Experimental quantum communication in demanding regimes

by

Evan Meyer-Scott

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

Waterloo, Ontario, Canada, 2011

AUTHOR'S DECLARATION

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.

Evan Meyer-Scott

Abstract

Quantum communication promises to outperform its classical counterparts and enable protocols previously impossible. Specifically, quantum key distribution (QKD) allows a cryptographic key to be shared between distant parties with provable security. Much work has been performed on theoretical and experimental aspects of QKD, and the push is on to make it commercially viable and integrable with existing technologies. To this end I have performed simulations and experiments on QKD and other quantum protocols in regimes previously unexplored.

The first experiment involves QKD via distributed entanglement through the standard telecommunications optical fibre network. I show that entanglement is preserved, even when the photons used are a shorter wavelength than the design of the optical fibre calls for. This surprising result is then used to demonstrate QKD over installed optical fibre, even with co-propagating classical traffic. Because the quantum and classical signals are sufficiently separated in wavelength, little cross-talk is observed, leading to high compatibility between this type of QKD and existing telecommunications infrastructure.

Secondly, I demonstrate the key components of fully-modulated decoy-state QKD over the highest-loss channel to date, using a novel photon source based on weak coherent (laser) pulses. This system has application in a satellite uplink of QKD, which would enable worldwide secure communication. The uplink allows the complex quantum source to be kept on the ground while only simple receivers are in space, but suffers from high link loss due to atmospheric turbulence, necessitating the use of specific photon detectors and highly tailored photon pulses. My results could be applied in a near term satellite mission.

Acknowledgements

My heartfelt thanks go to my supervisor Thomas Jennewein, for his guidance, support, enthusiasm and counsel on How Science Works. I also thank the members of my committee, Kevin Resch and Norbert Lütkenhaus, for finding subtle problems previously unknown and answering my many questions. Finally I thank Melanie Campbell for agreeing to examine this thesis.

Many thanks go to my collaborators Zhizhong Yan, Allison MacDonald, Jean-Philippe Bourgion, Max Julian, Catherine Holloway, Hannes Hübel, and especially Chris Erven for his loads of help with QKD over the installed fibre link.

I am grateful for my desk's location, as it offered the opportunity for many good discussions with Dave Pitkänen, Rolf Horn, Botan Khani and ultimately Deny Hamel, who helped me in all aspects of science and life.

For the local area QKD experiment I would like to thank Greg Cummings and Bruce Campbell of IST UW, John McCormick, Joy Montgomery, Hon Lau, and Joe Stauttener of IT at PI and Châteauneuf François of INO for test fibres.

I acknowledge Matthew Skala for this thesis template and Florian Knorn for the M-code package for MATLAB code in LaTeX.

I should also like to acknowledge the various funding agencies that have contributed to this work: NSERC (QuantumWorks, Discovery), OCE, CIFAR, CFI, and ERA. I was personally funded by NSERC (CGS), the Bell Family Fund for Quantum Computing, the IQC Achievement Award and OGS, for which I am very grateful.

Dedicated to my wife Kirstyn.
Thank you for being there and here.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Quantum information

Broadly speaking, the study of quantum information involves the data storage, manipulation, and computational abilities of quantum systems. In contrast to classical bits which can take only values 0 and 1, qubits (quantum bits) instead reside in quantum states $|0\rangle$ and $|1\rangle$. Since the two level qubit is a quantum system, the states can also exist in arbitrary superpositions, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. These superpositions, along with entanglement between qubits (i.e. stronger-than-classical correlations) allow quantum information to perform tasks impossible classically, such as quantum teleportation [8] and quantum key distribution [34], and perform other tasks much faster, such as factoring [103]. In this chapter I will detail the components of quantum information that lead to quantum communication, and review the basic principles of quantum key distribution.

1.1.1 Photons as qubits

Though there are many quantum systems that can be used to encode qubits, I will focus only on photons as they are most relevant to communication. A photon is the smallest unit of light, with energy E related to the wavelength λ by $E = \frac{hc}{\lambda}$, where h is Planck's constant and c is the speed of light. Qubits can be encoded onto photons in a number of different ways, including polarisation, location, time-bin and frequency. This thesis focuses on polarisation encoding, where the logical state $|0\rangle_L$ is encoded as horizontal polarisation of one photon $|H\rangle$ and $|1\rangle_L$ as vertical polarisation $|V\rangle$. Other states of importance are $|\pm\rangle_L = \frac{1}{\sqrt{2}}\left(|0\rangle_L \pm |1\rangle_L\right)$, or in polarisation encoding, $|\pm\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle \pm |V\rangle\right)$. Thus single qubit rotations are easily performed with half- and quarter-waveplates, and entanglement in the

form of two-photon Bell-states is easy produced through spontaneous parametric down-conversion (see Subsection 4.2.1). Photons interact weakly with the environment, leading to low decoherence, but making multi-qubit gates difficult. Nonetheless, this problem can be overcome with two-photon entangling gates that rely on post-selection [56].

1.1.2 No-cloning theorem

A significant property of quantum information is that an arbitrary unknown state cannot be perfectly cloned [128, 21]. Classically, of course, information can be copied arbitrarily many times without penalty, but the no-cloning theorem enforces a restriction on quantum cloners. The proof by counterexample is as follows [78]: Suppose I have a quantum cloner with unitary U capable of copying a state $|\psi\rangle$ to some ancilla qubit $|z\rangle$: $U|\psi\rangle \otimes |z\rangle = |\psi\rangle \otimes |\psi\rangle$. The cloner must also be able to copy another state $|\phi\rangle$: $U|\phi\rangle \otimes |z\rangle = |\phi\rangle \otimes |\phi\rangle$. Taking the inner product of these two equations gives

$$\left(\langle\phi| \otimes \langle z|U^\dagger\right)\left(U|\psi\rangle \otimes |z\rangle\right) = \left(\langle\phi| \otimes \langle\phi|\right)\left(|\psi\rangle \otimes |\psi\rangle\right) \tag{1.1}$$

$$\langle\phi|\psi\rangle\langle z|z\rangle = \langle\phi|\psi\rangle\langle\phi|\psi\rangle \tag{1.2}$$

$$\langle\phi|\psi\rangle = \left(\langle\phi|\psi\rangle\right)^2. \tag{1.3}$$

This has two solutions, $\langle\phi|\psi\rangle = 0$ or $\langle\phi|\psi\rangle = 1$, meaning that $|\phi\rangle$ and $|\psi\rangle$ are either the same state or orthogonal states. Thus the perfect quantum cloner cannot work on arbitrary states. This significant result has the implication that an unknown state cannot simply be cloned and measured many times to gain information, a requirement for the security of quantum key distribution.

1.1.3 Entanglement and tests of quantum mechanics

Entanglement is seen as a hallmark of quantum mechanics as it cannot be simulated classically. A common example of maximally-entangled two-qubit states are the four Bell-states on Hilbert spaces A and B (tensor products between A and B are omitted for brevity):

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\right) \tag{1.4}$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right) \tag{1.5}$$

If qubits A and B were classically correlated instead of entangled, measurement in the $0/1$ basis would reveal perfect correlation, but measurement in the $+/-$ basis would lead to no correlation, as each qubit would then independently and randomly fall into the $|+\rangle$ or $|-\rangle$ eigenstate. By contrast, rewriting $|\Phi^+\rangle$ in the $+/-$ basis through the substitution $|0/1\rangle = \frac{1}{\sqrt{2}}(|+\rangle \pm |-\rangle)$ gives:

$$|\Phi^+\rangle = \frac{1}{2\sqrt{2}}\left[\left(|+\rangle_A + |-\rangle_A\right)\left(|+\rangle_B + |-\rangle_B\right) + \left(|+\rangle_A - |-\rangle_A\right)\left(|+\rangle_B - |-\rangle_B\right)\right] \quad (1.6)$$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B\right) \quad (1.7)$$

Similar to the other Bell-states, $|\Phi^+\rangle$ will give perfect correlations in the H/V and $+/-$ measurement bases, a hallmark of entanglement's stronger than classical correlations.

Indeed this distinction between classical correlations and entanglement led to the Bell-type inequalities [5] following Einstein, Podolsky and Rosen's argument that quantum mechanics is incomplete [26]. The Bell-type inequalities assume local, realistic theories and local hidden variables to derive a bound on some value based on independent measurements of correlated but distant systems. For example, the Clauser-Horne-Shimony-Holt (CHSH) inequality (Equation 1.8) bounds the parameter S_{CHSH} by 2, while quantum mechanics predicts a maximal value of $2\sqrt{2}$.

$$S_{CHSH} = |E(\phi_A, \phi_B) - E(\phi_A, \phi'_B)| + |E(\phi'_A, \phi_B) + E(\phi'_A, \phi'_B)| \leq 2, \quad (1.8)$$

As shown in Subsection 3.3.1, the correlation values $\left|E(\phi_A, \phi_B)\right| \leq 1$ are determined by many measurement outcomes with measurement settings ϕ_A and ϕ_B respectively on distant photons A and B in correlated (or entangled) states. The measurement settings $\{\phi_{A/B}\}$ determine, for example, the polarisation angles to be measured on photons A and B respectively.

1.2 Quantum key distribution

Quantum cryptography, and specifically quantum key distribution (QKD), promise to remove assumptions on computational power of an eavesdropper and allow provably secure communication between distant parties. The general idea is that quantum states are used as information carriers, with randomly chosen bits encoded in randomly chosen mutually unbiased bases. These bases are chosen such that their measurement operators are non-commuting, i.e. information

cannot be learned about the quantum state in both bases simultaneously. For photons, two such polarisation bases are H/V and $+/-$: a photon prepared in $|H\rangle$ and measured in the $+/-$ basis will give either outcome with equal probability and end up in either the $|+\rangle$ or $|-\rangle$ eigenstate, leaving no information on its previous state. Therefore if photons are sent in a randomly chosen basis, an eavesdropper cannot directly measure to gain full information about a single photon as she does not know the correct basis, and in fact disturbs the state [42]. Thanks to the no-cloning theorem, the eavesdropper is also unable to clone the photon and perform many measurements to gain knowledge [128, 21]. The disturbances introduced by eavesdroppers (call them Eve) allow the legitimate parties (call them Alice and Bob) to detect eavesdropping, and abort the protocol. If there is no eavesdropping, the protocol produces a shared, random, private key between Alice and Bob, which they can then use in the provably secure Vernam cipher (one-time pad) [123] to communicate. The Vernam cipher requires a private and random key as long as the message to be sent, and is secure so long as the key is used only once, then discarded. Thus QKD addresses the question begged by the Vernam cipher, namely the problem of distributing many keys between distant parties with provable and compassable security. For a good review of QKD see Reference [34].

1.2.1 Relationship to classical cryptography

Classical public key cryptography such as RSA [93], commonly used over the internet, relies on assumptions on an eavesdropper's computing power: if a quantum computer were realised, RSA would be immediately insecure due to the quantum computer's speedup in factoring. Additionally, an attacker could store the public key and cipher text until computing power advances, and recover the secret message then. QKD, by contrast, is only vulnerable during key exchange. Once the private key is shared, the security of the Vernam cipher makes the communication invulnerable to attacks. Of course, side-channel attacks on specific implementations of QKD during and after key exchange are a problem (Subsection 2.1.2), and individuals can always surrender information, but the underlying protocol is secure indefinitely.

1.2.2 QKD Protocols

BB84: 4-state qubit protocol

Charles Bennett and Gilles Brassard invented the first QKD protocol, dubbed BB84 in 1984 [7]. In this protocol, Alice sends photonic qubits to Bob, with random basis and bit value, then Bob measures each in a randomly chosen basis.

Afterwards, they perform basis sifting over a classical channel, wherein they compare the basis value for each of Bob's detections, discarding those where they do not agree. Now, crucially, Alice and Bob compare some of their remaining bits to determine the quantum bit error rate (QBER). If this QBER is greater than a predetermined security limit, Eve could have gained too much information, and the protocol must be aborted. If not, Alice and Bob perform error correction and privacy amplification over the classical channel. Error correction and privacy amplification are classical protocols that ensure Alice and Bob's keys agree, and that they are uncorrelated to the eavesdropper respectively. Privacy amplification consumes key to reduce the eavesdropper's information on the remaining bits; how much key must be consumed is determined by the QBER.

Security of QKD

Security of the theoretical QKD protocol is well proven. Mayers first proved security in 1996 [74], inspiring future proofs based on the uncertainty principle by Koashi [57]. Shor and Preskill in 2000 [104] made a simple and compelling proof based on entanglement distillation. They used the property of quantum mechanics that if Alice and Bob can verify that they share a *pure* entangled state, no one else can be correlated with it. This therefore removes the possibility of Eve's knowledge as she is not correlated with Alice and Bob's state before they measure. Through a series of reductions, the security of BB84 is then derived, resulting in a secret key for $QBER \lesssim 11\%$.

Renner, Gisin, and Kraus improved these proofs with information theoretic notions rather than entanglement purification [91]. Their proof introduces ε-security, where the key shared between Alice and Bob is identical and perfectly secure except with probability ε. This ε is bounded from below:

$$\delta\left(\rho_{S_A S_B E'}\ ,\ \rho_{SS} \otimes \rho_{E'}\right) \leq \varepsilon. \tag{1.9}$$

Here $\delta(x, y)$ is the trace distance between density operators x and y, and $\rho_{S_A S_B E'}$ is the total joint state between Alice, Bob, and Eve, based on Alice's key S_A, Bob's key S_B and Eve's state E', which may be partially correlated with Alice and Bob. The perfectly secure situation is described by $\rho_{SS} \otimes \rho_{E'}$, where Alice and Bob are separable from Eve, and Alice and Bob each hold the same uniformly random key S. Thus the lower the probability of failure (insecure key) required by the application, the closer the state held by Alice, Bob and Eve must be to the perfect case. Based on this "closeness," a lower bound on the secret key rate can be derived from the entropy (uncertainty) of Eve's knowledge of the key.

A loophole is introduced in BB84 if the information carriers are not perfect single photons, but rather photonic modes that may contain one or more photons. Modes of light are solutions to Maxwell's equations and are defined by polarisation $\boldsymbol{\sigma}$ and momentum vector $\boldsymbol{k}$. Fock states are simple occupation numbers of photons in modes and form a basis, e.g. $|2\rangle_{\boldsymbol{\sigma},\boldsymbol{k}}$ means two photons in the mode defined by $(\boldsymbol{\sigma},\boldsymbol{k})$. They are states not generally found in nature and difficult to produce and control exactly. A laser, which would be very convenient to use as a photon source for QKD, produces the so-called coherent state, which can be represented as a sum over all Fock states.

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{1.10}$$

The "strength" of the coherent state is given by α, and $\mu = |\alpha|^2$ is the average number of photons in the mode. Also relevant to photonic states are the creation and annihilation operators $\hat{a}^\dagger$ and $\hat{a}$, with actions $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$, $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$, and $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ for Fock state $|n\rangle$ or coherent state $|\alpha\rangle$.

The upshot of Equation 1.10 for QKD is that, when using a laser as the photon source, one can never be assured of true single photons as there is a chance for higher photon numbers in every pulse. This allows Eve to perform a photon number splitting attack [67], preferentially admitting pulses with more than one photon such that she can store one and measure it later when Alice and Bob reveal their bases, gaining full information without detection.

Hence the decoy-state protocol was invented [48, 71], wherein Alice changes randomly the average photon number of the pulses she sends between signal states (used for key generation) with high average photon number and decoy states with lower average photon number. Intuitively, using decoy states allows Alice and Bob to detect the photon number splitting attack in the following way. The detection probability for a coherent state with average photon number μ after a channel with single-photon transmission η (assuming threshold detectors) is

$$P_{det}(\mu) = 1 - e^{-\mu\eta} + Y_0 \tag{1.11}$$

for background count probability Y_0 and assuming both Y_0 and η are small. This assumes η is independent of the average photon number, which is true for a passive channel but not during the case of the photon number splitting attack. Since Eve's attack depends on blocking all single-photon pulses (since she can gain no information from these) and admitting only multi-photon pulses, Eve will be more likely to block decoy pulses with lower average photon number. To

ensure the Bob's detection rate is undisturbed by this blocking, Eve may employ a (so far unrealized but physically allowed) lossless channel for the remaining pulses, effectively increasing the transmission of multi-photon pulses. So now Alice and Bob measure two different values of P_{det} for signal states μ and decoy states ν, with $\mu > \nu$:

$$P_{det}(\mu) = 1 - e^{-\mu\eta_\mu} + Y_0 \tag{1.12}$$

$$P_{det}(\nu) = 1 - e^{-\nu\eta_\nu} + Y_0 \tag{1.13}$$

where now η, the channel transmission, is allowed to depend on μ and ν to allow for the possibility of the photon number splitting attack. If Alice and Bob determine through the two values of P_{det} that $\eta_\mu \neq \eta_\nu$, i.e. the channel acts nonlinearly on their signal and decoy states, they cannot rule out the photon number splitting attack and must assume it is occurring.

In practice, Alice and Bob use the multiple P_{det} values to place an upper bound on Eve's information on the shared key through quantum optical and information theoretic relations as shown in Section 5.3. The decoy-state protocol allows Alice and Bob to put much tighter bounds on the number of pulses exchanged that contained exactly one photon and so were secure against the photon number splitting attack, and also the error rate of these single-photon pulses. It is assumed Eve has full information on pulses with more than one photon, so the maximum length of the secure key is upper bounded by this number of single photon pulses, and therefore no secure key is generated if the photon number splitting attack occurs since Eve blocks all single photon pulses. If Eve attacks only some pulses or none at all, the tighter bounds on single photon detection and error rates allow higher average photon number while maintaining security, such that the BB84 protocol with decoy states maintains the same loss scaling of secure key rate as with perfect single photons. I used the decoy-state protocol in an experiment over a high loss channel below (Chapter 5).

BBM92: implementation with entangled states

A number of years after BB84, it was discovered that entanglement could be used for QKD as well, by Ekert (E91 protocol) [27] and also by Bennet, Brassard and Mermin (BBM92 protocol) [9]. These protocols use the perfect correlations of Bell-states (Equation 1.7) that remain even as the measurement basis (on both sides) is rotated to an arbitrary angle. Like BB84, it is sufficient to detect pairs in both the H/V and $+/-$ bases to estimate Eve's information. The protocol and security from Bob's point of view is equivalent to BB84, while Alice, instead of preparing states based on random bit and basis choices, measures her half

of the entangled pairs just as Bob does. BB84 and BBM92 can be seen as formally equivalent if Alice's source in BB84 is replaced an entangled source and a projective measurement; thus the security of BBM92 follows from the security of BB84. In Chapter 4, I modified a free-space QKD system based on BBM92 to provide keys from entanglement through optical fibres.

1.2.3 Exploring demanding regimes

As seen in subsequent chapters, I considered a number of experiments and protocols in new regimes. First, in Chapter 3 I simulated quantum communication in the context of a satellite mission. These would of course be the longest distance to date Bell-type tests, teleportation, or QKD, and so would have to cope with high optical losses and short time intervals for transmission. Nonetheless, these tests are important fundamentally to ensure entanglement is preserved over long distances and through changing gravitational fields, to verify long distance teleportation as a precursor to entanglement swapping, and to enable global QKD respectively. Next in Chapter 4, I performed QKD using short wavelength entangled photons in standard telecom optical fibres. This is unique in that it was unclear if entanglement would be preserved due to higher order spatial modes in the fibre. This work enables QKD in installed optical fibres with classical communication present, with no crosstalk due to the large separation in wavelength. Finally in Chapter 5, I present an experimental verification of the feasibility of QKD for a satellite uplink. To cope with the high channel losses in this new regime, I constructed a novel source for QKD, which output photons at shorter wavelength than any QKD source previously, allowing optimised transmission and detection. This is an important test as it verified the feasibility of QKD over a very lossy channel, showing such a satellite mission is achievable.

Chapter 2

Implementations of quantum communication

In this chapter I shall draw a distinction between *local area QKD* and *global QKD*. The former defines QKD on the scale of campuses and cities, and brings secure keys to the end user. The latter enables worldwide secure communication, and so should operate without distance limitations. Global QKD, however, may not be able to deliver keys directly to the user, possibly connecting only one central node per region from which local area QKD can operate. Additionally I will address some other long distance quantum communications experiments, as extending the range over which we can control quantum transmissions is important both for fundamental experiments and in practical applications.

2.1 Local area QKD

Local area QKD operates on the scale of tens of kilometres to allow key sharing between different offices in a university or divisions of a large company across a campus or city. It should fit smoothly into existing information technology infrastructure and not require installing dedicated optical fibres or construction of free space optical links. In this section I will highlight work on point-to-point QKD links and networks, and address integrability in current telecommunications infrastructure. In addition to the hardware discussed below, key generation and management software is required to interface between the quantum layer and the user layer [98], serving up keys to various users as required.

2.1.1 Point-to-point links

The essential form of QKD is the two-user point-to-point link. This allows key sharing between two distant users (Alice and Bob) and requires either direct photon transmission from Alice to Bob [7], or a source of entangled photons with direct transmission to both [27, 9]. Many such QKD systems have been constructed (Table 2.1), both with entanglement [52, 84, 29] and without [6, 115, 31, 45, 46, 59, 37, 36]. Some offer secure key rates beyond 1 Mbit/s [22, 23, 130], while others have distributed keys over fibre lengths up to 250 km [25, 107, 65] or free space links 144 km long [101, 100].

Group	System	Distance	Secure key rate
Zeilinger, 2000 [52]	Ent.	360 m (1 km fibre)	400 bits/s
Zeilinger, 2004 [84]	Ent.	1.45 km installed fibre	80 bits/s
Weihs, 2008 [29]	Ent.	1.6 km free space	85 bits/s
Bennett, 1992 [6]	LED	32 cm free space	1.2 bits/s
Townsend, 1994 [115]	WCP	10 km fibre	16 kbits/s
Franson, 1994 [31]	WCP	10 m fibre	0.3 bits/s
Hughes, 2002 [45, 46]	WCP	10 km free space (day)	245 bits/s
Rarity, 2002 [59]	WCP	23.4 km free space	200 bits/s
Buller, 2004 [37]	WCP	3.75 km fibre	140 kbits/s
Shields, 2004 [36]	WCP	122 km fibre	0.2 bits/s
Shields, 2008 [22]	WCP	20 km fibre	1.02 Mbit/s
Shields, 2010 [23]	WCP	50 km fibre	1.002 Mbits/s
Yamamoto, 2009 [130]	WCP	10 km fibre	1.3 Mbits/s
Shields, 2009 [25]	Ent.	200 km fibre	0.1 bits/s
Pan, 2010 [65]	WCP	200 km fibre	15 bits/s
Gisin, 2009 [107]	WCP	250 km fibre	15 bits/s
Zeilinger, 2007 [101]	WCP	144 km free space	12.8 bits/s
Zeilinger, 2009 [100]	Ent.	2×144 km free space	0.02 bits/s

Table 2.1: Summary of previous experimental implementations of QKD. Ent. means entanglement-based QKD, and WCP means weak coherent pulses from a laser were used. A general progression to higher key rates and longer distances is evident, but it is also clear that a particular system does not have to break each record each time to be notable.

Commercial availability

In addition to the experimental implementations above, a number of commercial QKD systems have emerged. Three products are currently on the market: IDQ

offers a plug-and-play system based on the SARG protocol which is capable of key distribution up to 100 km and can provide around 12 AES 256 bit keys per minute [49]. MagiQ offers a solution aimed at enterprise Virtual Private Networks, which can distribute keys over 140 km when decoy states are employed, and refresh AES keys up to 100 times per second, though this key rate comes at a much shorter distance than the maximum [72]. Finally, the newest entry, Quintessence Labs, uses continuous variable bright lasers to distribute keys, limiting distance to 20 km. Their claims are more vague and no definable product is apparent [86].

2.1.2 Quantum hacking

To learn about and protect against attacks not covered in security proofs (side-channel attacks), groups in Toronto, Ontario, (Hoi-Kwong Lo) and Tronheim, Norway (Vadim Makarov) are very active in the new field of quantum hacking. They seek to compromise implementations of QKD and in doing so learn how to improve security through theoretical and experimental adjustments. The general idea is to control Bob's detectors such that Eve and Bob have identical results in both basis and bit value, while introducing few or no errors. Eve then simply follows along as Bob and Alice perform basis sifting, error correction and privacy amplification, resulting in full knowledge of the key.

Makarov began in 2001 with an attack that used bright light to interrogate Bob's basis settings, allowing Eve to intercept Alice's signal and resend the correct signal to avoid increasing the error rate. The solution proposed is to add a delay line before Bob's detectors, such that Bob can set his detection basis faster than Eve can interrogate it [121]. Lo then demonstrated the so-called time-shift attack on a commercial QKD system employing gated photon detectors [131]: As two or more detectors are generally used in QKD systems and detectors cannot be made to match perfectly, there may be a time during the opening and closing of the detector gates where the detectors have a mismatched efficiency. Eve can exploit this mismatch by shifting Alice's legitimate signals in time, thereby biasing Bob's results to the detector with higher efficiency and gaining probabilistic information. Quantum hacking then rose to prominence with the advent of detector control attacks, whereby bright light is used to push detectors (specifically, avalanche photodiode single-photon detectors) into linear mode, such that the output signal is proportional to the input illumination and no longer registers single photons. Thus Eve has full control of Bob's detectors and can implement an intercept-resend attack with impunity. This detector control attack and variants have been recently been characterised [73], implemented [69, 127, 32], and secured against [68]. All this hacking underscores the importance of considering security

of specific implementations of QKD and subjecting them to rigorous trials.

2.1.3 QKD Networks

In order to connect multiple users without dedicated point-to-point links between each pair, some form of networking is required. The most readily achievable format is to connect trusted nodes (i.e. nodes which exclude Eve) with point-to-point links. Consider two users, Alice and Bob, connected by single links to an independent trusted node (see Figure 2.1). Alice and Bob each perform QKD with the trusted node to establish separate secure keys, and the node transfers Alice's key to Bob using Bob's key as a one time pad. The node must be trusted since it knows both the interim and final keys.

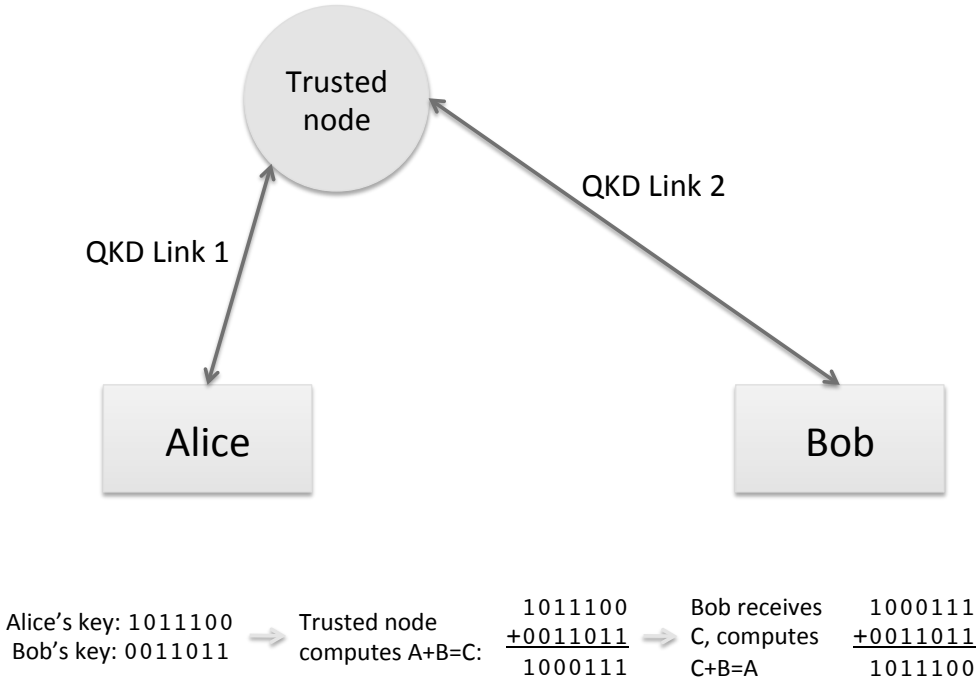

Figure 2.1: Schematic of trusted node architecture for QKD network. QKD Links 1 and 2 perform independent key distributions, leading to Alice and Bob's independent keys, both known also to the trusted node. The node combines the keys in a bitwise XOR, and sends the combined key to Bob. By performing again a bitwise XOR, Bob can use his key to extract Alice's. In effect, Bob's key is used as a one time pad for Alice's key.

Another possibility to connect multiple users is using entanglement. A central source of entangled photon pairs could act as a service provider selling entanglement to end users. When two specific users want to communicate, half of each entangled pair is routed to each user, allowing them to perform the BBM92 protocol and generate a secure key. This scheme has the added benefit that the source need not be trusted, as the protocol relies only the final entanglement correlations, and can handle the case of entanglement faked by an eavesdropper [9].

Network implementations

Three major (and many smaller) QKD network demonstrations have taken place around the world. First, the DARPA Quantum Network was operational with six users by 2004, stretching 20 km around Boston, Massachusetts [28]. It comprises weak coherent pulse, entanglement, and free space QKD over its various links plus photon switching, as in Figure 2.2a. Next in 2008, the SECOQC QKD Network in Vienna, Austria focused on the trusted node architecture and included a similar variety of point-to-point technologies [79]. The eight links between six nodes are shown in Figure 2.2b, and featured more automation and improved key management. Most recently in 2010, the Tokyo QKD Network, spanning 90 km on its longest link as shown in Figure 2.2c, demonstrated automatic rerouting around eavesdropping (Figure 2.3), ensuring uninterrupted key refreshing [98].

2.1.4 QKD integration in existing infrastructure

One of the challenges for local area QKD is to integrate key distribution into existing infrastructure, namely installed optical fibres. Most implementations mentioned above require dark fibres, i.e. single-use fibres carrying no classical traffic. By contrast, QKD has been shown at an early stage to be compatible with classical traffic so long as the two are separated in wavelength, e.g. 1300 nm and 1550 nm [116]. Difficulty arises in moving the QKD to a densely multiplexed scheme to increase transmission distance where the quantum and classical carriers are separated by only a few hundred GHz around the standard telecommunications wavelength of 1550 nm. As the classical information has many orders of magnitude more optical power, crosstalk into the quantum channel becomes a major issue due to four-wave mixing or Raman scattering in the fibre [81]. Hence, local networks would best be served with lossier short wavelength QKD to ensure good quality transmission compatible with classical traffic, while longer distances require dark fibres or other solutions.

