UNIVERSITY OF CALGARY

Real world quantum cryptography

by

Itzel Lucio Martínez

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

August, 2014

Abstract

Quantum cryptography uses the quantum properties of individual photons to provide two or more users with means to communicate securely and efficiently. Specifically, quantum key distribution (QKD) focuses on the secure communication between two distant parties and guarantees the security of a transmitted message between them. Although QKD is the most mature application of quantum cryptography, applications of quantum mechanics in communication systems are not limited to QKD and other cryptographic protocols can be implemented as well.

This thesis focuses on the implementation of quantum cryptographic systems over deployed fiber. A first QKD system was built and used to demonstrate the BB84 protocol over deployed fiber between the University of Calgary and SAIT. The system implemented a novel tool called quantum frames that allow for the quantum signals to be routed, for clock synchronization, and for channel stabilization in a network scenario. The same system was used to examine the scalability of the secret key generation rate in different steps of the process in order to detect potential bottlenecks for key generation rate of high speed systems. A second QKD system was developed to demonstrate the measurement-device independent QKD protocol. The system worked over deployed fiber between the University of Calgary, SAIT, and Foothills Hospital in the City of Calgary. The advantage of the measurement-device independent QKD protocol over previous QKD protocols is that it eliminates the possibility of side-channel attacks that target single photon detectors used in QKD systems. This demonstration also involved the first demonstration of a Bell state measurement over deployed fiber. Bell state measurements were further studied by using novel single photon detectors, which allowed demonstrating a highly efficient Bell measurement. Finally, a cryptographic protocol known as private queries was demonstrated between the University of Calgary and SAIT. Quantum private queries were demonstrated for the first time over deployed fiber by

developing and implementing an error correction scheme to make the protocol noise and loss tolerant.

Acknowledgements

Working at the QC2 laboratory has been an incredible opportunity and a great experience. I would like to thank all of the past and present members of the QC2 lab. To my supervisor, Wolfgang Tittel, thanks for the opportunity to join your group. I have always admired the energy that you have on a daily basis as well as the intuition you have to solve any kind of problem. Thanks for your guidance through the course of my studies. I have learned a lot from you.

I would like to thank the members of my committee Dr. Christoph Simon and Dr. Carey Williamson for the feedback they gave me through the course of my studies. I would also like to thank Dr. Li Qian and Dr. Henry Leung for agreeing to be part of my thesis defence committee.

Thanks to the supporting staff of the Department of Physics and Astronomy, specially to Leslie Holmes, Tracy Krosgaard, Catherine Barrett and Nancy Jing Lu.

I would also like to thank the Consejo Nacional de Ciencia y Tecnologia de México (CONACyT) which made possible my master's studies and for the scolarship they provided for the first half of my Phd.

To all my fellow students and postdocs thank you all. Special thanks to Dr. Xiaofan Mo who guided me through 'the lab life' in my first years. Steve Hosier, Dr. Cecilia La Mela, Dr. Daniel Oblak, Dr. Felix Bussiéres, Dr. Morgan Hedges, Dr. Michael Lamont, Dr. Yang Tan, Dr. Joshua Slater, Dr. Jeongwan Jin, Dr. Lucile Veissier, Dr. Lambert Giner, Dr. Erhan Saglamyurek, Dr. Qiang Zhou, Neil Sinclair, Allison Rubenok, Philip Chan, Chris Healey, Ahdiyeh Delfan, Dr. Michael Underwood, Gina Howard, Sean Blancher, John Nguyen, Randy Squires, Hassan Mallahzadeh, Raju Valivarthi, Terence Stuart, Marcel-li Grimau, Thomas Lutz and Vladimir Kiselyov, you are all great lab mates, thank you for all the help, discussions and great moments we shared.

Thanks to Lucile Veissier and Pascal Huynh who, for the last six months of my studies, were willing to share an apartment and share with me their delicious meals.

