to the
74              % link, optics efficiency, and detector efficiency, and darks
75              [apd_link1 un_linkapd1]= ...
                    BucketDetector_noise(N,effc_link1,noise_factor1);
76
77
78
79              %double link with arbitrary losses in each arm, measure ...
                    on fock space
80              %N, state psi, and detector modules 1 and 2
81              if detector_channels==2
82              probs2f=real(measure_2modes_2detectors(N,psi,apd_link1, ...
                    un_linkapd1));
83              probs2f_nu=real(measure_2modes_2detectors(N,psi_nu, ...
                    apd_link1,un_linkapd1));
84              elseif detector_channels==4
85              probs2f=real(measure_4modes_4detectors(N,psi,apd_link1, ...
                    un_linkapd1));
86              probs2f_nu=real(measure_4modes_4detectors(N,psi_nu, ...
                    apd_link1,un_linkapd1));
```

```
87              end
88
89              %Double click rate
90              if detector_channels==2
91              double1=probs2f(3);
92              double1_nu=probs2f_nu(3);
93              elseif detector_channels==4
94              %Here we only care about the multi click where one clicks was
95              %in the correct basis (H click and/or v click)
96              double1=probs2f(5);
97              double1_nu=probs2f_nu(5);
98              end
99
100
101             %Rates returned are 'per pulse', so multiply by source rate
102             if detector_channels==2
103                         rate=(sum(probs2f(1:2)))*net_source_rates;
104                         rate_nu=sum(probs2f_nu(1:2))*net_source_rates;
105             else
106                     rate=(sum(probs2f(1:4)))*net_source_rates;
107                     rate_nu=(sum(probs2f_nu(1:4)))*net_source_rates;
108             end
109             %Determine visibility and QBER from returned detection ...
                   probabilities
110             QBER=(probs2f(2)+double1/2)/(sum(probs2f(1:2))+double1);
111             QBER_nu=(probs2f_nu(2)+double1_nu/2)/ ...
                   (sum(probs2f_nu(1:2))+double1_nu);
112
113 vis=1-2*QBER;
114 vis_nu=1-2*QBER_nu;
115
116
117
118
119
120 end
```

```
1  %Evan Meyer-Scott, 10.17.2010 from Thomas Jennewein, 8.10.2008
2  %Determin the singles count rates for a 2 mode state, e.g. |H1,V1>
3
4  function probs=measure_2modes_2detectors(N,in,proj,unproj)
5
6  ida=identity(N);
```

```
7
8  final_state=in;
9
10 %singles
11 H=sum(expect(tensor(proj,unproj),final_state));
12 V=sum(expect(tensor(unproj,proj),final_state));
13 %Double clicks
14 HV=sum(expect(tensor(proj,proj),final_state));
15
16 probs=[H,V,HV];
```

```
1  %Jean-Philippe Bourgoin, 08.05.2013 from Evan Meyer-Scott, 10.17.2010 ...
       and Thomas Jennewein, 8.10.2008
2  %Determin the singles count rates for a 2 mode state, e.g. |H1,V1,D2,A2>,
3  %detected in 4 detectors with a passive basis choice.
4
5  function probs=measure_4modes_4detectors(N,in,proj,unproj)
6
7  ida=identity(N);
8
9  final_state=in;
10
11 %singles
12 H=sum(expect(tensor(proj,unproj,unproj,unproj),final_state));
13 V=sum(expect(tensor(unproj,proj,unproj,unproj),final_state));
14 D=sum(expect(tensor(unproj,unproj,proj,unproj),final_state));
15 A=sum(expect(tensor(unproj,unproj,unproj,proj),final_state));
16 %multi clicks
17 HV=sum(expect(tensor(proj,proj,ida,ida),final_state));
18 HD=sum(expect(tensor(proj,unproj,proj,ida),final_state));
19 HA=sum(expect(tensor(proj,unproj,unproj,proj),final_state));
20 VD=sum(expect(tensor(unproj,proj,proj,ida),final_state));
21 VA=sum(expect(tensor(unproj,proj,unproj,proj),final_state));
22 DA=sum(expect(tensor(unproj,unproj,proj,proj),final_state));
23 multi_HV_basis=HV+HD+HA+VD+VA;
24
25 probs=[H,V,D,A,multi_HV_basis];
```

C.1.2 Key generation with decoy pulse method

```
function [Keylength]=keyrate_weak_sent_pulse(loss,vis,Nreceived,Nsent)

% This function computes the number of extractable secure key bits ... given a
% received polarization visibility vis and Nreceived raw key bits between
% Alice and Bob (Nreceived = number of Bob's detections in any ... basis). For
% decoy states the average channel loss is also needed.
%The final key rate is per sent pulse and must be multiplied by the ... total number of sent pulse (Nsent)

%To maximize key generation one must use a visibility cut-off to ... ignore the worst parts of the pass (this can be optimized for each ... passes, for simplicity we used a fixed cut-off of 0.85 in this ... work). One can also combine multiple passes to reduce finite size ... effects (instead of generating a key with the individual passes).

% Decoy state security analysis from Sun, Liang and Li, PLA 373, 2533
% (2009), and Ma, Qi, Zhao, Lo, PRA 72, 012326 (2005) and Cai and ... Scarani,
% NJP 11 045024 (2009).

% Decoy state finite key analysis is incomplete, so the formulas here
% follow mostly Sun et al, with corrections from the other papers. One
% signal and one decoy level are assumed, with the "Tighter bound" of E.2
% in Ma's paper.


% Set decoy protocol parameters
% mu is the average photon number of the signal states
mu=.5;
% nu is the average photon number of the decoy states: this could be
% optimized for positive key rates at higher loss.
nu=.1;

% Convert the loss from decibels to a fraction
loss=10^(-loss/10);

% Calculate the gain Q (detection probability) for signal and decoy ... states
Qmu=1-exp(-loss*mu);
Qnu=1-exp(-loss*nu);

% Error rate for signal states from visibility (vis<1)
```

```
if vis≥1
    error('Visibility must be less than 1')
end
Emu=(1-vis)/2;


% Initialize key rate to zero
SK_rate_finite=0;

% Total failure probability for each key: the probability that the ...
   protocol
% fails and the key is not secure, but we don't know.
% 10^-9 is sufficient for a few-year satellite mission, but this is
% something to be discussed, possibly increased for better performance.
epsilon=1e-9;

% Error correction failure probability: 10^-10 is standard
epsilonEC=1e-10;

% Also optimize over epsilonbar and epsilonbarprime, two parameters of
% information theoretic origin that have little operational meaning, and
% can carry the condition epsilon-epsilonEC>epsilonbar>epsilonbarprime>0

% How many search iterations to perform
sear=10;

% Begin search over N_mu and N_nu, the number of signals to devote to
% signal and decoy states respective
for kk=1:sear

    N_mu=Nreceived*kk/(sear+1);
    N_nu=Nreceived-N_mu;

    % Set statistical fluctuation bound to 10 standard deviations
    ualpha=10;


    % Estimate worst case upper or lower bounds on signal and decoy
    % detection probabilities given ualpha standard deviations
    Qnu_L=Qnu*(1-ualpha/sqrt(N_nu));
    Qmu_U=Qmu*(1+ualpha/sqrt(N_mu));

    % Estimate worst case upper bound on error rate
    Emu_U=Emu*(1+ualpha/sqrt(N_mu*Emu));
```

```
79
80      % Estimate worst case detection probability of single photon states,
81      % since only single photon states are secure against eavesdropping
82      Q1=(mu^2)*exp(-mu)/(mu*nu-nu^2)*(Qnu_L*exp(nu)- ...
            Qmu_U*exp(mu)*nu^2/(mu^2));
83
84      % Estimate worst case error rate due to single photon states
85      e1=Emu_U*Qmu_U/Q1;
86
87      % Begin search over epsilonbar
88      for ii=logspace(0,-5,sear)
89          epsilonbar=(epsilon-epsilonEC)*(1-ii);
90          Δ2=2*log2(1/(2*(epsilon-epsilonbar-epsilonEC)));
91
92          % Begin search over epsilonbarprime
93          for jj=logspace(0.1,17,sear)
94              epsilonbarprime=epsilonbar/jj;
95              Δ1=7*sqrt(log2(2/(epsilonbar-epsilonbarprime))*N_mu);
96
97              % Secure key rate per channel use (i.e. per laser pulse ...
                    sent by
98              % Alice) is 1/2 for the basis sifting, N_mu/Nreceived since
99              % only signal states are used to generate key,
100             % -Qmu*1.22*H2(Emu) for the information leaked to Eve during
101             % error correction, Q1*(1-H2(e1)) for the information Eve
102             % gained by attacking single photon pulses causing error rate
103             % e1, and Qmu*(Δ1+Δ2)/N_mu for the information
104             % theoretic security proofs.
105             SK_rate_finite_new=1/2*N_mu/Nreceived*(-Qmu*1.22*H2(Emu)+ ...
                    Q1*(1-H2(e1))-Qmu*(Δ1+Δ2)/N_mu); %per channel use, ...
                    decoy or signal included from Scarani 2009, since Sun ...
                    doesn't have enough Qmu on his Δs!
106
107             % If the new key rate is better, use that
108             if   isreal(SK_rate_finite_new)&&SK_rate_finite_new ...
                    >SK_rate_finite
109
110                 SK_rate_finite=SK_rate_finite_new;
111
112
113             end
114         end
115     end
116 end
```

```
117
118 % The total number of secure key bits is then the key rate per laser ...
       pulse
119 % times the numebr of laser pulses sent, or the number received ...
       divided by
120 % the average loss.
121 %Keylength=SK_rate_finite*Nreceived/loss;
122
123 Keylength=SK_rate_finite*Nsent;
124
125 end
```

C.2 Entangled source QKD and Bell test

C.2.1 Entanglement visibility and count rate

```
1  function [twofold_rate vis]=Visibility(loss1,loss2,darks1,darks2)
2
3  %% Initializations
4  N=4; %Fock space dimension, N must be minimum of 2
5  standard_defintions_qo_toolbox;
6
7
8
9  % 2-channel detectors with active basis choices or 4-channel passive?
10 detector_channels=4;
11
12 % Set some parameters like source rate, coincidence window, average ...
       photon
13 % number (for faint lasers); optics and detector efficiency should be in
14 % loss already
15
16 %net source rates (i.e. backcalculated from the singles) gives ...
       approximately
17 %the epsilon, but for faint lasers, net source rate is the laser rep ...
       rate:
18 net_source_rates=100e6;
19 % coinc_window is the  maximal source emission time slots - a ...
       somewhat simple model
```