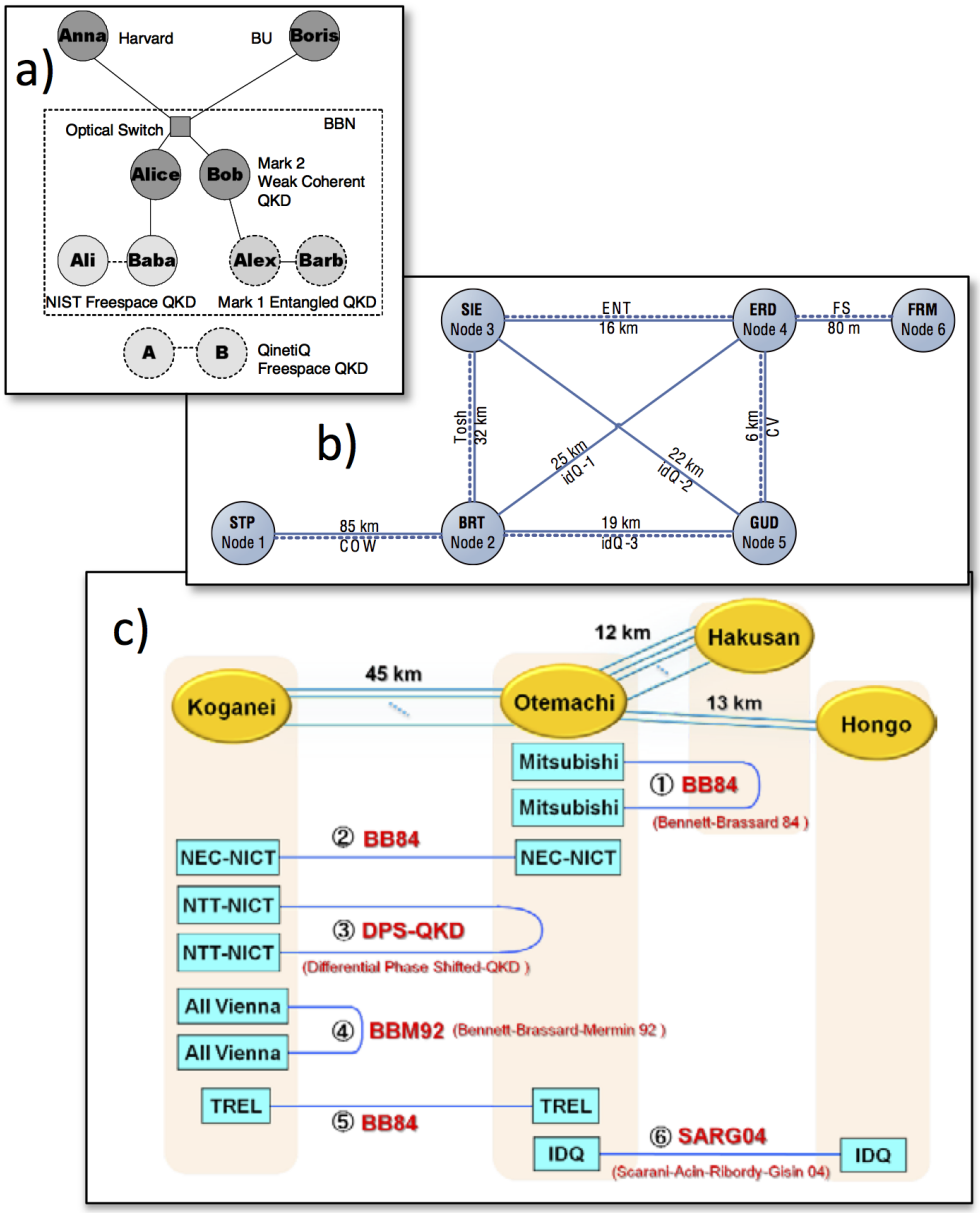

Figure 2.2: Major QKD network implementations. Each network comprises multiple QKD links and technologies in the trusted node scheme. Figures a, b, and c are from the DARPA Quantum Network [28], the SECOQC QKD Network [79] and the Tokyo QKD Network [98] respectively

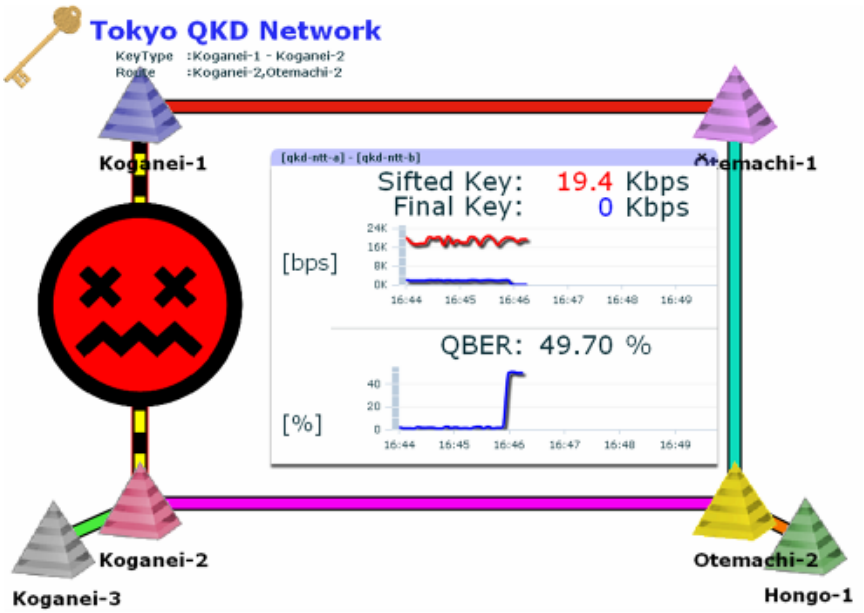

Figure 2.3: Tokyo QKD Network rerouting from [98]. In this screen capture of the Tokyo QKD networks's response to an attack, the software sees a spike in QBER and so shuts down the link, rerouting key distribution around the eavesdropper. Realistic attacks would be much more subtle than to create a 50 % QBER, but in principle the rerouting succeeds.

2.2 Global QKD

As discussed above, many implementations of point-to-point QKD and networks have been demonstrated on the scale of tens to hundreds of kilometres. However, the longest distances over which QKD has been demonstrated are 250 km in ultra-low-loss fibre [107], and 144 km in free space [101, 100]. Global QKD should bridge the gaps between local networks and operate essentially without distance limitation. In this section I will show why QKD has a distance limitation, and three different but possibly compatible proposals to overcome it.

2.2.1 Distance limitation for direct transmission

Unlike classical cryptography, QKD depends on the specific physical system used for data transmission: it must be a quantum system comprised of two or more nonorthogonal quantum states. A major drawback of the photons used in QKD is channel transmission loss. The best optical fibres today show a loss of 0.18 dB/km, which means they lose 50 % of the photons after only 16 km, and require a specific photon wavelength to achieve even this performance [113]. At a 500 MHz source rate, this loss means only one photon would make the 900 km from Ottawa to Washington, D.C. every 15 months! Through free space, the channel loss is highly dependent on atmospheric conditions, and can range a full order of magnitude from 25 dB to 35 dB over a 144 km link [120]. (See Table 2.1 for a list of QKD implementations and their distance limitations.) Since quantum mechanics guarantees by the no-cloning theorem that the unknown quantum state required for QKD cannot be copied [128, 21], there is no way to directly amplify the photons. But even at very long distance, some photons, probabilistically, will arrive at the receiver, so why cannot a secure key be generated from them? Since QKD relies on the quantum bit error rate (QBER) to estimate an eavesdropper's information, spurious detections have a deleterious effect on the ability to prove security. Practical detectors exhibit dark counts (i.e. register detections with no photon present), so at long distances so few photons arrive that dark counts determine the QBER, which reaches 50 % since the dark counts occur randomly. This leads to the typical sharp cutoff (beyond which no secure key can be generated) on plots of secure key rate versus distance, as exemplified in Figure 2.4.

To be specific, I assume a BB84 QKD protocol using perfect single photons (i.e. qubits) with perfect encoding and no decoherence, and asymptotically large in number. I will hence calculate the maximum distance in fibre for positive key rate given a dark count rate per second d. Assuming also that the QBER E is identical in each basis, and that one basis used preferentially with probability

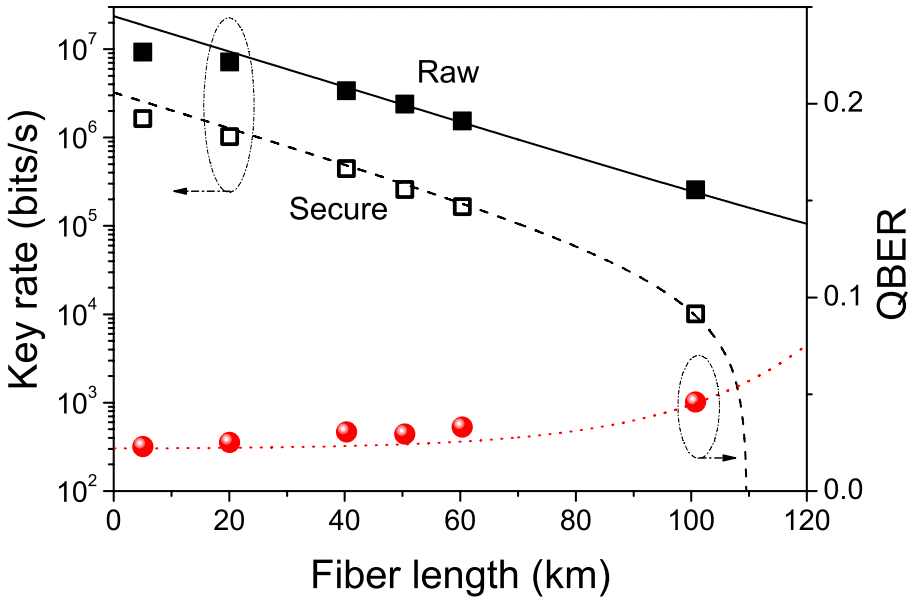

Figure 2.4: Distance limitation in QKD from [22]. The raw key rate falls linearly on the log scale, but as the arriving photon rate falls near the dark count rate, the QBER rises rapidly, causing secure key rate to drop to zero.

approaching 1, the secure key rate per second is [38]

$$R = R_{det}(1 - H_2(E)) \tag{2.1}$$

where R_{det} is Bob's total detection rate and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Secure key rate R stays positive for $E < 0.11$, so to determine the maximum distance possible, the dependence of E on distance must be calculated:

$$E = \frac{0.5d}{R_{det} + d} = \frac{0.5d}{S10^{\frac{-\eta L}{10}} + d}. \tag{2.2}$$

Here S is the source rate of emitted qubits, η is the efficiency of the quantum channel in dB/km and L is the length of the quantum channel. (Photon detectors are assumed to have perfect efficiency.) Solving for L given $E < 0.11$ gives

$$L < \frac{-10}{\eta}\log_{10}\left(\frac{3.54d}{S}\right). \tag{2.3}$$

For realistic values of $S = 500$ MHz, $d = 1000$ counts/s and $\eta = 0.2$ dB/km, the maximum secure distance for QKD is 257 km, before taking into account any other experimental imperfections or information theoretic security considerations. It is clear then that other solutions are needed to extend the range of QKD beyond simple point-to-point links for global coverage.

2.2.2 Quantum repeaters

Quantum repeaters hold the promise of sharing entanglement over arbitrarily long distances using entanglement swapping [50] and quantum memories [66, 41, 30]. The idea of quantum repeaters is to distribute entanglement along many pairs of short links, and store the entanglement in (potentially untrusted) quantum memories, as in Figure 2.5. Multiple levels of entanglement swapping are subsequently performed between neighbours, resulting in a final entangled state between the most distant nodes, which can be used in the BBM92 protocol to generate a secure key.

A significant proposal for the implementation of quantum repeaters was made in 2001 by Duan, Lukin, Cirac and Zoller [24]. This scheme uses atomic ensembles as both the source of entanglement and the quantum memory, relying on a stimulated Raman transition to both emit a photon and excite the ensemble. As these events occur only together, entanglement is present between the photon mode and the atomic ensemble. Modes from adjacent ensembles are interfered on a 50:50 beamsplitter and if one photon is detected, the atomic ensembles are

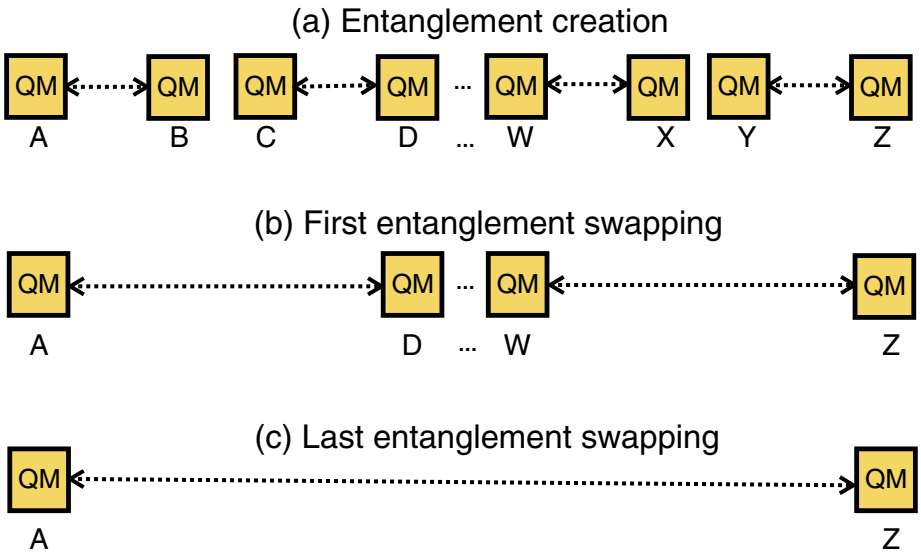

Figure 2.5: Quantum repeater operation from [97]. In step a), entanglement is distribution on each of the short links A-B, C-D, etc. Next in b), the first entanglement swapping is performed between B & C and between X & Y, leading to entanglement between A & D and between W & Z. This step is performed multiple times as more nodes are added. Finally in c) the last entanglement swap is performed, entangling the two end nodes A & Z.

cast into a state of the form

$$|\Psi_\phi\rangle_{LR}^{\pm} = \frac{\left(S_L^\dagger \pm e^{i\phi} S_R^\dagger\right)}{\sqrt{2}} |0\rangle_L |0\rangle_R. \tag{2.4}$$

Here L and R mean the left-hand and right-hand atomic ensembles, ϕ is an unknown phase between them, and $S^\dagger$ is the creation operator on the atomic ensemble. This satisfies step a) of Figure 2.5. Next, entanglement swapping is performed by converting the collective atomic excitations of the two memories (e.g. B & C) into a photon by applying a Raman retrieval pulse. These two modes impinge on a beamsplitter as in step a) to cast the distant quantum memories A & D into an entangled state given by Equation 2.4; repeating this step allows finally the end nodes to share entanglement.

Despite the soundness of the proposal and experimental progress [18, 129], quantum repeaters have yet to surpass the performance of direct photon transmissions, and the way forward is not clear [97]. The limited success thus far is due partly to the difficulty in combining good fidelity, long storage time, and high efficiency in a single quantum memory, and partly to the difficulty of performing high fidelity entanglement swapping (see Subsection 2.3.2). In the end, quantum repeaters would be an excellent solution for future as they require only untrusted nodes, but are so far impractical to implement, and may require thousands of memories even to span 1000 km [89], leaving open the question of near-term global QKD.

2.2.3 Ground-based trusted nodes

A somewhat weaker version of the quantum repeater is to use a string of trusted nodes to generate a secure key between distant Alice and Bob. Similar to the networks of Subsection 2.1.3, the trusted nodes perform independent key distributions to adjacent nodes and so build up security until the end nodes share a key. To reach long distances, many nodes are required, and each one must be completely trusted for final security between the end users. This constraint can be relaxed by allowing multiple trusted-node paths from Alice to Bob and taking a final key as a combination of the keys from all paths; so long as at least one path is uncorrupted, Alice and Bob's key is secure [96]. Additionally, the cost-effectiveness of such trusted node chains has been calculated, with the conclusion that an optimum is achieved at much shorter link distances than the maximum of each individual QKD system [2]. However, the question of maintaining security in so many intermediate nodes and the difficulty of crossing oceans leads to consideration of satellites as trusted nodes.

2.2.4 QKD with satellites

Orbiting satellites as intermediate nodes for QKD present the most viable method of distributing keys globally, as it is generally accepted that some level of key distribution is possible with current technology [88, 124, 11]. Whether the first upcoming demonstration missions can evolve to a functioning commercial quantum network is unclear and requires more technology development [77].

Satellite QKD falls into two main categories, dependent on whether the satellite acts as an untrusted or trusted node. In the former case, the satellite contains a source of entangled photon pairs. One photon of each pair is then sent directly to each receiving party who use entanglement correlations to verify security; this is secure even if the source is operated by Eve [9]. The difficulty in this implementation arises in that, for a satellite to be in view of very distant ground stations simultaneously, it must be far from Earth, leading to a very high channel loss. It would be rather convenient to use a Geostationary satellite, as it could distribute keys to approximately half the earth essentially indefinitely. Unfortunately, this puts the satellite 36 000 km from Earth, leading to a channel loss far beyond the capability of current technology, despite the optimistic conclusions of Reference [76]. Architectures beyond the simple triangular key distribution above have been considered as well [4], including satellites as passive relays [94] and inter-satellite links [82], but these scenarios are even more difficult.

A more readily implemented case is to allow the satellite to be trusted, so that it acts as in Figure 2.6, reconciling Alice's and Bob's independent key distributions into a shared key known to Alice, Bob and the satellite. In contrast to the ground-based trusted nodes, a satellite is generally not static, meaning it can perform key distribution with Alice first as it passes over her location, then with Bob some time later at an arbitrarily distant point, transforming it into a "trusted courier." Routine orbit analysis is necessary to ensure the satellite passes over the desired ground stations within a reasonable time interval, allowing frequent key refreshes. This implementation is the most readily achievable as it requires only single quantum links upward or downward and can be implemented on a Low Earth Orbit satellite of height $400 - 1000$ km, keeping the channel loss to reasonable levels. This is therefore the most likely scenario to be realised first, with demonstration launches expected in $2013 - 2015$.

Proof-of-principle Satellite QKD experiments

A number of experiments have sought to confirm the feasibility of ground-to-satellite key exchange, usually concentrating on the single downlink case. Richard Hughes and colleagues demonstrated key exchange over a 0.5 km [45] and then 10 km [46] free-space link in daylight, and suggested their results could

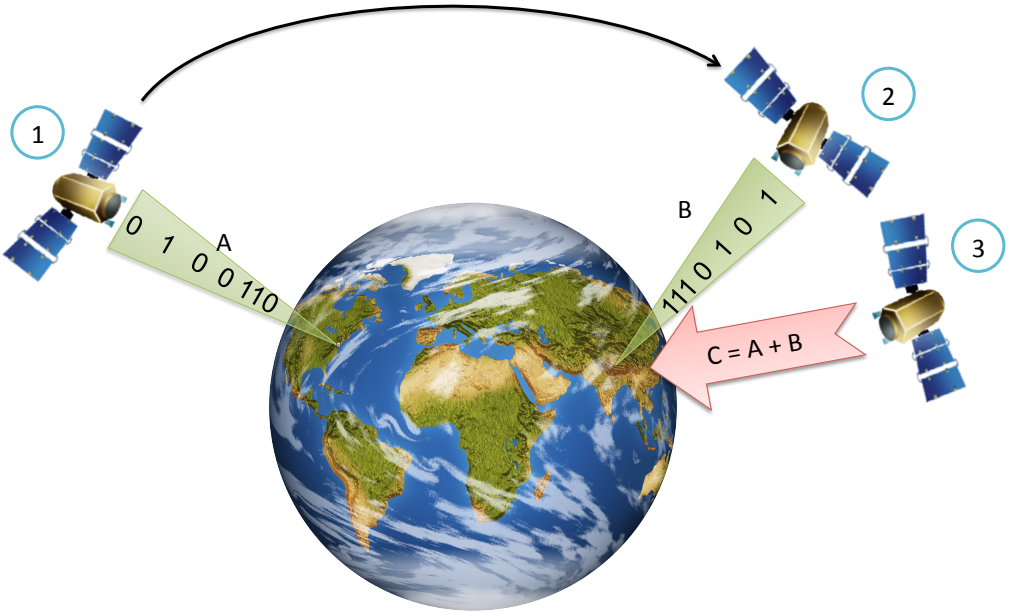

Figure 2.6: Satellite as a trusted node for QKD. The satellite performs key distribution with Alice (step 1) to obtain key A and subsequently with Bob (step 2) to obtain key B as it passes over his location. The satellite computes $C = A + B$ then returns C to Bob through a classical channel (step 3) who can use his key B to decrypt Alice's key $A = C + B$.

extend to satellite links. Tobias Schmitt-Manderbach, et al., later demonstrated QKD over a 144 km free-space link, passing through much more atmosphere than would be encountered on a satellite link, and again suggesting satellite QKD should be possible [101]. The same link was used by Thomas Scheidl, et al., to demonstrate the feasibility of entanglement-based QKD from space to ground [100]. Finally, an experiment was performed by Paolo Villoresi, et al., which directed weak laser pulses at an retro-reflective orbiting satellite 1485 km high, allowing measurement of return single photon statistics, and showing only present-day technology is required [124].

2.3 Further long distance quantum communication experiments

A number of other interesting experiments comprise active areas of research. In this section I will detail a few relevant experiments and their impacts.

2.3.1 Long distance fundamental tests

Since quantum mechanics' formulation in the early 20th century, many experiments have been derived to test its veracity. From Sir G.I. Taylor's first double-slit experiments with "feeble light" [112] to Alain Aspect's violation of a Bell-type inequality [3], photons have emerged as a convenient and versatile quantum system. Aspect's experiment (Figure 2.7) was the first in a long line to use entangled photons to attempt to deny a classical description of the world and confirm quantum mechanics. Aspect, et al., used a source of entangled photon pairs, with one photon directed to each of two receivers. These receivers made uncorrelated but nonrandom measurement choices, and a violation of Bell's inequality by five standard deviations was observed. Weihs, et al. [126], made an improvement in that they separated spatially the two receiving stations, allowing no information to travel between the receivers. Their measurement choices were set by quantum random number generators, and were fast enough such that no influence (at light speed or less) could reach the other receiver before detection. Thus quantum mechanics was shown to be incompatible with theories that are both local and realistic. More recently, a violation of Svetlichny's inequality was demonstrated [63], showing quantum mechanics incompatible with some *non*local and realistic theories. This experiment requires three-photon entanglement and observation of detection probabilities with many combinations of measurement settings, and so far has not been performed with separated observers. As more complex entangled states are produced, tighter bounds will be able to be placed on classes of acceptable theories and our understanding of quantum mechanics' place in science will deepen.

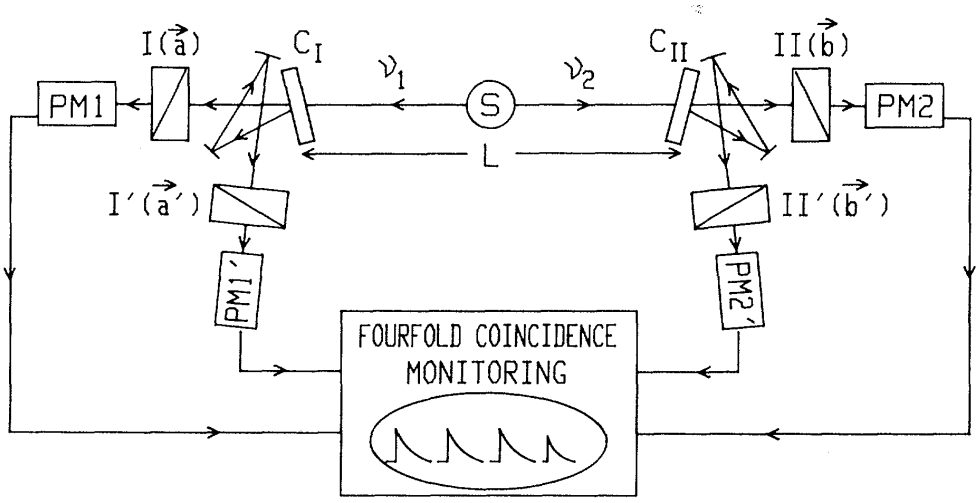

Figure 2.7: Aspect's test of quantum mechanics from [3]. A source S of entangled photons ν_2 and ν_2 is placed midway between observers a and b. The switching device C_I chooses the measurement ($\overrightarrow{a}$ or $\overrightarrow{a}'$) to give the outcome $I\left(\overrightarrow{a}\right)$ or $I'\left(\overrightarrow{a}'\right)$ respectively. PM means photomultiplier, the single photon detectors used which output electrical signals to the coincidence monitoring device.

Longer transmission distances on these tests are required for two fundamental reasons: First, the farther apart each party, the tighter locality is enforced; i.e. no "hidden variable" information can be transmitted between stations, even with slower switching speeds or randomness generation. Secondly, longer distance is intrinsically interesting, as new physics may emerge as entangled photons are brought farther apart, or made to pass through differing gravitational fields. Furthermore, if a quantum link to a satellite is realised, additional tests become possible. For a single link, there is a non-standard theory which predicts gravitationally-induced decoherence when half of an entangled pair is sent through a gravitational gradient as would be seen from ground to a satellite [87]. Violations of Bell's inequality additionally become possible over larger distances than ever, which is of debatable importance, as known gravitational effects are predicted to be too weak to measure [62]. Of perhaps more interest is the idea to test quantum entanglement with fast moving satellite observers, which could be arranged such that neither observer appears to have measured first in its own reference frame [80]. Quantum mechanics predicts no change of outcomes based on time ordering, and so this interplay with relativity could be directly tested.

2.3.2 Quantum teleportation

Charles Bennett and coauthors in 1993 proposed a method of "teleporting an unknown quantum state" of an input qubit $|\psi\rangle_{in}$ without those systems having interacted, destroying the input state in the process [8]. It requires initial entanglement between Bob's distant qubit B and Alice's local qubit A to interact with the input system, for example in the Bell-state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$. The total state between the three qubits is then $\frac{1}{\sqrt{2}}|\psi\rangle_{in} \otimes \left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$. In a photonic context, the particle to be teleported is interacted with Alice's half of an entangled pair, and these photons ($in \otimes A$) are projected onto a Bell-state and measured. The two-bit outcome c of this projection measurement is forwarded to Bob whose qubit was projected into one of four states correlated with c. Bob performs one of four unitaries depending on c on his photon to correct it to the initial input state $|\psi\rangle_B$. Thus information transfer is still bounded by light speed, but the quantum state is transferred with theoretically perfect fidelity, though only 2 classical bits were sent. Teleportation was first demonstrated experimentally by Bouwmeester, et al., who showed a decrease in detection probability when Bob's photon is measured with polarisation perpendicular to Alice's input photon, evidence that Alice's input state was teleported to Bob [13]. Ursin, et al., improved upon these results, teleporting a state across the river Danube with much higher fidelities [118].

The most immediate application of teleportation is as a precursor to entanglement swapping and hence to quantum repeaters. Here the input state $|\psi\rangle_{in}$ itself is entangled to another distant system D, resulting in entanglement between D and B after teleportation. The difference from previously mentioned experiments is that for entanglement swapping, the photons that interfere in the joint Bell-state measurement are from independent sources and have travelled long distance. This makes it much more difficult to get sufficient indistinguishability between these photons for a high-fidelity measurement, due to spectral, timing, and spatial mode differences. Some progress has been made interfering entangled photons from separate sources connected with only electrical timing, giving hope to long-distance entanglement swapping [53].

Chapter 3

Modelling and simulation of quantum communication

Quantum optics experiments are generally an expensive endeavour, and their initial setup and incremental improvements are sometimes quite slow. In this light it is important to have a fast and flexible system to determine which experiments are possible under what conditions, and what level of performance is needed for success. At the same time, theorists at times need to test their work in an accessible setting as close to the laboratory as possible. The simulation solution developed in this chapter is based on matrix representations of photon number states, and is underpinned by the quantum computational toolbox by Sze M. Tan [111], available as of this date at http://qwiki.stanford.edu/index.php/Quantum_Optics_Toolbox. Parts of this work were done in collaboration with co-op student Allison MacDonald, and some were based on previous simulations by Thomas Jennewein [51], the files of which are available at http://info.iqc.ca/qpl/lab-tools/. I adapted the entanglement simulations to our new experiments and regimes, created weak coherent pulse simulations, added QKD theory and retrieved results.

3.1 The need for quantum optical simulation

Pedagogically, quantum optics is usually introduced in terms of single photons, entangled pairs, unity transmission, and perfect detectors. In practise, of course, photonic systems are more complicated, and so some method is required to get a handle on interactions and outcomes of effects such as higher photon number states, multi-pair emission, channel loss, and inefficient detectors with dark counts. Quantum optical simulations are useful first in deciding which

experiments are possible, next in choosing technology with performance required for success, and finally in comparing experiment to theory.

3.1.1 Range of possible simulations

The quantum optics toolbox is well suited for simulating any linear optical system, considering maximum photon numbers per mode of around 8, depending on the number of modes; fewer modes means more photons in each mode can be considered. Nonlinear actions are also possible, so long as the Hamiltonian governing the process is known, as in parametric down-conversion or creation of coherent states. Thus the toolbox can simulate the optical part of the BB84 and BBM92 protocols, Bell-type tests with two or more entangled photons (e.g. CHSH, Mermin, Svetlichny), and of course linear optics quantum computing experiments. Beamsplitters, waveplates, bucket and photon-number resolving detectors, and post-selection/heralding are all readily included.

3.2 Generalised experiment simulation

The format and function of a generalised simulation is presented here. For MATLAB code for specific implementations, please see the Appendix A.

```
Initialise Fock state dimension, e.g. N=7

Set up standard toolbox definitions, e.g. beamsplitters, ...
    waveplates, annihilation operator, vacuum state

Input experimental parameters like timing window, photon ...
    production rates (pair sources), source repetition rate, ...
    average photon number (weak coherent pulse sources), ...
    channel loss, detector dark count rate

Create initial photon state by down-conversion operator or ...
    displacement operator

Combine channel and detector efficiencies and detect photon ...
    state (projective measurement) in appropriate basis with ...
    total efficiency and noise added

Use returned detection probabilities to calculate QBER, ...
    secure key rate, inequality violations or other desired ...
    results.
```

```
Loop over one or greater parameters such as loss or ...
    integration time to determine dependence
```

As noted in Reference [51], spectral dependencies of the systems and the time evolution under creation and entangling operations are not simulated, but rather the detectable outcomes of these operations are calculated. This is sufficient when the photon wavepacket is much shorter in time than the detector resolution, a condition generally satisfied in quantum optics experiments examined here.

3.3 Simulation outcomes

3.3.1 Simulation of Bell-type tests and teleportation

The goal of these simulations is generally to determine how many detections are needed in an experiment and with what visibility or fidelity to show quantum behaviour. For Bell-type tests, the final outcome is the CHSH [19], Mermin [75], Svetlichny [109], or other parameter on the left hand side of the inequality, which must be superior to some classical limit with some statistical certainty. For teleportation, the (single qubit) fidelity F of the initial input with the final teleported state is calculated, and needs to exceed the value possible with only a classical channel, $F \leq 2/3$ [83], or the cloning limit $F \leq 5/6$ [16].[1] These can also be formulated in terms of visibility V, related to fidelity as $V = 2F - 1$ [12] with classical limit $V \leq 1/3$ and cloning limit $V \leq 2/3$.

To be useful, these simulations require realistic entangled photon states, which can be created via the down-conversion unitary acting on a two-mode vacuum:

$$\begin{aligned} \hat{H}_{d-c} &= \epsilon \left(\hat{a}_1 \hat{a}_2 + \hat{a}_1^\dagger \hat{a}_2^\dagger \right) \\ \hat{U}_{d-c} &= \exp\left(-i \hat{H}_{d-c} \right) \end{aligned} \tag{3.1}$$

Here $\hat{a}_j^{(\dagger)}$ is the annihilation (creation) operator acting on the j-th mode and ϵ, which contains $\chi^{(2)}$ nonlinear coupling, source strength, geometry and interaction time, is determined from source singles and pair production rates. A good estimation of ϵ is required for accurate simulations, and so it can be calculated from measured source parameters as follows: First of all, a source repetition frequency f_{source} is defined, which is the laser repetition rate for pulsed sources, but is rather ambiguous for continuous wave sources, and set to the inverse of the coincidence window for convenience. Then the pair production

[1] It should be noted that, in References [83, 16] and subsequent teleportation papers, fidelity is defined as $F = \mathrm{Tr}\left(\sigma^{1/2}\rho\sigma^{1/2}\right)$ or $F = |\langle\psi|\phi\rangle|^2$ for arbitrary density operators ρ and σ or arbitrary pure states $|\psi\rangle$ and $|\phi\rangle$, as compared to the usual definition $F_{usual} = \sqrt{F} = \mathrm{Tr}\left(\sqrt{\sigma^{1/2}\rho\sigma^{1/2}}\right)$ or $F_{usual} = \sqrt{F} = |\langle\psi|\phi\rangle|$.

rate directly after down-conversion is back-calculated from detected pairs and singles rates in a real or proposed source. The detected coincidence rate C is roughly $C = \eta_1\eta_2 P$, where η_j is the efficiency of the j-th mode from production to detection, and P is the pair production rate. The detected singles rate for mode j is $S_j = \eta_j P$, and thus $\eta_1 = \frac{C}{\eta_2 P} = \frac{C}{S_2}$ and $\eta_2 = \frac{C}{S_1}$, so finally $P = \frac{C}{\eta_1\eta_2} = \frac{S_1 S_2}{C}$. The down-conversion coupling ϵ is then the square root of the probability (i.e. amplitude) of pair creation per source time slot, $\epsilon = \sqrt{\frac{P}{f_{source}}}$. Though this analysis is simplified, it gives final results of pair rates and entanglement visibility in good agreement with experiment.

Svetlichny inequality violation

The Svetlichny inequality [109] allows pairwise nonlocal correlations over a multipartite system, and so can be violated in quantum mechanics with tripartite entanglement, as present in a three photon GHZ state [39]. The Svetlichny parameter S_v is at most 4 for three-particle correlations when nonlocal correlations are allowed between any two particles at a time:

$$\begin{aligned} S_v = |&E(\phi_A,\phi_B,\phi_C) + E(\phi_A,\phi_B,\phi'_C) + E(\phi_A,\phi'_B,\phi_C) - E(\phi_A,\phi'_B,\phi'_C) \\ &+ E(\phi'_A,\phi_B,\phi_C) - E(\phi'_A,\phi_B,\phi'_C) - E(\phi'_A,\phi'_B,\phi_C) - E(\phi'_A,\phi'_B,\phi'_C)| \leq 4 \end{aligned} \tag{3.2}$$

where the correlation values $E(\phi_A,\phi_B,\phi_C)$ are the ensemble average over many measurements with settings (ϕ_A,ϕ_B,ϕ_C) at sites A, B, and C respectively. Each measurement can have one of two outcomes, assigned the value $+1$ or -1 respectively, implying $|E| \leq 1$.

In Reference [63], the Svetlichny inequality was violated in the lab without spacelike separated receivers, leading to a loophole where the setting of one detector could influence the setting of another to simulate nonclassical results. The next step is to move to separated receivers, but as this would introduce lossy free space channels, it was unclear what source performance was required and what channel loss was tolerable. I simulated the experiment (code in Appendix A) to determine permissible operational parameters and the integration time required to violate the inequality with a given statistical certainty or number of standard deviations p above the classical limit. (A usual requirement for success is $p = 3$ for a 3σ violation of the classical limit.) For this simulation, it was assumed that only two arms had the free-space links, each with identical transmission, as the third photon can be detected locally. For transmission above 0.1, the fidelity of the heralded three photon state with the ideal GHZ state and Svetlichny parameter S_v are essentially constant and the only change is the detection rate (Figure 3.1), indicating the experiment will be feasible with only

a change in integration time. In Figure 3.2, the statistical certainty is plotted against integration time, to show how long an integration time would be required for, say, a 3σ violation.