Finally, thanks to my parents, José Luis and Alejandrina, and my brother, Toño, who are always there for me and supporting me in all aspects of my life. I am thankful to have you by my side. To you, Tim Friesen, thanks for all the support and love you always give me, more than anybody, this thesis wouldn't have been possible without you.

List of Publications

The following list contains the papers published during the author's Ph.D. program according to order of appearance in the thesis. Supplemental Materials and Supplementary Information of the publications are contained in the appendices at the end of the thesis.

1.- I. Lucio-Martinez, P. Chan, X. F. Mo, S. Hosier and W. Tittel, *Proof-of-concept of real-world quantum key distribution with quantum frames*, New Journal of Physics 11(9): 095001 (26 pp.), 2 September 2009, arXiv:0901.0612.

2.- X. F. Mo, I. Lucio-Martinez, P. Chan, C. Healey, S. Hosier and W. Tittel, *Time-cost analysis of a quantum key distribution system clocked at 100 MHz*, Optics Express 19(18): 17729 - 17737, 25 August 2011, arXiv:1105.3761v1.

3.- P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok and W. Tittel, *Modeling a measurement-device-independent quantum key distribution system*, Optics Express 22(11): 12716 - 12736 , 2 June 2014, arXiv:1204.0738.

4.- A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez and W. Tittel, *Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks*, Physical Review Letters 111(13): 130501 (5 pp.), 23 September 2013, arXiv:1304.2463.

5.- R. Valivarthi, I. Lucio-Martinez, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak, S. W. Nam, W. Tittel, *Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors.* Submitted for publication to Optics Express.

6.- P. Chan, I. Lucio-Martinez, X. F. Mo, C. Simon and W. Tittel, *Performing private database queries in a real-world environment using a quantum protocol*, Scientific Reports 4: 5233, 10 June 2014, arXiv:1303.0865.

Chapter in book:

P. Chan, I. Lucio-Martinez, X. F. Mo and W. Tittel, *Quantum key distribution*, Anatoli V. Andreev, eds., Chapter 13, Published by InTech, Rijeka, Croatia, 2011 (ISBN 978-953-307-769-7). arXiv:1111.4501.

Table of Contents

Abstract . . . i
Acknowledgements . . . iii
List of Publications . . . v
Table of Contents . . . vi
List of Tables . . . ix
List of Figures . . . x
List of Symbols . . . xii
1 Introduction . . . 1
1.1 Motivation . . . 1
1.2 Background . . . 4
1.3 QKD implementations . . . 6
1.4 This thesis . . . 9
2 Elements of quantum cryptography . . . 11
2.1 Introduction . . . 11
2.2 Qubit preparation . . . 12
2.3 Qubit measurement . . . 13
2.4 Entanglement . . . 14
2.5 No-cloning theorem . . . 15
2.6 Shannon entropy . . . 16
3 Quantum key distribution . . . 20
3.1 Assumptions . . . 20
3.2 Quantum and classical channel . . . 21
3.3 Authentication . . . 21
3.4 Qubit exchange . . . 22
3.5 Post-processing . . . 23
3.6 Photon number splitting attack and countermeasures . . . 24
3.6.1 Decoy states . . . 25
3.6.2 SARG protocol . . . 27
4 Implementation of quantum frames in a QKD system . . . 28
4.1 Proof-of-concept of real-world quantum key distribution with quantum frames 33
4.1.1 Introduction . . . 34
4.1.2 Q-frames . . . 35
4.1.3 Our QKD system . . . 37
4.1.4 Polarization and IMs . . . 38
4.1.5 The fibre link . . . 43
4.1.6 Field tests . . . 48
4.1.7 Security issues . . . 55
4.1.8 Classical post-processing . . . 61
4.1.9 Conclusion and outlook . . . 67
4.1.10 Acknowledgements . . . 67
5 Analyzing QKD system performance . . . 69
5.1 Time-cost analysis of a quantum key distribution system clocked at 100 MHz 72