```
% is to take 1/single_photon_coherence (in the limit that the single ...
    photon
% coherence is shorter than the pump coherence)
% But it might be set to the coincidence window for simplification
coinc_window=0.5e-9;
f_source=1/coinc_window;

% Convert loss in dB to loss
var_link1=10.^(-loss1/10);
var_link2=10.^(-loss2/10);

% Add initial visibility, i.e. polarization misalignment
initial_vis=.98;

    %% Run it
    %Make an entangled state from SPDC
    epsilon=asinh(sqrt(net_source_rates/f_source/2));


    %SPDC in chi2:
    H_chi2=(tensor(a,a)+tensor(a',a'))*epsilon;
    U_chi2=expm(-1i*H_chi2);

    %SPDC input state for pair of photons in HH
    spdc_state=tensor(U_chi2*tensor(vacc,vacc));

    % create entangled SPDC state
    psi=permute(tensor(spdc_state,spdc_state),[1 3 4 2]);

    %Use a slightly misaligned HWP to simulate polarization misalignment

    eta=acos(initial_vis)/2;
    H_bs = (tensor(a,a') + tensor(a',a))*eta;
    U_bs = tensor(expm(-1i*H_bs),ida,ida);
    psi=U_bs*psi;

    % Define constant link2 stuff
    effc_link1=var_link1;
    effc_link2=var_link2;
    noise_factor1=darks1/f_source;
    noise_factor2=darks2/f_source;


```

```
62          %if we have 4 detector channel the state must be converted to ...
                a 8 mode
63          %state (|H1,V1,D2,A2,H3,V3,D4,A4>). To do this we use two ...
                four mode beam splitter
64          if detector_channels==4
65              %50:50 beam-splitter
66              H_bs = (tensor(a,a') + tensor(a',a))*pi/4;
67              U_bs = expm(-1i*H_bs);
68              four_mode_U_bs=permute(tensor(U_bs,U_bs),[1 3 2 4]);
69              eight_mode_U_bs=tensor(four_mode_U_bs,four_mode_U_bs);
70              %convert psi to 8 modes and apply beam splitter
71              psi=permute(tensor(psi,vacc,vacc,vacc,vacc),[1 2 5 6 3 4 ...
                    7 8]);
72              psi=eight_mode_U_bs*psi;
73          end
74
75
76              % Create detectors, including fock space N, combined ...
                    losses due to the
77              % link, optics efficiency, and detector efficiency, and darks
78              [apd_link1, un_linkapd1]= ...
                    BucketDetector_noise(N,effc_link1,noise_factor1);
79              [apd_link2, un_linkapd2]= ...
                    BucketDetector_noise(N,effc_link2,noise_factor2);
80
81
82              %double link with arbitrary losses in each arm, measure ...
                    on fock space
83              %N, state psi, and detector modules 1 and 2
84              if detector_channels==2
85                  probs2f=real(measure_2folds_4modes_unsymetric_detectors...
86                      (N,psi,apd_link1,un_linkapd1,apd_link2,un_linkapd2));
87              elseif detector_channels==4
88                  probs2f=real(measure_2folds_8modes_unsymetric_detectors...
89                      (N,psi,apd_link1,un_linkapd1,apd_link2,un_linkapd2));
90              end
91
92
93              %Double click rate
94              if detector_channels==2
95                  double1=probs2f(9);
96                  double2=probs2f(10);
97              elseif detector_channels==4
98                  double1=probs2f(9);
```

```
                double2=0;
            end


            %Rates returned are 'per pulse', so multiply by source rate
            if detector_channels==2
                twofold_rate=sum(probs2f(1:4))*f_source;
            %Determine visibility and QBER from returned detection ...
               probabilities
            QBER=(probs2f(1)+probs2f(4)+double1+double2)/(probs2f(1)+ ...
               probs2f(2)+probs2f(3)+probs2f(4)+probs2f(9)+probs2f(10));
            elseif detector_channels==4
                twofold_rate=sum(probs2f(1:8))*f_source*2;
            %Determine visibility and QBER from returned detection ...
               probabilities
            QBER=(sum(probs2f(1:4))+double1/2+double2/2)/ ...
                (sum(probs2f(1:8))+double1+double2);
            end


     vis=1-2*QBER;


end
```

```
%Thomas Jennewein, 8.10.2008
%Determin the 2fold count rates for a 4 mode state, e.g. |H1,V1,H2,V2>

%Thoams Jennewein, 12.11.2008, extension for usymetric detectors, ...
   such as
%in a unsymmetric entangled photon expeirment.

function ...
   probs=measure_2folds_4modes_unsymetric_detectors(N,in,proj1,unproj1,...
    proj2,unproj2)

ida=identity(N);

final_state=in;
HH=sum(expect(tensor(proj1,unproj1,proj2,unproj2),final_state));
VV=sum(expect(tensor(unproj1,proj1,unproj2,proj2),final_state));
HV=sum(expect(tensor(proj1,unproj1,unproj2,proj2),final_state));
```

```
VH=sum(expect(tensor(unproj1,proj1,proj2,unproj2),final_state));

%singles1
H1=sum(expect(tensor(proj1,unproj1,ida,ida),final_state));
V1=sum(expect(tensor(unproj1,proj1,ida,ida),final_state));

%singles2
H2=sum(expect(tensor(ida,ida,proj2,unproj2),final_state));
V2=sum(expect(tensor(ida,ida,unproj2,proj2),final_state));

%doubleclicks
H1V1=sum(expect(tensor(proj1,proj1,ida,ida),final_state));
H2V2=sum(expect(tensor(ida,ida,proj2,proj2),final_state));

probs=[HH,HV,VH,VV,H1,V1,H2,V2,H1V1,H2V2];
```

```
%Thoams Jennewein, 12.11.2008, extension for usymetric detectors, ...
    such as
%in a unsymmetric entangled photon expeirment.

%Thomas Jennewein, 8.10.2008
%Determin the 2fold count rates for a 4 mode state, e.g. |H1,V1,H2,V2>

%Evan Meyer—Scott, 2010, added double clicks

%Jean—Philippe Bourgoin, 08.05.2013
%Modified to Determine the 2fold count rates for a 8 mode state, e.g. ...
    |H1,V1,D2,A2,H3,V3,D4,A4>

function probs=measure_2folds_8modes_unsymetric_detectors(N,in,proj1,...
    unproj1,proj2,unproj2)

ida=identity(N);

final_state=in;
HH=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    proj2,unproj2,unproj2,unproj2),final_state));
VV=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    unproj2,proj2,unproj2,unproj2),final_state));
DD=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    unproj2,unproj2,proj2,unproj2),final_state));
AA=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    unproj2,unproj2,unproj2,proj2),final_state));
```

```
26
27 HV=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
28     unproj2,proj2,unproj2,unproj2),final_state));
29 VH=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
30     proj2,unproj2,unproj2,unproj2),final_state));
31 DA=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
32     unproj2,unproj2,unproj2,proj2),final_state));
33 AD=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
34     unproj2,unproj2,proj2,unproj2),final_state));
35
36 %multi-clicks
37 H1V1H3=sum(expect(tensor(proj1,proj1,ida,ida,...
38     proj2,ida,ida,ida),final_state));
39 H1V1V3=sum(expect(tensor(proj1,proj1,ida,ida,...
40     unproj2,proj2,ida,ida),final_state));
41 H1V1D4=sum(expect(tensor(proj1,proj1,ida,ida,...
42     unproj2,unproj2,proj2,ida),final_state));
43 H1V1A4=sum(expect(tensor(proj1,proj1,ida,ida,...
44     unproj2,unproj2,unproj2,proj2),final_state));
45 H1D2H3=sum(expect(tensor(proj1,unproj1,proj1,ida,...
46     proj2,ida,ida,ida),final_state));
47 H1D2V3=sum(expect(tensor(proj1,unproj1,proj1,ida,...
48     unproj2,proj2,ida,ida),final_state));
49 H1D2D4=sum(expect(tensor(proj1,unproj1,proj1,ida,...
50     unproj2,unproj2,proj2,ida),final_state));
51 H1D2A4=sum(expect(tensor(proj1,unproj1,proj1,ida,...
52     unproj2,unproj2,unproj2,proj2),final_state));
53 H1A2H3=sum(expect(tensor(proj1,unproj1,unproj1,proj1,...
54     proj2,ida,ida,ida),final_state));
55 H1A2V3=sum(expect(tensor(proj1,unproj1,unproj1,proj1,...
56     unproj2,proj2,ida,ida),final_state));
57 H1A2D4=sum(expect(tensor(proj1,unproj1,unproj1,proj1,...
58     unproj2,unproj2,proj2,ida),final_state));
59 H1A2A4=sum(expect(tensor(proj1,unproj1,unproj1,proj1,...
60     unproj2,unproj2,unproj2,proj2),final_state));
61 V1D2H3=sum(expect(tensor(unproj1,proj1,proj1,ida,...
62     proj2,ida,ida,ida),final_state));
63 V1D2V3=sum(expect(tensor(unproj1,proj1,proj1,ida,...
64     unproj2,proj2,ida,ida),final_state));
65 V1D2D4=sum(expect(tensor(unproj1,proj1,proj1,ida,...
66     unproj2,unproj2,proj2,ida),final_state));
67 V1D2A4=sum(expect(tensor(unproj1,proj1,proj1,ida,...
68     unproj2,unproj2,unproj2,proj2),final_state));
69 V1A2H3=sum(expect(tensor(unproj1,proj1,unproj1,proj1,...
```