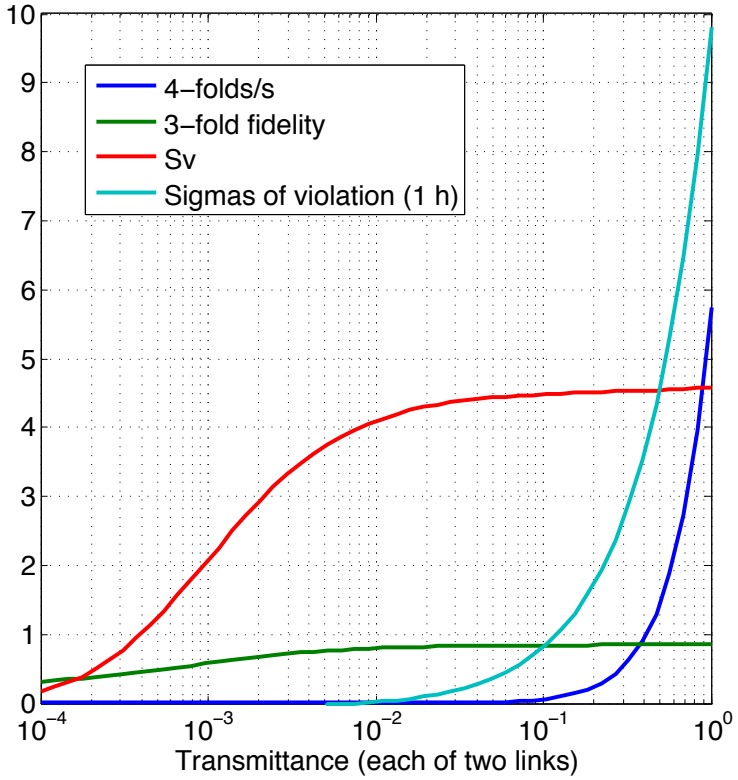

Figure 3.1: Simulation results for Svetlichny Violation. All curves refer to the left axis with appropriate units. "4-folds/s" is the rate of detection of 4-fold coincidences per second, made up of the three photons used in the violation and one for heralding. "3-fold Fidelity" is the fidelity of the three-photon state with the desired $\frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle)$. "Sv" is the Svetlichny parameter, which must be Sv > 4 for a violation, and "Sigmas of violation" is the experimental certainty of Sv given 1 hour integration time.

Quantum teleportation

Teleportation is the act of moving a quantum state from one particle to a distant one, without those two ever having interacted [8]. It is usually accomplished by interfering the input state with one half of an entangled pair, projecting the

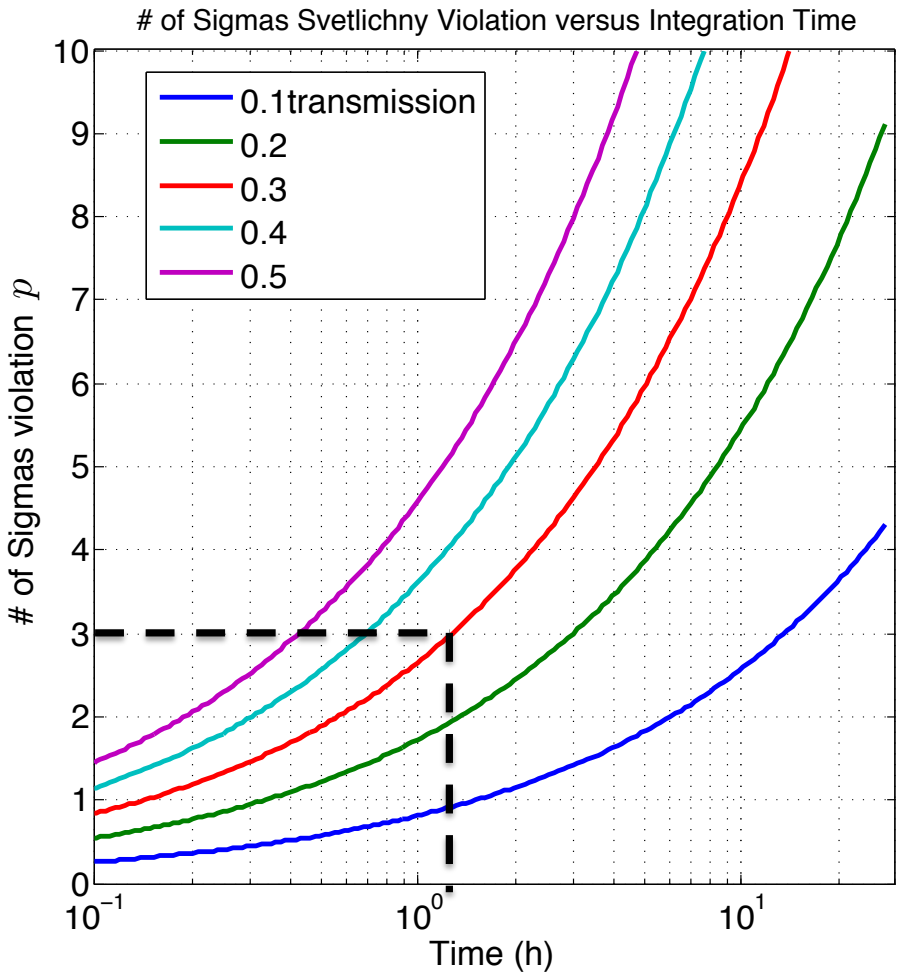

Figure 3.2: Statistical certainty for Svetlichny Violation. As integration time is extended, more signals accumulate and the value of S_ν is more certain, leading to a greater certainty (# of Sigmas p) of violation. The most likely experimental scenario is transmission of about 0.3, requiring about 80 minutes for a 3σ violation, given a local detection rate of about 80 four-fold coincidences per second.

two previously unentangled photons into a Bell-state, and leaving the third in a transformed version of the input state. A unitary, which is chosen conditionally on the Bell-state measurement outcome transforms the state of the third photon into the initial input state. See Figure 3.3 for a diagram of teleportation.

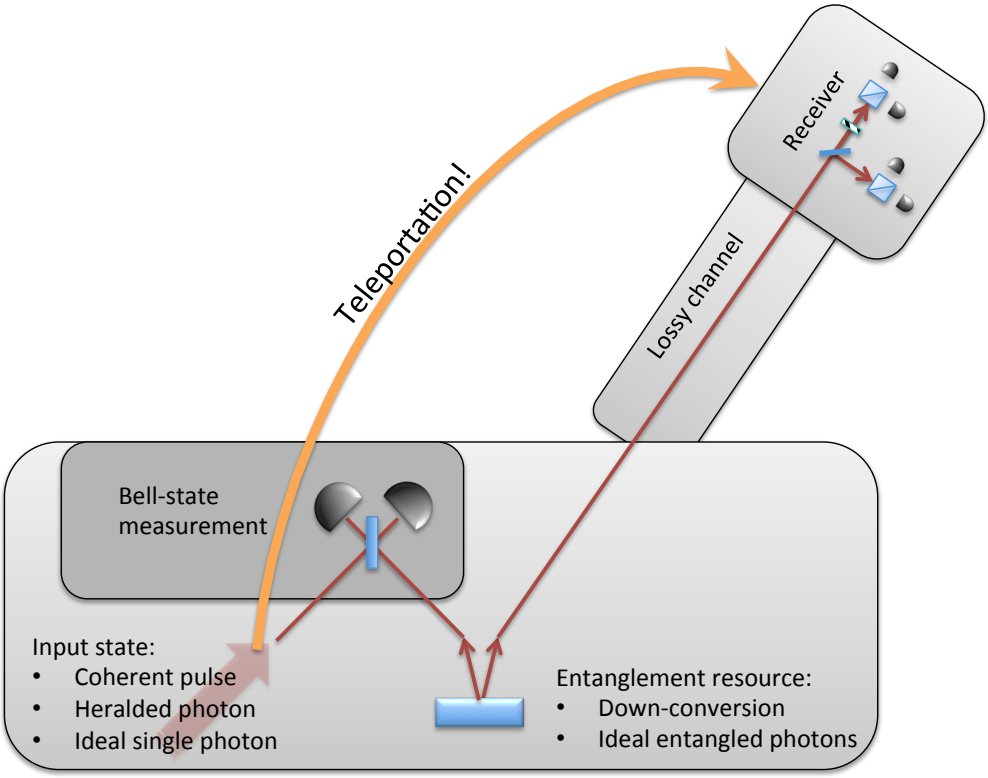

Figure 3.3: Diagram of quantum teleportation. Two sources for the entanglement resource and three different kinds of input photon state are considered.

A number of situations for teleportation were considered (code in Appendix A), including, for the entangled resource pair a down-conversion source or an ideal entangled photon source, and for the input photon a coherent state, an ideal single photon, or a heralded photon from down-conversion. Figure 3.4 shows results when an entangled down-conversion source is used as the resource and compares results for the three types of input states versus loss. Here the two photons that interfere are created locally, and the third is detected at a distant location after undergoing loss. Three figures of merit are the teleportation rate per second, the visibility of the teleported state, and the visibility less p standard deviations of uncertainty σ, which still must be greater than the cloning limit of 2/3 for success. Figure 3.5 then shows the results using an ideal entangled pair,

for example from a quantum dot source. These results are much improved and allow far higher channel losses.

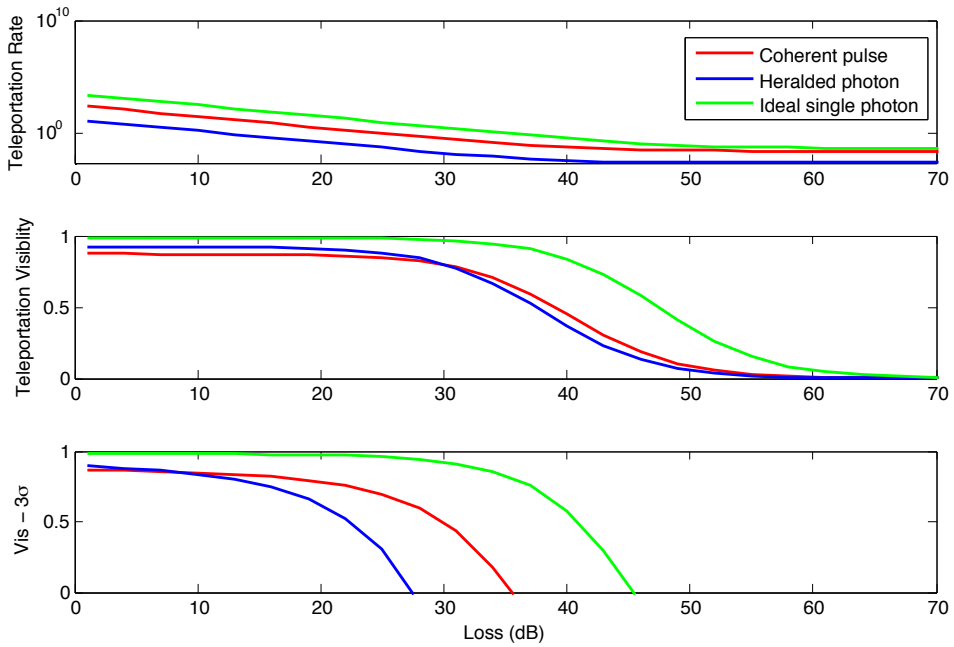

Figure 3.4: Teleportation simulation with down-conversion. Three types of input photon state are compared, with ideal single photons providing the best results due to a lower error rate from higher photon number states. Additionally, coherent states are far easier to produce than heralded photons, leading to higher rates and high permissible loss. The third plot takes $p = 3$, for a 3σ violation.

Minimum number of coincidence counts required for a Bell-type test

In addition to simulations based on the quantum optics toolbox, it was necessary to perform analyses to determine the minimum number of received signals required for success of various experiments. Here I will show the calculation for a CHSH violation, which readily extends to other Bell-type tests. This section was originally written in altered form by me for the Quantum Entanglement Feasibility Study for the Canadian Space Agency.

The CHSH-parameter S_{CHSH}, from Equation 1.8 depends on the correlation values $E(\phi_A, \phi_B)$, where $\phi_{A/B}$ is the setting of Alice/Bob's analyser. Quantum mechanics predicts a maximal violation of the CHSH inequality for the set of polarisation angles $(\phi_A, \tilde{\phi_A}, \phi_B, \tilde{\phi_B}) = (0°, 45°, 22.5°, 67.5°)$, given an initial state

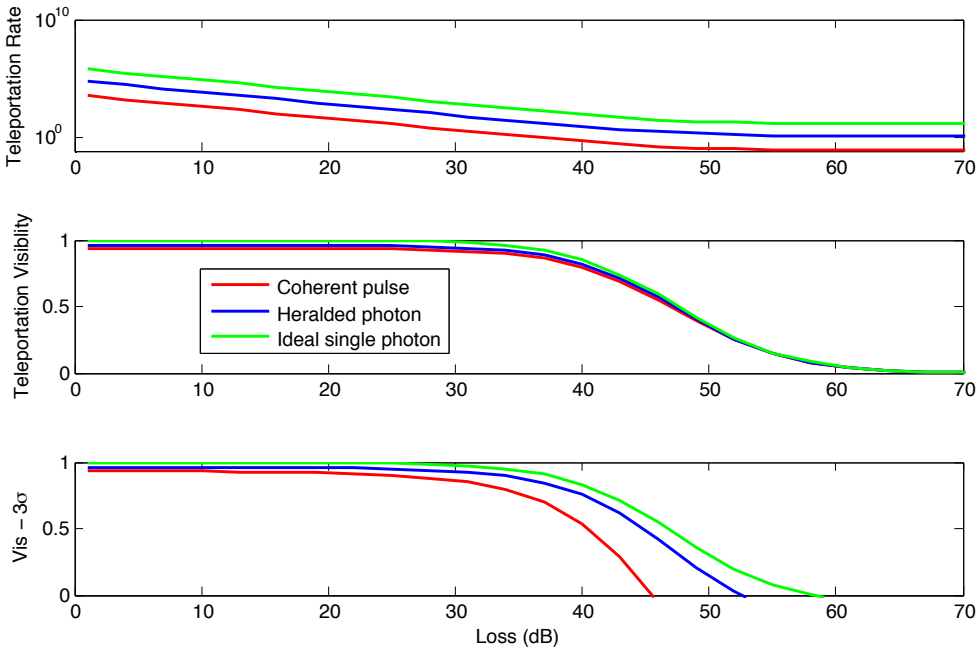

Figure 3.5: Teleportation simulation with ideal entangled pairs. The ideal entangled pairs perform significantly better than the pairs from down-conversion, due to a lack of double emissions leading to a reduced error rate.

of the form $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. This choice of measurement settings leads to a value of $S_{CHSH} = 2\sqrt{2}$ well beyond the classical limit of $S_{CHSH} \leq 2$

In a typical experiment, the obtained counts of photon pairs depend on Poissonian count statistics and are therefore subject to uncertainty. A successful experiment requires that a Bell-inequality be violated by at least $p\sigma$; i.e. the experimental value must be p times the uncertainty larger than the classical value. For an average number of photon counts N, the uncertainty is $\Delta N = \sqrt{N}$. This is relevant for the expression of the correlation values E, which are determined through coincident photon counts as

$$E(\phi_A, \phi_B) = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{total}}. \tag{3.3}$$

with N_{++} corresponding to the number of photon pairs counted in the two + outputs of the analysers set to ϕ_A and ϕ_B respectively, and so on for N_{+-}, N_{-+}, N_{--}. Each N_{xy} is therefore also a function of the measurement settings ϕ_A and ϕ_B. I perform Gaussian error propagation and obtain the following uncertainty for E:

$$\Delta E(\phi_A, \phi_B) = \frac{2\sqrt{(N_{++} + N_{--})^2(N_{+-} + N_{+-}) + (N_{++} + N_{--})(N_{+-} + N_{+-})^2}}{(N_{total})^2} \tag{3.4}$$

In a real experiment, the entanglement will not be perfect, but rather will exhibit entanglement visibility $V < 1$. This causes a reduction in the maximum S_{CHSH} to $S_{experiment} = 2\sqrt{2}V$ and leads N_α, the number of photon pairs detected with analysers at relative angle α to be somewhat altered from the usual $N_{\alpha(ideal)} = \frac{N_{total}}{2}\cos^2(\alpha)$ to

$$N_\alpha = \frac{N_{total}}{2}\left(\frac{1}{2} + \left(\cos^2(\alpha) - \frac{1}{2}\right)V\right). \tag{3.5}$$

When $V = 0$, the number of pairs is independent of angle, and for $V = 1$, $N_\alpha = N_{\alpha(ideal)}$. For $\phi_A = 0°$ and $\phi_B = 22.5°$, this gives

$$N_{++} = N_{--} = \frac{N_{total}}{2}\left(\frac{1}{2} + \left(\cos^2(22.5°) - \frac{1}{2}\right)V\right) = \frac{N_{total}}{2}\left(\frac{1}{2} + \frac{V}{\sqrt{8}}\right) \tag{3.6}$$

$$N_{+-} = N_{-+} = \frac{N_{total}}{2}\left(\frac{1}{2} + \left(\cos^2(112.5°) - \frac{1}{2}\right)V\right) = \frac{N_{total}}{2}\left(\frac{1}{2} - \frac{V}{\sqrt{8}}\right). \tag{3.7}$$

Equation 3.4 simplifies, and I obtain

$$\Delta E(\phi_A, \phi_B) = \sqrt{\frac{1 - \frac{V^2}{2}}{N_{total}}}. \tag{3.8}$$

The derivation proceeds similarly for the other three measurement combinations, and since $S_{experiment} = |E(\phi_A, \phi_B) - E(\phi_A, \tilde{\phi_B})| + |E(\tilde{\phi_A}, \phi_B) + E(\tilde{\phi_A}, \tilde{\phi_B})|$,

$$\Delta S_{experiment} = 2\sqrt{\frac{1 - \frac{V^2}{2}}{N_{total}}}. \tag{3.9}$$

The goal is to perform a CHSH-inequality violation with $p\sigma$ violation above the classical limit:

$$S_{experiment} - p\Delta S_{experiment} \geq 2 \tag{3.10}$$

Thus, given $S_{experiment} = 2\sqrt{2}V$ and $\Delta S_{experiment}$, the minimum number of recorded pairs is

$$N_{total} > \left(\frac{p \times 2}{2\sqrt{2}V - 2}\right)^2 \left(1 - \frac{V^2}{2}\right), \tag{3.11}$$

which is plotted versus visibility in Figure 3.6 for $p = 3$, allowing experimentalists to determine how many received signals are required to violate the CHSH inequality with 3σ certainty, given their achievable entanglement visibility. This visibility can be calculated from simulation of down-conversion or measured experimentally. This analysis is readily extended to Mermin, Svetlichny, and other Bell-type inequalities.

Minimum number of signals required for teleportation

For teleportation, success can be characterised with only one measurement parallel to and one orthogonal to the original input state, assuming measurements on qubits. This leads to a teleportation visibility, V_t, defined as

$$V_t = \frac{N_{\parallel} - N_{\perp}}{N_{\parallel} + N_{\perp}}, \tag{3.12}$$

where $N_{\parallel}$ are photon counts on the detector channel with analyser set to the same as the input state and $N_{\perp}$ are those on the orthogonal channel. This assumes that the receiver knows the initial input state and hence somewhat weakens the argument that teleportation is good for arbitrary states. However, as this analysis is targeted at satellite-based missions, a full tomography for each input state takes many more measurement runs, and so a smaller set of measurements is more cost-effective. The measurement can be repeated for a few nonorthogonal input states and if all are shown to have high teleportation visibility, true teleportation is occurring.

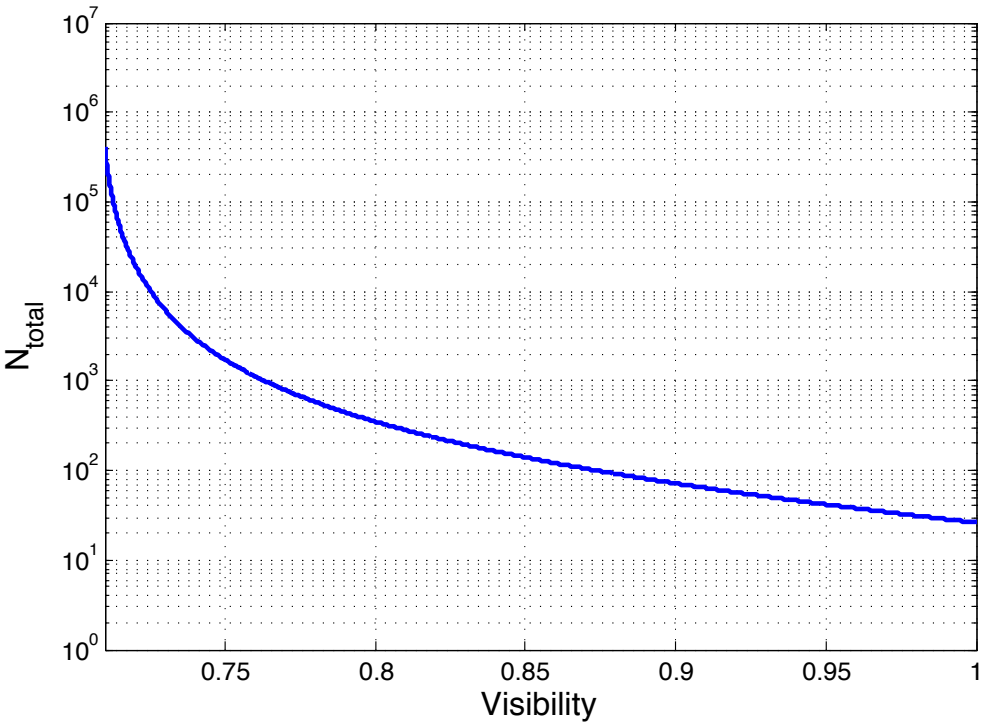

Figure 3.6: Number of photon pairs for CHSH inequality. Plot of the required total number of detected photon pairs in order to violate a CHSH-inequality with 3σ certainty, versus the entanglement visibility V. As visibility approaches the minimum required for violation (70.7 %), the number of pairs required tends to infinity.

As before, Poissonian errors are assumed ($\Delta N = \sqrt{N}$) and Gaussian error propagation is performed to find

$$\Delta V_t = \frac{1}{(N_{total})^2}\sqrt{N_{\|}(2N_{\perp})^2 + N_{\perp}(2N_{\|})^2} \tag{3.13}$$

This equation, through $N_{\|/\perp} = \frac{N_{total}}{2}(1 \pm V_t)$ simplifies to

$$\Delta V = \sqrt{\frac{(1-V)(1+V)}{N_{total}}} \tag{3.14}$$

except as V approaches 1. Then $N_{\perp} = \frac{N_{total}}{2}(1-V) < 1$, which is unphysical since photons can only arrive in discrete quanta. Therefore, a lower bound of the uncertainty in $N_{\perp}$ of $\Delta N_{\perp} = 1$ is imposed, causing the total counts required to saturate and not tend to zero as V approaches 1. In this regime,

$$\Delta V = \sqrt{\frac{2 + 2V + N_{total}(1+V)^2}{N_{total}^3}}. \tag{3.15}$$

Equations 3.14 and 3.15 are solved for N_{total} given a $p\sigma$ violation of the cloning limit ($V_t - p\Delta V_t > 2/3$) and the result is plotted in Figure 3.7 for $p = 3$, allowing experimental teleportists to find the minimum number of signals received to violate an optimal quantum cloner with 3σ certainty. Of course this is somewhat circular: if one measures such visibility V_t, then one needs N measurements to measure visibility V_t, but the result is nonetheless useful in planning experiments, as an expected teleportation visibility is easily simulated (Subsection 3.3.1), and hence the required number of signals can be calculated.

3.3.2 Simulation of QKD

Beyond simulations of quantum optical experiments above, the quantum optics toolbox is well suited for simulating QKD systems. As security of QKD is strongly dependent on the presence of noise and higher photon numbers [38], the Fock space simulations allow good predictions of secure key rates and transmission distance for QKD.

As seen in Figure 2.4, QKD exhibits generally a logarithmic drop in key rate with distance, followed by a final sharp cutoff beyond which no key can be generated. It is important in design of QKD systems to know the location of this cutoff, and to be able to optimise parameters to extend transmission distance as far as possible. The detection rate at long distance is equally important, as many signals must be detected in order to combat finite size effects. Therefore I constructed simulations (see code in Appendix A) to determine the detection

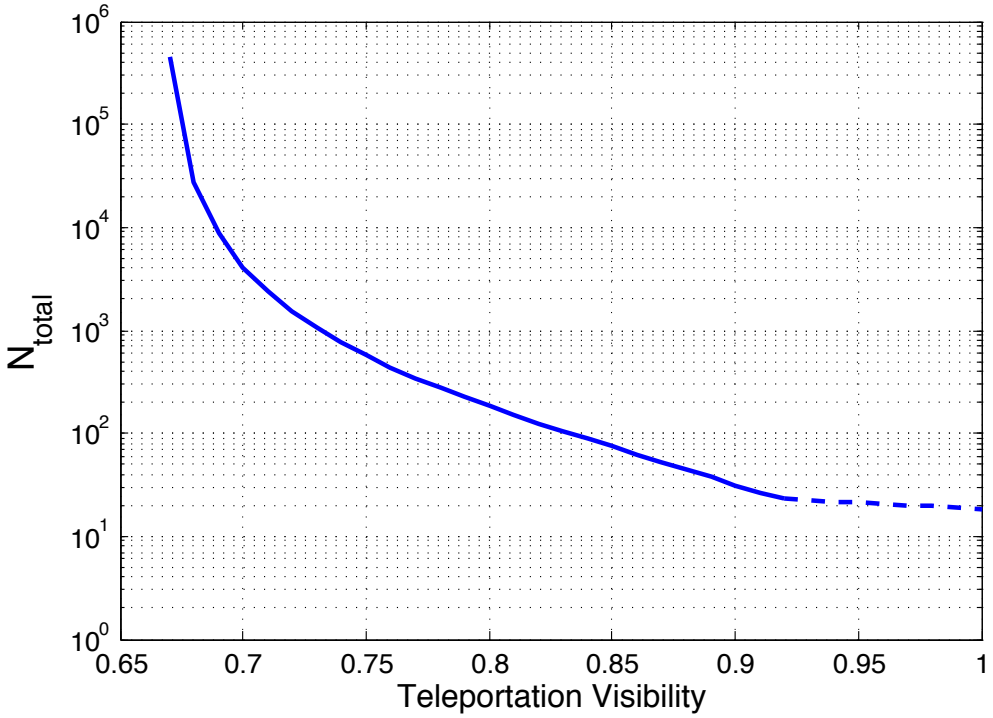

Figure 3.7: Number of detections for teleportation. Plot of the required total number of detected third photons (conditioned on a successful Bell-state measurement) versus teleportation visibility required to violate the cloning limit of $V_t = 2/3$ with 3σ certainty. The dashed portion of the curve is where the error estimation breaks down, as fewer than one erroneous photon count is predicted, requiring enforcement of a minimum uncertainty of $\Delta N_\perp = 1$.

rate and QBER at various channel loss values, incorporating as before realistic photon states and background noise, and additionally assigning double clicks a random value.

Double clicks

As required by the squashing model of QKD security (which allows to treat incoming optical modes as qubits) [38], double clicks (coincident detections by both detectors in the same basis) must be assigned a random bit value. This requires just a slight modification of the QBER calculated from detection probabilities as follows. Let $P(right)$ be the probability of detecting the correct qubit value, $P(wrong)$ be the probability of an error, and $P(double)$ the probability of a double click. $P(right)$ is measured by projecting onto the subspace of one or more photons in the correct detector and no photons in the other detector, and similarly for $P(wrong)$. $P(double)$ is measured by projecting onto the subspace of one or more photons in each detector simultaneously. Thus the total click probability P is $P = P(right) + P(wrong) + P(double)$ and the QBER is

$$QBER = \frac{P(wrong)}{P} + \frac{P(double)/2}{P} \tag{3.16}$$

since double clicks are assigned randomly. This modification has negligible effect as most simulations here consider long distance, making the double-click probability small. Nonetheless it is important to include for security at short distances or very high pair production rates, as multiphoton events are more likely.

Loss dependence and coincidence window

One important determination is the coincidence window (for entangled photon schemes) or the detection window (for single photon schemes). This is a unit of time during which detections are accepted for QKD (detections outside are excluded), and it is generally desired to be as small as afforded by detector jitter to exclude background noise and dark counts. Here I give an example simulation for an asymmetric entanglement-based QKD system, with one photon detected at the source and the other sent over a lossy channel. I found the detected two-photon rate and secure key rate versus loss for various coincidence windows, as shown in Figure 3.8. Thus if the channel is only 35 dB, one needs just a 2 ns coincidence window, but to go beyond 45 dB channel loss, one needs to reduce jitter of detectors and electronics to allow a 200 ps window, in order to exclude more dark counts. These simulations assumed a pair production rate in the crystal of 3.2×10^7 pairs per second, 2000 background and dark counts per second, 60 %

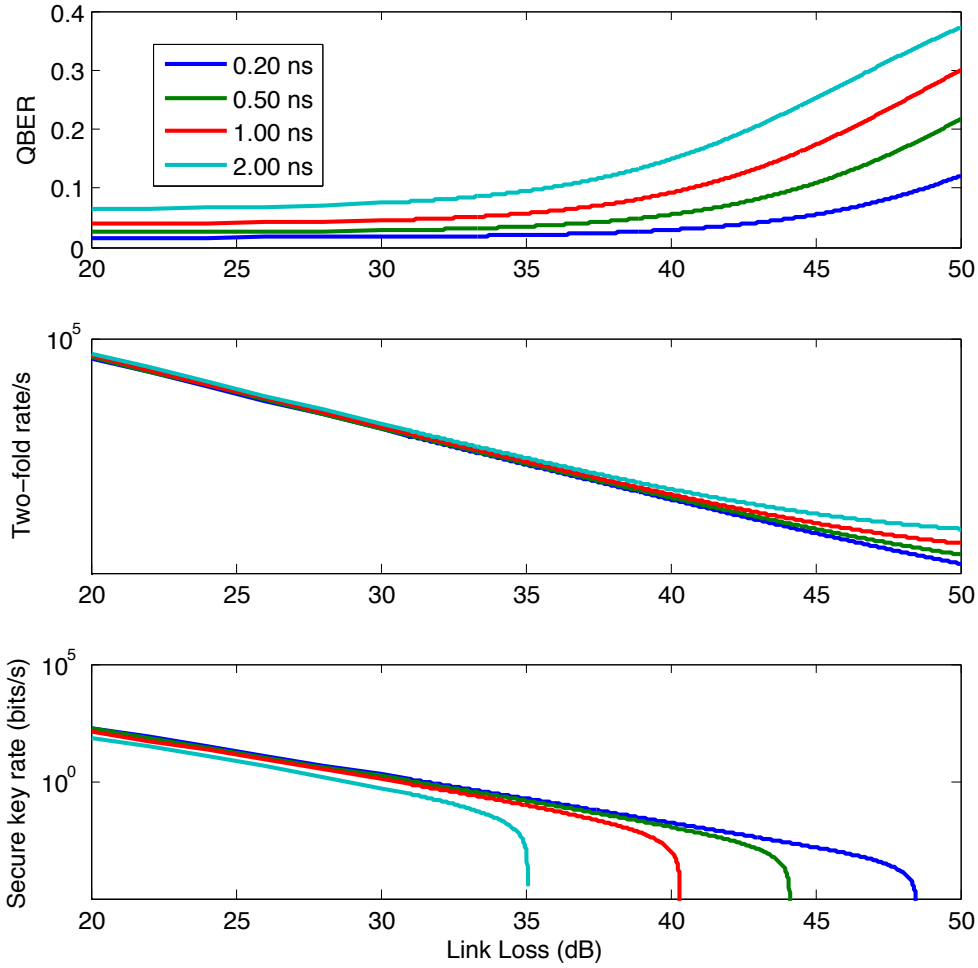

Figure 3.8: Entangled QKD and coincidence windows. Smaller coincidence windows give lower QBER and therefore higher keyrates, neglecting that smaller windows may cut out legitimate signal. Thus the narrowest window above allows longest distance QKD, as determined by the cutoff due to QBER higher than the security limit. The two-fold rate saturates to the detector dark count rate at high loss. These simulations are for symmetric links, i.e. each arm has the Link Loss shown.

efficient single photon detectors, and a misalignment of polarisation optics which introduces a 1 % QBER. These parameters can of course all be tuned, including adding photon number resolution or idealised photon sources.

Qubit analyser choice and dark counts

Another important parameter is the dark count rate in each detector. More dark counts mean a higher QBER and less secure key. This has implications for the receiver design: is it better to have active basis choice with two detectors, or passive basis choice with four, as seen in Figure 3.9? I analysed this problem in the case of weak coherent pulse QKD, and found that the difference in QBER and secure key rate is negligible when loss is low. However, when the received count rate approaches the dark count rate, the passive (four-detector) analyser performs worse as the signal on each detector is halved, leading to a lower signal-to-noise ratio, higher QBER and hence a shorter QKD range, as in Figure 3.10.