5.1.1 Introduction . . . 72
5.1.2 Our QKD System . . . 74
5.1.3 System Performance . . . 78
5.1.4 Proposed Improvements . . . 81
5.1.5 Conclusions . . . 84
6 Modelling and implementing a measurement-device-independent QKD system 85
6.1 Modeling a measurement-device-independent quantum key distribution system 92
6.1.1 Introduction . . . 92
6.1.2 Side-channel attacks . . . 94
6.1.3 The measurement-device-independent quantum key distribution protocol 95
6.1.4 The model . . . 97
6.1.5 Characterizing experimental imperfections . . . 107
6.1.6 Testing the model, and real-world tests . . . 116
6.1.7 Optimization of system performance . . . 119
6.1.8 Discussion and conclusion . . . 122
6.2 Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks . . . 125
7 Efficient Bell state measurement . . . 135
7.1 Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors . . . 139
7.1.1 Introduction . . . 139
7.1.2 Superconducting single photon detectors with short dead-times . . . 143
7.1.3 Experimental setup . . . 146
7.1.4 Results . . . 148
7.1.5 Error rates . . . 148
7.1.6 Conclusions and Outlook . . . 151
8 Quantum private queries . . . 153
8.1 Performing private database queries in a real-world environment using a quantum protocol . . . 157
8.1.1 Results . . . 162
8.1.2 Discussion . . . 174
8.2 Acknowledgements . . . 175
9 Conclusions and Outlook . . . 176
9.1 Conclusions . . . 176
9.2 Outlook . . . 177
Bibliography . . . 179
A Error Correction . . . 190
A.1 Low-density parity check matrices . . . 190
B Security proofs . . . 195
B.1 Types of attacks . . . 195
B.2 Security proofs . . . 196
B.2.1 Shor & Preskill, 2000 . . . 197
B.2.2 Gottesman, Lo, Lütkenhaus and Preskill (GLLP), 2004 . . . 201
C Bell state measurements . . . 204
C.1 Applications of quantum communication employing Bell state measurements 204

C.1.1 Quantum teleportation 204
C.1.2 Entanglement swapping 206
C.1.3 Superdense coding 207
C.2 Exceeding the 50% limit of a Bell state measurement 208
D Supplementary Information: Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks 212
D.1 Ensuring Indistinguishability 212
D.2 Decoy-State Analysis 213
D.3 Secure key distribution using MDI-QKD 216
D.4 Discussion of error rates $e_{\mu\sigma}^{x,z}$ 221
E Supplementary Information: Performing private database queries in a real-world environment using a quantum protocol 223
E.1 Review of Oblivious Transfer and Private Queries 223
E.2 Quantum State Identification 226
E.3 Error Correction 228
E.4 Requirements for security 230
E.5 Cheating Strategies 232
E.5.1 User Privacy 232
E.5.2 Database Privacy 235
E.5.3 Error rate estimation 237

List of Tables

4.1 4-Detector measurement 54
4.2 Results for $r_{\alpha j=1}(i,j)$. 63
4.3 Results for $P'_0(j)$ and $P'_1(j)$ values. 63
4.4 Simulation results for LDPC decoding 66

6.1 Experimentally established values required to describe the generated quantum states 115
6.2 Measured error rates 117
6.3 Length and loss (ℓ_A, l_A, ℓ_B, l_B) of the individual fiber links used to connect Alice and Charlie, and Charlie and Bob, respectively, for all tested setups. The table also lists the total length ℓ and total loss $l = l_A + l_B$ (in dB). The last line details measurements outside the laboratory with deployed fiber. . . 131

7.1 Bounded error rates e_{11}^z and e_{11}^x for two single photon inputs 149
7.2 Bell state measurement efficiencies extracted from measured data using a decoy state method 150

8.1 Comparison of the ability of various protocols for private queries to meet the two criteria for deployment (security and implementability) 161
8.2 Parameters for the private query protocol as measured in our experiment with standard detectors 173
8.3 Experimental and simulated results for the quantum private queries 174

A.1 Probability of each bit of Bob's sifted key to be 0 or 1 192
A.2 Computation of the probability of occurrence for each combination of bits . . 193