```
    proj2,ida,ida,ida),final_state));
V1A2V3=sum(expect(tensor(unproj1,proj1,unproj1,proj1,...
    unproj2,proj2,ida,ida),final_state));
V1A2D4=sum(expect(tensor(unproj1,proj1,unproj1,proj1,...
    unproj2,unproj2,proj2,ida),final_state));
V1A2A4=sum(expect(tensor(unproj1,proj1,unproj1,proj1,...
    unproj2,unproj2,unproj2,proj2),final_state));
D2A2H3=sum(expect(tensor(unproj1,unproj1,proj1,proj1,...
    proj2,unproj2,unproj2,unproj2),final_state));
D2A2V3=sum(expect(tensor(unproj1,unproj1,proj1,proj1,...
    ida,proj2,unproj2,unproj2),final_state));
D2A2D4=sum(expect(tensor(unproj1,unproj1,proj1,proj1,...
    ida,ida,proj2,unproj2),final_state));
D2A2A4=sum(expect(tensor(unproj1,unproj1,proj1,proj1,...
    ida,ida,ida,proj2),final_state));

H1H3V3=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    proj2,proj2,ida,ida),final_state));
H1H3D4=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    proj2,unproj2,proj2,ida),final_state));
H1H3A4=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    proj2,unproj2,unproj2,proj2),final_state));
H1V3D4=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    unproj2,proj2,proj2,ida),final_state));
H1V3A4=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    unproj2,proj2,unproj2,proj2),final_state));
H1D4A4=sum(expect(tensor(proj1,unproj1,unproj1,unproj1,...
    unproj2,unproj2,proj2,proj2),final_state));
V1H3V3=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    proj2,proj2,ida,ida),final_state));
V1H3D4=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    proj2,unproj2,proj2,ida),final_state));
V1H3A4=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    proj2,unproj2,unproj2,proj2),final_state));
V1V3D4=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    unproj2,proj2,proj2,ida),final_state));
V1V3A4=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    unproj2,proj2,unproj2,proj2),final_state));
V1D4A4=sum(expect(tensor(unproj1,proj1,unproj1,unproj1,...
    unproj2,unproj2,proj2,proj2),final_state));
D2H3V3=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    proj2,proj2,unproj2,unproj2),final_state));
D2H3D4=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    proj2,ida,proj2,unproj2),final_state));
```

```
D2H3A4=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    proj2,ida,ida,proj2),final_state));
D2V3D4=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    unproj2,proj2,proj2,ida),final_state));
D2V3A4=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    unproj2,proj2,unproj2,proj2),final_state));
D2D4A4=sum(expect(tensor(unproj1,unproj1,proj1,unproj1,...
    unproj2,unproj2,proj2,proj2),final_state));
A2H3V3=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    proj2,proj2,unproj2,unproj2),final_state));
A2H3D4=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    proj2,ida,proj2,unproj2),final_state));
A2H3A4=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    proj2,ida,ida,proj2),final_state));
A2V3D4=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    unproj2,proj2,proj2,ida),final_state));
A2V3A4=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    unproj2,proj2,unproj2,proj2),final_state));
A2D4A4=sum(expect(tensor(unproj1,unproj1,unproj1,proj1,...
    unproj2,unproj2,proj2,proj2),final_state));

multi_click_shared_bases=H1V1H3+H1V1V3+H1D2H3+H1D2V3+H1D2D4+H1D2A4+...
    H1A2H3+H1A2V3+H1A2D4+H1A2A4+V1D2H3+V1D2V3+V1D2D4+V1D2A4+V1A2H3+...
    V1A2V3+V1A2D4+V1A2A4+D2A2D4+D2A2A4+H1H3V3+H1H3D4+H1H3A4+H1V3D4+...
    H1V3A4+V1H3V3+V1H3D4+V1H3A4+V1V3D4+V1V3A4+D2H3D4+D2H3A4+D2V3D4+...
    D2V3A4+D2D4A4+A2H3D4+A2H3A4+A2V3D4+A2V3A4+A2D4A4;
multi_click_unshared_basis=H1V1D4+H1V1A4+D2A2H3+D2A2V3+H1D4A4+V1D4A4+...
    D2H3V3+A2H3V3;

probs=[HH,VV,DD,AA,HV,VH,DA,AD,multi_click_shared_bases,...
    multi_click_unshared_basis];
```

C.2.2 Key generation

```
function [keyLength]=keyrate_entangled(vis,Nreceived)       %uses the ...
    average entanglement visibility and total counts received to ...
    estimate the lenght of the secure key. To maximize key generation ...
    one must use a visibility cut-off to ignore the worst parts of the ...
    pass (this can be optimized for each passes, for simplicity we ...
    used a fixed cut-off of 0.85 in this work). One can also combine ...
    multiple passes to reduce finite size effects (instead of ...
```

```
    generating a key with the individual passes).
2
3 % This function computes the number of extractable secure key bits ...
    given a
4 % received entanglement visibility vis and Nreceived raw key bits between
5 % Alice and Bob (Nreceived = number of concident detections in any ...
    basis).
6
7 % Key rate formula from Scarani & Renner PRL 100, 200501, (2008) for ...
    qubits.
8 % This is acceptable since the security of BB84 with qubits and our
9 % entangled protocol is equivalent
10
11 %N=total signals - get from JP's simulation of satellite passage
12 N=Nreceived;
13
14 % Convert entanglement visibility to QBER for subsequent calculation
15 QBER=(1-vis)/2;
16
17 % The fraction of each bit leaked to Eve by error correction, assuming
18 % error correction efficiency 1.22
19 leakEC_over_n=1.22*H2(QBER);
20
21 % Total failure probability for each key: the probability that the ...
    protocol
22 % fails and the key is not secure, but we don't know.
23 % 10^-9 is sufficient for a few-year satellite mission, but this is
24 % something to be discussed, possibly increased for better performance.
25 epsilon=1e-9;
26
27 % Error correction failure probability: 10^-10 is standard
28 epsilonec=1e-10;
29
30 % Initialize maximum key rate to 0
31 rateMax=0;
32
33 % Optimize over n&m, the number of bits used to generate key and for
34 % parameter estimation respectively. We may be able to set m=n or avoid
35 % this entirely, since our error correction protocol should return ...
    the QBER
36 % exactly.
37 % Also optimize over epsilonbar and epsilonbarprime, two parameters of
38 % information theoretic origin that have little operational meaning, and
39 % can be set to any value >0.
```

```
40
41 % How many search iterations to perform
42 Sear=10;
43
44 % Initialize searching values
45 ii=1:Sear;
46 n_s = ii/(Sear+1);
47 epsilonbar_s = ii/(Sear+1);
48 epsilonbarprime_s=ii/(Sear+1);
49
50 % Begin search over n: any bits not used to generate key (n) are used for
51 % parameter estimation (m)
52 for iNS = 1:Sear
53     n = n_s(iNS)*N;
54     m=N-n;
55
56         % Begin search over epsilonbar
57         for iebar= 1:Sear
58             epsilonbar=epsilonbar_s(iebar)*(epsilon-epsilonec);
59
60             % Begin search over epsilonbarprime; if
61             % epsilonbarprime>epsilonbar, skip this loop
62             for iebarprime=1:Sear
63                 epsilonbarprime=epsilonbarprime_s(iebarprime)...
64                     *(epsilon-epsilonec);
65                 if epsilonbarprime>epsilonbar
66                     continue;
67                 end
68
69                 % Delta is another information theoretic parameter ...
                       related
70                 % to the finite number of bits exchanged
71                 Δ=2*log2(1/(2*epsilon-epsilonbar-epsilonec)) + ...
                       7*sqrt(n*log2(2/(epsilonbar-epsilonbarprime)));
72
73                 % Squiggle is related to estimating the QBER on a finite
74                 % number of bits m
75                 squiggle=sqrt((2*log(1/epsilonbarprime)+2*log(m+1))/m);
76
77                 % The worst case error rate is QBER + squiggle
78                 e1bar=QBER+squiggle;
79
80                 % H2 is the binary entropy function, and quantifies how
```

```
81                  % much privacy amplification must be performed based ...
                       on the
82                  % worst case error rate, so Hsquiggle is how much extra
83                  % information Alice and Bob share beyond Eve's knowledge
84                  Hsquiggle=1-H2(e1bar);
85
86                  % The final key rate per received coincident pair is then
87                  % 1/2 for the basis sifting, (n/N) for the fraction of
88                  % signals not used for QBER estimation, Hsquiggle for the
89                  % information Alice and Bob share that Eve doesn't know,
90                  % leakEC for the fraction of bits leaked during error
91                  % correction, and Δ as a finite size parameter.
92                  rate=1/2*(n/N)*(Hsquiggle-leakEC_over_n-Δ/n);
93
94                  % If the new rate is better than the old one, take ...
                       this new
95                  % rate and keep searching
96              if  rate>rateMax
97                  rateMax=rate;
98                  nold=n;
99                  mold=m;
100                 epsilonbarold=epsilonbar;
101                 epsilonbarprimeold=epsilonbarprime;
102             end
103
104             end
105 %         end
106     end
107 end
108
109     % The number of secure key bits is then the key rate per coincident
110     % pair times the number of received pairs N.
111     keyLength=rateMax*N;
112
113 end
```

C.2.3 Estimating the success of a Bell test

```
1 function [Bell_paramter]=Bell_paramterer(vis,Nreceived)     %uses the ...
    average entanglement visibility and total counts received to ...
    estimate the Bell parameted. To maximize the Bell violation one ...
```

```
    must use a visibility cut-off to ignore the worst parts of the ...
    pass (this can be optimized for each passes, for simplicity we ...
    used a fixed cut-off of 0.85 in this work). One can also combine ...
    multiple passes to accumulate more statistics (instead of ...
    violating the Bell inequality in a single pass.
2
3 Bell_paramter=2*sqrt(2)*vis-12*sqrt((1-(vis^2)/2)/(Nreceived)); ...
            %Estimates the Bell parameter -3 standard deviations based ...
    on the average entanglement visibility and total received counts.
4
5 %The success of a bell test requires a Bell parameter to be greater ...
    than the classical bound of 2 by 3 standard deviation (the 3 ...
    standard deviations are included in the calculations of ...
    Bell_paramter), if Bell_parameter>2 the the experiment is a succes
```

C.3 Quantum teleportation

A separate program was needed to estimate the performance of quantum teleportation because is uses both an entangled source and a WCP source.

C.3.1 Signal visibility and count rate