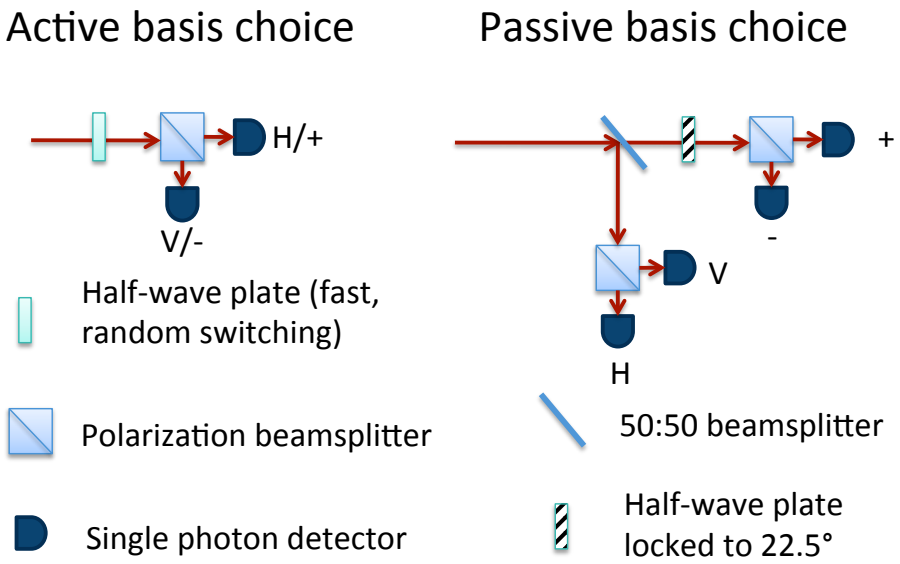

Figure 3.9: Active and passive QKD polarisation analysers. The active analyser has a fast switching half-waveplate to choose to measure in the H/V or +/- basis, while the passive analyser accomplishes basis choice with a 50:50 beamsplitter, meaning the incoming photons randomly move to one of the measurement bases.

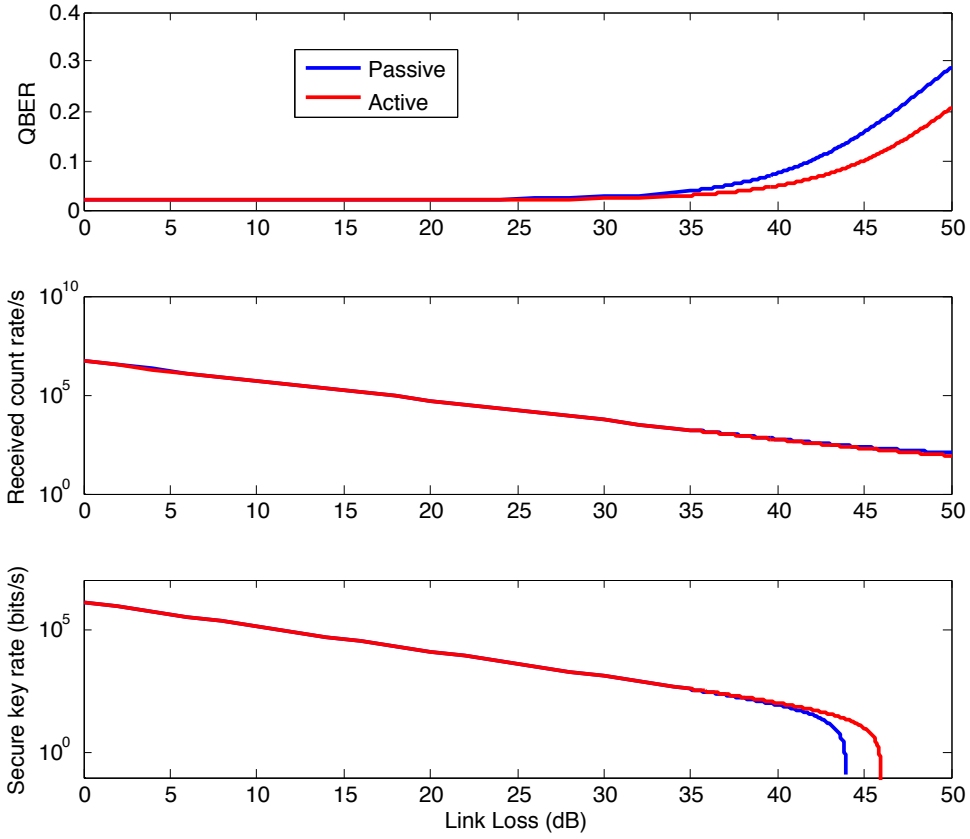

Figure 3.10: Effect of active vs. passive analyser on results for weak coherent pulse QKD. Little difference is evident at low loss, but the higher signal-to-noise ratio of the two detector active analyser allows QKD to reach higher channel losses.

3.4 Discussion

These types of loss-dependence analysis were instrumental in deciding on required technology for the high-loss QKD system below (Chapter 5). Being able to see precisely the effect of small adjustments to the dark count rate on the attainable channel loss made the choice of detectors much easier and removed guesswork from the decision. Additionally, it is clear that the optimal high-loss system would use fast active basis choice rather than four-detector passive choice.

A deficiency of the software in its current form is the limited photon number when many modes are considered. For example, the Svetlichny inequality violation simulation above (Subsection 3.3.1) consisted of eight modes, and my 32-bit computer could only handle $N = 3$, i.e. 0, 1, or 2 photons in each mode. Thus for simulations of larger entangled states it would be important to optimise or find efficiencies in the code such that more photons can be considered in more modes. This could be accomplished by considering separate Hilbert spaces for modes that never interact, or performing a partial trace after interaction to remove modes no longer needed. A related drawback is that this toolbox is unsuited for continuous variable simulations, as these typically have many photons per mode. This would require a drastic rethink of the software, and better solutions probably exist.

Nonetheless, it is clear that the quantum optics toolbox and related functions are exceedingly helpful in simulating many relevant aspects of experiments before any lab work is done. From teleportation to QKD, its versatility is sufficient to allow broad use by experimentalists or theorists.

Chapter 4

Local area quantum key distribution in telecommunications optical fibres

This chapter is based on an experiment performed in late 2009, involving local area QKD through standard telecommunications fibre. The content of this chapter was published in altered form in:

Evan Meyer-Scott, Hannes Hübel, Alessandro Fedrizzi, Chris Erven, Gregor Weihs, and Thomas Jennewein. Quantum entanglement distribution with 810 nm photons through telecom fibres. Applied Physics Letters, 97(3):031117, 2010.

I am allowed by the policies of Applied Physics Letters and the American Institute of Physics to reprint this content here, from section (2) of Author Rights in the Transfer of Copyright agreement.[1]

Author contributions

Hannes, Alessandro and Thomas conceived the experiment. Chris and Gregor provided the photon source, detectors and QKD software. I performed the fibre spool measurements and analysed the data. Hannes, Chris and I performed measurements over the fibre link between UW and PI. Allison MacDonald performed calculations regarding propagation speeds in fibre (see Appendix B). I wrote the paper with input and feedback from all authors.

[1]The exact text is that I retain "The nonexclusive right, after publication by AIP, to give permission to third parties to republish print versions of the Article or a translation thereof, or excerpts therefrom, without obtaining permission from AIP, provided the AIP-prepared version is not used for this purpose, the Article is not published in another journal, and the third party does not charge a fee."

4.1 Introduction

The ability to distribute entanglement is an important building block in the field of quantum information processing. It is employed in protocols such as quantum teleportation [13], quantum key distribution (QKD) [34], and quantum computing [56]. Many quantum information experiments so far have been performed at wavelengths around 800 nm, making use of the high performance (low noise, high speed, and around 70 % efficiency) of silicon avalanche photodiodes (Si-APDs) for single-photon detection. Such systems have been demonstrated in laboratories, over free space links [59, 119] or with custom laid 800 nm single mode fibres [84], the latter of which face the difficulty of installing a dedicated link. In addition, most quantum memory implementations and quantum dot photon-sources are designed around 800 nm optical transitions [129]. On the other hand, quantum communication setups have been built to make use of existing telecom fibre infrastructure and low fibre loss at 1550 nm [44]; however, single-photon detectors based on APDs designed for these wavelengths (InGaAs-APDs) add considerable complexity, require elaborate synchronisation of detector gates, and suffer from low detector efficiencies ($\sim$15 %). In fact, based on the efficiencies above, and fibre losses of 3 dB/km for 800 nm light and 0.22 dB/km for 1550 nm light, overall attenuation will be lower for 800 nm photons for up to 7.3 dB of fibre losses, corresponding to 2.4 km of telecom fibre. In spite of the common perception that entanglement distribution at 800 nm strictly requires wavelength-specific components, it is obvious that such short wavelength systems would greatly benefit if used with the existing fibre infrastructure. Toward this goal we report on the high fidelity distribution of entangled photon pairs at 810 nm through several kilometres of standard telecom fibres, which provides a path for demonstrating quantum information applications, like entanglement based QKD, and other quantum optics experiments in existing fibre networks.

4.2 Experimental setup

We adapted a polarisation-entanglement based quantum communication system [29] at 810 nm using the BBM92 protocol [9] to transmit photons to Alice and Bob through varying lengths of single mode telecom fibres (core radius of 4.1 μm] ranging from 250 m to 6000 m (Figure 4.1) or short stretches of 810 nm single mode fibres with a core radius of 2.75 μm.

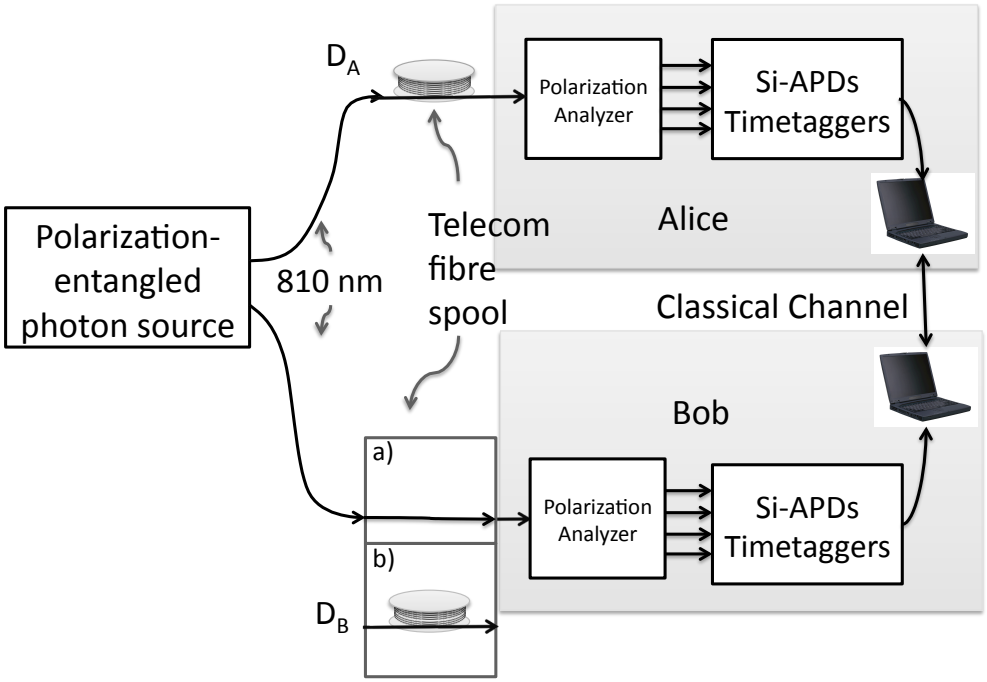

Figure 4.1: Schematic of setup. (a) Asymmetric distribution scheme, with only a short 810 nm single mode fibre to Bob. (b) Symmetric scheme, with long 1550 nm telecom fibres to both Alice (length D_A) and Bob (length D_B)

4.2.1 Down-conversion source of photons

The source of entangled photons mentioned above is based on spontaneous parametric down-conversion [55] in a Sagnac loop [54]. The basic operation of the source is illustrated in Figure 4.2.

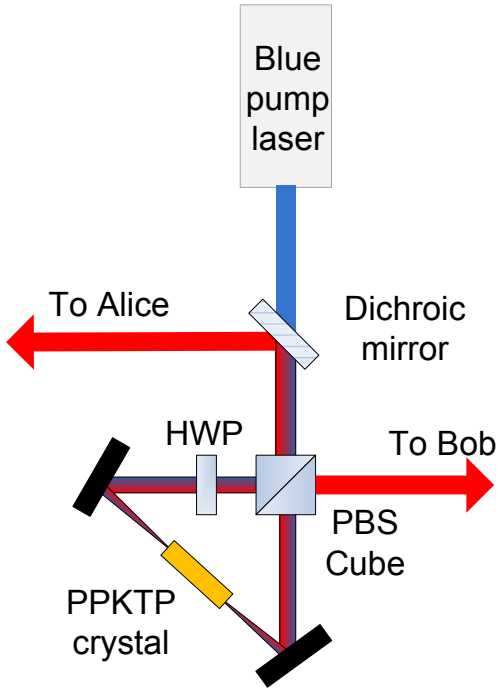

Figure 4.2: Sagnac source of entangled photons. HWP means half-wave plate to rotate the polarisation of all three beams 90°, PBS is polarisation beamsplitter, and PPKTP is periodically poled potassium titanyl phosphate for type-II down-conversion. The blue pump laser is polarised at 45°, leading to a coherent superposition of propagation clockwise around the loop and counterclockwise. If clockwise, the pump photon down-converts into an $|HV\rangle$ pair, such that the $|V\rangle$ photon is sent to Alice and the $|H\rangle$ to Bob. If counterclockwise, the same down-conversion occurs, except now due to entering the polarisation beamsplitter through the other port, the $|V\rangle$ photon is sent to Bob and the $|H\rangle$ to Alice, leading to a state of the form $\frac{1}{\sqrt{2}}\left(|H_A V_B\rangle + e^{i\phi}|V_A H_B\rangle\right)$.

Down-conversion is a quantum mechanical process in the realm of nonlinear optics, which effectively splits one pump photon into two (called signal and idler) of lower energy. Nonlinearities occur in optical materials where the material's polarisation response is not proportional to the driving electromagnetic field: for

example, second harmonic generation occurs when a significant component of the polarisation response is at double the frequency of the input field, leading to an output field at this doubled frequency. Second harmonic generation, along with sum frequency generation and down-conversion, rely on a $\chi^{(2)}$ nonlinearity, meaning electromagnetic waves of up to three distinct frequencies can mix in the material. Second harmonic generation and sum frequency generation can be described classically (see Subsection 5.2.3), but down-conversion is distinctly quantum mechanical, as classical optics predicts no growth in the amplitude of the signal and idler modes if no initial signal is present in these modes. If the fields are quantised, however, field amplitude appears in the signal and idler modes and due to mixing with vacuum fluctuations [43]. For signal and idler photons to be produced with any reasonable probability, the phase matching conditions between the three waves must be satisfied for both momentum and energy. For momentum, the wavevectors of the down-converted light must sum to the wavevector of the pump beam:

$$\boldsymbol{k}_{pump} = \boldsymbol{k}_{signal} + \boldsymbol{k}_{idler} \tag{4.1}$$

For energy, the frequencies of the down-converted light must sum to the pump frequency:

$$\omega_{pump} = \omega_{signal} + \omega_{idler} \tag{4.2}$$

If crystals with a $\chi^{(2)}$ nonlinearity are constructed in such a way that Equations 4.1 and 4.2 are satisfied (for example, with quasi-phasematching through periodic poling [47]), down-conversion will occur from the pump frequency to pairs of photons at the signal and idler frequencies.

In order to generate entanglement from down-conversion, two down-conversion processes, different in some degree of freedom but indistinguishable in others must occur coherently. Thus the entanglement is between the output states of each of the processes occurring, for example, the direction travelled around a Sagnac loop as in Figure 4.2. Another possibility is to use two collinear but orthogonally oriented crystals, one of which produces photon pairs on the modes (A, B) with polarisation state $|H_A H_B\rangle$ and the other $|V_A V_B\rangle$. If temporal, spatial and spectral distinguishability between the pairs is washed out, an entangled state of the form $\frac{1}{\sqrt{2}}\left(|H_A H_B\rangle + e^{i\phi}|V_A V_B\rangle\right)$ is produced [60].

4.2.2 Polarisation analysis and detection

Photon analysis at Alice and Bob is done with four-detector passive polarisation analysers (Figure 3.9). After transmission through the fibres, each photon of the

entangled pair passes through a 50:50 beamsplitter to randomly choose either the H/V or +/- measurement basis. The photon hence passes through a polarisation beamsplitter to determine the polarisation value, either (H (0°) or V (90°)), or (+45° or -45°), depending on the basis choice. A time-tagging unit then records the state and the time of the detection. This information is bundled and passed to Alice and Bob's computers, which communicate classically to find the optimal time offset to maximise the number of coincidences between Alice's and Bob's detection events.

4.3 Theory and observation of guided modes in optical fibre

Since standard telecom fibre is slightly multimode for 810 nm light we expect the appearance of higher-order spatial modes. Guided wave theory predicts two linearly polarised modes of propagation (LP_{01} and LP_{11}) [95] for 810 nm photons in a telecom fibre. Here the modes are labeled based on the distribution arm (Alice or Bob) and the azimuthal index l (e.g., A_{l1}).

The full derivation is presented in Appendix B as a report from co-op student Allison MacDonald and summarised here. Light in an optical fibre core and cladding obeys the Helmholtz wave equation, which admits solutions in the form $U(r,\phi,z) = u(r)e^{-il\phi}e^{-i\beta z}$ where r is the radial distance from the centre of the fibre, ϕ and l are the azimuthal angle and index respectively, and β is the propagation parameter in the direction of propagation z. The solutions for the radial function $u(r)$ are the Bessel functions

$$u(r) \propto \begin{cases} J_l(X(r)), & r < a \\ K_l(Y(r)), & r > a. \end{cases} \tag{4.3}$$

By enforcing continuity of these functions and their derivative at the boundary between core and cladding $r = a$, I obtain the characteristic equation:

$$X\frac{J_{l\pm1}(X)}{J_l(X)} = \pm Y\frac{K_{l\pm1}(Y)}{K_l(Y)} \tag{4.4}$$

This equation is (graphically) solvable for the number of supported modes and each mode's propagation constant β, through relations involving X, Y, the numerical aperture of the fibre, the wavelength and the core radius (which determine the fibre V parameter). Figure 4.3 shows the graphical solution to the characteristic equation for the propagation of 810 nm light in 1550 nm single mode fibre. Two solutions are admitted, one for each of $l = 0$ and $l = 1$, with the $l = 2$ solution being excluded as the curves do not intersect before the fibre V parameter is reached, as $X \leq V$ through $X^2 + Y^2 = V^2$.

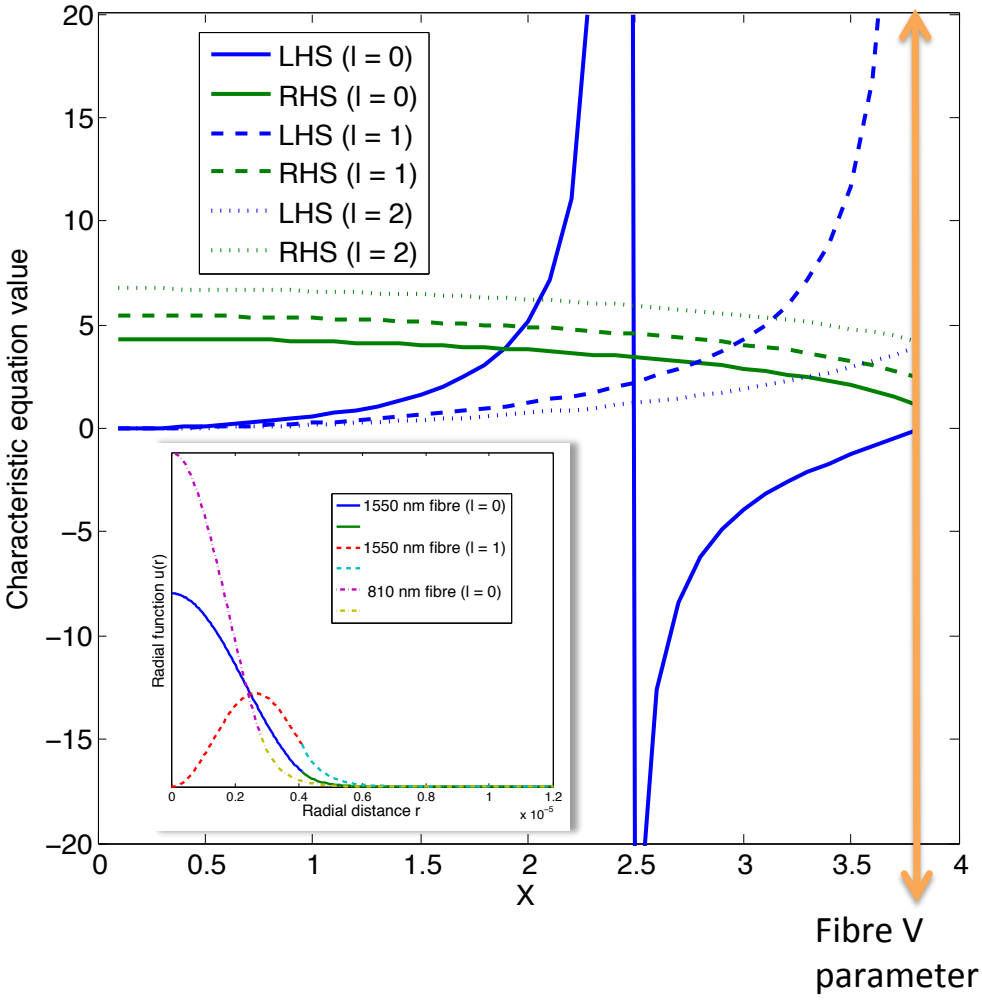

Figure 4.3: Plot of solutions to characteristic equation for optical fibre. The intersections of the LHS and RHS of the characteristic equation give solutions to modes of propagation in fibre, of which there are two in this case, $l = 0$ and $l = 1$. (The $l = 2$ curves do not intersect until after the fibre V parameter, which is forbidden by definition of the parameter, and the vertical line for the $l = 0$ curve is an asymptote and not a true intersection.) Inset is a plot of the radial distribution functions $u(r)$ for 810 nm light in 810 nm and 1550 nm single mode fibres. One mode is supported in the former and two in the latter, and it is clear that the $l = 0$ modes overlap much better than the $l = 0$ and $l = 1$ modes between fibres.

Consistent with the guided wave theory above, the two propagation modes in 1550 nm single mode fibre show modal dispersion; i.e., the group velocity of the A_{11} mode is different from that of the A_{01} mode, resulting in two distinct arrival times [117]. Detecting Bob's photons locally and Alice's after 3 km of telecom fibre resulted in a histogram of coincidences with two pronounced peaks, as seen in Figure 4.4. The relative offset of the two peaks varied linearly with fibre length (Figure 4.5) leading to a measured modal dispersion of 2.20 ns/km, in excellent agreement with the theoretical value of 2.19 ns/km (see calculations in Appendix B). As evidenced by the well-defined peaks in Figure 4.4, there is little crosstalk between the two modes after the initial insertion, so the polarisation state in the fundamental mode is well preserved and the timing signature of each mode is evident.

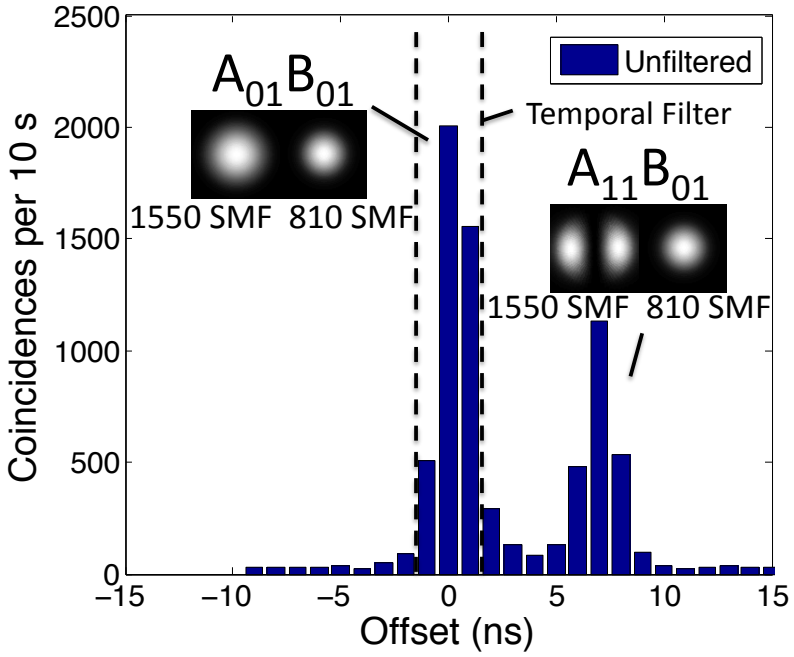

Figure 4.4: Asymmetric distribution (D_A=3 km, D_B=0 km): histogram of coincident detection events with delay between Alice's and Bob's detection. The slower A_{11} mode in Alice's arm is intentionally excited to illustrate the effect, then filtered. The theoretical power distribution of the propagating spatial modes at 810 nm for different fibre types is inset (SMF = single mode fibre).

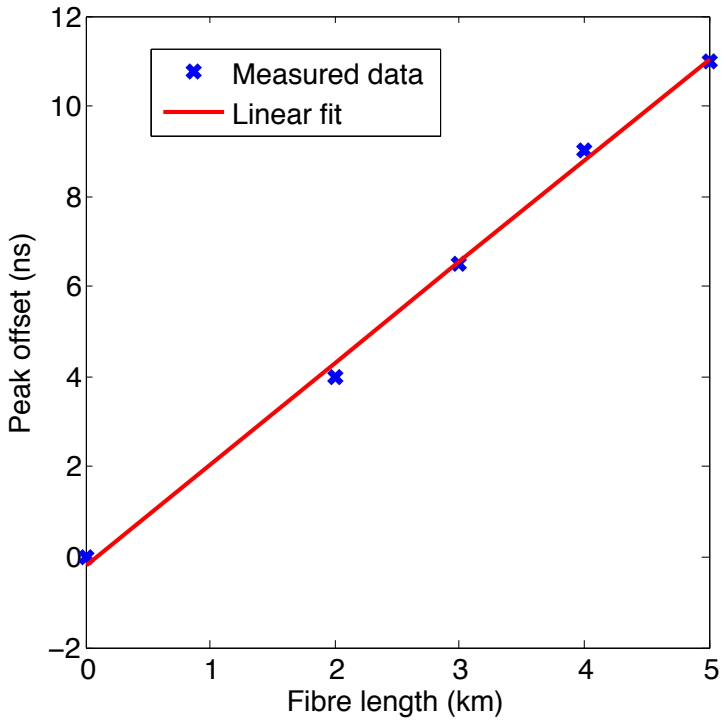

Figure 4.5: Modal dispersion in telecom optical fibre. The relative time offset between the $A_{01}B_{01}$ and $A_{11}B_{01}$ coincidence peaks varies linearly with fibre length, leading to a modal dispersion of 2.2 ns per km of fibre.

4.4 Experimental results

4.4.1 Filtering of spatial fibre modes

For a high fidelity transmission of polarisation entangled photons it is necessary to select only the fundamental mode in both arms ($A_{01}B_{01}$), as higher order modes will lead to an increased error in the polarisation contrast since only one of the polarisation rotations experienced by different modes in the fibre can be compensated for. In principle, the modes could be separated and compensated individually, but without such elaborate mode extraction two methods for filtering out the higher modes at the receiver are developed:

(i) In the case of an asymmetric distribution, where the fibre lengths to Alice and Bob are not identical, a temporal filter can be applied in the form a of a narrow coincidence window, which will cut out the higher order peak, as demonstrated in Figure 4.4. This technique introduces no additional optical losses.

(ii) In a symmetric distribution, where both Alice and Bob receive photons through telecom fibre and where the difference in fibre lengths is less than 2 km, the $A_{01}B_{01}$ and $A_{11}B_{11}$ peaks become inseparable in time, as seen in the central peak of Fig. 3. In this case, in addition to the temporal filter to eliminate the side peaks, a spatial filter (810 nm single mode fibre) is used before detection. Since the radial extent of the power in the higher order modes is greater than that in the fundamental mode, the smaller core of the 810 nm fibre (shown as a ring in Figure 4.6) removes around 98% of the A_{11} or B_{11} mode while preserving at least 75% of the A_{01} or B_{01} mode.

4.4.2 Entanglement visibility

In order to quantify our filtering methods we performed entanglement distribution measurements with telecom fibre spools of lengths up to $D_A = 6$ km (asymmetrically), and up to $D_A = D_B = 2$ km (symmetrically). We extracted the entanglement visibility (a measure of the quality of entanglement) [44] and raw coincidences (Table 4.1). To set a benchmark for comparison, measurements were performed locally with short 810 nm fibres (2 m), resulting in 95.7±0.4 % visibility, averaged over the H/V and +/- bases[1]. Visibility for entanglement is defined based on the number of coincident detection events N as

$$V = \frac{N_{right} - N_{wrong}}{N_{right} + N_{wrong}}, \tag{4.5}$$

[1]Differences in count rates are due to a realignment of the source between measurements.

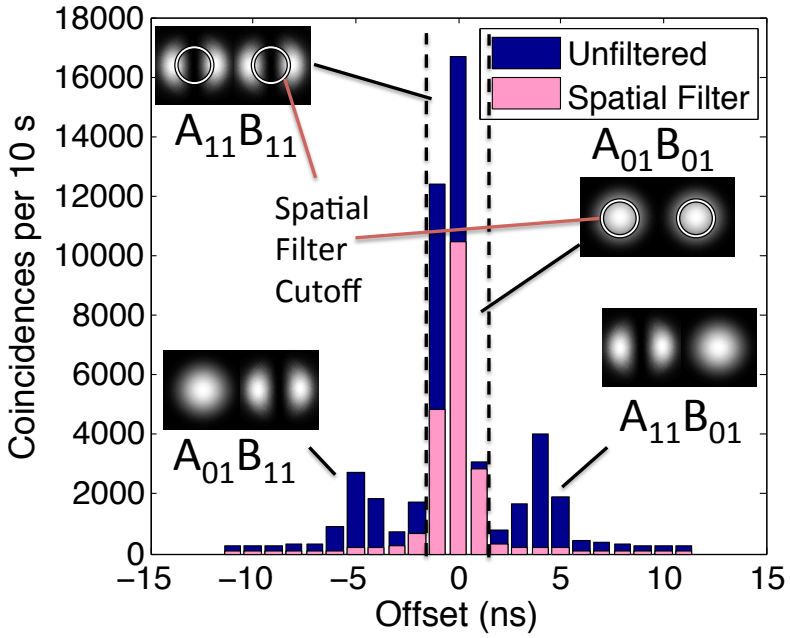

Figure 4.6: Symmetric distribution (D_A=2 km,D_B=2 km): selection of $A_{01}B_{01}$ mode by spatial filtering. The spatial filter (core radius superimposed on power distribution) eliminates not only the side peaks (due to photons coupling into cross modes) but also those coincidences in the central peak that are a result of both photons coupling into the higher mode ($A_{11}B_{11}$), such that they give little or no betraying time offset, and thus cannot be filtered temporally.

where the definition of "right" coincidences is those that agree with the desired (pure) entangled state. For example, anti-correlations are the "right" coincident events for the state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B \pm |V\rangle_A|H\rangle_B\right)$.

D_A/D_B (km)	Trans. Loss (dB)	Filtering	Visibility (%)	Coinc. (rate/s)	Secure Key (rate/s)
2/0	6	None	88.0±0.2	3000	420
(Asym)	7	Temporal	94.6±0.2	2700	800
5/0	15	Temporal	91.6±0.5	430	90
2/2	12	None	62.9±0.4	5200	0
(Sym)	14	Temporal	92.2±0.3	3600	850
	16	Temporal+spatial	95.6±0.2	1950	650

Table 4.1: Summary of entanglement distribution for various telecom fibre lengths, including QKD key rates. Transmission loss includes attenuation in the optical fibres, as well as loss from the filtering processes. Local measurements gave an average visibility of 95.7±0.4%. Uncertainty is taken as due to Poissonian count fluctuations. "Asym" and "sym" respectively indicate whether the source is located asymmetrically at Alice, or symmetrically between Alice and Bob.

For the asymmetric distribution we employed a 3 ns coincidence window as the temporal filter: at 2 km of fibre in one arm, for example, overall visibility was improved from 88.0 % to 94.6 % with this method. Figure 4.7 shows the visibility for asymmetric distribution distances up to 6 km. In the case of symmetric distribution (see Table 4.1), we employed both filtering techniques to raise visibility from 62 % to 95.6 %. For this and the asymmetric case, visibility is brought close to the benchmark which implies that the higher order modes are suppressed using the filtering detailed above, and that there is no significant crosstalk along the length of the fibre.

4.4.3 Quantum key distribution

To illustrate the utility of this form of entanglement distribution, we additionally extracted the secure key rate for QKD based on realistic error correction and privacy amplification [70]. Figure 4.7 also shows this calculated secure key rate, dropping linearly (on the log scale) with increasing lengths of fibres, with a sharp cut-off around 6 km due to increased loss and detector dark counts.