D.1 List of experimentally obtained error rates and gains 215

E.1 Comparison of simulation results to select an error-correcting code 237

List of Figures and Illustrations

2.1 Representation of a qubit on a Bloch sphere 12

4.1 Illustration of a simplified quantum network 29
4.2 Quantum frames 36
4.3 Schematic of the QKD system 36
4.4 Schematics of intensity and polarization modulators 38
4.5 Test of the two-way polarization modulator 44
4.6 Tests of the two-way IM 44
4.7 Satellite view of Calgary 45
4.8 OTDR traces of the installed fibres 46
4.9 Time evolution of Stokes parameters 47
4.10 Schematic of the QKD setup 49
4.11 Average quantum bit error rate and key generation probabilities 52
4.12 Results of the long-term measurement of the polarization stabilization 53
4.13 Comparison of secret key rates versus mean number of photons in the signal states 58
4.14 Classical post-processing steps 61
4.15 Simulation of the LDPC code 66

5.1 Structure of the quantum frames 76
5.2 Schematics of the optical and some electronic components of our QKD system 77
5.3 Sifted and error corrected key rates as a function of the raw key rate 80

6.1 Voltage across avalanche photodiode 87
6.2 Schematics for MDI-QKD 94
6.3 Description of the MDI-QKD system 109
6.4 Sketch of the probability density for a detection event 111
6.5 Afterpulse probability per time-bin as a function of the average number of photons arriving at the detector per gate 113
6.6 Modelled and measured results 118
6.7 Optimum signal state intensity and corresponding secret key rate as a function of total loss 121
6.8 Optimum signal state intensity and corresponding secret key rate as a function of total loss 123
6.9 Drift of differential arrival time and variation in the overlap of the polarization states 129
6.10 Aerial view showing Alice, Bob and Charlie 130
6.11 Measured error rates $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ for Alice and Bob 133

7.1 Typical Bell state measurement experimental setup 137
7.2 Experimental setup used to perform BSMs for polarization qubits and time-bin qubits 140

7.3 General setup for Bell state measurement for time-bin qubits using linear optics and single photon detectors 142
7.4 SNSPD detector setup and signal 144
7.5 Detection dead-times 145
7.6 Schematic of the experimental setup employed for a BSM with time-bin qubits 147

8.1 The picture shows how the database encodes the database elements using an oblivious key 155
8.2 Graphical representation of the private query protocol 166
8.3 Diagram of the experimental setup 171
8.4 Histograms for the information gained by the user in the 104 queries performed 174

C.1 Quantum teleportation 205
C.2 Entanglement swapping 206
C.3 Bell state measurement with auxiliary entangled photons 209

E.1 Quantum states used in the private query protocol shown on a plane of the Bloch sphere 226

List of Abbreviations

ATT	Attenuator
APD	Avalanche Photo Diode
AWG	Arbitrary Waveform Generator
BB84	Bennet and Brassard's QKD proposal made in 1984
BS	Beamsplitter
BSM	Bell State Measurement
CW	Continuous Wave
DI-QKD	Device Independent QKD
FPGA	Field Programmable Gate Array
HOM	Hong-Ou-Mandel
InGaAs	Indium Gallium Arsinide
IM	Intensity Modulator
LD	Laser Diode
LDPC	Low Density Parity Check
LiNbO3	Lithium Niobate
MC	Master Clock
MDI-QKD	Measurement Device Independent Quantum Key Distribution
OT	Oblivious Transfer
PBS	Polarizing Beam Splitter
PMBS	Polarizing Mantaining Beam Splitter
PC	Personal Computer
PD	Photodiode
PNS	Photon Number Splitting
PM	Phase Modulator
POC	Polarization Controller
QBER	Quantum Bit Error Rate
QC2	Quantum Cryptography and Communication Laboratory
QKD	Quantum Key Distribution
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SAIT	Southern Alberta Institute of Technology
SPD	Single Photon Detector
SSPD	Superconducting Single Photon Detector
SNSPD	Superconducting Nanowire Single Photon Detector
UofC	University of Calgary
WSi	Tungsten Silicide