```
1 function [counts ...
    vis]=Teleportation(link_dB,darks,eff_local,darks_local,alpha,epsilon)
2 %calculates the count rate and signal visibility from loss and ...
    background count estimates. For the transmitter, eff_local is the ...
    efficiency of the detector and optical components (not in dB), ...
    i.e. eff_local=optical_components*detector, and dark_local is the ...
    dark counts of each the detector. In addition, the strengths of ...
    the WCP ($\alpha$) and of the SPDC ($\epsilon$) must be specified ...
    (optimized for the loss and background).
3 %%Important: darks is the total background counts per detectors ...
    (typically 4 detectors for QKD). The background count (which is ...
    the summed background counts for all detectors) must therefore be ...
    adjusted by dividing by the number of detectors.
4
5 %definitions
6 N=5; %Fock space dimension, N must be minium of 2
7 standard_defintions_qo_toolbox;
```

```
8  no_sources=1;
9  f_laser=1e9;
10 coinc_window=1e-9;
11
12 %coherent state "strength"; mean photon number = alpha^2
13 % alpha=0.55;
14
15 %select type of input
16 % (0) triggered photon from spdc
17 % (1) coherent pulse, with strength alpha
18 % (2) ideal single photon
19 % 4 June 2012: made modificaiton on which mode is transmitted that ...
       renders
20 % triggered spdc and ideal single photos useless.
21 type_input=1;
22
23 %morecomeplete BSM? (0) no, (1) yes
24 mc_bsm=1;
25
26 %Initial efficiencies for detectors and optics
27 effc_apd=0.6;
28
29 effc_optics=0.19;
30 effc_hrld=0.2;
31
32 %detecor noise factor: darks per laser pulse
33 % noise conjector: probability for one click:
34 %Pclick=min(Expect(proj_apd + noise_factor*ida, 1)
35 %exept: if Trace(proj_apd + noise_factor*ida) =< 1
36 % then it is fine!
37 % variation over the darks is simply achieved by making it a vector
38
39 noise_factor=darks*coinc_window;
40 % Darks for local detector
41 noise_factor_local=darks_local*coinc_window;
42
43 %************************ LOOP for the darks ...
       ************************************
44
45 %APD (Bucket Detector) for the Bell analysis
46 [apd_proj un_projapd]=BucketDetector_noise(N,eff_local,noise_factor);
47
48  %APD heralder (Bucket Detector)
49 [apd_hrld un_hrldapd]=BucketDetector_noise(N,effc_hrld*effc_apd,...
```

```
    noise_factor_local);

%Source rate estimation, based on the observed singles and coincidences

singles=1e6;
sgl_n=singles/f_laser;

%solve quadratic euqation for epsilon (determined by the geomtric sum ...
   over
%all elements
% eff=effc_apd*effc_optics;
% epsilon1 = ...
   (eff*sgl_n+sqrt(eff^2*sgl_n^2+4*(eff+sgl_n)*sgl_n))/(2*(eff+sgl_n));
% epsilon2 = ...
   (eff*sgl_n-sqrt(eff^2*sgl_n^2+4*(eff+sgl_n)*sgl_n))/(2*(eff+sgl_n));
% epsilon=(max((epsilon1),(epsilon2)))*sqrt(0.5);
%epsilon for the heralded SPDC input
epsilon_herald=0.2;

% link attenuation

effc_link=10.^(-link_dB/10)/eff_local;

%APD (Bucket Detector) for the final teleported state

[apd_link ...
   un_linkapd]=BucketDetector_noise(N,eff_local,noise_factor_local);

%SPDC in chi2:
H_chi2=(tensor(a,a)+tensor(a',a'))*epsilon;
U_chi2=expm(-1i*H_chi2);

%SPDC input state for pair of photons in HH
spdc_state=tensor(U_chi2*tensor(vacc,vacc));
% spdc_state=tensor(vacc,oneph,oneph,vacc)+tensor(oneph,vacc,vacc,oneph);

% create entangled SPDC state
psi=permute(tensor(spdc_state,spdc_state),[1 3 4 2]);

% Rearrage and add vacuum to apply loss
psi=permute(tensor(psi,vacc,vacc),[1,2,3,5,4,6]);

%Lossy beamspliter
eta=acos(sqrt(effc_link));
```

```
H_bs_loss = (tensor(a,a') + tensor(a',a))*eta;
U_bs_loss = expm(-1i*H_bs_loss);

psi=tensor(ida,ida,ida,ida,U_bs_loss)*psi;
psi=tensor(ida,ida,U_bs_loss,ida,ida)*psi;
psi=permute(psi,[3,5,1,2,4,6]);
%define input states as tensors(H,V); i.e. input polarization=H;
% state: |H1,V1,H2,V2,H3,V3>
% where mode 1 carries the heralded input state, and mode 2 and 3 are the
% entangled state
if type_input==1
    %create input from coherent state
    %Displacement operator, |alpha|^2 = mean photon number
    U_dis=expm(alpha*(a'-a));
    cohr_state=U_dis*vacc;
    in_state=tensor(cohr_state,vacc,psi);
elseif type_input==2
    p_1=alpha^2;
    g_2=0.008;  %from Claudon et al., Nature Photonics 4:174-177 (2010)
    p_2=(1-sqrt(1-4*g_2*alpha^2))/sqrt(8*g_2);
    in_state=tensor(sqrt(1-p_1-p_2)*vacc+sqrt(p_1)*oneph+...
        sqrt(p_2)*twoph,vacc,psi);
elseif type_input==0
    %create  input state from heralded SPDC photons, represented as ...
       an array of the various
    %components as an array of number states (essentially mixed ...
       number state):
    %SPDC for the heralded input photon:
    H_chi2=(tensor(a,a)+tensor(a',a'))*epsilon_herald;
    U_chi2=expm(-1i*H_chi2);

    %SPDC input state for pair of photons in HH
    spdc_hrld=tensor(U_chi2*tensor(vacc,vacc));

    [herald_state ...
       count_prob]=herald_source3(N,spdc_hrld,no_sources,apd_hrld);
    in_state=qo;
    size_hrld=N-1;
    %since we herald the output photons on the trigger event, we need ...
       to only
    %consider the heralded outputs with index one or more.
%     for j=1:size_hrld
%        indx = j;
%        in_state{indx,1}=tensor(herald_state{j+1},vacc,psi);
```

```
%     end
in_state=tensor(herald_state,vacc,psi);
end

%rotate input to +45 input
in_state=tensor(U_had,ida,ida,ida,ida,ida,ida)*in_state;

%****************************************
%Apply the Bell-measurement with a BS
% first move the polarizations together |H1,H2,V1,V2,H3,V3>
out_state=permute(in_state,[1,3,2,4,5,6,7,8]);
%apply BS to the H1,H2, and V1,V2 term
out_state=tensor(U_bs,U_bs,ida,ida,ida,ida)*out_state;
% permute back to |H1,V1,H2,V2>
out_state=permute(out_state,[1,3,2,4,5,6,7,8]);
%****************************************

%measurements, 2 channel analyzers

probs=real(msrmt_3qb_2ch_6mode_mc_BSM2_WCP_transmit(N,out_state,...
    apd_link,un_linkapd,apd_proj,un_projapd,mc_bsm));

det_prob=probs;

vis_hv=(det_prob(1)-det_prob(2))./(det_prob(1)+det_prob(2));
vis_ad=(det_prob(3)-det_prob(4))./(det_prob(3)+det_prob(4));
vis_lr=(det_prob(5)-det_prob(6))./(det_prob(5)+det_prob(6));
count_r=det_prob*f_laser;
vis=vis_ad;
counts=(count_r(:,1)+count_r(:,2));

end
```

```
% perform the tomography measurments for a single channel detector ...
    with a
% the projector matrix on the input state
% State nomenclature is |H1,V1,H2,V2,H3,V3> of the qubit 1 and 2 ...
    respectively
% N is the size of the fock space per mode
% Thomas Jennewein 19.8.2008
% 8. October 2008 Adaptation for teleportation, i.e. modes 1 and 2 are
% projected onto an anticoincidence (BSM), and the mode 3 is observed in
% various polarizations
```

```
%8.8.2008 adaption for more-complete BSM (improves quality!)
% 14.11.2008 choice of more complet ore less complete BSA mcbsa=0 or 1

function ...
    probs=msrmt_3qb_2ch_6mode_mc_BSM2_WCP_transmit(N,in,proj3,unproj3,...
     proj,unproj,mcbsa)
% definitions
ida=identity(N);
a=destroy(N);

%Beam splitter 50:50 = Quater wave plate @ 4 5
eta=1*pi/4;
H_bs = (tensor(a,a') + tensor(a',a))*eta;
U_bs = expm(-1i*H_bs);

%phase operator with i-phase shift
H_ph_i = a'*a.*pi/2;
U_ph_i = expm(-1i*H_ph_i);

%check if in is density operator?
in_shape=in.shape;

% HV basis one mode 3
final_state=in;
HHH=(expect(tensor(proj,unproj,proj,unproj,proj3,unproj3,ida,ida),...
    final_state));
VVH=(expect(tensor(unproj,proj,unproj,proj,proj3,unproj3,ida,ida),...
    final_state));
HVH=(expect(tensor(proj,unproj,unproj,proj,proj3,unproj3,ida,ida),...
    final_state));
VHH=(expect(tensor(unproj,proj,proj,unproj,proj3,unproj3,ida,ida),...
    final_state));

VHV=(expect(tensor(unproj,proj,proj,unproj,unproj3,proj3,ida,ida),...
    final_state));
VVV=(expect(tensor(unproj,proj,unproj,proj,unproj3,proj3,ida,ida),...
    final_state));
HHV=(expect(tensor(proj,unproj,proj,unproj,unproj3,proj3,ida,ida),...
    final_state));
HVV=(expect(tensor(proj,unproj,unproj,proj,unproj3,proj3,ida,ida),...
    final_state));

%P_H3=HHH+VHH+HVH+VVH;
%P_V3=HHV+VHV+HVV+VVV;
```

```
if mcbsa==1
P_H3=VHH+HVH;
P_V3=VHV+HVV;
else
P_H3=VHH+HVH+VVH+HHH;
P_V3=VHV+HVV+VVV+HHV;
end

% LR basis one mode3,
if in_shape(1)==in_shape(2)
    %density matrix
    final_state=tensor(ida,ida,ida,ida,U_bs,ida,ida)'*in...
        *tensor(ida,ida,ida,ida,U_bs);
else
    %state
    final_state=tensor(ida,ida,ida,ida,U_bs,ida,ida)*in;
end