QKD over installed fibre link

As a realistic example of a network implementation, we performed a full QKD protocol over two symmetric 2.2 km channels of installed telecom fibres. Two

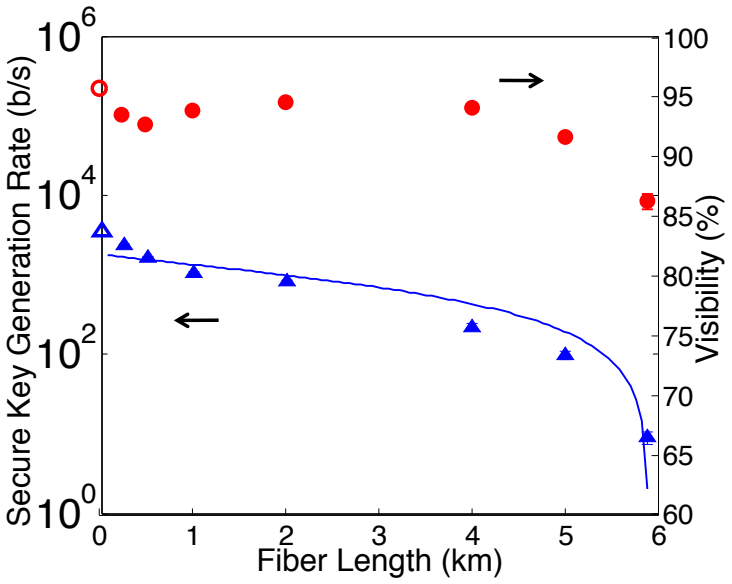

Figure 4.7: Secure key generation rates (triangles) and measured visibility (circles) as a function of fibre length in Alice's arm. The open symbols are local data, and the line is a fit to the secure key rate with realistic parameters (see Reference [70]). Error bars are smaller than symbol size.

parallel fibres were used between the Mathematics and Computer Building on the University of Waterloo's campus (source of entangled photons) and the Perimeter Institute (detection modules Alice and Bob), leading to a total distribution distance of 4.4 km. The quantum bit error rate (QBER) was higher than for the fibre spools, likely due to disturbances from passing cars, trains, and thermal fluctuations. For example, over 15 minutes, the average QBER was 4.3 % (i.e., 91.4 % visibility) with both temporal and spatial filtering, leading to an average secure key rate of 350 bits/s (see Figure 4.8). During longer runs, the errors tended to increase with time due to polarisation drifts in the fibres.

QKD with classical traffic

As the quantum signals around 800 nm wavelength are so far separated from the classical traffic at 1310 nm or, more commonly, 1550 nm, it was expected that there should be little or no cross-talk when these two signals are sent through the same fibre. This would allow QKD to take place over fibres that are in use

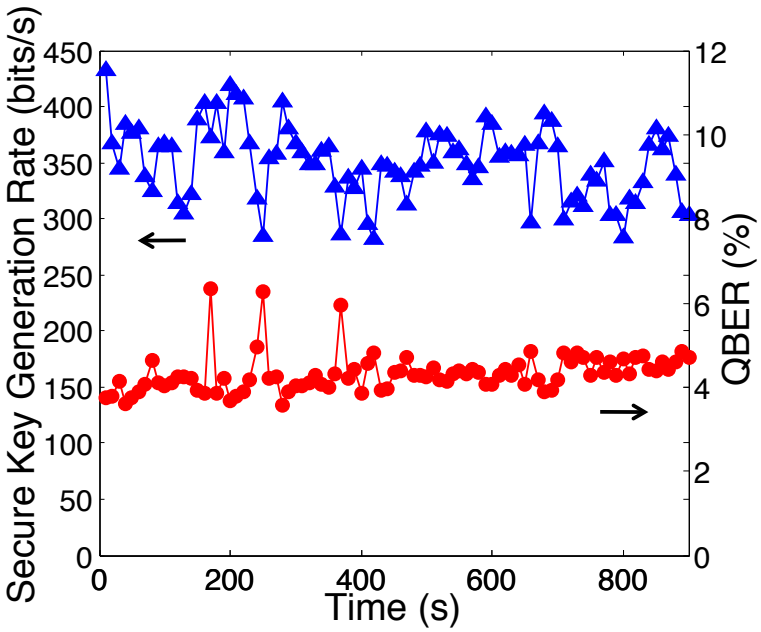

Figure 4.8: Secure key generation rate (triangles) and measured QBER (circles) in a symmetric installed fibre link. Each data point is the average over 20 s.

for internet traffic, including the classical communication for the QKD protocol. One small data run was taken over the UW to PI fibre link (Figure 4.9) including classical internet traffic at 1310 nm over the same fibre. The results for QBER are presented in Figure 4.10, and show no appreciable increase in QBER when the classical traffic is activated. Catherine Holloway later took much more complete data on the interplay of classical and quantum photons in fibre, confirming the compatibility of the two signals: QBER is essentially independent of classical bit rate (tested up to 100 Mbps), and the classical traffic is unaffected by the quantum transmissions.

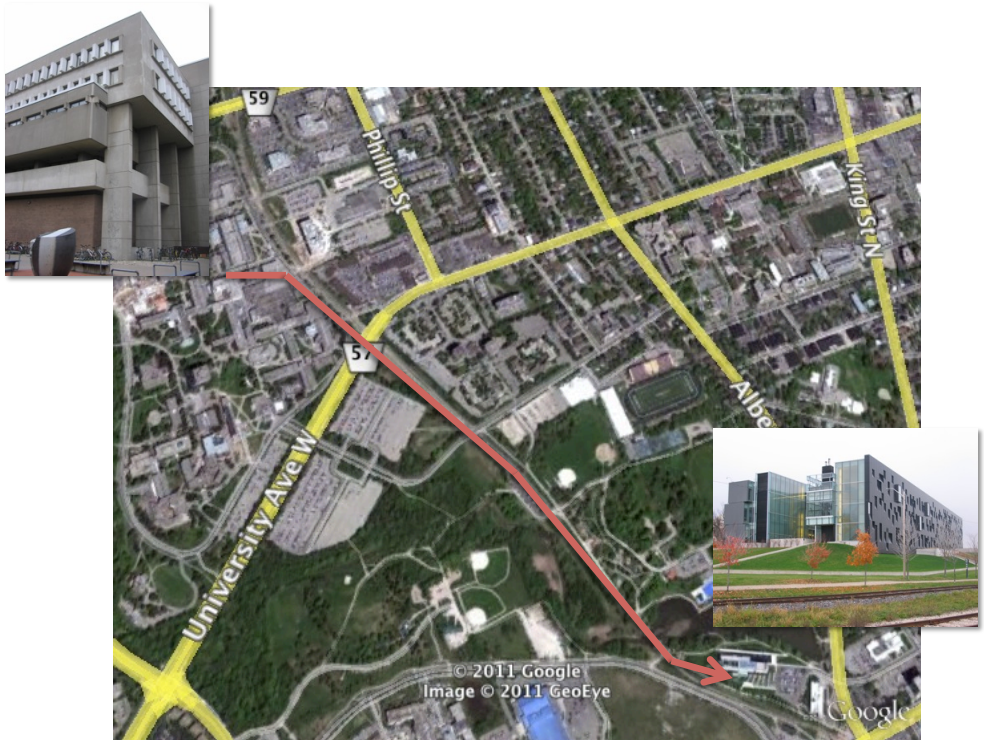

Figure 4.9: Path of installed fibre optic link. Two parallel fibres run from the Mathematics & Computer building on the University of Waterloo's campus to the Perimeter Institute for Theoretical Physics in uptown Waterloo. Map © 2011 Google and GeoEye.

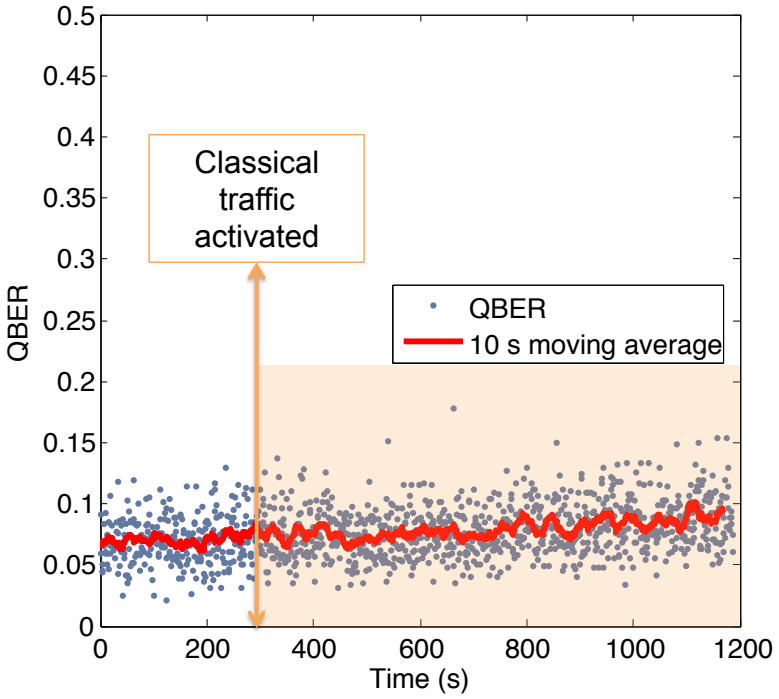

Figure 4.10: QBER of entangled signal with classical traffic over same fibre. The QBER gradually increases with time due to temperature drifts and fibre relaxation, but shows no appreciable increase at the moment the classical traffic is activated.

4.5 Discussion

Our approach has the potential for much higher distribution rates, as local coincidence rates of 2.5 MHz have been achieved with short-wavelength entanglement sources [100]. Assuming the same fibre loss observed here, secure key rates of 500 kb/s are possible over a 4 km symmetric link using only standard telecom fibres. Previous systems based on weak laser pulses around 800 nm were limited to key rates of 100 kb/s over 4 km of telecom fibre [20]. Given the superior functionality and lower complexity of detectors at 800 nm combined with the multiuser networking capabilities of entanglement [64], we believe that such QKD systems will find applications in inner city links or corporate networks. In addition, the possibility to address multiple modes in a fibre could be useful for implementations of higher-dimensional quantum information.

We have demonstrated the viability of entanglement distribution in standard optical fibres using 810 nm photons, including the compatibility of quantum communications with classical traffic. With suitable filtering, error rates are not affected by higher order modes in the fibre and high fidelity distribution can be achieved over several kilometres. We believe our results pave the way for a wide usage of telecom optical infrastructure together with the well established quantum information systems at shorter wavelengths.

Chapter 5

Demonstration of quantum key distribution system for high loss satellite uplink

This chapter is based on an experiment performed 2010-2011. The content of this chapter is in preparation for journal submission in altered form with the following authorship:

Evan Meyer-Scott, Zhizhong Yan, Allison MacDonald, Jean-Philippe Bourgoin, Hannes Hübel and Thomas Jennewein.

Author contributions

Thomas and Hannes conceived the experiment and photon source, and supervised the project. Jean-Philippe performed the satellite simulations. Zhizhong built Alice's modulation system. Allison built Bob's receiver and wrote the timing synchronisation software. I built the photon source, performed the experiment and analysed the data. I wrote the paper with input from all authors.

5.1 Introduction

Quantum key distribution (QKD) is the most successful application to arise thus far from quantum information theory [7, 34], but it carries the drawback of a distance limitation [107, 65, 110, 120, 101]: even with future advances, no more than 400 km of direct transmission in optical fibres is expected [33]; however, quantum repeaters and satellites both have the potential to enable worldwide quantum communication. The former is very appealing with recent promising results [30], but is still in the fundamental research stage. Satellite QKD, by contrast, is achievable by today's satellite and quantum technologies, which already have the required performance [11]. In the most feasible scenario, the

satellite acts as a trusted node and performs consecutive key distributions to two different ground stations allowing a symmetric key sharing between any two locations [1]. Both a downlink and uplink of photons from/to a satellite have been considered to transmit quantum keys. The downlink is expected to experience lower attenuation, since the uplink beam is much more affected by atmospheric turbulence [11]. Nonetheless, an uplink may be more practical since it keeps the complex and power-hungry source of photons on the ground, and permits the use of cutting-edge sources which may include weak coherent pulses, heralded or entangled photons, single photon emitters, and possibly quantum memories. With respect to satellite technology, the uplink is beneficial due to looser telescope pointing requirements, less demanding opto-mechanics (no precision coupling or fibres), and lower data processing needs. Additionally, all required components for the receiver have flown in space, most notably single-photon detectors [58]. However, the channel loss in an uplink is estimated to be above 40 dB, beyond the capability of current QKD systems, and generally deemed impossible. Here we show it is indeed feasible by implementing a photonic system capable of QKD in this high loss regime, which includes a novel photon source, advanced timing analysis, and single photon detectors with the highest overall figure of merit [40]. Our system can perform QKD up to 57 dB total loss in the infinite key limit [71], and has the potential to overcome finite size effects on a single satellite passage [108]. Our approach could be implemented immediately in a satellite mission.

In support of our experimental work, we have performed a rigorous analysis of channel performance for uplinks and downlinks, including diffraction, atmospheric turbulence, pointing error, multiphoton statistics, optical/detector inefficiencies, satellite orbit statistics, and background noise, to produce secure key rate statistics for a variety of conditions and systems (see Methods). As a specific example, for an uplink to a satellite 600 km high, using a 25 cm diameter telescope on the ground and 30 cm on the satellite, our model shows about 80% of total satellite passages over the ground station will be usable for QKD asymptotically (infinite key limit), with an average total loss of 52 dB, an order of magnitude beyond the capability of current QKD systems.

5.2 Experimental setup

5.2.1 Technology considerations

The most obvious challenge in a satellite uplink is the sheer link distance: it can be 500 km to more than 30,000 km depending on the satellite orbit, with no possibility for an intermediate node, making the quantum channel extremely

lossy. Additionally, noise due to detector dark counts and stray light, especially moonlight and terrestrial light, will make satellite QKD more demanding. Finally, the short duration of each satellite passage, on the order of hundreds of seconds, makes proving security of QKD difficult, given the small number of quantum signals received. To address the challenges of a satellite uplink, both physical and technical parameters must be tuned. The first variable that can be chosen to minimize loss is the wavelength of the photons. Beam spread due to diffraction is the main source of loss and is proportional to wavelength, so short wavelength photons are preferred. After considering the optical transmission of the atmosphere and single photon detector capabilities, the best choice is $\lambda = 532$ nm, which enables the use of thin silicon avalanche photodiodes [90]. This type of detector has the highest figure of merit for single photon quantum information applications [40], based on efficiency, timing jitter and dark count rate. In order to limit background noise, the system must employ short pulses and temporally precise detection which allow temporal filtering of received signals. The optimisation of this temporal filtering is described below. Furthermore, a high system clock rate is important to generate enough signals to account for statistical fluctuations in estimation of an eavesdropper's information (finite size effects). As a final consideration, the QKD system must have phase randomization such that subsequent pulses share no phase relation, which is assumed in security proofs to limit information given to an eavesdropper.

5.2.2 System configuration

Our weak coherent pulse decoy-state system satisfies all the above requirements through the sum-frequency generation, or up-conversion method of photon production. The design and implementation are illustrated in figure 5.1.

To provide short pulses and fast modulation, light from a mode-locked titanium sapphire laser at 810 nm is combined in two type-I Periodically-Poled KTP crystals with light from a 1550 nm continuous-wave laser to produce, due to energy conservation, photons at 532 nm. The arrangement is equivalent to an asymmetric down-conversion entanglement source run in reverse [44], and uses two orthogonally-oriented PPKTP crystals, for polarisation-insensitive up-conversion (see Subsection 5.2.3 for a description of up-conversion). The source employs phase precompensation using birefringent wedges in the 810 nm beam to compensate for temporal walkoff in the PPKTP crystals. The pulsed 810 nm beam is set to 45° polarisation (coherent superposition of horizontal and vertical), while the 1550 nm pump light is modulated in polarisation (qubit state) and intensity (signal or decoy). In this configuration, the output pulses at 532 nm follow the pulse length of the 810 nm laser and the polarisation and

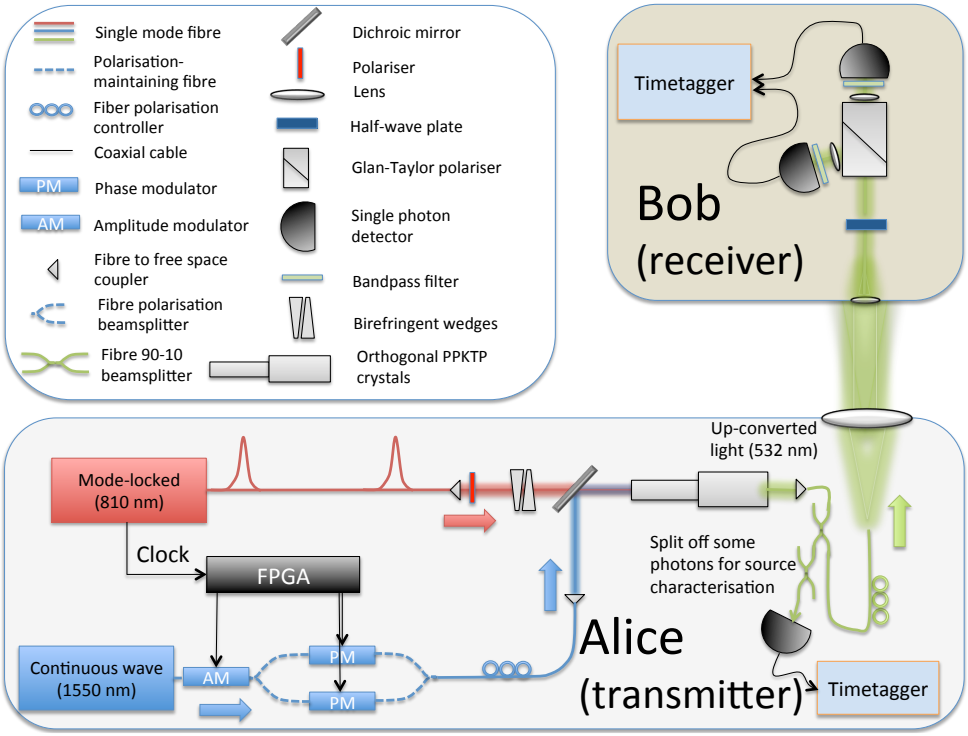

Figure 5.1: Simplified schematic of QKD system for high loss link. The colour of the beams and fibre optics indicates the wavelength of light: red for 810 nm, blue for 1550 nm and green for 532 nm. Alice's up-conversion photon source produces photons at 532 nm which are sent through the controllable-loss channel to Bob's receiver, a mock-up of a satellite receiver.

amplitude of the modulated 1550 nm beam. The modulation is accomplished with off-the-shelf telecom waveguide modulators, which show high stability and switching contrast, and switching speeds of a few GHz. The power of the two input beams is controlled such that the output pulses at 532 nm contain around one photon per pulse, as determined by the optimal average photon number for decoy-state QKD. The phase randomization is also accomplished with the telecom laser, whose coherence time is less than the period between adjacent pulses emitted from the mode-locked laser (see Methods).

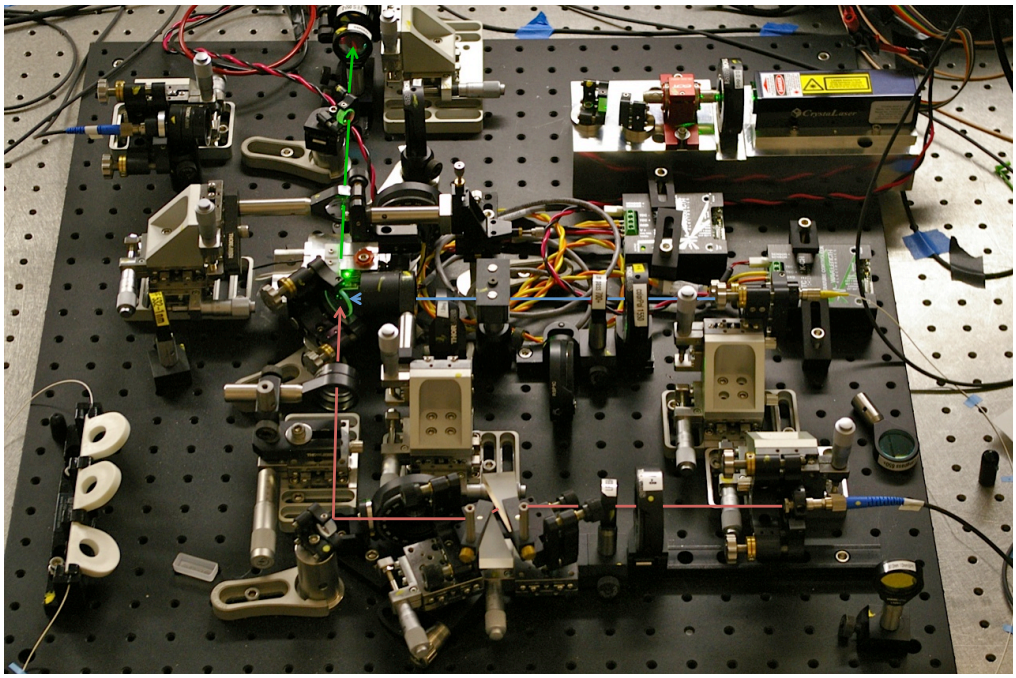

Figure 5.2: Picture of QKD source for high loss link. The 810 nm (red) and 1550 nm (blue) beams converge in the crystals and up-convert to 532 nm (green), which is collected in fibre and routed to Alice's sending telescope.

The up-converted photons are collected into single mode fibre, then Alice splits off 10 % of the photons with a 90-10 fibre beamsplitter for source characterisation (another 90-10 beamsplitter is used in series to further attenuate the signal Alice must measure). The remaining photons (90 %) are allowed to exit at the fibre tip to the quantum channel, then pass through an adjustable lens to control the beam size at Bob's receiver and therefore the channel loss. Bob's lens selects a small portion of the beam to simulate a high loss channel to space. Bob performs active basis choice with a half-wave plate (see Methods), then the light passes through a polariser (to determine the bit value) and narrow-band filters before arriving

at silicon single-photon detectors from Micro Photon Devices. The detectors have a peak efficiency of 48% at 550 nm, 10 dark counts per second and 30 ps timing resolution, which allows temporal exclusion of much background noise. The detector events are registered and digitised using a timetagging module with 156 ps resolution. All these components are commercially available, making this system practical for satellite applications.

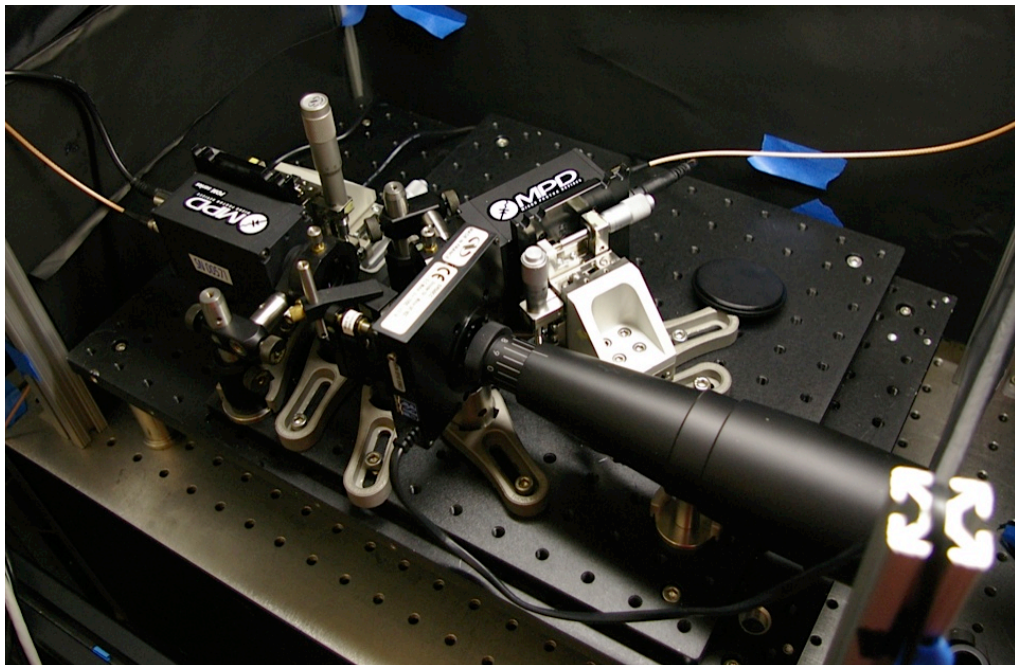

Figure 5.3: Picture of QKD receiver for high loss link. Bob's receiver includes telescope, motorised half-waveplate, polarising beamsplitter and two detectors from MPD.

5.2.3 Up-conversion or sum frequency generation

Generally speaking, up-conversion and sum frequency generation are equivalent terms describing a second order ($\chi^{(2)}$) nonlinear optical process in which two low frequency input beams are converted into a higher frequency output beam. The term up-conversion is used preferentially here to highlight the fact that this particular source can operate as both an up-converter and down-converter, the former producing light at 532 nm and the latter producing entangled pairs which are asymmetric in wavelength, at 810 nm and 1550 nm. The aim here is to provide polarisation- and amplitude-modulated output light pulses at 532 nm, a wavelength previously inaccessible for QKD due to a lack of fast modulators.

Though up-conversion can be treated quantum mechanically as down-conversion (see Subsection 4.2.1), here I will derive it classically following Reference [14], as it is indeed a purely classical process, especially when involving strong pump lasers as is the case in this source. I show that up-conversion output power is linear in each of the input pump powers and not subject to quantum mechanical noise.

First, I assume the three relevant waves are monochromatic and collinear, and label $\omega_{1,2}$ as the frequency associated with the pump light at 810 nm and 1550 nm respectively, and $\omega_3 = \omega_1 + \omega_2$ as the output light at 532 nm. Then I start from the driven wave equation as follows:

$$\nabla^2 \tilde{E}_j - \frac{n_j^2}{c^2}\frac{\partial^2 \tilde{E}_j}{\partial t^2} = \frac{1}{\epsilon_0 c^2}\frac{\partial^2 \tilde{P}_j^{NL}}{\partial t^2} \tag{5.1}$$

Here $\tilde{E}_j$ denotes the electric field amplitude of the j-th frequency, and the tilde means fast varying; n_j is the index of refraction of the crystal at ω_j; c is the speed of light in vacuum; ϵ_0 is the permittivity of free space; and $\tilde{P}_j^{NL}$ is the result of the nonlinearity, in effect a driving term at frequency ω_j. Concentrating on the output frequency $j = 3$, and assuming plane waves I define

$$\tilde{E}_3(z,t) = A_3(z)e^{i(k_3 z - \omega_3 t)} + c.c. \tag{5.2}$$

where z is the distance along the propagation direction in the crystal, $A_3(z)$ is the slowly varying amplitude of the field, and $k_3 = \frac{n_3\omega_3}{c}$ is the wavenumber in the crystal. Similarly for the nonlinear driving term, with $c.c =$ complex conjugate,

$$\tilde{P}_3^{NL}(z,t) = 4\epsilon_0 d_{eff} E_1 E_2 e^{-i\omega_3 t} + c.c. \tag{5.3}$$

where d_{eff} is the effective nonlinearity which can be calculated from the nonlinear susceptibility tensor, and $E_j(z) = A_j(z)e^{ik_j z}$ is the pump electric fields, with slowly varying amplitude $A_j(z)$. As the pump powers in my source are $1-20$ mW and the output power is around 30 pW, it is a very good approximation that the pump fields are constant, i.e. $A_{1,2}(z) = A_{1,2} = const$. Thus the nonlinear driving term is

$$\tilde{P}_3^{NL}(z,t) = 4\epsilon_0 d_{eff} A_1 A_2 e^{i\left[(k_1+k_2)-\omega_3 t\right]} + c.c. \tag{5.4}$$

Substituting into Equation 5.1 and reducing ∇^2 to $\frac{\partial^2}{\partial z^2}$ due to plane waves, I obtain the following and simplify.

$$\frac{\partial^2}{\partial z^2}\left[A_3(z)e^{i(k_3 z-\omega_3 t)}+c.c.\right]-\frac{n_j^2}{c^2}\frac{\partial^2}{\partial t^2}\left[A_3(z)e^{i(k_3 z-\omega_3 t)}+c.c.\right] = \frac{1}{\epsilon_0 c^2}\frac{\partial^2}{\partial t^2}\left[4\epsilon_0 d_{eff}A_1A_2e^{i\left[(k_1+k_2)-\omega_3 t\right]}+c.c.\right] \tag{5.5}$$

$$\left[\frac{d^2A_3(z)}{dz^2}+2ik_3\frac{dA_3(z)}{dz}-k_3^2A_3(z)+\frac{\omega_3^2n_3^2}{c^2}A_3(z)\right]e^{i(k_3z-\omega_3t)}+c.c. = \frac{-4d_{eff}A_1A_2\omega_3^2}{c^2}e^{i\left[(k_1+k_2)-\omega_3t\right]}+c.c \tag{5.6}$$

$$\frac{d^2A_3(z)}{dz^2}+2ik_3\frac{dA_3(z)}{dz}=\frac{-4d_{eff}A_1A_2\omega_3^2}{c^2}e^{i(k_1+k_2-k_3)z} \tag{5.7}$$

I drop the complex conjugate terms as they satisfy equality independently. I now invoke the slowly varying amplitude approximation to drop the second derivative, i.e. $\left|\frac{d^2A_3(z)}{dz^2}\right| \ll \left|k_3\frac{dA_3(z)}{dz}\right|$. Finally I introduce $\Delta k = k_1+k_2-k_3$ to get

$$\frac{dA_3(z)}{dz}=\frac{2id_{eff}A_1A_2\omega_3^2}{k_3c^2}e^{i\Delta kz}. \tag{5.8}$$

A simple integration over z from 0 to the crystal length L gives

$$A_3(L)=\frac{2id_{eff}A_1A_2\omega_3^2}{k_3c^2}\left(\frac{e^{i\Delta kL}-1}{i\Delta k}\right). \tag{5.9}$$

Finally, I calculate the intensity I_3 of the output field at ω_3 as

$$I_3=2n_3\epsilon_0c|A_3|^2=\frac{8n^3\epsilon_0d_{eff}|A_1|^2|A_2|^2\omega_3^4}{k_3^2c^3}\left|\frac{e^{i\Delta kL}-1}{\Delta k}\right|^2. \tag{5.10}$$

Of note is that the output intensity is perfectly linear in each of the input intensities, thus, modulating the input beam at 1550 nm in intensity will cause proportional modulation of the output beam for decoy and signal states. Interestingly, even when a quantum mechanical picture is considered where the field amplitudes A_k become annihilation operators $\hat{a}_k$, no additional noise is added by the up-conversion process as there are no terms independent of both operators on the pump modes. This is especially relevant in the sense that one of the pump beams cannot spontaneously up-convert to 532 nm without the presence of the other beam, in contrast to spontaneous down-converison. Additionally, there is no analog to the error-inducing double emission of down-conversion, as any additional photons are emitted into the same polarisation mode. Unfortunately, there

is a second-order source of noise as the 810 nm photons can be down-converted to photons at 1550 nm and 1697 nm, the former of which can subsequently be up-converted as an erroneous photon in the output 532 nm beam. Though the phasematching is extremely weak, this is still a major problem when using up-conversion for single photon detection in the 1550 nm range [122]. Thankfully, the effect is neglectable here as the both pump beams are relatively strong lasers, completely overpowering the single photon level of this spurious down- and up-conversion.

Resuming the derivation, the final factor in Equation 5.10 is

$$\begin{aligned}\left|\frac{e^{i\Delta kL}-1}{\Delta k}\right|^2 &= \frac{1}{\Delta k^2}(e^{-i\Delta kL}-1)(e^{i\Delta kL}-1)\\ &= \frac{1}{\Delta k^2}\left(2-(e^{i\Delta kL}+e^{-i\Delta kL})\right)\\ &= \frac{2}{\Delta k^2}(1-\cos(\Delta kL))\\ &= \frac{2}{\Delta k^2}\left(2\sin^2(\Delta kL/2)\right)\\ &= L^2\mathrm{sinc}^2(\Delta \mathrm{kL}/2).\end{aligned} \tag{5.11}$$

Thus the output intensity is

$$I_3 = \frac{8n^3\epsilon_0 d_{eff}|A_1|^2|A_2|^2\omega_3^4L^2}{k_3^2c^3}\mathrm{sinc}^2(\Delta \mathrm{kL}/2). \tag{5.12}$$

This leads to the phasematching condition of $\Delta k = 0$, as the sinc(x) function has a maximum at $x = 0$. This equation is impossible to satisfy in normally dispersive materials, leading to other solutions such as birefringent phasematching or quasi-phasematching [47], which gives a phasematching condition of

$$\Delta k = 0 = k_1 + k_2 - k_3 - 2\pi/\Lambda, \tag{5.13}$$

where Λ is now a parameter of the material controllable through periodic poling. This method was used to construct the type-I periodically poled KTP crystals used here for up-conversion. As the type-I crystals used satisfy phasematching only when the polarisations of all fields are the same, two crystals are needed to provide polarisation-insensitive up-conversion. Two crystals are placed back to back, such that one crystal performs up-conversion for horizontally polarised light, and the other for vertically polarised. So long as distinguishability (in spectrum and time) between the two crystals is removed (by temperature tuning and phase compensation respectively), the two crystals can also up-convert coherent

superpositions of horizontal and vertical polarisations, such that all four qubit states necessary for QKD can be produced by the up-conversion process. [1]

5.2.4 Timing synchronisation

As seen in figure 5.4, the timetagging clock at Bob may drift hundreds of nanoseconds relative to the laser clock (period = 13 ns) at Alice. As an example, if the laser clock period is shortened by only 1 fs, the clocks will be offset by 76 ns after one second, making signal identification impossible. Therefore, timing synchronisation between Alice and Bob is necessary, and is accomplished here by timetagging a frequency-divided version of the laser clock. Bob then sends his timetags to Alice who uses her timetagged laser clock signal to stretch or compress portions of Bob's detection timetags depending on the fluctuations as caused by cavity length changes in the laser or drifts in the timetagger's clock. Thus Alice can identify which tags to keep based on timing and relay this information to Bob. This could be performed over a satellite's communication channel, and since only detection times and not bit or basis values are revealed, no information is leaked to Eve beyond what she is already assumed to know.