Chapter 1

Introduction

Secure communication is pivotal in our modern world. Current electronic communications include the use of e-mail, e-banking, e-commerce, e-government, etc. The security of the information transmitted is crucial for the users of these services. Modern cryptography, in this thesis referred to as classical cryptography, protects this information by relying on algorithms that are computationally difficult to break. The security of these algorithms is not guaranteed however, as an eavesdropper with sufficient computational resources can still break the algorithms and have unauthorized access to the private information that is being transmitted. Quantum mechanics offers an exciting potential solution to this problem. If a key can be generated and transmitted using quantum systems then, in principle, that key can be distributed securely without requiring any assumptions on the computational power of an eavesdropper. This is due to the fact that any measurement of a quantum system disturbs its state, and because unknown quantum states cannot be copied. This promising solution is called quantum key distribution (QKD). In this thesis I will present work on the implementation and study of QKD systems and other quantum cryptographic protocols in a real world environment using existing telecommunication components. This work was done in the QC2 laboratory at the University of Calgary and experiments and measurements were performed between the University of Calgary, SAIT Polytechnic and Foothills Hospital in the City of Calgary.

1.1 Motivation

"Classical cryptography" relies on the use of 'keys' (specific sequence of bits) to encode and decode private messages. The encoding of a message, which is assumed to be represented

in binary form, makes it illegible to any party who does not have access to the private key to decode it. In this way the security of a message in transmission through a public channel depends on the security of the key that was used to encode it. An example of the way cryptography is performed today is through the Rivest, Shamir, and Adleman (RSA) encryption-decryption algorithm [1]. In RSA, when two parties want to communicate securely, they use two keys, a private key and a public key. The sender encrypts the private message using a public key and transmits the encrypted message through a public channel to the receiver. The receiver uses the private key in order to decode or recover the message. In order to have security, the communicating parties (users) need to find a mathematical function that is easy to perform in one direction but hard to invert. These functions are called one-way functions, an example is multiplication and factorization. It is easy to multiply two large prime numbers, however it is hard (i.e. computationally demanding) to find the prime factors of a large number. The security of the RSA algorithm, as well as other classical encryption-decryption algorithms, is based on the assumption that the eavesdropper has limited computational power and is not able to efficiently find a solution to a hard mathematical problem (e.g. finding the prime factors of a large number) within a time relevant to the security of the message. The algorithms that can only promise the security of the message under assumptions about the computational power of the eavesdropper are called computationally secure. The need for this assumption has the drawback that the the security of the private message can not be proven. If the eavesdropper has access to more computational power than assumed it is possible for her or him to find the private message in a short time. Specifically, the algorithms are always breakable provided the eavesdropper has enough computational time.

An alternative to computational security is to use an encoding-decoding algorithm for which the security of the private message is independent of the computational power that the eavesdropper has access to. These kinds of algorithms are called *information theoretic*

secure, after Shannon who in 1949 introduced the concept of information theoretic security [2]. The *one-time pad* [3] is an example of an information theoretic secure algorithm. In the one-time pad, the sender and receiver share a secret random key. The secret key is composed of a sequence of random bits and it must be as long as the message to be encrypted. The sender encodes the private message with the random secret key via the addition modulo 2 of each bit of the message with a bit of the key. The receiver, who knows the random secret key, decodes the encrypted message by adding it modulo 2 with the secret key. The security of the one-time pad was mathematically proven by Shannon [2]. If implemented correctly, the one-time pad can not be broken at any point, even if the eavesdropper has unlimited computational power. The problem with the one-time pad is that the key has to be as long as the message, random, kept secret, and it should be used only once for encryption. Without these conditions, the security of the private message can not be proven. Hence, the problem of secure communication between two parties translates into a problem of distributing random secret keys between them.