HHL=sum(expect(tensor(proj,unproj,proj,unproj,proj3,unproj3,ida,ida),...
    final_state));
VVL=sum(expect(tensor(unproj,proj,unproj,proj,proj3,unproj3,ida,ida),...
    final_state));
HVL=sum(expect(tensor(proj,unproj,unproj,proj,proj3,unproj3,ida,ida),...
    final_state));
VHL=sum(expect(tensor(unproj,proj,proj,unproj,proj3,unproj3,ida,ida),...
    final_state));


VHR=sum(expect(tensor(unproj,proj,proj,unproj,unproj3,proj3,ida,ida),...
    final_state));
VVR=sum(expect(tensor(unproj,proj,unproj,proj,unproj3,proj3,ida,ida),...
    final_state));
HHR=sum(expect(tensor(proj,unproj,proj,unproj,unproj3,proj3,ida,ida),...
    final_state));
HVR=sum(expect(tensor(proj,unproj,unproj,proj,unproj3,proj3,ida,ida),...
    final_state));

if mcbsa==1
    P_L3=VHL+HVL;
    P_R3=VHR+HVR;
else
    P_L3=HHL+VHL+HVL+VVL;
    P_R3=HHR+VHR+HVR+VVR;
end
```

```
96
97  % AD basis one mode3,
98  if in_shape(1)==in_shape(2)
99      %density matrix
100     final_state=(tensor(ida,ida,ida,ida,ida,U_ph_i)...
101         *tensor(ida,ida,ida,ida,U_bs))'*in...
102         *(tensor(ida,ida,ida,ida,ida,U_ph_i)*...
103         tensor(ida,ida,ida,ida,U_bs));
104 else
105     %state
106     final_state=tensor(ida,ida,ida,ida,U_bs,ida,ida)...
107         *tensor(ida,ida,ida,ida,ida,U_ph_i,ida,ida)*in;
108 end
109 HHA=sum(expect(tensor(proj,unproj,proj,unproj,proj3,unproj3,ida,ida),...
110     final_state));
111 VVA=sum(expect(tensor(unproj,proj,unproj,proj,proj3,unproj3,ida,ida),...
112     final_state));
113 HVA=sum(expect(tensor(proj,unproj,unproj,proj,proj3,unproj3,ida,ida),...
114     final_state));
115 VHA=sum(expect(tensor(unproj,proj,proj,unproj,proj3,unproj3,ida,ida),...
116     final_state));
117
118 VHD=sum(expect(tensor(unproj,proj,proj,unproj,unproj3,proj3,ida,ida),...
119     final_state));
120 VVD=sum(expect(tensor(unproj,proj,unproj,proj,unproj3,proj3,ida,ida),...
121     final_state));
122 HHD=sum(expect(tensor(proj,unproj,proj,unproj,unproj3,proj3,ida,ida),...
123     final_state));
124 HVD=sum(expect(tensor(proj,unproj,unproj,proj,unproj3,proj3,ida,ida),...
125     final_state));
126
127 if mcbsa==1
128 P_A3=VHA+HVA;
129 P_D3=VHD+HVD;
130 else
131 P_A3=HHA+VHA+HVA+VVA;
132 P_D3=HHD+VHD+HVD+VVD;
133 end
134
135 probs=[P_H3,P_V3,P_A3,P_D3,P_L3,P_R3];
136 end
```

C.3.2 Estimating the success of teleportation