5.3 Decoy-state protocol

Weak coherent pulse sources based on (up-conversion of) highly attenuated lasers are attractive for QKD; however, because of the Poissonian statistics of photon number in laser pulses, some pulses will have more than one photon and be subject to the photon number splitting attack [67]. In this attack, an adversary Eve splits off one photon from the pulse and stores it to measure only after the legitimate party Bob reveals his measurement basis. Eve then measures in the correct basis, and so gains full information about multi-photon pulses without leaving a trace. To combat this attack, the decoy-state protocol was introduced, wherein Alice changes the average photon number of randomly interspersed pulses from the signal level μ to the decoy level ν. Since Eve cannot know whether a given pulse is a signal or decoy pulse, the decoy pulses allow much better bounds on how much information Eve has gained from multiphoton signals, and thus how much privacy amplification must be performed. The asymptotic key rate (adapted from Reference [71]) per laser pulse obtainable

[1] Down-conversion is a similar process to up-conversion, but its derivation requires quantisation of the light fields for spontaneous pair creation. Thus the field amplitudes A_k become mode annihilation operators $\hat{a}_k$, and the non-commuting nature of these operators allows photon creation in the output even with no initial field in those modes.

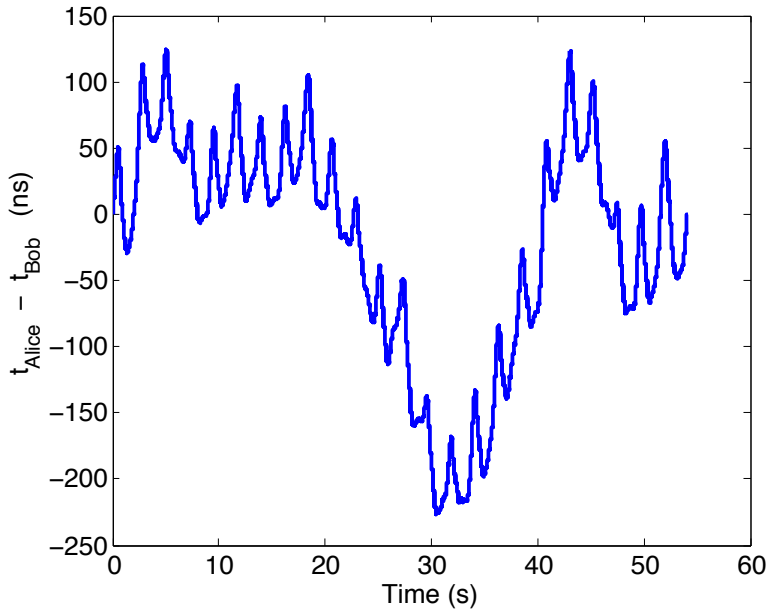

Figure 5.4: Typically observed drift between Alice's and Bob's clocks. Alice's clock is determined by the repetition rate of the mode-locked laser and Bob's comes from his timetagger. Drifts in the clock are large compared to the nominal laser clock period of 13 ns, making timing synchronisation a necessity. Our synchronisation scheme correctly aligns Bob's detection events independent of which device is drifting.

from a decoy pulse protocol is

$$R \geq q \frac{N_\mu}{N_\mu + N_\nu} \{ -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1 \left[1 - H_2(e_1) \right] \}, \tag{5.14}$$

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 for signal pulses, $f(E_\mu) = 1.22$ is the error correction efficiency for practical error correction codes, $H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, and Q_1 and e_1 are the estimated gain and error rate for single photon pulses. The factor $\frac{N_\mu}{N_\mu + N_\nu}$ is added since only detections of the signal state μ contribute to the final key, and $N_{\mu/\nu}$ is the number of signal/decoy detections. The key rate is then the gain of single-photon pulses, less the error correction on all signal pulses, less the privacy amplification on single-photon pulses. Note that this key rate should be multiplied by the laser pulse rate to obtain secure key bits per second.

We chose the two-decoy protocol from Reference [71]. In this protocol, Alice sends randomly a signal pulse with average photon number μ, a decoy pulse with average photon number $\nu < \mu$, or the vacuum. In our case, to illustrate the utility of the two-decoy method, we took the vacuum as being sent between adjacent laser pulses. Q_1 and e_1 can be estimated without loss of security as

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2} \left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0 \right) \tag{5.15}$$

$$e_1 = \frac{E_\nu Q_\nu}{Q_1} - \frac{e_0 Y_0}{Q_1 e^\mu}; \tag{5.16}$$

where Y_0 and $e_0 = 0.5$ are the vacuum yield and error rate.

5.4 Experimental results

Our main results are summarised in figure 5.5. Simulations of satellite orbits over one year were performed (see Methods) to predict the total channel loss (including receiver) in an uplink versus passage time of the satellite. Using a realistic orbit at 600 km height, 712 satellite passages over our hypothetical ground station near Ottawa, Canada were predicted, about 80% of which have a portion with low enough loss for QKD. The total loss versus time of the overall best single passage and of the 80th percentile passage are plotted in figure 5.5a. We then performed a quantum optical simulation including photon production, channel transmittance and detection, to produce a secure key rate versus total

loss as shown in figure 5.5b. The simulations show key generation is possible up to 63 dB asymptotically, well over the 52 dB average loss of the simulated satellite uplink.

Using our experimental setup, the detection rate and quantum bit error rate (QBER $= E_\mu$) in each of the rectilinear and diagonal bases for signals and decoys were measured and a final secure key rate from equation (5.14) was calculated. A pseudorandom sequence of 256 pulses was repeated and the resulting timetags formed into a histogram (Figure 5.6) to give information on each individual pulse state, allowing full characterisation of the system's capability. The results versus loss in figure 5.5b, based on many 1000 second data collection runs at a clock rate of 76 MHz, show secure key distribution is possible up to 57 dB experimentally, and agree well with the quantum optical simulation. The secure key generation rate at this maximum 57 dB is 2 bits/s, highlighting the viability of the quantum optics and detectors required for a satellite uplink. Allowing 6 dB for receiver and detector efficiency, this permits channel losses up to 51 dB, higher than any decoy-state systems previously built [110, 107, 65].

Finally, the total loss versus time for a satellite passage and secure key rate versus total loss can combine to produce figure 5.5c, secure key rate versus time for a satellite passage. The rate is given in bits per laser pulse on the left axis and bits per second on the right, based on our clock rate of 76 MHz. To determine secure key rate at a given time, map points from figure 5.5a to 5.5b to determine the key rate at the corresponding loss, and then map this value to figure 5.5c. The curves in figure 5.5c can be integrated to find total bits of secure key generated over one passage. For the 80th percentile passage shown here, a total of 5.7×10^4 bits of secure key could be generated with our 76 MHz system. Additionally, as seen in figure 5.7, our source and transmitter are stable enough over a satellite passage not to require active correction.

5.4.1 Timing analysis for noise reduction

To separate legitimate detections from background noise, all detections were timetagged and these timetags binned with a bin width equal to a fraction of the laser clock cycle. Then the detections from the QKD source should be tightly peaked around the laser pulse times with a width determined by the jitter (see Methods), and the background noise distributed randomly. The true signals were separated from dark counts and stray light by choosing an optimal window width around the peaks, which narrows with increasing loss as more background counts must be excluded to maintain an acceptable QBER (figure 5.8). Therefore only timetags within the window contribute to the final key calculations, and those outside are discarded. The optimal timing window in figure 5.8c decreases from

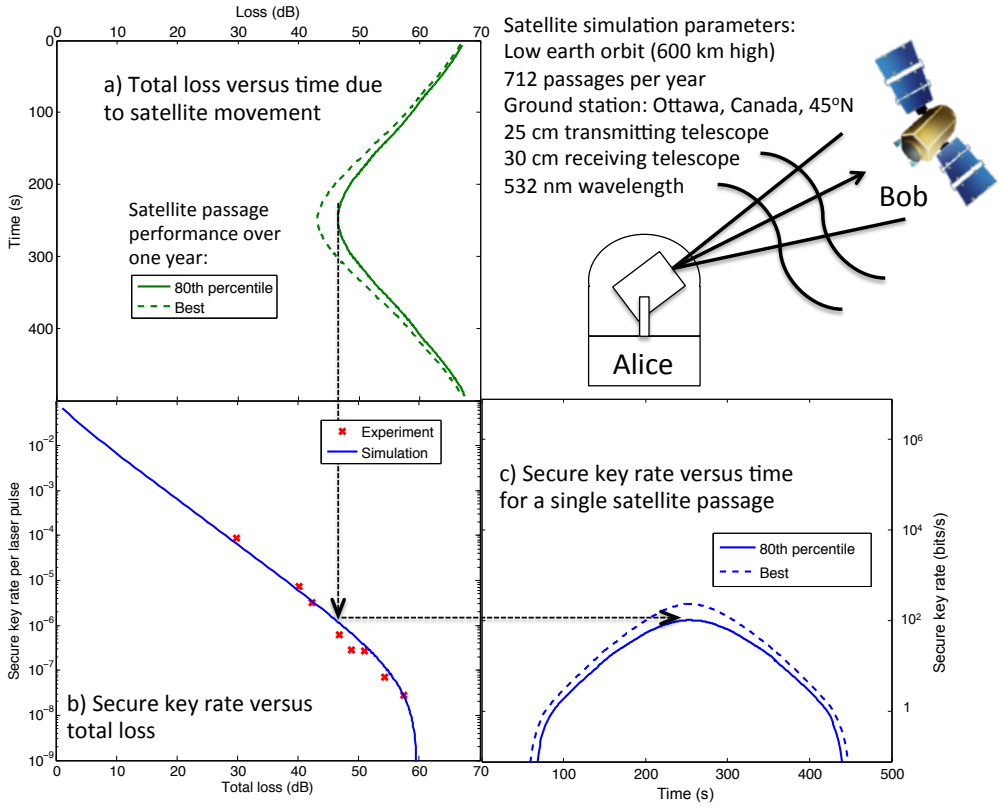

Figure 5.5: Secure key rate for a satellite passage. We calculated the trajectory of a low earth orbit satellite for one year to determine the number of passages (712) over a given ground station and the loss as a function of time for each one. Here we show simulation data for the best overall passage in that year and, for comparison, the 142nd best passage, i.e. 80th percentile. a) Simulation of total loss versus visible passage time for a satellite uplink. The loss is minimum as the satellite is closest to the ground station (highest elevation angle) and increases as the satellite approaches the horizon. b) Experimental results and simulation of secure key rate versus loss. Our data agree well with the theoretical curve, which uses a quantum optical simulation to predict key rates. Treatment of error analysis is included in QKD security proofs, and is generally based on upper bounding the information given to an eavesdropper compatible with measurement results. c) Expected secure key rate versus time for a satellite passage, based on simulations and experimental parameters. The secure key rate in bits/s on the right axis assumes the 76 MHz clock rate of our source. The loss versus time and secure key rate versus loss curves combine to produce the output key rate over one satellite passage.

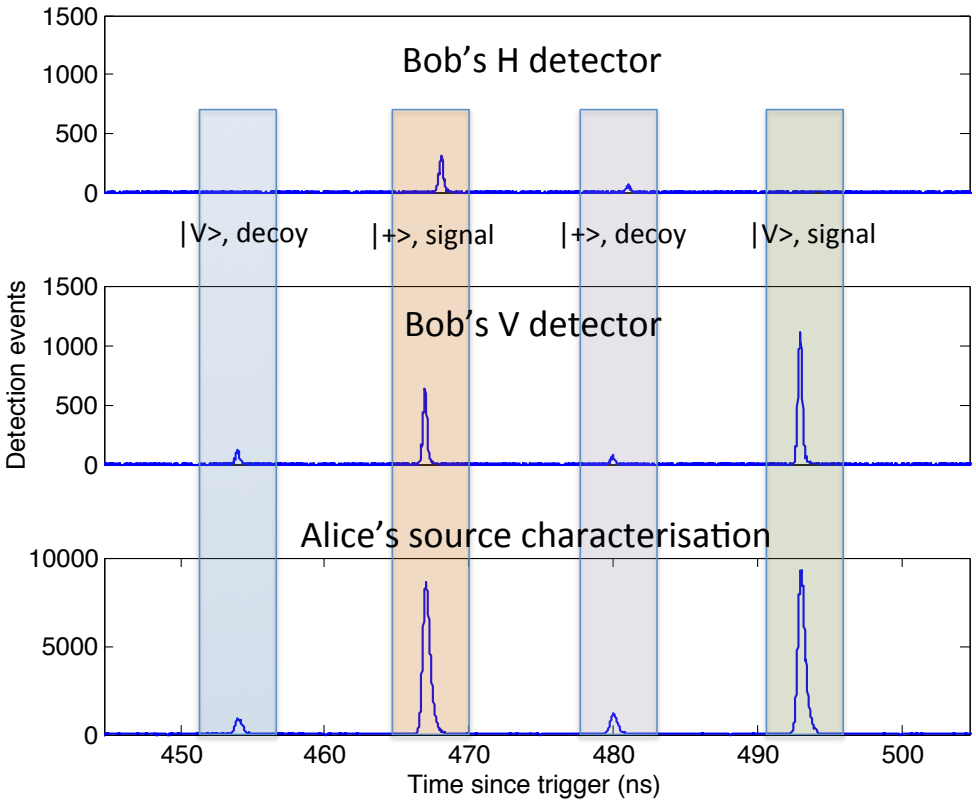

Figure 5.6: Detection histograms for Alice and Bob, showing polarisation (qubit) and amplitude (signal/decoy) modulation. The histograms are constructed by binning together detections versus the time after Alice's laser trigger. Bob's detections are the top two plots, with Alice's source characterisation on the bottom. Alice and Bob's intensities correspond to each other, as the output is randomly modulated between signal and decoy pulses. Bob also sees polarisation modulation; the first and last pulses are vertically polarised, while the middle two are diagonal. Alice monitors her source locally to ensure she is sending the correct average photon number for signal and decoy pulses.

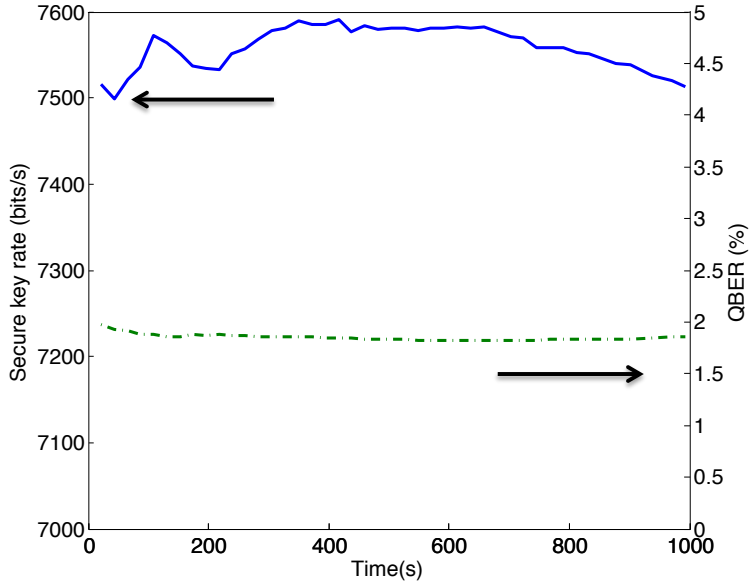

Figure 5.7: Stability of secure key rate (solid line) and QBER (dashed line). Data were taken at 30 dB total loss over 1000 s, and the mean secure key rate and QBER are 7560 ± 24 bits/s and $1.85 \pm 0.03\%$ respectively. The small drifts are likely due to temperature fluctuations which alter the polarisation transformation the in connecting optical fibres.

2 ns at low loss, to 40 ps at 57 dB, making full use of the good timing afforded by our system.

5.4.2 Finite size effects

Until this point, all discussion of QKD has assumed an infinite key length, allowing exact estimation of QBER and signal/decoy gains. In implementations this is of course not the case, and the finite size of the raw key plays an important role in how much privacy amplification must be performed [99], especially in the case of short satellite passages. Here I will therefore consider statistical fluctuations [108] of the measured parameters $Q_{\mu/\nu}$ and $E_{\mu/\nu}$, as well as information theoretic security definitions based on the deviation of the final key from a perfect key [91].

Specifically, for statistical fluctuations, 10 standard deviations are added to or subtracted from 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, a parameter Δ is added that is the outcome of information theoretic security proofs based on smooth min-entropy [99].

$$\Delta = 2\log_2\left[\frac{1}{2(\epsilon-\overline{\epsilon}-\epsilon_{EC})}\right] + 7\sqrt{N_\mu \log_2\left[\frac{2}{\overline{\epsilon}-\overline{\epsilon}'}\right]} \tag{5.17}$$

Where ϵ is the total allowable probability that the final key is insecure, chosen to be $\epsilon = 10^{-6}$ due to the finite lifetime of a satellite, $\epsilon_{EC} = 10^{-10}$ is the error correction failure probability, and $\overline{\epsilon}$ and $\overline{\epsilon}'$ can be optimised numerically with the constraint $\epsilon - \epsilon_{EC} > \overline{\epsilon} > \overline{\epsilon}' \geq 0$. The final key rate with finite size effects is then

$$R \geq q\frac{N_\mu}{N_\mu + N_\nu}\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1\left[1 - H_2(e_1)\right] - Q_\mu\Delta/N_\mu\}, \tag{5.18}$$

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 experimental runs, a secure key rate R can be calculated versus total loss for each loss setting in Figure 5.5. This is plotted in Figure 5.9, with the asymptotic experimental results for comparison. A secure key is still possible with our system including all finite size effects up to 48 dB average total loss over an assumed 300 s satellite passage, which would require larger telescopes or more efficient detectors to be feasible. However, the source rate of our system could be easily increased, requiring only a mode-locked laser with shorter cavity length and possibly faster electronics to drive the modulators. Given an achievable 1 GHz clock rate, Figure 5.10 shows an average total loss up to 55 dB is feasible over a 300 s passage, giving hope for a truly secure satellite uplink. Additionally,

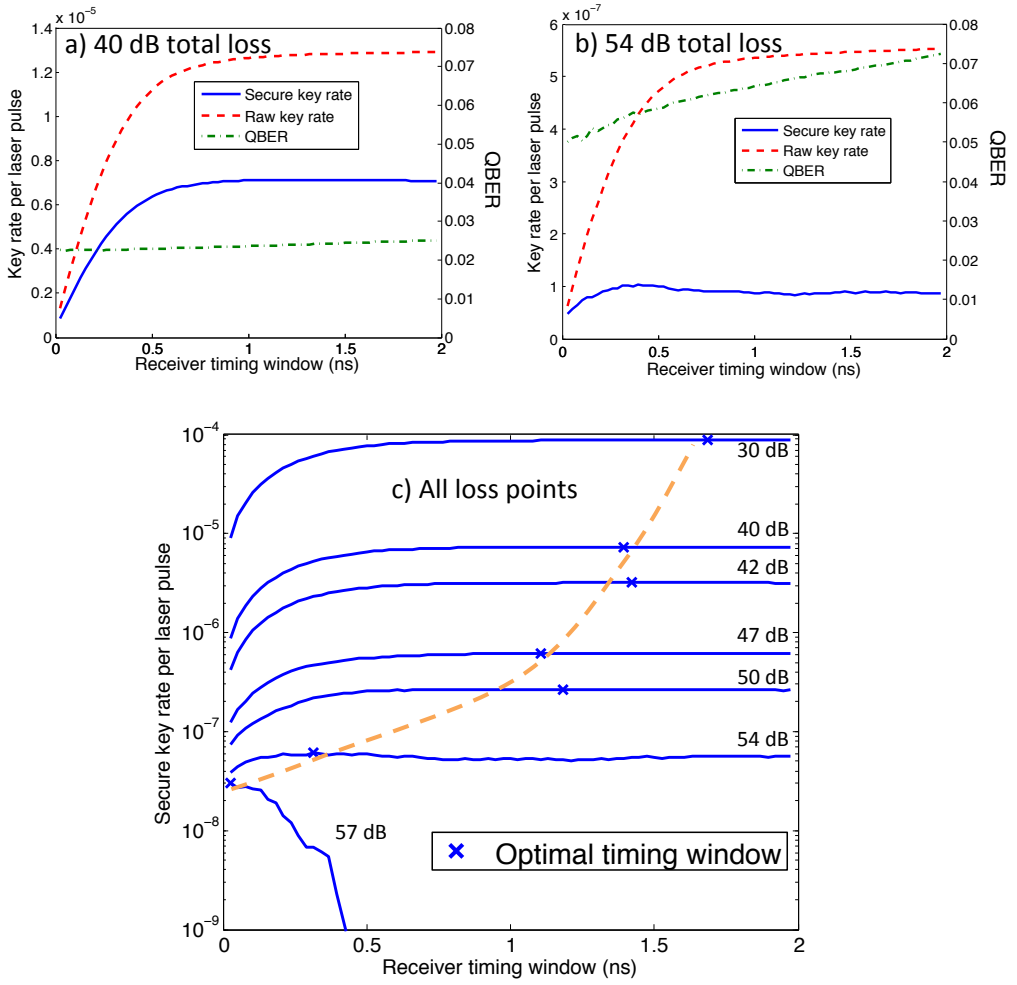

Figure 5.8: Raw key rate (all signal detection events), secure key rate, and QBER versus timing window from experimental data. a) At 40 dB total loss, b) At 54 dB total loss. Note that raw key rate and QBER both increase with timing window, as more dark and background counts are admitted. Secure key rate shows a maximum at 1.2 ns timing window for the 40 dB case and 0.4 ns for the 54 dB case, as the benefit of increasing the raw key rate is offset by the detriment of increasing the QBER. c) Secure key rate versus timing window for various loss points. The observed optimal timing window is marked on each curve with an X, and the dashed line is a guide to the eye for the optimal window width trend.

recent work on the finite key problem for qubits [114] should allow channel losses to be extended further (once optical modes are considered), making a larger number of yearly satellite passages usable for QKD.

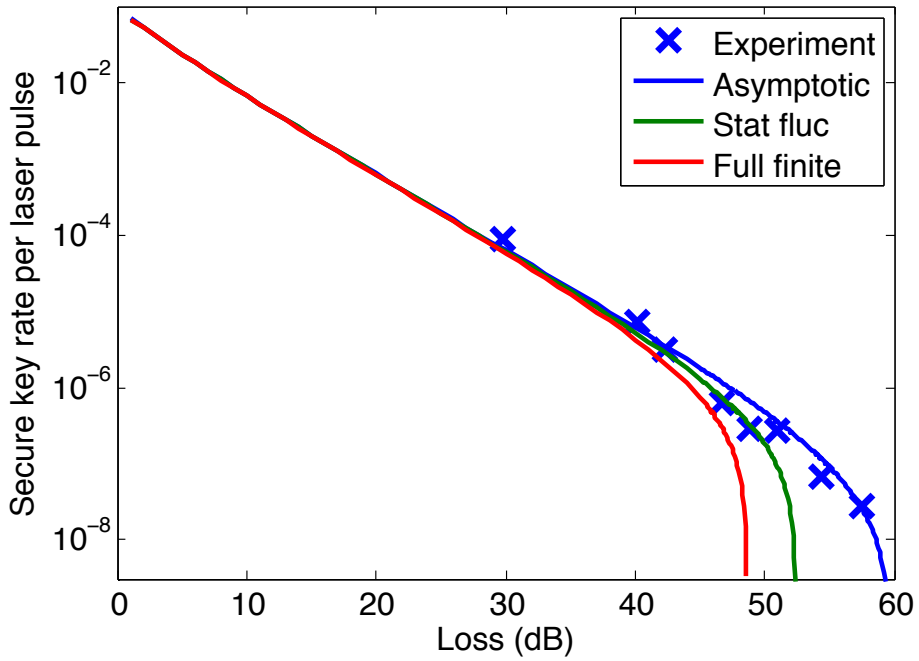

Figure 5.9: Finite size effects on secure key rate. The asymptotic curve assumes an infinite number of signals is received, while the others assume the number received over a 300 s satellite passage with average total loss given by the x-axis "Loss". "Stat fluc" includes only statistical fluctuation of parameters, while "Full finite" includes also Δ from information theoretic security proofs [99].

5.5 Discussion

We have demonstrated the design and viability of a QKD system capable of operation under ultra-high channel losses of up to 57 dB. Our system therefore satisfies the challenging requirements for uplink of quantum keys to a satellite, and future improvements will allow the technical requirements to be satisfied with full information theoretic security. As noted above, a space-based quantum receiver is less demanding than a quantum source, as all required components for the receiver have flown in space [85], so a near-term satellite mission using our approach as a prototype is immediately viable.

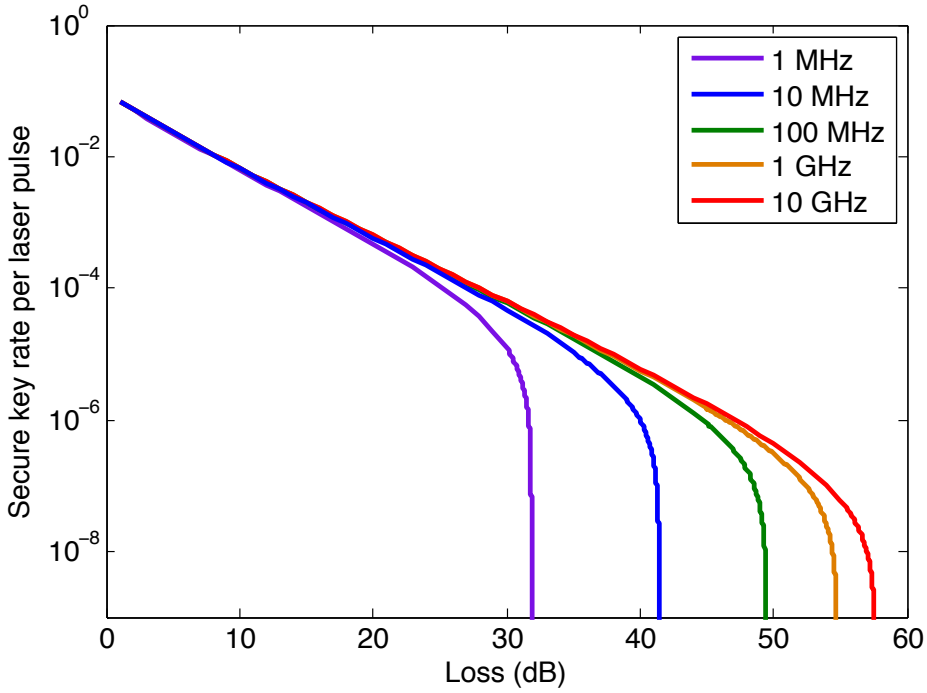

Figure 5.10: Finite size effects for various source repetition rates. Every curve here includes all finite size effects for a 300 s satellite pass with average total loss given by the x-axis "Loss". The benefit of increasing the source rate diminishes as the asymptotic limit is reached, but with a 1 GHz source, QKD is possible out to 55 dB total loss.

5.5.1 Next steps

We are working on a full-scale QKD mission, the next steps of which include determining sufficient classical processing and communication bandwidth and designing a reference frame system to compensate for the slow rotation of the satellite [17, 61]. Additionally, how best to deal with a strongly fluctuating channel while maintaining security is an open question [11, 102], and putting tighter bounds on the finite-key problem for realistic implementations is a great challenge for theorists, to enable the use of lossier channels than ever [114, 15]. Our system must be updated to include a truly random pulse sequence on Alice's side, and a receiver on Bob's side capable of measuring in both rectilinear and diagonal bases simultaneously with passive basis choice (see Methods). To bring our system to the desired 1 GHz clock rate is not difficult, as the modulators can handle a few GHz and the up-conversion process is clock rate independent. We would simply require a mode-locked laser with shorter cavity length and updated electronics.

5.5.2 Future advances

Finally, with a quantum receiver in space and a suitable photon source, a number of additional quantum physics experiments over ground-space distance become viable, including teleportation and entanglement swapping [4], fundamental tests of quantum mechanics [35], and tests of new physical theories [87]. In addition, an entangled photon source which emits one photon around the desired 532 nm is envisaged for the future [106, 105]. This photon would be directed to the satellite while the other photon of the entangled pair would be in the telecom band around 1550 nm, suitable for long-distance transmission in optical fibres. A central ground station containing the source could be connected locally by fibres to end-users, and globally via satellite to another such ground station. Furthermore, it is possible that the uplink transmission can be enhanced by implementing wave-front corrections of the transmitted optical beam, through adaptive optics [10]. This technology is used in astronomic observation, and could be realized at the ground station even once the mission is deployed. In summary, the future for QKD using satellites is bright, the uplink is demonstrably feasible, and in the near term we expect to see multiple satellite missions for quantum information, both for fundamental science and applications.

5.6 Methods

Satellite performance simulation. Naturally, the channel loss will vary on each satellite passage as the satellite passes from horizon to horizon. QKD will be possible for only during the overhead portion of each passage as too shallow an elevation angle gives too high a channel loss. Additionally only some of the satellite passages will be viable for QKD since the degree to which the satellite passes directly over the ground station varies with each passage. Our simulations include satellite orbit statistics over one year and allow for a comprehensive calculation of loss and background noise with time. Completing the satellite and channel simulations allows a further quantum optical simulation including multiphoton statistics, detector efficiencies and dark counts.

Phase randomisation. To confirm that the coherence length of the 1550 nm continuous wave laser was short enough to ensure phase randomisation of the outgoing pulses, we used an imbalanced fibre-based Mach-Zehnder interferometer on the 1550 nm light. By increasing the length of fibre in one arm, the interference fringes at the output beamsplitter were made to disappear. At 1 m of fibre the fringes were already weak, and by 2 m of fibre they were negligible. To further confirm that the output pulses at 532 nm were not coherent, a similar fibre interferometer was constructed to measure the 532 nm up-converted coherence directly. Due to the difficulty in interfering subsequent laser pulses, the source was operated in continuous wave mode, and when 2 m of fibre was introduced to imbalance the interferometer the interference fringes dropped from 77 % visibility to 6.6 %. Therefore the coherence length of the output 532 nm light is sufficiency less than the distance between pulses (4 m) for phase randomisation, assuming that each frequency component of the source in pulsed mode is affected similarly.

Receiver basis choice. The optimal solution for this short wavelength is to use passive basis choice, wherein the incoming photon passes through a 50:50 beamsplitter and is measured in either the rectilinear or diagonal basis depending on the path randomly taken out of the beamsplitter. Because only two detectors were available for this experiment, we implemented a slow, active basis choice: a motorised rotation stage containing a half-wave plate was rotated to 0° or 22.5° to choose to measure in the rectilinear and diagonal bases respectively.

Receiver timing system. In practical QKD systems, the use of timing information is necessary to exclude illegitimate detections [20]. Our system employs free-running detectors and timetags every detection event, in contrast to gated detection schemes which only open detectors during the specified arrival time of a pulse. Both are subject to detector control attacks [73, 127, 125] with most effort being focused on gated avalanche photodiodes for telecom applications

[69]. For satellite applications, the timetagging method is preferable as it requires much less data transmission. A recent precise timing experiment [92] required every gate pulse to be sent classically in parallel to the quantum channel from Alice to Bob, a vast overhead which is impractical for space applications, due to both fast and slow changes in optical path length. By contrast, using the timetagging approach, Bob can send back to Alice only the timetags generated by his receiver, which will be small in number due to the high channel loss. Alice can then align them to her source rate and tell Bob which to keep. As an example, with a clock rate of 1 GHz Alice would have to send 10^9 gate pulses per second independent of the loss for gated operation, while if using timetags, Bob would have to transmit only about 5000 timetags per second back to Alice for 50 dB total loss.

Jitter analysis. The final jitter of Alice's mode-locked laser timetags is about 300 ps. Given the 156 ps resolution of the timetagger, and jitter of Alice's electronics of 200 ps, this leaves 160 ps for jitter of the laser. Therefore, improvement is possible most easily in the laser stability and timetag resolution, making this timing method even more appealing.

Chapter 6

Conclusion

The projects of this thesis aimed at first estimating experimental parameters through simulation and consequently developing and implementing quantum communication in regimes so far untested. The two main experimental results were:

1. An implementation of entangled quantum key distribution using short-wavelength photons over standard telecom optical fibres.