```
1 function ...
      [teleportation_vis]=teleportation_visibility(vis,Nreceived)        ...
      %uses the average entanglement visibility and total counts ...
      received to estimate the visibility of quantum teleportation. To ...
      maximize the teleportation visibility one must use a visibility ...
      cut-off to ignore the worst parts of the pass (this can be ...
      optimized for each passes, for simplicity we used a fixed cut-off ...
      of 0.70 in this work, lower than for the previous simulations). ...
      One can also combine multiple passes to accumulate more statistics ...
      (instead of violating the Bell inequality in a single pass.
2
3 teleportation_vis=(vis)-3*sqrt((1-vis)*(1+vis)/(Nreceived));          ...
      %Estimates the teleportation visibility -3 standard deviations ...
      based on the average entanglement visibility and total received ...
      counts.
4
5 %The success of a teleportation requires a teleportation visibility ...
      to be greater than the classical bound of 2/3 by 3 standard ...
      deviation (the 3 standard deviations are included in the ...
      calculations of teleportation_visibility), if ...
      teleportation_visibility>2/3 the the experiment is a success.
6 end
```

Appendix D

List of input parameters used for MODTRAN

For our performance analysis it was necessary to include realistic atmospheric transmission. In order to estimate this transmission we used a software package designed to calculate atmospheric radiative transfer: MODTRAN [80]. MODTRAN is a widely used software distributed by Ontar corporation that was co-developed by the US Air Force Research Laboratory and Spectral Sciences Incorporated. Using this software one can estimate the atmospheric transmittance by appropriately choosing various input parameters to suit a particular situation. In this section we list the input parameters used for our predictions. The descriptions are based on the descriptions in MODTRAN 5.2.1 user's manual with the inputs divided into "cards".

D.1 Rural (5 km vis.) sea-level

This atmosphere type reflects a worst case scenario that would occur if the ground station was restricted to a location close to a city and a sea level. It is unlikely that any real implementations of satellite QKD would be done at a worst location and thus this atmosphere type gives a lower bound on the expected performance.

Table D.1: Card 1: Main radiation transport driver.

Name	**Value**	**Description**
MODTRN	M	MODTRAN band model
SPEED	S	Slow speed Correlated-k option using 33 absorption coefficients (k values) per spectral bin (1 cm^{-1} or 15 cm^{-1})
LYMOLC	blank	Do not include auxiliary species with model atmosphere
MODEL	2	Mid-Latitude Summer (45° North Latitude)
ITYPE	3	Vertical or slant path to space or ground
IEMSCT	0	Program executes in spectral transmittance only mode
IMULT	-1	Program executes with multiple scattering
I_RD2C	0	Normal operation of program
NOPRNT	0	Normal writing to tape6 and tape7
TPTEMP	0	No surface emission if H2 is above ground
SURREF	0.3	Albedo of the earth

Table D.2: Card 1A: Radiative transport driver cont'd.

Name	**Value**	**Description**
DIS	f	The less accurate but faster Isaac's two-stream algorithm is used
DISAZM	f	Not using azimuth dependence with DISORT
DISALB	f	Not calculating the spectral spherical albedo of the atmosphere and diffuse transmittance for the line-of-sight and sun-to-ground paths
NSTR	8	Number of streams to be used by DISORT
SFWHM	0	Use default top-of-atmosphere (TOA) solar data
CO2MX	365	CO_2 mixing ratio in ppmv
H2OSTR	0	Default vertical water vapor column character string
O3STR	0	Default vertical ozone column character string
C_PROF	0	Do not scale default profiles
LSUNFL	f	The solar irradiance data to be used depends on the spectral resolution of the MODTRAN band model
LBMNAM	f	The default (1 cm^{-1} bin) band model database files are to be used
LFLTNM	f	Do not read file name for user-defined instrument filter function from card 1A3
H2OAER	f	Aerosol optical properties are not modified to reflect the changes from the original relative humidity profile arising from the scaling of the water column
SOLCON	0	Do not scale the TOA solar irradiance
CDASTM	blank	Use Angstrom Law description of boundary layer and tropospheric aerosol extinction data
NSSALB	0	Use reference aerosol spectral single scattering albedo values

Table D.3: Card 2: Main aerosol and cloud options.

Name	**Value**	**Description**
APLUS	Blank	Don't use "Aerosol Plus" option
IHAZE	2	RURAL extinction, default VIS=5 km
CNOVAM	Blank	Don't use Navy Oceanic Vertical Aerosol Model (NOVAM)
ISEASN	0	Season determined by the value of MODEL
ARUSS	blank	Don't use user-defined aerosol optical properties
IVULCN	0	Background stratospheric profile and extinction
ICSTL	5	Air mass character (1–10, 1=open ocean, 10=strong Continental influence)
ICLD	0	No clouds or rain
IVSA	0	Army Vertical Structure Algorithm (VSA) not used
VIS	0	Uses the default meteorological range set by IHAZE
WSS	0	Default wind speeds are set according to the value of MODEL
RAINRT	0	Rain rate (mm/hr)
GNDALT	0	Altitude of surface relative to sea level (km)

Table D.4: Card 3: Line-of-sight geometry.

Name	**Value**	**Description**
H1	0	Initial altitude (km)
H2	0	Final altitude, not used for ITYPE=3
RANGE	0	Not used in this case for ITYPE=3
BETA	0	Not used in this case for ITYPE=3
RO	0	Default mid-latitude radius of the Earth (km) of 6371.23 km
LENN	0	Default
PHI	0	Zenith angle at H2 towards H1

Table D.5: Card 4: Spectral range and resolution.

Name	**Value**	**Description**
DV	0.1	Wavelength increment used for spectral outputs (in nm)
FWHM	2	Slit function Full Width at Half Maximum (in nm)

Appendix E

List of publications

E.1 Published papers from prior research

J.-P. Bourgoin, S. Doiron, M. Deveaux, and A. Haché. Single laser beam measurement of thermal diffusivity. *Applied Optics*, 47(35):6530-6534, 2008.

J.-P. Bourgoin, G.-G. Allogho, and A. Haché. Thermal measurement on subnanoliter sample volumes. *Applied Optics*, 49(14):2547-2551, 2010.

J.-P. Bourgoin, G.-G. Allogho, and A. Haché. Thermal conduction in thin films measured by optical surface thermal lensing. *Journal of Applied Physics*, 108(7):073520, 2010.

E.2 Published papers from PhD research

E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss. *Phys. Rev.* A, 84:062326, 2011.

C. Erven, B. Heim, E. Meyer-Scott, J.-P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New J. Phys.*, 14:123018, 2012.

J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J. Phys.*, 15(2):023006, 2013.

E. Meyer-Scott, V. Roy, J.-P. Bourgoin, B. L. Higgins, L. K. Shalm, and T. Jennewein. Generating polarization-entangled photon pairs using cross-spliced birefringent fibers. *Optics Express*, 21(5):6205-6212, 2013.

C. Holloway, J. A. Doucette, C. Erven, J.-P. Bourgoin, and T. Jennewein. Optimal pair-generation rate for entanglement-based quantum key distribution. *Physical Review* A, 87(2):022342, 2013.

Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel, and T. Jennewein. Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links. *J. Lightwave Technol.*, 31(9):1399–1408, 2013.

C. Erven, E. Meyer-Scott, K. Fisher, J. Lavoie, B. L. Higgins, Z. Yan, C. J. Pugh, J.-P. Bourgoin, R. Prevedel, L. K. Shalm, L. Richards, N. Gigov, R. Laflamme, G. Weihs, T. Jennewein, and K. J. Resch. Experimental three-photon quantum nonlocality under strict locality conditions. *Nature Photonics*, 8:292296, 2014.

E.3 Papers in preparation

J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. L. Lütkenhaus, and T. Jennewein. Experimentally simulating quantum key distribution with ground-satellite channel losses and processing limitations.

S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, L. Monat, M. Legré, and V. Makarov. Attacks exploiting deviation of mean photon number in quantum key distribution and coin-tossing.

J.-F. Lavigne, C. J. Pugh, J.-P. Bourgoin, B. L. Higgins, and T. Jennewein. Adaptive Optics for Quantum Key Distribution between an Earth station and a Satellite.

K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Global quantum communication with satellites and quantum repeaters.

J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein. Free-space quantum key distribution link to a moving receiver.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[2] D. R. Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[3] Stefania Cavallar, Bruce Dodson, ArjenK. Lenstra, Walter Lioen, PeterL. Montgomery, Brian Murphy, Herman te Riele, Karen Aardal, Jeff Gilchrist, Grard Guillerm, Paul Leyland, Jel Marchand, Franois Morain, Alec Muffett, Chrisand-Craig Putnam, and Paul Zimmermann. Factorization of a 512-bit rsa modulus. In B. Preneel, editor, *Advances in Cryptology EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 1–18. Springer Berlin Heidelberg, 2000.

[4] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[5] D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post-quantum cryptography*. Springer, 2009.

[6] F. Miller. *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. C.M. Cornwell, 1882.

[7] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.*, 45:295–301, 1926.

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

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, 2009.

[10] M. P. Silverman. *Quantum Superposition: Counterintuitive Consequences of Coherence, Entanglement, and Interference*. Springer, 2008.

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

[12] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989.

[13] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984.

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

[15] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[16] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992.

[17] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford University Press, 2007.

[18] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[19] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696–702, 1935.

[20] E. S. Fry and R. C. Thompson. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 37:465–468, 1976.

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

[22] A. Aspect, P. Grangier, and G. Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1981.

[23] A. Aspect, J. Dalibard, and G. Roger. Experimental test of bell's inequalities using time- varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[24] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.*, 81(23):5039–5043, 1998.

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

[26] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, 2009.

[27] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992.

[28] J. D. Franson and H. Ilves. Quantum cryptography using optical fibers. *Appl. Opt.*, 33(14):2949–2954, 1994.

[29] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84(20):4729–4732, 2000.

[30] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Phys. Rev. Lett.*, 84:4737–4740, 2000.

[31] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.*, 96:070502, 2006.

[32] ID Quantique. http://www.idquantique.com, 2001.

[33] MagiQ Technologies. http://www.magiqtech.com, 1999.

[34] Z. Yan, D. R. Hamel, A. K. Heinrichs, X. Jiang, M. A. Itzler, and T. Jennewein. An ultra low noise telecom wavelength free running single photon detector using negative feedback avalanche diode. *Rev. Sci. Intrum.*, 83:073105, 2012.

[35] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40dB channel loss using superconducting single-photon detectors. *Nature Photonics*, 1:343, 2007.

[36] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11:075003, 2009.

[37] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Exp.*, 18(8):8587–8594, 2010.

[38] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbacha, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Free-space distribution of entanglement and single photons over 144 km. *Nature Physics*, 3:481–486, 2007.

[39] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98(1):010504, 2007.

[40] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han. Field test of wavelength-saving quantum key distribution network. *Opt. Lett.*, 35(14):2454–2456, Jul 2010.

[41] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[42] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma. Network-centric quantum communications. In *Frontiers in Optics 2013*, page FW2C.1. Optical Society of America, 2013.

[43] J. Qiu. Quantum communications leap out of the lab. *Nature*, 508:441442, 2014.

[44] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993.

[45] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932, 1998.

[46] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. de Riedmatten, W. Rosenfeld, A. J. Shields N., Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young. Quantum memories. *The European Physical Journal D*, 58:1–22, 2010.

[47] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33, 2011.

[48] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreuax, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Quantum cryptography for secure satellite communications. In *Aerospace Conference Proceedings, 2000 IEEE*, volume 1, pages 191–200 vol.1, 2000.

[49] G. Gilbert and M. Hamrick. Practical quantum cryptography: A comprehensive analysis (part one). Technical Report MTR00W0000052, The MITRE Corporation, 2000. arXiv:quant-ph/0009027.

[50] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.*, 4:82, 2002.

[51] E. Miao, Z. Han, T. Zhang, and G. Guo. The feasibility of geostationary satellite-to-ground quantum key distribution. *Phys. Lett.* A, 361:29–32, 2007.

[52] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, and A. Setharaman. Performance comparison of BB84 and B92 satellite-based free space quantum optical communication systems in the presence of channel effects. *J. Opt. Commun.*, 32:37–47, 2011.

[53] A. Tomaello, C. Bonato, V. Da Deppo, G Naletto, and P. Villoresi. Link budget and background noise for satellite quantum key distribution. *Advances in Space Research*, 47:802–810, 2011.

[54] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7:382386, 2013.

[55] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photonics*, 7:387393, 2013.

[56] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Daylight quantum key distribution over 1.6 km. *Phys. Rev. Lett.*, 84:5652, 2000.

[57] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf. Present and future free-space quantum key distribution. *Free-Space Laser Communication Technologies XIV*, 4635:116–126, 2002.

[58] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lütkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger. Space-QUEST, experiments with quantum entanglement in space. *Europhysics News*, 40:26–29, 2009.

[59] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss. *Phys. Rev.* A, 84:062326, 2011.

[60] H. Xin. Chinese academy takes space under its wing. *Science*, 332:904, 2011.

[61] H. Takenaka, M. Toyoshima, Y. Takayama, Y. Koyama, and M. Akioka. Experiment plan for a small optical transponder onboard a 50 kg-class small satellite. In *2011 International Conference on Space Optical Systems and Applications*, pages 113–116, 2011.

[62] B. L. Higgins, J.-P. Bourgoin, N. Gigov, E. Meyer-Scott, Z. Yan, and T. Jennewein. Detailed performance analysis of the proposed QEYSSAT quantum receiver satellite. In *Quantum Electronics and Laser Science Conference (QELS)*, 2012.

[63] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A com-

prehensive design and performance analysis of low Earth orbit satellite quantum communication. *New J. Phys.*, 15(2):023006, 2013.

[64] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012.

[65] Analytical Graphics, Inc. STK9. http://www.agi.com, 2010.

[66] J. W. Goodman. *Introduction To Fourier Optics*. Roberts & Compagny Publishers, second edition, 1996.

[67] J. S. Accetta and D. L. Shumaker. *The Infrared and electro-optical systems handbook*, volume 2. Infrared Information Analysis Center and SPIE Optical Engineering Press, 1993.

[68] A. A. M. Saleh. 9.4 - an investigation of laser wave depolarization due to atmospheric transmission. *Quantum Electronics, IEEE Journal of*, 3(11):540–543, 1967.

[69] A. A. Semenov and W. Vogel. Quantum light in the turbulent atmosphere. *Phys. Rev.* A, 80:021802, 2009.

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

[71] D. Y. Vasylyev, A. A. Semenov, and W. Vogel. Toward global quantum communication: Beam wandering preserves nonclassicality. *Phys. Rev. Lett.*, 108:220501, 2012.

[72] C. Erven, B. Heim, E. Meyer-Scott, J.-P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New J. Phys.*, 14:123018, 2012.

[73] L. C. Sinclair, F. R. Giorgetta, W. C. Swann, E. Baumann, I. Coddington, and N. R. Newbury. Optical phase noise from atmospheric fluctuations and its impact on optical time-frequency transfer. *Phys. Rev. A*, 89:023805, Feb 2014.

[74] C. Bonato, A. Tomaello, V. Da Deppo, G Naletto, and P. Villoresi. Feasibility of satellite quantum key distribution. *New J. Phys.*, 11:045017, 2009.

[75] R. Tyson. *Principles of Adaptive Optics*. Taylor & Francis Group, third edition, 2011.

[76] D. H. Tofsted, S. G. O'Brien, and G. T. Vaucher. An atmospheric turbulence profile model for use in army wargaming applications I. Technical Report ARL-TR-3748, U.S. Army Research Laboratory, 2006.

[77] N. Baddour. Operational and convolution properties of two-dimensional fourier transforms in polar coordinates. *J. Opt. Soc. Am.* A, 26:1767–1777, 2009.

[78] M. Toyoshima, Y. Takayama, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, W. Klaus, M. Toyoda, H. Kunimori, T. Jono, and K. Arai. Ground-to-satellite laser communication experiments. *Aerospace and Electronic Systems Magazine, IEEE*, 8:10, 2008.

[79] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics*. Wiley-Interscience, second edition, 2007.

[80] Ontar Corporation. MODTRAN5. http://www.ontar.com, 2010.

[81] R. H. Hadfield. Single-photon detectors for optical quantum information applications. *Nature Photonics*, 3:696–705, 2009.

[82] Micro Photon Devices. http://www.micro-photon-devices.com.

[83] Excelitas. http://www.excelitas.com.

[84] Hamamatsu. http://www.hamamatsu.com.

[85] Photon Spot. http://www.photonspot.com.

[86] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *Journal of Modern Optics*, 51(9-10):1267–1288, 2004.

[87] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields. High speed single photon detection in the near infrared. *Appl. Phys. Lett.*, 91:041114, 2007.

[88] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, A. Dzardanov B. Voronov, C. Williams, and R. Sobolewski. Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.*, 79:705, 2001.

[89] A. J. Miller, S. W. Nam, J. M. Martinis, and A. V. Sergienko. Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination. *Appl. Phys. Lett.*, 83:791, 2003.

[90] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W Nam. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev.* A, 71:061803, 2005.

[91] A. Korneev, V. Matvienko, O. Minaeva, I. Milostnaya, I. Rubtsova, G. Chulkova, K. Smirnov, V. Voronov, G. Gol'tsman, W. Sysz, A. Pearlman, A. Verevkin, and R. Sobolewski. Quantum efficiency and noise equivalent power of nanostructured NbN single-photon detectors in the wavelength range from visible to infrared. *IEEE Transactions on Applied Superconductivity*, 15:571, 2005.

[92] K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren. Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating. *Opt. Exp.*, 14:527, 2006.

[93] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Exp.*, 16:3032, 2008.

[94] B. Baek, A. E. Lita, V. Verma, and S. W. Nam. Superconducting a-W_xSi_{1-x} nanowire single-photon detector with saturated internal quantum efficiency from visible to 1850 nm. *Appl. Phys. Lett.*, 98:251105, 2011.

[95] F. Marsili, F. Najafi, E. Dauler, F. Bellei, X. Hu, M. Csete, R. J. Molnar, and K. K. Berggren. Single-photon detectors based on ultranarrow superconducting nanowires. *Nano Letters*, 11:2048, 2011.

[96] W. L. Stutzman and G. Thiele. *Antenna Theory and Design.* John Wiley and sons, second edition, 1998.

[97] J. Bennett, M. Donahue, N. Schneider, and M. Voit. *The Cosmic Perspective.* Pearson Education, Inc., fifth edition, 2009.

[98] S. Chueca, B. García-Lorenzo, E. G. Mendizábal, T. Varela, J. J. Fuensalida, and C. Muñoz-Tuñón. Input parameters of the HV model above canarian observatories. *Proc. SPIE*, 5237:159–166, 2004.

[99] C. D. Elvidge, K. E. Baught, J. B. Dietz, T. Bland, P. C. Sutton, and H. W. Kroehl. Radiance calibration of DMSP-OLS low-light imaging data of human settlements. *Remote Sens. Environ.*, 68:77–88, 1999.

[100] P. Cinzano, F. Falchi, and C. D. Elvidge. The night sky in the world. www.lightpollution.it/dmsp/, 2001.

[101] K. Krisciunas, W. Sinton, D. Tholen, A. Tokunaga, W. Golisch, D. Griep, C. Kaminsky, C. Impey, and C. Christian. Atmospheric extinction and night-sky brightness at Mauna-Kea. *Publ. Astron. Soc. Pac.*, 99:887–894, 1987.

[102] C. R. Benn and S. L. Ellison. La Palma night-sky brightness. *New Astron. Rev.*, 42:503–507, 1998.

[103] F. Patat. The dancing sky: 6 years of night sky observations at Cerro Parana. *Astronomy & Astrophysics*, 481:575–591, 2008.

[104] K. Krisciunas and B. E. Schaefer. A model of the brightness of moonlight. *Publ. Astron. Soc. Pac.*, 103:1033–1039, 1991.

[105] C. Benn. La Palma sky-brightness calculator. http://catserver.ing.iac.es/signal/signalsky.php, 2010.

[106] P. Cinzano, F. Falchi, C. D. Elvidge, and K. E. Baugh. The artificial night sky brightness mapped from DMSP satellite Operational Linescan System measurements. *Mon. Not. R. Astron. Soc.*, 318:641–657, 2000.

[107] R. Baierlein. *Thermal Physics*. Cambridge University Press, 1999.

[108] K. D. Abhyankar. *Astrophysics of the Solar System*. Sangam Books Limited, 1999.

[109] C. D. Elvidge, P. Cinzano, D. R. Pettit, J. Arvesen, P. Sutton, C. Small, R. Nemani T. Longcore, C. Rick, J. Safran, J.Weeks, and S. Ebener. The Nightsat mission concept. *Int. J. Remote Sens.*, 28:2645–2670, 2007.

[110] R. L. Kurucz, I. Furenlid, J. Brault, and L. Testerman. Solar flux atlas from 296 to 1300 nm. *National Solar Observatory Atlas, Sunspot, New Mexico: National Solar Observatory, 1984*, 1, 1984.

[111] D. J. Rogers, J. C. Bienfang, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, L. Ma, D. H. Su, C. J. Williams, and C. W. Clark. Free-space quantum cryptography in the h-alpha fraunhofer window, 2006.

[112] C. Knight. Field surveys of the effect of lamp spectrum on the perception of safety and comfort at night. *Lighting Research and Technology*, 42(3):313–329, 2010.

[113] T. Jennewein, M. Barbieri, and A. G. White. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. *J. Mod. Opt.*, 58:276–287, 2011.

[114] J. C. Garrison and R. Y. Chiao. *Quantum Optics*. Oxford University Press, 2008.

[115] U. Leonhardt. *Essetial Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.

[116] X.-M. Jin, J.-G. Ren, B. Yang, Z.-H. Yi, F. Zhou, X.-F. Xu, S.-K. Wang, D. Yang, Y.-F. Hu, S. Jiang, T. Yang, H. Yin, K. Chen, C.-Z. Peng, and J.-W. Pan. Experimental free-space quantum teleportation. *Nature Photonics*, 4(6):376–381, 2010.

[117] S. M. Tan. A computational toolbox for quantum and atomic optics. *Journal of Optics B: Quantum and Semiclassical Optics*, 1(4):424, 1999.

[118] C. C. Gerry and P. L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[119] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.*, 4:325–360, 2004.

[120] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, M. Takeoka, M. Fujiwara, and M. Sasaki. Polarization-basis tracking scheme in satellite quantum key distribution. *International Journal of Optics*, 2011:254154–1–8, 2011.

[121] L. Kral, I. Prochazka, and K. Hamal. Optical signal path delay fluctuations caused by atmospheric turbulence. *Opt. Lett.*, 30(14):1767–1769, Jul 2005.

[122] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869, Mar 1995.

[123] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J. Phys.*, 4:44, 2002.

[124] A. Niederberger, V. Scarani, and N. Gisin. Photon-number-splitting versus cloning attacks in practical implementations of the bennett-brassard 1984 protocol for quantum cryptography. *Phys. Rev. A*, 71:042316, Apr 2005.

[125] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 3*, ISIT'09, pages 1879–1883. IEEE Press.

[126] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev.* A, 72(1):012326, 2005.

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

[128] S.-H. Sun, L.-M. Liang, and C.-Z. Li. Decoy state quantum key distribution with finite resources. *Phys. Lett.* A, 373(30):2533–2536, 2009.

[129] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100(20):200501, 2008.

[130] C. Erven, X. Ma, R. Laflamme, and G. Weihs. Entangled quantum key distribution with a biased basis choice. *New J. Phys.*, 11:045025, 2009.

[131] X. Ma, C.-H. F. Fung, and H.-K. Lo. Quantum key distribution with entangled photon sources. *Phys. Rev.* A, 76:012307, 2007.

[132] H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi. Stable source of high quality telecom-band polarization-entangled photon-pairs based on a single, pulse-pumped, short ppln waveguide. *Opt. Express*, 16(17):12460–12468, Aug 2008.

[133] R. Colbeck and R. Renner. No extension of quantum theory can have improved predictive power. *Nature Communications*, 2:411–1–5, 2011.

[134] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, and A. Zeilinger. Violation of local realism with freedom of choice. *Proc. Natl. Acad. Sci. USA*, 107:19708, 2010.