2. A demonstration of the feasibility of quantum key distribution at high loss, towards a satellite uplink.

For the QKD in fibres, this work could lead to an entanglement server model, where a central facility (e.g. on a campus or office park) houses an entangled photon source connected by optical fibres to nearby buildings. The entangled source can be untrusted, and provides pairs of photons to two users who want to communicate securely. Only existing optical fibres are required, as the photons for QKD are compatible with classical traffic. This contribution to local area QKD would allow short range, highly secure networks with lower initial investment than dedicated quantum links. Entanglement distribution may also have some application in distributed quantum computing, or as a quantum bus between computing nodes or experiments.

The demonstration of QKD towards a satellite uplink, by contrast, is an important step forward for global QKD. This would allow key distribution without distance limitation using satellites as trusted nodes. As this demonstration of QKD provided full qubit and decoy-state modulation over an extremely lossy channel, it shows that current technology with novel implementations hold promise for increasing the range and key rates of QKD. Our next plans are to implement in the lab and outside a full QKD protocol as would be seen with a satellite, including

error correction and privacy amplification, automatic polarization compensation for satellite rotation, and a method to deal with the strongly fluctuating link loss. This should move the world ever closer to its first quantum satellite mission, whether an uplink based on our work, or a downlink or entangled double-downlink. Any of these technologies is capable of demonstrating QKD on a global scale, and would likely spark widespread commercial and government interest.

Bibliography

The numbers at the end of each entry list pages where the reference was cited. In the electronic version, they are clickable links to the pages.

[1] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. SECOQC white paper on quantum key distribution and cryptography, 2007. 66

[2] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus. Topological optimization of quantum key distribution networks. *New Journal of Physics*, 11(7):075002, 2009. 20

[3] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804–1807, Dec 1982. 23, 24

[4] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551, Nov.-Dec. 2003. 21, 85

[5] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964. 3

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992. 10.1007/BF00191318. 10

[7] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems & Signal Processing*, 1984. 4, 10, 65

[8] 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, Mar 1993. 1, 25, 31

[9] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5), 02 1992. 7, 10, 13, 21, 48

[10] T. Berkefeld, D. Soltau, R. Czichy, E. Fischer, B. Wandernoth, and Z. Sodnik. Adaptive optics for satellite-to-ground laser communication at the 1m telescope of the esa optical ground station, tenerife, spain. In B. L. Ellerbroek, M. Hart, N. Hubin, and P. L. Wizinowich, editors, *Adaptive Optics Systems II*, volume 7736, page 77364C. SPIE, 2010. 85

[11] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017 (25pp), 2009. 21, 65, 66, 85

[12] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 80(6):1121–1125, Feb 1998. 29

[13] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 12 1997. 25, 48

[14] R. Boyd. *Nonlinear Optics, Third Edition*. Academic Press, 2008. 71

[15] S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß. Min-entropy and quantum key distribution: Nonzero key rates for "small" numbers of signals. *Phys. Rev. A*, 83(2):022330, Feb 2011. 85

[16] 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, Apr 1998. 29

[17] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng. Stable quantum key distribution with active polarization control based on time-division multiplexing. *New Journal of Physics*, 11(6):065004 (13pp), 2009. 85

[18] C.-W. Chou, J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto, and H. J. Kimble. Functional quantum nodes for entanglement distribution

over scalable quantum networks. *Science*, 316(5829):1316–1320, 2007. 20

[19] 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, Oct 1969. 29

[20] R. J. Collins, R. H. Hadfield, V. Fernandez, S. W. Nam, and G. S. Buller. Low timing jitter detector for gigahertz quantum key distribution. *Electronics Letters*, 43(3):180–181, Feb. 1 2007. 63, 86

[21] D. Dieks. Communication by EPR devices. *Physics Letters A*, 92(6):271–272, 11 1982. 2, 4, 16

[22] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express*, 16(23):18790–18979, 2008. 10, 17

[23] 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. *Applied Physics Letters*, 96(16):161102, 2010. 10

[24] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413–418, 11 2001. 18

[25] J. F. Dynes, H. Takesue, Z. L. Yuan, A. W. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, and A. J. Shields. Efficient entanglement distribution over 200 kilometers. *Opt. Express*, 17(14):11440–11449, 2009. 10

[26] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935. 3

[27] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, Aug 1991. 7, 10

[28] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. Current status of the DARPA Quantum Network. *arXiv:quant-ph/0503058*, Mar. 2005. 13, 14

[29] C. Erven, C. Couteau, R. Laflamme, and G. Weihs. Entangled quantum key distribution over two free-space optical links. *Opt. Express*, 16(21):16840–16853, 10 2008. 10, 48

[30] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden. Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods. *Eur. Phys. J. D*, 30(1):143–148, jul 2004. 18, 65

[31] J. D. Franson and H. Ilves. Quantum cryptography using optical fibers. *Appl. Opt.*, 33(14):2949–2954, May 1994. 10

[32] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Perfect eavesdropping on a quantum cryptography system. *arXiv:1011.0105*, Oct. 2010. 11

[33] N. Gisin. Today's and tomorrow's challenges for quantum communication. In *Updating quantum cryptography and communications*, 2010. 65

[34] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002. 1, 4, 48, 65

[35] N. Gisin, V. Scarani, W. Tittel, and H. Zbinden. Optical tests of quantum nonlocality: from EPR-Bell tests towards experiments with moving observers. *Annalen der Physik*, 9(11-12):831–841, 2000. 85

[36] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004. 10

[37] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller. A short wavelength gigahertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics*, 40:900, 2004. 10

[38] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4:325–360, 2004. 18, 39, 41

[39] D. M. Greenberger, M. A. Horne, A. Zeilinger, and M. Kafatos (Ed.). Bell's theorem, quantum theory, and conceptions of the universe. *arXiv:0712.0921*, pages 69–72, 1989. 30

[40] R. H. Hadfield. Single-photon detectors for optical quantum information applications. *Nat Photon*, 3(12):696–705, 12 2009. 66, 67

[41] K. Hammerer, A. S. Sørensen, and E. S. Polzik. Quantum interface between light and atomic ensembles. *Rev. Mod. Phys.*, 82(2):1041–1093, Apr 2010. 18

[42] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik A Hadrons and Nuclei*, 43(3):172–198, 1927. 4

[43] C. K. Hong and L. Mandel. Theory of parametric frequency down conversion of light. *Phys. Rev. A*, 31(4):2409–2418, Apr 1985. 51

[44] H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger. High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber. *Opt. Express*, 15(12):7853–7862, 2007. 48, 56, 67

[45] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Free-space quantum key distribution in daylight. *Journal of Modern Optics*, 47(2/3):549–562, 2000. 10, 21

[46] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4(1):43, 2002. 10, 21

[47] D. S. Hum and M. M. Fejer. Quasi-phasematching. *Comptes Rendus Physique*, 8(2):180–198, 3 2007. 51, 73

[48] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, Aug 2003. 6

[49] IDQ. Cerberis layer 2 link encryption with quantum key distribution. http://www.idquantique.com/images/stories/PDF/cerberis-encryptor/cerberis-specs.pdf. 11

[50] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. 'Event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, Dec 1993. 18

[51] T. Jennewein, M. Barbieri, and A. G. White. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis. *Journal of Modern Optics*, 58(3):276–287, 2011. 27, 29, 105

[52] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84(20):4729–4732, May 2000. 10

[53] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger. High-fidelity entanglement swapping with fully independent sources. *Phys. Rev. A*, 79(4):040302, Apr 2009. 25

[54] T. Kim, M. Fiorentino, and F. N. C. Wong. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Phys. Rev. A*, 73(1):012316, Jan 2006. 50

[55] D. N. Klyshko. Coherent photon decay in a nonlinear medium. *Soviet Journal of Experimental and Theoretical Physics Letters*, 6:23, July 1967. 50

[56] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001. 2, 48

[57] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009. 5

[58] M. A. Krainak, G. Yang, W. Lu, and X. Sun. Photon-counting detectors for space-based applications. In E. L. Dereniak, J. P. Hartke, P. D. LeVan, R. E. Longshore, A. K. Sood, M. Razeghi, and R. Sudharsanan, editors, *Detectors and Imaging Devices: Infrared, Focal Plane, Single Photon*, volume 7780, page 77801J. SPIE, 2010. 66

[59] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419(6906):450–450, 10 2002. 10, 48

[60] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard. Ultra-bright source of polarization-entangled photons. *Phys. Rev. A*, 60(2):R773–R776, Aug 1999. 51

[61] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien. Reference-frame-independent quantum key distribution. *Phys. Rev. A*, 82(1):012304, Jul 2010. 85

[62] B. Lamine, R. Hervé, M. . Jaekel, A. Lambrecht, and S. Reynaud. Large scale EPR correlations and cosmic gravitational waves. *arXiv:1105.1897*, May 2011. 24

[63] J. Lavoie, R. Kaltenbaek, and K. J. Resch. Experimental violation of Svetlichny's inequality. *New Journal of Physics*, 11(7):073051, 2009. 23, 30

[64] H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi. Distribution of polarization-entangled photon pair produced via spontaneous parametricdown-conversion within a local-area fiber network: Theoretical model and experiment. *Opt. Express*, 16:14512, 2008. 63

[65] 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. Express*, 18(8):8587–8594, Apr 2010. 10, 65, 77

[66] M. D. Lukin. Colloquium: Trapping and manipulating photon states in atomic ensembles. *Rev. Mod. Phys.*, 75(2):457–472, Apr 2003. 18

[67] N. Lutkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44, 2002. 6, 74

[68] L. Lydersen, V. Makarov, and J. Skaar. Secure gated detection scheme for quantum cryptography. *Phys. Rev. A*, 83(3):032306, Mar 2011. 11

[69] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4(10):686–689, 10 2010. 11, 87

[70] X. Ma, C.-H. F. Fung, and H.-K. Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, 76(1):012307, July 2007. 58, 59

[71] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72(1):012326, Jul 2005. 6, 66, 74, 76

[72] MagiQ. MAGIQ QPN 8505 Security Gateway. http://magiqtech.com/MagiQ/Products_files/8505_Data_Sheet.pdf. 11

[73] V. Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):065003, 2009. 11, 86

[74] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology —CRYPTO '96*, volume 1109, pages 343–357. Springer Berlin / Heidelberg, 1996. 5

[75] N. D. Mermin. Quantum mechanics vs local realism near the classical limit: A bell inequality for spin *s*. *Phys. Rev. D*, 22(2):356–361, Jul 1980. 29

[76] E.-L. Miao, Z.-F. Han, T. Zhang, and G.-C. Guo. The feasibility of geostationary satellite-to-ground quantum key distribution. *Physics Letters A*, 361(1-2):29–32, 2007. 21

[77] L. Moli-Sánchez, A. Rodríguez-Alonso, and G. Seco-Granados. Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links. *IEEE J.Sel. A. Commun.*, 27(9):1582–1590, 2009. 21

[78] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 2

[79] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009. 13, 14

[80] A. Peres and D. R. Terno. Quantum information and relativity theory. *Rev. Mod. Phys.*, 76(1):93, Jan 2004. 24

[81] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi. Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of Physics*, 11(4):045012, 2009. 13

[82] M. Pfennigbauer, W. R. Leeb, M. Aspelmeyer, T. Jennewein, and A. Zeilinger. Free-space optical quantum key distribution using intersatellite links. In *Proceedings of the CNES - Intersatellite Link Workshop*, 2003. 21

[83] S. Popescu. Bell's inequalities versus teleportation: What is nonlocality? *Phys. Rev. Lett.*, 72(6):797–799, Feb 1994. 29

[84] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and

A. Zeilinger. Practical quantum key distribution with polarization entangled photons. *Opt. Express*, 12(16):3865–3871, 2004. 10, 48

[85] I. Prochazka and F. Yang. Photon counting module for laser time transfer via earth orbiting satellite. *Journal of Modern Optics*, 56(2):253–260, 2009. 83

[86] Quintessence Labs. Quintessence Labs Breakthrough Technology. http://www.quintessencelabs.com/application-areas.php. 11

[87] T. C. Ralph, G. J. Milburn, and T. Downes. Quantum connectivity of space-time and gravitationally induced de-correlation of entanglement. *Physical Review A*, 79:022121, 2009. 24, 85

[88] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics*, 4(1):82, 2002. 21

[89] M. Razavi, M. Piani, and N. Lütkenhaus. Quantum repeaters with imperfect memories: Cost and scalability. *Phys. Rev. A*, 80(3):032301, Sep 2009. 20

[90] I. Rech, G. Luo, M. Ghioni, H. Yang, X. S. Xie, and S. Cova. Photon-timing detector module for single-molecule spectroscopy with 60-ps resolution. *Selected Topics in Quantum Electronics, IEEE Journal of*, 10(4):788–795, July-Aug. 2004. 67

[91] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332, Jul 2005. 5, 81

[92] A. Restelli, J. C. Bienfang, C. W. Clark, I. Rech, I. Labanca, M. Ghioni, and S. Cova. Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate. *Selected Topics in Quantum Electronics, IEEE Journal of*, 16(5):1084–1090, Sept.-Oct. 2010. 87

[93] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21:120–126, February 1978. 4

[94] M. Safari and M. Uysal. Relay-assisted quantum-key distribution over long atmospheric channels. *Lightwave Technology, Journal of*, 27(20):4508–4515, Oct.15, 2009. 21

[95] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics, Ch. 9*. Wiley, 2 edition, 2007. 52, 127, 132

[96] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, 01 2010. 20

[97] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83(1):33–80, Mar 2011. 19, 20

[98] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, 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. Legre, S. Robyr, P. Trinkler, L. Monat, J. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the Tokyo QKD Network. *arXiv:1103.3566*, Mar. 2011. 9, 13, 14, 15

[99] 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, May 2008. 81, 83

[100] 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 300 km quantum key distribution with entangled states. *New Journal of Physics*, 11(8):085002 (13pp), 2009. 10, 16, 23, 63

[101] 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, Jan 2007. 10, 16, 23, 65

[102] A. A. Semenov and W. Vogel. Entanglement transfer through the turbulent atmosphere. *Phys. Rev. A*, 81(2):023835, Feb 2010. 85

[103] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999. 1

[104] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, Jul 2000. 5

[105] C. Söller, B. Brecht, P. J. Mosley, L. Y. Zang, A. Podlipensky, N. Y. Joly, P. S. J. Russell, and C. Silberhorn. Bridging visible and telecom wavelengths with a single-mode broadband photon pair source. *Phys. Rev. A*, 81(3):031801, Mar 2010. 85

[106] S. M. Spillane, M. Fiorentino, and R. G. Beausoleil. Spontaneous parametric down conversion in a nanophotonic waveguide. *Opt. Express*, 15(14):8770–8780, 07 2007. 85

[107] 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 Journal of Physics*, 11(7):075003, 2009. 10, 16, 65, 77

[108] S.-H. Sun, L.-M. Liang, and C.-Z. Li. Decoy state quantum key distribution with finite resources. *Physics Letters A*, 373(30):2533–2536, 7 2009. 66, 81

[109] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35(10):3066–3069, May 1987. 29, 30

[110] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nat Photon*, 1(6):343–348, 06 2007. 65, 77

[111] S. M. Tan. A computational toolbox for quantum and atomic optics. *Journal of Optics B: Quantum and Semiclassical Optics*, 1(4):424, 1999. 27, 105

[112] S. G. I. Taylor. Interference fringes with feeble light. *Proc. Cam. phil. Soc*, 15(114), 1909. 23

[113] S. Ten and H. Xenos. Nortel long-haul transmission gear and corning ultra-low-loss fiber entable longer span and longer reach network designs. White Paper, 2007. 16

[114] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. *arXiv:1103.4130*, Mar. 2011. 83, 85

[115] P. D. Townsend. Secure key distribution system based on quantum cryptography. *Electronics Letters*, 30(10):809–811, 12 May 1994. 10

[116] P. D. Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electronics Letters*, 33(3):188–190, 1997. 13

[117] P. D. Townsend. Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems. *Photonics Technology Letters, IEEE*, 10(7):1048–1050, 1998. 54

[118] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger. Communications: Quantum teleportation across the danube. *Nature*, 430(7002):849–849, 08 2004. 25

[119] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, 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, 2007. 48

[120] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nat Phys*, 3(7):481–486, 07 2007. 16, 65

[121] A. Vakhitov, V. Makarov, and D. R. Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038, 2001. 11

[122] A. P. Vandevender and P. G. Kwiat. High efficiency single photon detection via frequency up-conversion. *Journal of Modern Optics*, 51(9):1433–1445, 2004. 73

[123] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J Amer Inst Elect Eng*, 45(55):109–115, 1926. 4

[124] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and earth. *New Journal of Physics*, 10(3):033038 (12pp), 2008. 21, 23

[125] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter. Quantum Eavesdropping without Interception: An Attack Exploiting the Dead Time of Single Photon Detectors. *arXiv:1101.5289*, Jan. 2011. 86

[126] 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, Dec 1998. 23

[127] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043, 2011. 11, 86

[128] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 10 1982. 2, 4, 16

[129] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan. Experimental demonstration of a BDCZ quantum repeater node. *Nature*, 454(7208):1098–1101, 08 2008. 20, 48

[130] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto. Megabits secure key rate quantum key distribution. *New Journal of Physics*, 11(4):045010, 2009. 10

[131] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78(4):042333, Oct 2008. 11

Appendix A

Code for specific quantum optics simulations

Sze Tan's quantum computational toolbox [111] is available as of this date at http://qwiki.stanford.edu/index.php/Quantum_Optics_Toolbox, and Thomas Jennewein's additional functions [51] are available at http://info.iqc.ca/qpl/lab-tools/. An important function to note is `display_state4`, which displays the simulated photon states in a nice format.

A.1 MATLAB code for Svetlichny inequality violation

```
% Evan Meyer-Scott for GHZ Project March 10, 2011, ...
   modification of
% Thomas Jennewein, 8.10.2008

% This script simulates a double down-conversion source of ...
   four-photon states with one as a trigger to produce ...
   three-photon GHZ states. These states are subjected to ...
   loss and detector noise then used to violate Svetlichny's ...
   inequality.

clear

%% Initializations - vary these parameters to check performance
% Definitions for qotoolbox
N=3; %Fock space dimension
% Sets up standard quantum optics functions
standard_defintions_qo_toolbox_evan;
```

```
% Make a couple changes from the standard definitions to get ...
    phases right
H_ph_i = a'*a.*-pi/2;
U_ph_i = expm(-1i*H_ph_i);
U_had=tensor(ida,U_ph_i)*U_bs*tensor(ida,U_ph_i);

% This 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 coincidenc window for ...
    simplification
coinc_window=3e-9;
% f_source is then an effective source repetition rate
f_source=1/coinc_window;


% Source rate estimation, based on the observed singles and ...
    coincidences
coinc=19333; % Two-photon coincidence rate from ...
    down-conversion source
singles=400000; % Single count rate per second for ...
    down-conversion source
net_source_rate=singles^2/coinc; % Source rate in crystal
epsilon=sqrt(net_source_rate/f_source); % Squeezing parameter


% Integration time for uncertainty reduction
time=logspace(2,6);

%Link efficiencies
effc_source=coinc/singles; % Includes photon collection and ...
    detectors
link1=[.1 .2 .3 .4 .5]; % Efficiency of free space links, ...
    photons 1&3
link3=link1;
% Add 500 m fibre for delay of photon 2, at 3dB/km
link2=10^-.15;
% Efficiency of receiving optics/Pockels cell
effc_optics=.6;

%Include noise from darks counts and background light over ...
    freespace link
darks=600;
background=4000;
noise_factor_link=(darks+background)*coinc_window; % Noise ...
    over link
noise_factor_local=background*coinc_window; % Noise for ...
    locally detected photons
```

```
%% Create entangled state |HHV>+|VVH> (requires post selection)

% The photons are as follows: 1 & 3 are from independent ...
   down-conversions and are the ones interfered to create ...
   entanglement then sent over the links, 1 & 2 are an ...
   entangled pair from down-conversion and 3 & Trig are a ...
   correlated pair, with Trig being the trigger photon

%Use down-conversion
H_chi2=(tensor(a,a)+tensor(a',a'))*epsilon; % Hamiltonian
U_chi2=expm(-1i*H_chi2); % Unitary

% Act unitary on vacuum to create pair state |HH>
spdc_state=tensor(U_chi2*tensor(vacc,vacc));

% Permute to create entangled state, photons 1 & 2 |HH>+|VV>
% Modes here are |Q1H, Q1V, Q2H, Q2V>
phi_plus=permute(tensor(spdc_state,spdc_state),[1 4 2 3]);


% Create pair, photons 3 & Trig |HH>
% The modes here are: |TrigH, TrigV, Q3H, Q3V>
% Permute to separate Trig and 3
HH=permute(tensor(spdc_state,vacc,vacc),[1 4 2 3]);

%Rotate Q3 to 45deg before interference with Q1
HH=tensor(ida,ida,U_had)*HH;

%Polarization beamsplitter between Q1 and Q3 with permute
psi=permute(tensor(phi_plus,HH),[7,2,3,4,5,6,1,8]);


%Swap H&V in Q3 to make desired (|HHV>+|VVH>)⊗|Trig>
psi=permute(psi,[1,2,3,4,5,6,8,7]);


%% Looping and detection
% Loop over integration time and free space link transmission
for n=1:length(time)

    for m=1:length(link1)


        % Create projector for bucket detector for each photon
        [proj{1},unproj{1}]=BucketDetector_noise(N,effc_source...
                *link1(m)*effc_optics,noise_factor_link);
        [proj{2},unproj{2}]=BucketDetector_noise(N,effc_source...
```

```
        *link2*effc_optics,noise_factor_local);
[proj{3},unproj{3}]=BucketDetector_noise(N,effc_source...
        *link3(m)*effc_optics,noise_factor_link);
[proj{4},unproj{4}]=BucketDetector_noise(N,effc_source,...
        noise_factor_link);


% Svetlichny's ineqaulity
% Perform heralded 3-fold measurements and return ...
   E(a,b,c), for each of two analyser settings phi
phi_a=[3*pi/4 pi/4];
phi_b=[pi/2 0];
phi_c=[0 pi/2];

% E_Svetlichny returns the correlation value ...
   E(a,b,c) for a given set of
% measurement angles (\phi_a,\phi_b,\phi_c), and the ...
   uncertainty
% in this value
% Multiply source rate by time/8 since 8 measurement ...
   settings
[E(1),deltaE(1)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(1),phi_b(1),phi_c(1),f_source*time(n)/8);
[E(2),deltaE(2)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(1),phi_b(1),phi_c(2),f_source*time(n)/8);
[E(3),deltaE(3)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(1),phi_b(2),phi_c(1),f_source*time(n)/8);
[E(4),deltaE(4)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(1),phi_b(2),phi_c(2),f_source*time(n)/8);
[E(5),deltaE(5)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(2),phi_b(1),phi_c(1),f_source*time(n)/8);
[E(6),deltaE(6)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(2),phi_b(1),phi_c(2),f_source*time(n)/8);
[E(7),deltaE(7)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(2),phi_b(2),phi_c(1),f_source*time(n)/8);
[E(8),deltaE(8)]=E_Svetlichny(N,psi,proj,unproj,...
        phi_a(2),phi_b(2),phi_c(2),f_source*time(n)/8);

% Rate_Svetlichny simply returns the sum of all ...
   measurement
% outcomes, giving a total fourfold detection rate.
rate=Rate_Svetlichny(N,psi,proj,unproj);

% Now extract useful information:

% Fourfold count rate per second
counts(m)=rate*f_source;

% Entanglement visibility and fidelity
```

```
        vis=Vis_Svetlichny(N,psi,proj,unproj);
        fidelity(m)=vis/2+1/2;

        % Svetlichny parameter and uncertainty
        Sv(n,m)=abs(sum(E([1 2 3 5]))-sum(E([4 6 7 8])));
        deltaSv(n,m)=sqrt(sum(deltaE.^2));

        % Number of sigmas violation of the classical limit ...
           of 4
        sigmas=(Sv-4)./deltaSv;

    end

end

%% Plot results

% One useful plot is that of sigmas of violation versus ...
   time, to find out
% how long to integrate for a violation of, say, three ...
   standard deviations
semilogx(time/3600,sigmas,'.-')
xlabel('Time (h)')
ylabel('# of Sigmas violation')
title('# of Sigmas Svetlichny Violation versus Integration ...
   Time')


%% Required functions


function [probs, deltaE]=E_Svetlichny(N, ...
   in,proj,unproj,phi_a,phi_b,phi_c,f_source)
% Determine the four-fold count rates for an 8 mode state, ...
   e.g. |Q1H,Q1V,Q2H,Q2V,TrigH,TrigV,Q3H,Q3V>, measured ...
   along |H> +/- exp(i phi_j)|V> for j = a,b,c


standard_defintions_qo_toolbox;
H_ph_i = a'*a.*-pi/2;
U_ph_i = expm(-1i*H_ph_i);
U_had=tensor(ida,U_ph_i)*U_bs*tensor(ida,U_ph_i);
% Set the phase of the measurement
Hrot_a=a'*a*phi_a;
Urot_a=expm(-1i*Hrot_a);

Hrot_b=a'*a*phi_b;
Urot_b=expm(-1i*Hrot_b);
```

```
Hrot_c=a'*a*phi_c;
Urot_c=expm(-1i*Hrot_c);

% Outcome: mode1-> +1(good) mode2-> -1(bad)

%Apply phase shift to each mode2, then hadamard between each 1&2
final_state=tensor(U_had,U_had,ida,ida,U_had)...
*tensor(ida,Urot_a,ida,Urot_b,ida,ida,ida,Urot_c)*in;

% Expectation value to get probability of detection
HHH=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HHV=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
HVH=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HVV=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VVV=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VVH=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
VHV=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VHH=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));
good=real(HHH+HVV+VVH+VHV);
bad=real(HHV+HVH+VVV+VHH);

probs=(good-bad)/(good+bad);
deltaE=2/(good+bad)*sqrt((1-probs)^2*good+(1+probs)^2*bad);
end

function rate=Rate_Svetlichny(N,in,proj,unproj)

ida=identity(N);
final_state=in;


HHH=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HHV=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
HVH=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HVV=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VVV=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
```

```
VVH=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
VHV=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VHH=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));

rate=real(HHH+HHV+HVH+HVV+VVV+VVH+VHV+VHH);


end



function vis=Vis_Svetlichny(N,in,proj,unproj)

ida=identity(N);
final_state=in;


HHH=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HHV=f_source*sum(expect(tensor(proj{1},unproj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
HVH=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
HVV=f_source*sum(expect(tensor(proj{1},unproj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VVV=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VVH=f_source*sum(expect(tensor(unproj{1},proj{1},unproj{2},...
    proj{2},proj{4},ida,proj{3},unproj{3}),final_state));
VHV=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,unproj{3},proj{3}),final_state));
VHH=f_source*sum(expect(tensor(unproj{1},proj{1},proj{2},...
    unproj{2},proj{4},ida,proj{3},unproj{3}),final_state));

vis=real((HHV+VVH-HHH-HVH-HVV-VVV-VHV-VHH)...
    /(HHH+HHV+HVH+HVV+VVV+VVH+VHV+VHH));

end
```

A.2 MATLAB code for teleportation simulation

```
function [counts vis Vp]=Teleportation_thesis(loss,time,darks)
% Evan Meyer-Scott 23 Septermber 2010,
% Modification of Thomas Jennewein 2008
```

```
% This function takes the inputs loss (channel loss in dB), ...
   measurement time (in seconds) and darks (dark count rate ...
   per second in each detector) and simulations a ...
   teleportation experiment, where two photons are ...
   interfered locally and the third photon onto which the ...
   initial state is teleported is sent over long distance, ...
   e.g. to a satellite. To get plots versus time or loss, ...
   simply loop over this function with different values

%% Setup

% Definitions for qotoolbox
% Fock space dimension
N=5;
% Sets up standard quantum optics functions
standard_defintions_qo_toolbox;


% Repetition rate of entangled pair source pump laser
f_laser=1e9;


% Select type of input photon
% (0) Triggered photon from down-conversion
% (1) Coherent pulse, with strength alpha
% (2) Ideal single photon
type_input=2;


% Select type of entantlement resource
% (0) Down-conversion
% (1) Ideal entangled pair
type_entanglement=0;


% More complete Bell-state measurement? (0) No, (1) Yes
mc_bsm=1;


% Efficiencies
effc_apd=0.6; % Bucket detector efficiency
effc_optics=0.19; % Analysing optics efficiency


% Link attenuation, from decibels to fractional
effc_link=10.^(-loss/10);
```

```
% Detector noise factor: dark counts per laser pulse
noise_factor=darks/f_laser;


%Source rate estimation, based on the observed singles and ...
    coincidences
singles=1e6; % Single count rate per second for ...
    down-conversion source
coinc=1e5; % Two-photon coincidence rate frowm ...
    down-conversion source
net_source_rate=singles^2/coinc; % Source rate in crystal
epsilon=sqrt(net_source_rate/f_laser); % Squeezing parameter


%% Create modes and photons

%Create entanglment resource state
if type_entanglement==0; % Create entangled pair from ...
    down-conversion

    H_dc=(tensor(a,a)+tensor(a',a'))*epsilon; % Hamiltonian
    U_dc=expm(-1i*H_dc); % Unitary
    % Act unitary on vacuum to create pair state |HH>
    dc_state=tensor(U_dc*tensor(vacc,vacc));
    % Permute to create entangled state |HV>+|VH>
    psi=permute(tensor(dc_state,dc_state),[1 3 4 2]);


else % Create ideal entangled pair |HV>+|VH>

    ideal_state=tensor(oneph,vacc,vacc,oneph)...
        +tensor(vacc,oneph,oneph,vacc);
    psi=ideal_state;

end

% The Hilbert space will be 6 modes, 2 (H or V) for each ...
    photon, with mode 1 being the input, mode 2 being ...
    interfered with mode 1, and mode 3 being the distant mode ...
    onto which the input state is teleported.
% Therefore modes 2 and 3 are the entanglement resource.
% |H1, V1, H2, V2, H3, V3>



% Create input photon
if type_input==0 % Create heralded photon from down-conversion

    effc_hrld=0.2; % Heralding efficiency
```

```
    % Heralding bucket detector (Avalanche Photodiode, APD)
    [apd_hrld un_hrldapd]=BucketDetector_noise(N,effc_hrld...
        *effc_apd,noise_factor);

    % Epsilon for the heralded down-conversion
    epsilon_herald=0.2;

    H_herald=(tensor(a,a)+tensor(a',a'))*epsilon_herald; % ...
       Hamiltonian
    U_herald=expm(-1i*H_herald); % Unitary

    % Act unitary on vacuum to create pair state for heralding
    dc_herald=tensor(U_herald*tensor(vacc,vacc));

    num_sources=1; % An array of heralded sources can be ...
       used for better
    % efficiency, but keep at 1 for now

    % This function performs heralding and gives a ...
       conditional state in a
    % single mode
    [herald_state ...
       count_prob]=herald_source3(N,dc_hrld,num_sources,apd_hrld);

    % The total initial state is therefore
    in_state=tensor(herald_state,vacc,psi);


elseif type_input==1 % Create coherent state from weak laser
    % Coherent state "strength"; mean photon number = alpha^2
    alpha=0.3;

    U_dis=expm(alpha*(a'-a)); % Displacement operator
    cohr_state=U_dis*vacc; % Act displacement operator on vacuum

    %Total input state is therefore
    in_state=tensor(cohr_state,vacc,psi);


elseif type_input==2 % Create ideal single photon

    %Total input state is therefore
    in_state=tensor(oneph,vacc,psi);
end

% Rotate input to +45 input, or any other state to check ...
   teleportation of
% various nonorthogonal states
```

```
in_state=tensor(U_had,ida,ida,ida,ida)*in_state;

%% Measurement
%****************************************
% Apply the Bell-state measurement with a beamsplitter:
% First move the polarizations together |H1,H2,V1,V2,H3,V3>
out_state=permute(in_state,[1,3,2,4,5,6]);
% Apply bgeamsplitter to the (H1,H2) and (V1,V2) terms
out_state=tensor(U_bs,U_bs,ida,ida)*out_state;
% Permute back to |H1,V1,H2,V2,H3,V3>
out_state=permute(out_state,[1,3,2,4,5,6]);
%****************************************

% Create measurement projectors
% Long link bucket detector (Avalanche Photodiode, APD)
[apd_link ...
    un_linkapd]=BucketDetector_noise(N,effc_link*effc_optics...
     *effc_apd,noise_factor);
% Local bucket detector (Avalanche Photodiode, APD)
[apd_proj ...
    un_projapd]=BucketDetector_noise(N,effc_optics*effc_apd,...
     noise_factor);



% This function performs a simplified Bell-state measurement ...
    on modes 1 and 2 with 25% success probability and a ...
    measurement on mode 3 to return detection probabilities ...
    for the teleported state in each of the three standard ...
    bases: H/V, +/-, L/R
det_prob=real(msrmt_3qb_2ch_6mode_mc_BSM2(N,out_state,apd_proj,...
     un_projapd,apd_link,un_linkapd,mc_bsm));

% det_prob is a vector of the detection probabilities of ...
    mode 3 in the
% following states: (H, V, +, -, L, R)
% The visibility in each basis is therefore:

vis_hv=(det_prob(1)-det_prob(2))./(det_prob(1)+det_prob(2));
vis_pm=(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));

% The +/- basis is of interest, since input photon was |+>
vis=vis_pm;

% The count rate in each detector is
count_r=det_prob*f_laser;

% Which gives for a 2-detector analyser a total count rate
```

```
counts=(count_r(1)+count_r(2));

%Thus the uncertainty in this visibility is
deltavis=sqrt((1-vis)*(1+vis)/(counts*time));

% And finallyt the violation parameter is (Vp>2/3 to violate ...
    cloning limit)
Vp=vis-3*deltavis;
end
```