[135] D. Rideout, T. Jennewein, G. Amelino-Camelia, T. F. Demarie, B. L. Higgins, A. Kempf, A. Kent, R. Laflamme, X. Ma, R. B. Mann, E. Martn-Martnez, N. C. Menicucci, J. Moffat, C. Simon, R. Sorkin, L. Smolin, and D. R. Terno. Fundamental quantum optics experiments conceivable with satellitesreaching relativistic distances and velocities. *Classical and Quantum Gravity*, 29(22):224011, 2012.

[136] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969.

[137] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher T. Jennewein, and A. Zeilinger. High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics*, 5:389–392, 2009.

[138] Y. Zhang, S. Glancy, and E. Knill. Asymptotically optimal data analysis for rejecting local realism. *Phys. Rev. A*, 84:062118, Dec 2011.

[139] J. R. Taylor. *An Introduction to Error Analysis: The Study of Uncertainties in Physical Measurements*. University Science Books, 1997.

[140] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[141] O. Landry, J. A. W. van Houwelingen, A. Beveratos, H. Zbinden, and N. Gisin. Quantum teleportation over the Swisscom telecommunication network. *J. Opt. Soc. Am.* B, 24:398, 2007.

[142] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488:185, 2012.

[143] X. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489:269, 2012.

[144] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Phys. Rev.* A, 57(4):2368–2378, 1998.

[145] J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Grard. A highly efficient single-photon source based on a quantum dot in a photonic nanowire. *Nature Photonics*, 4:174–177, 2010.

[146] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical Bell-state analyzer. *Applied Physics B*, 72:67–71, 2001.

[147] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[148] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.*, 96:161102, 2010.

[149] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.*, 6:1008, 2012.

[150] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger. Feasibility of 300km quantum key distribution with entangled states. *New J. Phys.*, 11:085002, 2009.

[151] D. Wylie, D. L. Jackson, W. P. Menzel, and J. J. Bates. Trends in global cloud cover in two decades of HIRS observations. *Journal of Climate*, 18:3021, 2005.

[152] W. H. Mott, R. B. Sheldon, P. O. McVay, and L. P. Sheldon. *Laser Satellite Communication: The Third Generation*. Quorum Books, 2000.

[153] X. Sun, M. A. Krainak, J. B. Abshire, J. D. Spinhirne, C Trottier, M Davies, H. Dautet, G. R. Allan, A. T. Lukemire, and J. C. Vandiver. Space-qualified silicon avalanche-photodiode single-photon-counting modules. *J. Mod. Opt.*, 51(9-10):1333–1350, 2004.

[154] M. Marisaldi, P. Maccagnani, F. Moscatelli, C. Labanti, F. Fuschino, M. Prest, A. Berra, D. Bolognini, M. Ghioni, I. Rech, A. Gulinatti, A. Giudice, G. Simmerle, D. Rubini, A. Candelori, and S. Mattiazzo. Single photon avalanche diodes for space applications. *IEEE Nuclear Science Symposium Conference Record*, pages 116–126, 2011.

[155] O. Keskin, L. Jolissaint, and C. Bradley. Hot-air optical turbulence generator for the testing of adaptive optics systems: principles and characterization. *Appl. Opt.*, 45(20):4888–4897, Jul 2006.

[156] E. Meyer-Scott. Experimental quantum communication in demanding regimes. Master's thesis, University of Waterloo, 2011.

[157] A. Gulinatti, I. Rech, P. Maccagnani, M. Ghioni, and S. Cova. Improving the performance of silicon single-photon avalanche diodes, 2011.

[158] A. Gulinatti, I. Rech, F. Panzeri, C. Cammi, P. Maccagnani, M. Ghioni, and S. Cova. New silicon SPAD technology for enhanced red-sensitivity, high-resolution timing and system integration. *Journal of Modern Optics*, 59(17):1489–1499, 2012.

[159] Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel, and T. Jennewein. Novel high-speed polarization source for decoy-state

BB84 quantum key distribution over free space and satellite links. *J. Lightwave Technol.*, 31(9):1399–1408, 2013.

[160] EOspace. http://www.eospace.com.

[161] Xilinx. http://www.xilinx.com.

[162] Hittite Microwave Corporation. https://www.hittite.com.

[163] M. Jofre an A. Gardelein, G. Anzolin, W. Amaya, J. Capmany, R. Ursin, L. Penate, D. Lopez, J. L. S. Juan, J. A. Carrasco, F. Garcia, F. J. Torcal-Milla, L. M. Sanchez-Brea, E. Bernabeu, J. M. Perdigues, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri. Fast optical source for quantum key distribution based on semiconductoroptical amplifiers. *Opt. Exp.*, 19(5):38253834, 2011.

[164] Thorlabs. http://www.thorlabs.com.

[165] J. B. Altepeter, D. F. V. James, and P. G. Kwiat. Qubit quantum state tomography. *Lect. Notes Phys.*, 649:113–145, 2004.

[166] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger. A fully automated entanglement-based quantum cryptography system for telecom fiber networks. *New J. Phys.*, 11(4):045013, 2009.

[167] Dotfast Consulting. http://www.dotfast-consulting.at/.

[168] Freescale. i.MX53 Quick Start Board. http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=IMX53QSB.

[169] N. Gigov. Quantum key distribution data post-processing with limited resources: Towards satellite-based quantum communication. Master's thesis, University of Waterloo, 2013.

[170] D. J. C. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. *Electronics Lett.*, 33:457–458, 1997.

[171] H. Krawczyk. LFSR-based hashing and authentication. In Y. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, volume 839", year = 1994 of *Lecture Notes in Computer Science*, pages 129–139. Springer Berlin / Heidelberg.

[172] X.-Y. Hu, E. Eletheriou, and D. Arnold. Source code for Progressive Edge Growth parity-check matrix construction. http://www.inference.phy.cam.ac.uk/mackay/PEG_ECC.html, 2003.

[173] X.-Y. Hu, E. Eleftheriou, and D.M. Arnold. Regular and irregular progressive edge-growth Tanner graphs. *IEEE Transactions on Information Theory*, 51(1):386–398, 2005.

[174] J. Martinez Mateo. *Efficient Information Reconciliation for Quantum Key Distribution*. PhD thesis, Universidad Politecnica de Madrid, 2011.

[175] D. Pearson. High-speed qkd reconciliation using forward error correction. In *Proc. 7th International Conference on Quantum Communication, Measurement and Computing (QCMC)*, pages 299–302, 2004.

[176] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel. Proof-of-concept of real-world quantum key distribution with quantum frames. *New J. Phys.*, (9):095001.

[177] P. Chan. Low-density parity-check codes for quantum key distribution. Master's thesis, University of Calgary.

[178] U. Raviteja and A. Thangaraj. In *The National Conference on Communications (India)*.

[179] T. Tsurumaru, W. Matsumoto, and T. Asai. QKD post-processing algorithms of mitsubishi electric corporation. AIT QKD Post Processing Workshop 2011, 2011.

[180] R. M. Gray. Toeplitz and circulant matrices: A review. *Foundations and Trends in Communications and Information Theory*, 2(3):155–239, 2005.

[181] G. H. Golub and C. F. Van Loan. *Matrix Computations*. The Johns Hopkins University Press, 1996.

[182] M. Hayashi. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Transactions on Information Theory*, 57(6):3989–4001, 2011.

[183] R. Y. Q. Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.*, 11(4):045024, 2009.

[184] L. Alkalai. An Overview of Flight Computer Technologies for Future NASA Space Exploration Missions. *Acta Astronautica*, 52:857–867, 2003.

[185] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[186] T. M. Cover and J. A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006".

[187] D. Elkouss, J. Martinez-Mateo, and V. Martin. Information reconciliation for quantum key distribution. *Quantum Info. Comput.*, 11(3):226–238, 2011.

[188] M. Bajracharya, M. W. Maimone, and D. Helmick. Autonomy for Mars Rovers: Past, Present, and Future. *Computer*, 41(12):44–50, 2008.

[189] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss. Fundamental finite key limits for information reconciliation in quantum key distribution. 2014. arXiv:1401.5194.

[190] W. L. Harper and C. A. Hooker. *Foundations of Probability Theory, Statistical Inference, and Statistical Theories of Science: Volume II Foundations and Philosophy of Statistical Inference*. The Western Ontario Series in Philosophy of Science. Springer, 1975.

[191] B. J. Nicholson. On the f-distribution for calculating bayes credible intervals for fraction nonconforming. *Reliability, IEEE Transactions on*, R-34(3):227–228, Aug 1985.

[192] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S. Gigan. Measuring the transmission matrix in optics: An approach to the study and control of light propagation in disordered media. *Phys. Rev. Lett.*, 104:100601, 2010.

[193] I. M. Vellekoop and C. M. Aegerter. Scattered light fluorescence microscopy: imaging through turbid layers. *Opt. Lett.*, 35(8):1245–1247, 2010.

[194] S. Popoff, G. Lerosey, M. Fink, A. C. Boccara, and S. Gigan. Image transmission through an opaque material. *Nature Communications*, 1(81):1–5, 2010.

[195] C.-L. Hsieh, Y. Pu, R. Grange, G. Laporte, and D. Psaltis. Imaging through turbid layers by scanning the phase conjugated second harmonic radiation from a nanoparticle. *Opt. Exp.*, 18(20):20723–20731, 2010.

[196] X. Xu, H. Liu, and L. V. Wang. Time-reversed ultrasonically encoded optical focusing into scattering media. *Nature Photonics*, 5:154157, 2011.

[197] E. G. van Putten, D. Akbulut, J. Bertolotti, W. L. Vos, A. Lagendijk, and A. P. Mosk. Scattering lens resolves sub-100 nm structures with visible light. *Phys. Rev. Lett.*, 106:193905, 2011.

[198] Y. Choi, T. D. Yang, C. Fang-Yen, P. Kang, K. J. Lee, R. R. Dasari, M. S. Feld, and W. Choi. Overcoming the diffraction limit using multiple light scattering in a highly disordered medium. *Phys. Rev. Lett.*, 107:023902, 2011.

[199] A. Velten, T. Willwacher, O. Gupta, A. Veeraraghavan, M. G. Bawendi, and R. Raskar. Recovering three-dimensional shape around a corner using ultrafast time-of-flight imaging. *Nature Communications*, 3(745):1–8, 2012.

[200] O. Katz, E. Small, and Y. Silberberg. Looking around corners and through thin turbid layers in real time with scattered incoherent light. *Nature Photonics*, 6:549553, 2012.

[201] M. Malik, O. S. Magana-Loaiza, and R. W. Boyd. Quantum-secured imaging. *Appl. Phys. Lett.*, 101(24):241103, 2012.

[202] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, S. R. McNown, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, C. G. Peterson, K. T. Tyagi, L. Mercer, and H. Dardy. Optical networking for quantum key distribution and quantum communications. *New Journal of Physics*, 11(10):105001, 2009.

[203] B. Qi, W. Zhu, L. Qian, and H.-K. Lo. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, 12(10):103042, 2010.

[204] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan. Metropolitan all-pass and inter-city quantum communication network. *Opt. Exp.*, 18(26):27217–27225, 2010.

[205] C. Holloway, E. Meyer-Scott, C. Erven, and T. Jennewein. Quantum entanglement distribution with 810 nm photons through active telecommunication fibers. *Opt. Exp.*, 19(21):20597–20603, 2011.

[206] D. Elkouss, J. Martinez-Mateo, A. Ciurana, and V. Martin. Secure optical networks based on quantum key distribution and weakly trusted repeaters. *J. Opt. Commun. Netw.*, 5(4):316–328, 2013.

[207] B. Frhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields. A quantum access network. *Nature*, 501:6972, 2013.

[208] Da-Lite. http://www.da-lite.com.

[209] E Hecht. *Optics*. Pearson Education, fourth edition, 2002.

[210] Photon Engineering. http://www.photonengr.com.

[211] Ming Zhang, Liang Zhang, Jincai Wu, Shiji Yang, Xiong Wan, Zhiping He, Jianjun Jia, D. S. Citrin, and Jianyu Wang. Detection and compensation of basis deviation in satellite-to-ground quantum communications. *Opt. Exp.*, 22(8):9871–9886, 2014.

[212] T. Zhongkan, R. Chandrasekara, Y. Y. Sean, C. Cheng, C. Wildfeuer, and A. Ling. Near-space flight of a correlated photon system. 2014. arXiv:1404.3971.

[213] Newport. http://search.newport.com.

[214] Google. Google Earth. http://www.google.com/earth.

[215] E. Bagan, M. Baig, and R. Mu noz Tapia. Quantum reverse engineering and reference-frame alignment without nonlocal correlations. *Phys. Rev. A*, 70:030301, 2004.

[216] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

[217] J. Bae and A. Acín. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A*, 75:012334, 2007.

[218] U. M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, May 1993.

[219] R. J. Hughes and J. E. Nordholt. Long-range quantum cryptography: Amplified quantum key distribution (aqkd). 2014. arXiv:1406.6990.

[220] EMCORE. http://www.emcore.com.

[221] HC Photonics. http://www.hcphotonics.com.