A.3 MATLAB code for QKD simulation

```
% Evan Meyer-Scott 30 August 2010, modification of
% Thomas Jennewein, 8.10.2008

% This script seeks to find the QBER (or entanglement ...
    visibility), detection rate, and final secure key rate ...
    for QKD based on entangled sources or weak coherent pulses.


clear

%%Setup
N=7; % Fock space dimension
% Sets up standard quantum optics functions
standard_defintions_qo_toolbox;

% Create photons based on down-conversion (0) or ideal ...
    entangled pair (1) or weak coherent pulses (2)
photon_type=0;

% Choose (for entanglement) whether to plot symmetric ...
    (2xloss) or asymmetric (one photon measured locally) links
if photon_type==0||photon_type==1
    plot_sym=0;
    plot_asym=0;
end

% Choose active basis choice (2 detectors) or passive (4 ...
    detectors)
% (0) active
% (1) passive
basis_choice=0;

% Define average photon number mu and displacement parameter ...
    alpha=sqrt(mu) if using weak coherent pulses
if photon_type==2
```

```
    mu=0.56;
    alpha=sqrt(mu);
    end

% Define intial QBER due to polarisation misalignment etc.
initial_QBER=0.01;

% Efficiencies for detectors (bucket Avalanche Photodiodes) ...
   and receiving optics
effc_apd=0.6;
effc_optics=0.475;

% Detecor noise factor: background per second, taken from ...
   intrinsic APD dark
% counts + stray light
darks=500;

% Net source rate (i.e. backcalculated from the singles and ...
   coincidences for down-conversion) gives approximately the ...
   epsilon, but for weak coherent pulses, net source rate is ...
   the laser rep rate
net_source_rate=32e6;

% The coincidence window is the time interval in which pairs ...
   of photons are accepted (for entanglement) or the time ...
   interval around the expected laser pulse time around ...
   which single detections are accepted (for weak coherent ...
   pulses) This can be a vector as it is looped over
coinc_window=[1]*1e-9;


% Link attenuation in dB (2nd for 2 'symmetric' links), i.e. ...
   link_dB1 is used as the first link in a two-link scenario ...
   and the only link in a one-link scenario. This is ...
   generally a vector as it is looped over; add another loop ...
   to loop over link_dB2 as well if needed. It is nice to ...
   have finer resolution near the QKD cutoff
link_dB1=[0:2:34 35:.1:45];
x1=10.^(-link_dB1/10);

link_dB2=link_dB1;
x2=10.^(-link_dB2/10);

% Looping variable lengths
m=numel(x1);
n=numel(coinc_window);

% Initialise to zeros for faster looping
twofold_rate=zeros(1,m);
```

```
singles_rate=zeros(1,m);
vis=zeros(1,m);
twofold_rate_asym=zeros(1,m);
singles_rate1=zeros(1,m);
singles_rate2=zeros(1,m);
vis_asym=zeros(1,m);
twofolds=zeros(m,n);
singles=zeros(m,n);
visibilities=zeros(m,n);
visibilities_asym=zeros(m,n);
twofolds_asym=zeros(m,n);
singles1_asym=zeros(m,n);
singles2_asym=zeros(m,n);
QBER=zeros(1,m);
QBER_sym=zeros(1,m);
QBER_asym=zeros(1,m);
final_bits_sym=zeros(m,n);
final_bits_asym=zeros(m,n);
e1=zeros(1,m);
Q1=zeros(1,m);

 %% Weak coherent pulses
if photon_type==2


    % Make a coherent state with displacement operator
    D = expm(alpha*a'-alpha'*a);
    % Put the coherent state in mode 1, and vacuum in mode ...
       2, therefore detections in
    % mode 2 are errors
    psi = tensor(D*vacc,vacc);

    % Add initial QBER with partially transmitting ...
       beamsplitter between
    % modes 1 and 2
    eta=asin(sqrt(initial_QBER));
    H_bs = (tensor(a,a') + tensor(a',a))*eta;
    U_bs = expm(-1i*H_bs);
    psi=U_bs*psi;


    %Loop over coincidence window
    for n=1:numel(coinc_window)

        % Noise factor per pulse is  (darks/s)x(s/pulse) of ...
           coincidence
        % window
        noise_factor=darks*coinc_window(n);
```

```
%Loop over link loss
for m=1:numel(x1)
    effc_link1=x1(m);

    % Create detectors, including fock space N, ...
       combined losses due to the link, optics ...
       efficiency, and detector efficiency, and noise

    % The way to treat active vs passive analyser is ...
       to halve the input (at 50:50 beamsplitter) ...
       for the passive analyser before creating the ...
       projector (decreasing SNR), then double the ...
       output count rate (since there are 2 bases)

    if basis_choice==0
        [apd_link1 ...
           un_linkapd1]=BucketDetector_noise(N,...
            effc_link1*effc_optics*effc_apd,noise_factor);
    else
        [apd_link1 ...
           un_linkapd1]=BucketDetector_noise(N,...
            0.5*effc_link1*effc_optics*effc_apd,noise_factor);
    end


    % Now measure on fock space N, state psi, and ...
       detector modules 1 and 2 to return ...
       measurement probabilities
    % probs(1) = mode 1 probability
    % probs(2) = mode 2 probability
    % probs(3) = double click probability (must ...
       randomise)
    if basis_choice==0
        probs=real(measure_2modes_2detectors ...
            (N,psi,apd_link1,un_linkapd1));
    else
        probs=2*real(measure_2modes_2detectors ...
            (N,psi,apd_link1,un_linkapd1));
    end

    %Rates returned are 'per pulse', so multiply by ...
       source rat
    singles_rate(m)=sum(probs)*net_source_rate;

    %Determine visibility and QBER from returned ...
       detection
    %probabilities, with randomised double clicks
    doubles=probs(3);
```

```
            QBER(m)=(probs(2))/sum(probs)+doubles/2/sum(probs);
            vis(m)=1-2*QBER(m);

            % Weak coherent pulse values: these can be taken ...
               directly from the simulation as below, or a ...
               more realistic decoy state system can be ...
               simulated by sending and detecting signal ...
               states with average photon number mu, and ...
               decoy states with nu < mu

            % Total signal gain
            Qmu=sum(probs);
            % Single photon gain
            if basis_choice==0
                 Q1(m)=(apd_link1(2,2)-apd_link1(1,1)) ...
                     *exp(-mu)*(mu);
            else
                 Q1(m)=2*(apd_link1(2,2)-apd_link1(1,1)) ...
                     *exp(-mu)*(mu);
            end


            % Single photon error rate
            e1(m)=(0.5*apd_link1(1,1)+initial_QBER* ...
                (apd_link1(2,2)-apd_link1(1,1)))/(apd_link1(2,2));
        end

        %Rearrange data by coincidence window
        singles(:,n)=singles_rate;
        visibilities_asym(:,n)=vis;

        % Calculate final key rate from Lo & Ma, PRA 2005
        Emu=QBER;
        % Binaray entropy function
        H2=-Emu.*log2(Emu) - (1-Emu).*log2(1-Emu);
        H21=-e1.*log2(e1) - (1-e1).*log2(1-e1);
        final_bits_asym(:,n)=0.5*net_source_rate* ...
            (-Qmu*1.22.*H2+Q1.*(1-H21));
    end
else
%% Use Entangled States
    %Loop over coincidence window
    for n=1:numel(coinc_window)

        % Source frequency is approximated to inverse of ...
           coincidence window
        f_source=1/coinc_window(n);
```

```
% Determine squeezing parameter epsilon and dark ...
    count probability 'per pulse'  from source rates, ...
    dark rates and source frequency

epsilon=sqrt(net_source_rate/f_source);
noise_factor=darks/f_source;

if photon_type==0; % Create entangled pair from ...
    down-conversion

    H_dc=(tensor(a,a)+tensor(a',a'))*epsilon; % ...
        Hamiltonian
    U_dc=expm(-1i*H_dc); % Unitary
    % Act unitary on vacuum to create pair state |HH>
    dc_state=tensor(U_dc*tensor(vacc,vacc));
    % Permute to create entangled state |HV>+|VH>
    psi=permute(tensor(dc_state,dc_state),[1 3 4 2]);

else % Create ideal entangled pair |HV>+|VH>
    ideal_state=tensor(oneph,vacc,vacc,oneph)+ ...
        tensor(vacc,oneph,oneph,vacc);
    psi=ideal_state;
end

%Loop over link loss
for m=1:numel(x1)

    effc_link1=x1(m);
    effc_link2=x2(m);


    % Create detectors, including fock space N, ...
        combined losses due to two links, optics ...
        efficiency, and detector efficiency, and noise

    % The way to treat active vs passive analyser is ...
        to halve the input (at 50:50 beamsplitter) ...
        for the passive analyser before creating the ...
        projector (decreasing SNR), then double the ...
        output count rate (since there are 2 bases)

    if basis_choice==0
        [apd_link1 ...
            un_linkapd1]=BucketDetector_noise(N, ...
            effc_link1*effc_optics*effc_apd,noise_factor);
        [apd_link2 ...
            un_linkapd2]=BucketDetector_noise(N, ...
            effc_link2*effc_optics*effc_apd,noise_factor);
```

```
    %For asymmetric, i.e. only one link, this is ...
       the local arm
    [apd un_apd]=BucketDetector_noise(N, ...
       effc_optics*effc_apd,noise_factor);
else
    [apd_link1 ...
       un_linkapd1]=BucketDetector_noise(N, ...
       0.5*effc_link1*effc_optics*effc_apd,noise_factor);
    [apd_link2 ...
       un_linkapd2]=BucketDetector_noise(N, ...
       0.5*effc_link2*effc_optics*effc_apd,noise_factor);
    [apd un_apd]=BucketDetector_noise(N, ...
       effc_optics*0.5*effc_apd,noise_factor);
end

% Double link with arbitrary losses in each arm, ...
   measure on Fock space N, state psi, and ...
   detector modules 1 and 2
% probs(1) = HH
% probs(2) = HV
% probs(3) = VH
% probs(4) = VV
% probs(5:6) = singles on link 1
% probs(7:8) = singles on link 2
% probs(9:10) = double clicks on links 1/2

probs=real(measure_2folds_4modes_unsymetric_detectors( ...
   N,psi,apd_link1,un_linkapd1,apd_link2,un_linkapd2));
% Rates returned are 'per pulse', so multiply by ...
   source rate
twofold_rate(m)=sum(probs(1:4))*f_source;
singles_rate(m)=sum(probs(5:6))*f_source;

% Determine visibility and QBER from returned ...
   detection probabilities
QBER_sym(m)=(probs(1)+probs(4))/sum(probs([1:4 ...
   9:10]))+0.5*sum(probs(9:10))/sum(probs([1:4 ...
   9:10]));
vis(m)=1-2*QBER_sym(m);

% Single link with loss in only one arm, measure ...
   on Fock space N, state psi and detector ...
   modules 1 and local
probs=measure_2folds_4modes_unsymetric_detectors( ...
   N,psi,apd_link1,un_linkapd1,apd,un_apd);
twofold_rate_asym(m)=sum(probs(1:4))*f_source;
singles_rate1(m)=sum(probs(5:6))*f_source;
singles_rate2(m)=sum(probs(7:8))*f_source;
```

```
            QBER_asym(m)=(probs(1)+probs(4))/sum(probs([1:4 ...
                9:10]))+0.5*sum(probs(9:10))/sum(probs([1:4 ...
                9:10]));
            vis_asym(m)=1-2*QBER_asym(m);

        end

    %Rearrange data by coincidence window or source rate
        twofolds(:,n)=twofold_rate;
        singles(:,n)=singles_rate;
        visibilities(:,n)=vis;

        twofolds_asym(:,n)=twofold_rate_asym;
        singles1_asym(:,n)=singles_rate1;
        singles2_asym(:,n)=singles_rate2;
        visibilities_asym(:,n)=vis_asym;

        % Calculate final secure key bits from Ma et al., ...
            PRA 2007
        z=QBER_sym;
        H2=-z.*log2(z) - (1-z).*log2(1-z);
        final_bits_sym(:,n)=twofold_rate*0.5.*(1-(1+1.22).*H2);


        z=QBER_asym;
        H2=-z.*log2(z) - (1-z).*log2(1-z);
        final_bits_asym(:,n)=twofold_rate*0.5.*(1-(1+1.22).*H2);
    end
end


%Get labels ready for plotting

if photon_type==0
    EPS_type='Down-conversion EPS';
elseif photon_type==1
    EPS_type='Idealised EPS';
else
    EPS_type='Weak coherent pulses';
end

if basis_choice==1
    channel_detector='Passive';
else
    channel_detector='Active';
end


    bbb=num2str(coinc_window'./1e-9, '%0.2f ns');
```

```
if photon_type==0||photon_type==1
    if plot_sym==1
    %%Plot symmetric links
    figure()
    subplot(3,1,1)
    plot(link_dB1,abs(visibilities));
    title(sprintf('Visibility for %s, symmetric links: ...
       FockSpace = %d, Darks=%0.2f, \n Detection-Effc=%0.2f, ...
       Coupling-Effc=%0.2f, %s analyser', EPS_type, N, ...
       darks, effc_apd, effc_optics, channel_detector))
    ylabel('polarisation Visibility')

    legend(cellstr(bbb));

    subplot(3,1,2)
    semilogy(link_dB1,twofolds);
    ylabel('Two-fold rate [cps]')
    xlabel('Link Loss [dB]')
    legend(cellstr(bbb));

    subplot(3,1,3)
    semilogy(link_dB1,final_bits_sym)
    ylabel('Secure key rate (bits/s)')
    xlabel('Link Loss (dB)')
     legend(cellstr(bbb));
     end
     %%Plot asymmetric links
     if plot_asym==1
    figure()
    subplot(3,1,1)
    plot(link_dB1,abs(1/2-abs(visibilities_asym)/2))
    title(sprintf('QBER for %s, assymetric links: FockSpace ...
       = %d, Darks=%0.2f, \n Detection-Effc=%0.2f, ...
       Coupling-Effc=%0.2f, %s analyser', EPS_type, N, ...
       darks, effc_apd, effc_optics, channel_detector))
    ylabel('QBER')

    legend(cellstr(bbb));

    subplot(3,1,2)
    semilogy(link_dB1,twofolds_asym);
    ylabel('Two-fold rate [cps]')
    xlabel('Link Loss [dB]')


    subplot(3,1,3)
    semilogy(link_dB1,final_bits_asym)
    ylabel('Secure key rate (bits/s)')
```

```
    xlabel('Link Loss (dB)')

     end

elseif photon_type==2
        %%Plot weak coherent pulse
    figure
    subplot(3,1,1)
    plot(link_dB1,1/2-abs(visibilities_asym)/2);
    title(sprintf('QBER for %s, symmetric links: FockSpace = ...
       %d, Darks=%0.2f, \n Detection-Effc=%0.2f, ...
       Coupling-Effc=%0.2f, %s analyser', EPS_type, N, ...
       darks, effc_apd, effc_optics, channel_detector))
    ylabel('QBER')
    legend(cellstr(bbb));

    subplot(3,1,2)
    semilogy(link_dB1,singles);
    ylabel('Received Count Rate [cps]')
    xlabel('Link Loss [dB]')


    subplot(3,1,3)
    semilogy(link_dB1,final_bits_asym)
    ylabel('Secure key rate (bits/s)')
    xlabel('Link Loss (dB)')

end

function probs=measure_2modes_2detectors(N,in,proj,unproj)

%Evan Meyer-Scott, 10.17.2010 from Thomas Jennewein, 8.10.2008
%Determin the singles count rates for a 2 mode state, e.g. ...
   |H1,V1>


final_state=in;

%singles
H=sum(expect(tensor(proj,unproj),final_state));
V=sum(expect(tensor(unproj,proj),final_state));
%Double clicks
HV=sum(expect(tensor(proj,proj),final_state));

probs=[H,V,HV];
end

function probs=measure_2folds_4modes_unsymetric_detectors( ...
   N,in,proj1,unproj1,proj2,unproj2)
```

```
%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.

%Evan Meyer-Scott, 2010, added double clicks
ida=identity(N);

final_state=in;
% Coincidences
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));

% Double clicks
H1V1=sum(expect(tensor(proj1,proj1,proj2,ida),final_state))+ ...
    sum(expect(tensor(proj1,proj1,ida,proj2),final_state));
H2V2=sum(expect(tensor(proj1,ida,proj2,proj2),final_state))+ ...
    sum(expect(tensor(ida,proj1,proj2,proj2),final_state));

probs=[HH,HV,VH,VV,H1,V1,H2,V2,H1V1,H2V2];
end
```

Appendix B

Calculating the dispersion of the (lm)=(01), (11) modes for 810 nm light in a 1550 nm optical fibre

This Appendix was written by Allison MacDonald as part of her co-op work term. It is included here for ease of reference.

B.1 Calculation of dispersion from guided wave theory

We introduce MATLAB code which calculates the dispersion between spatial modes in a fibre at a given wavelength, using both an exact method and an approximation which is valid for fibres with large V parameters (multimode fibres).

The following derivation is taken from [95]. In a step-index optical fiber, both the core ($r < a$) and cladding ($r > a$) exactly obey the Helmholtz equation:

$$\nabla^2 U + n^2(r) k_0^2 U = 0 \tag{B.1}$$

which can be expressed in polar coordinates as:

$$\frac{\partial^2 U}{\partial r^2} + \frac{1}{r}\frac{\partial U}{\partial r} + \frac{1}{r^2}\frac{\partial^2 U}{\partial \phi^2} + \frac{\partial^2 U}{\partial z^2} + n(r)^2 k_0^2 U = 0 \tag{B.2}$$

with

$$n(r) = \begin{cases} n_1, & r < a \\ n_2, & r > a \end{cases}$$

and $k_0 = \frac{2\pi}{\lambda}$. The modes of light in the fibre propagate in the z-direction, characterised by a propagation constant β, so $U(z) \propto e^{-i\beta z}$, and are periodic in ϕ with period 2π, so $U(\phi) \propto e^{-il\phi}$, with l an integer. Assuming separable solutions,

$$U(r,\phi,z) = u(r)e^{-il\phi}e^{-i\beta z},\ l = 0,\ \pm 1,\ \pm 2,\ \ldots \tag{B.3}$$

This leads to the following differential equation for $u(r)$:

$$\frac{d^2u}{dr^2} + \frac{1}{r}\frac{du}{dr} + \left(n^2(r)k_0^2 - \beta^2 - \frac{l^2}{r^2}\right)u = 0 \tag{B.4}$$

Making the following definitions:

$$k_T^2 = n_1^2k_0^2 - \beta^2 \tag{B.5}$$

$$\gamma^2 = \beta^2 - n_2^2k_0^2 \tag{B.6}$$

we obtain two equations for the core and cladding:

$$\frac{d^2u}{dr^2} + \frac{1}{r}\frac{du}{dr} + \left(k_T^2 - \frac{l^2}{r^2}\right)u = 0,\ r < a \tag{B.7}$$

$$\frac{d^2u}{dr^2} + \frac{1}{r}\frac{du}{dr} - \left(\gamma^2 + \frac{l^2}{r^2}\right)u = 0,\ r > a. \tag{B.8}$$

These are well-known differential equations, whose solutions are known as Bessel functions:

$$u(r) \propto \begin{cases} J_l(k_T r),\ r < a \\ K_l(\gamma r),\ r > a \end{cases} \tag{B.9}$$

In considering boundary conditions for the modes which may propagate inside a weakly guiding fibre ($n_1 \approx n_2$), the condition that must be obeyed by β is approximately equivalent to the condition that $u(r)$, the radial distribution for each mode, and its derivative be continuous at the boundary between core and cladding ($r = a$):

$$\frac{k_T a J_l'(k_T a)}{J_l(k_T a)} = \frac{\gamma a K_l'(\gamma a)}{K_l(\gamma a)} \tag{B.10}$$

where

$$J_l'(x) = \pm J_{l\mp 1}(x) \mp l\frac{J_l(x)}{x} \tag{B.11}$$

$$K_l'(x) = -K_{l\pm1}(x) \mp l\frac{K_l(x)}{x}. \tag{B.12}$$

Combining Equations B.10–B.12, we obtain the characteristic equation:

$$X\frac{J_{l\pm1}(X)}{J_l(X)} = \pm Y\frac{K_{l\pm1}(Y)}{K_l(Y)} \tag{B.13}$$

with $X = k_T a$ and $Y = \gamma a$. This can be solved graphically by plotting the left side and the right side, both versus X, and finding their intersections. (We see from Equations B.5 and B.6 that $X^2 + Y^2 = \left(n_1^2 - n_2^2\right) k_0^2 a^2 = NA^2 \left(2\pi\frac{a}{\lambda_0}\right)^2 = V^2$, where $NA = n_1^2 - {}_2^2$ is the numerical aperture of the fibre, with n_1 and n_2 the refractive indices of the core and cladding, respectively, and we have defined the fibre "V parameter").

In general, Equation B.13 has multiple solutions for each value of the index l, which are labeled by the index m. The number of solutions is limited by V, since Y becomes imaginary when $X > V$. The indices l and m characterise the azimuthal and radial distributions, respectively, of each mode. In our case, we modelled a fibre with a small V parameter, so there was only one solution for the azimuthal modes of interest ($l = 0,\ 1$).

We solved Equation B.13 by using the MATLAB interpolate function to find the value of X at which the $LHS - RHS = 0$. We did this for a small range ($800 - 820$ nm) of wavelengths around 810 nm, and deduced β as follows:

$$\beta_{lm} = \sqrt{\frac{4\pi^2 n_1^2}{\lambda^2} - \frac{X_{lm}^2}{a^2}} \tag{B.14}$$

for each wavelength. The group velocity of each mode is given by

$$v_{lm} = \frac{\partial\omega}{\partial\beta_{lm}} \tag{B.15}$$

so the inverse group velocity is the slope of the β versus $\omega = \frac{2\pi c}{\lambda}$ plot, which is simply calculated as the mean of $diff(\beta)/diff(\omega)$, since the plot is approximately a straight line. If this is done for two modes (specified by l and m), the dispersion can be calculated as

$$D = \frac{1}{v_{11}} - \frac{1}{v_{01}} \tag{B.16}$$

with appropriate unit conversion factors. We note that we obtained a value of 2.19823 ns/km for the two modes of 810 nm light in telecom fibre with core radius 4.1 μm, in good agreement with the experimentally obtained value of

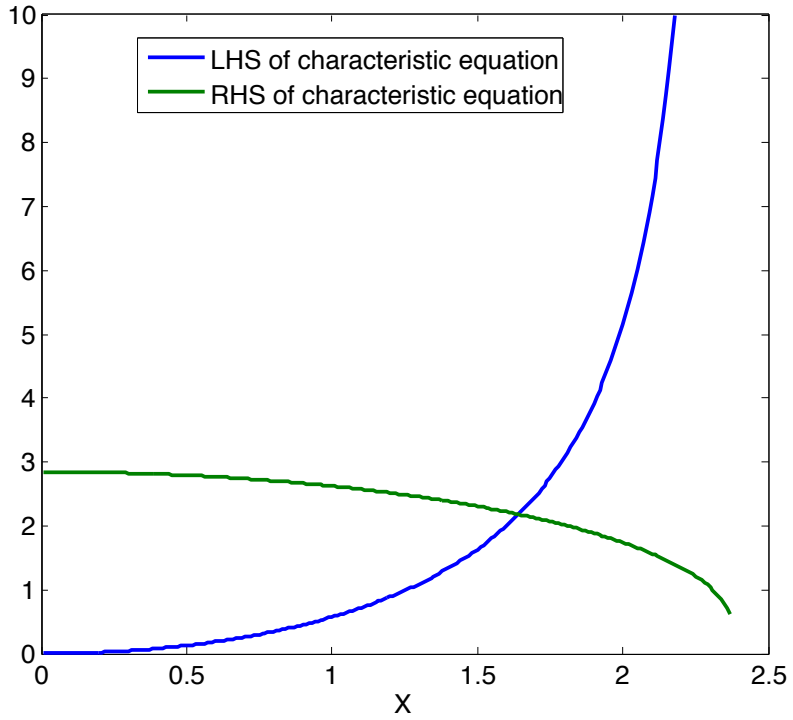

Figure B.1: Characteristic equation solution for fibre modes via graphical intersection, for single mode fibre at 810 nm (core radius 2.5 μm).

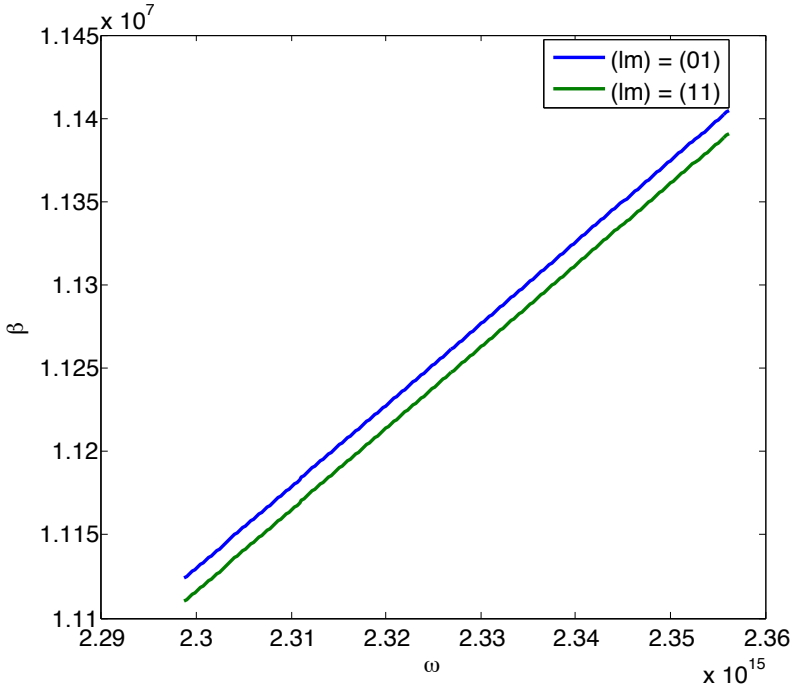

Figure B.2: Propagation constant β versus ω for two propagation modes of 810 nm light in telecom optical fibre. The very slight difference in slope of the two curves leads to modal dispersion.

2.2 ns/km. This means each kilometre of propagation causes the two modes to be temporally separated by an additional 2.2 ns.

The second, more approximate, method for calculating the dispersion assumes a large V parameter, which occurs either for a large numerical aperture (n_1 and n_2 are very different), or the core radius to wavelength ratio is large, making the fibre essentially multimode. A series of approximations based on a large V leads to [95]:

$$\begin{aligned}\beta_{lm} &\approx n_1 k_0 \left[1 - \frac{(l+2m)^2}{M}\Delta\right] \\ &\approx n_1 \frac{\omega}{c}\left[1 - \frac{(l+2m)^2}{M}\Delta\right]\end{aligned} \tag{B.17}$$

where

$$M \approx \frac{4}{\pi^2}V^2 \approx \frac{8a^2\omega^2 n_1^2 \Delta}{\pi^2 c^2} \tag{B.18}$$

is the approximate total number of modes allowed to propagate in the fibre, and $\Delta = \frac{n_1^2 - n_2^2}{2n_1^2}$, and m and l are the radial and azimuthal indices of each propagating mode. Given Equations B.15 and B.17, we can calculate the group velocity of each mode as:

$$v_{lm} \approx \frac{c}{n_1}\left[1 + \frac{(l+2m)^2}{M}\Delta\right]^{-1} \tag{B.19}$$

The dispersion is again given by Equation B.16.

For the core size of the fibres of interest, we found that the results of the two methods did not agree at all. Consequently, we investigated the results given by each method as a function of the core radius of the optical fibre. We found that the large V parameter approximation converges with the graphical solution for fibres with radii around 30 μm, or a V parameter of 2.8.

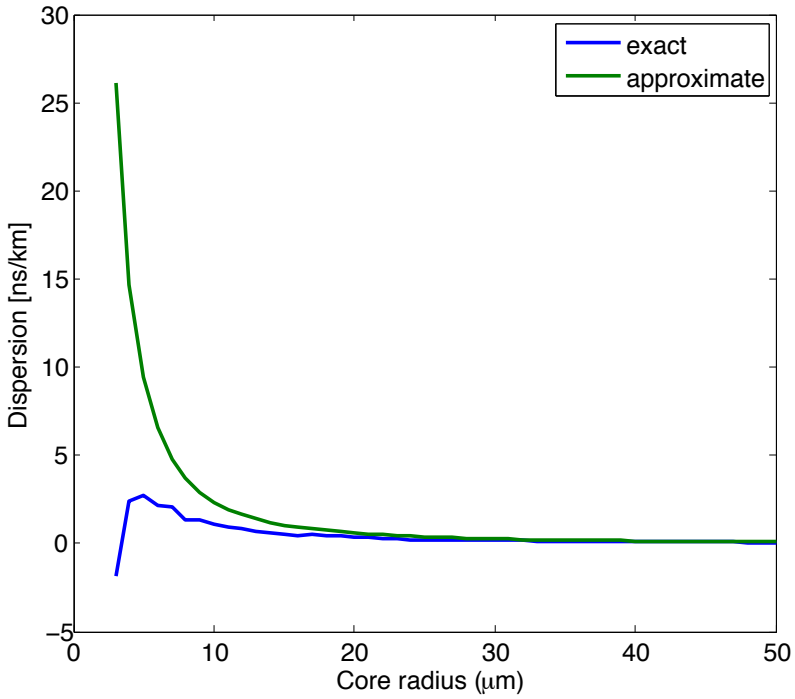

Figure B.3: Comparison of dispersion calculation methods. The “exact” curve is from the graphical fitting method, while the “approximate” curve is based on the large V parameter assumption.

B.2 MATLAB code to calculate dispersion

```
%Find the dispersion between the l=0,1 modes in SMF-28 fiber ...
    using 810 nm.

c=3.0e8;                        %speed of light
lambda=1e-9*(800:0.1:820);
a=4.1e-6;                       %radius of core
l=[0,1];
inverse_vel=zeros(1,numel(l));

for m=1:numel(l)


    nlambda=numel(lambda);
    beta=zeros(1,nlambda);
    omega=2*pi*c./lambda;
    solution=zeros(1,nlambda);
    for p=1:nlambda;
        d=0.6961663*(lambda(p)*1e6)^2/ ...
            ((lambda(p)*1e6)^2-0.0684043^2);
        e=0.4079426*(lambda(p)*1e6)^2/ ...
            ((lambda(p)*1e6)^2-0.1162414^2);
        f=0.8974794*(lambda(p)*1e6)^2/ ...
            ((lambda(p)*1e6)^2-9.896161^2);
        n1=sqrt(d+e+f+1);               %n of core, using ...
           Sellemeier equation
        n2=n1/1.0036;                   %n of cladding
        NA=sqrt(n1^2-n2^2);             %numerical aperture of ...
           fiber
        V=2*pi*a*NA/lambda(p);          %V parameter of the fiber
        X=(0.1:0.1:V-0.1);


        k=numel(X);
        Y=sqrt(V^2-X.^2);
        LHS=zeros(1,k);
        RHS=zeros(1,k);
        y=zeros(1,k);

        for n=1:k
            LHS(n)=X(n)*besselj(l(m)+1,X(n))/(besselj(l(m),X(n))); ...
                 %LHS of characteristic eqn
            RHS(n)=Y(n)*besselk(l(m)+1,Y(n))/(besselk(l(m),Y(n))); ...
                 %RHS of characteristic eqn
            y(n)=LHS(n)-RHS(n);
        end
```

```
    %find where LHS=RHS (xlm)
    solution(p)=interp1(y,X,0);
    beta(p)=sqrt(n1^2*4*pi^2/lambda(p)^2-solution(p)^2/a^2);
    end

%Calculate slope of each curve (beta vs omega)
slope=diff(beta)./diff(omega);
inverse_vel(m)=mean(slope);


%plot beta
hold on
plot(omega,beta,'*')
title(sprintf('Propagation constant for the l=%d mode',l(m)))
ylabel('Beta')
xlabel('Angular frequency')


end

%Calculate dispersion
dispersion=(inverse_vel(2)-inverse_vel(1))*1e+12;
sprintf('Dispersion is %g ns/km',dispersion)

%Calculate  dispersion  using  large  V  parameter  ...
   approximation
 m=1;
lambda2=810e-9;
d=0.6961663*(lambda2*1e6)^2/((lambda2*1e6)^2-0.0684043^2);
e=0.4079426*(lambda2*1e6)^2/((lambda2*1e6)^2-0.1162414^2);
 f=0.8974794*(lambda2*1e6)^2/((lambda2*1e6)^2-9.896161^2);
  n12=sqrt(d+e+f+1);

n22=n12/1.0036;
delta=(n12^2-n22^2)/(2*n12^2);
  w=2*pi*c/lambda2;
   c1=c/n12;
  M=8*a^2*w^2*delta/(pi^2*c1^2);

%l=0,m=1
 group_v1=c1/(1+((0+2*m)^2)*delta/M);
  %l=1,m=1
 group_v2=c1/(1+((1+2*m)^2)*delta/M);
    dispersion2=(1/group_v2-1/group_v1)*1e+12;
```