Quantum key distribution (QKD) is a proposal to solve the problem of key distribution between two distant parties. The first protocol for QKD was proposed in 1984 by Charles Bennett and Gilles Brassard[1], a protocol that is still widely used [4]. The goal of QKD is to establish a secure key between two parties, typically named Alice (the sender) and Bob (the receiver) who are communicating through a public channel. The idea behind QKD is to use quantum properties of single photons (particles of light) to distribute a secure key. These properties include the fact that the state of single photons are perturbed when they are measured and that it is not possible to create a perfect copy of them (see chapter 2). If Alice encodes information in single photons (quantum signals) and sends them to Bob, then the two parties can establish an identical and random sequence of bits that is only known to them and nobody else. This string of bits is typically simply referred to as a *secret key*. An eavesdropper can try to intercept the photons in transmission and measure them, but it

[1]The protocol is now known as BB84.

is impossible to do so without leaving a trace. The eavesdropper cannot copy the quantum signals either and therefore the security of the key in transmission is, in principle, guaranteed. The eavesdropper, or third malicious party is normally referred to as Eve. The goal of Eve is to obtain full or partial information about the key that is being distributed between Alice and Bob. If Eve obtains information about the key then she can obtain information about the private message, breaking the secure communication between Alice and Bob. Any errors (discrepancies) found in the secret key are attributed to information about the key that Eve has learned through some form of eavesdropping. Note that this means that Alice and Bob can quantify the amount of information that the eavesdropper has about the key. If the disturbance of the eavesdropper is below a specific limit, the information that Eve learned can be removed through classical post-processing to an arbitrarily small amount (see chapter 3). The possibility to verify the security of the key before it is used for encoding is a feature of QKD and is not possible with any classical protocol.

1.2 Background

The first implementation of QKD took place in 1989 and it was demonstrated by Bennett and coworkers [5]. In the first demonstration, Alice and Bob were separated by only 30 cm, a distance that cannot be considered practical for any real-world implementation. Despite all the work done on QKD up to this point, the physics community remained isolated from the results obtained since these were not presented in physics conferences or physics journals. In 1991 A. K. Ekert proposed independently QKD [6], triggering the interest on QKD in the physics community. The proposal by Ekert made use of entangled photons to perform QKD. A source sends pairs of entangled photons to Alice and Bob. Each party measures the photon received. Some of the photons are used to obtain a secret key, the rest of them are used to perform a test (Bell inequality test). If the result of the test shows that there are quantum correlations between the particles then Alice and Bob know that the photons used

to obtain the key could not have been disturbed by eavesdropping. The eavesdropper does not know which photons will be used to perform the test or to obtain the key as a result she cannot measure the photons without being discovered by Alice and Bob. Since then two approaches to implement QKD have developed, entanglement based QKD following the proposal by Ekert and prepare-and-measure QKD according to the proposal by Bennett and Brassard. Later on it was proven that both protocols are actually equivalent [7].

It is important to note that the protocols developed for QKD are noise and loss tolerant. This means that a failure of the protocol will not be declared solely due to the inevitable noise or loss of the communication channels. The resistance to loss is achieved by having Bob announce to Alice which photons were measured and which ones were not. Noise tolerance is achieved through the implementation of error correction protocols, just as in classical communication systems. We will see later on that noise and loss tolerance are not always straightforward to obtain, for example, this is the case in other cryptographic protocols in which Alice and Bob are not cooperating. However, noise and loss tolerance are properties that are needed in any protocol that intends to be implemented in the real world. The experimental demonstration of QKD from 1989 motivated further research to perform QKD over longer distances to demonstrate its practicality. The first QKD demonstration over a real world link was in 1995 [8] and more implementations of QKD followed. At the same time, developments of rigorous mathematical security proofs of QKD started to appear in the literature. In 2000, the first proposal of a hacking attack that took advantage of loopholes in some QKD implementations appeared [9]. The attack exploited the fact that perfect single photons are rarely implemented, and instead optical pulses that have a very low probability of having more than one photon are used. However, whenever there is more than one photon, it is possible for the eavesdropper to "steal" one of the photons in the optical pulse and measure it without leaving a trace for Alice and Bob. The proposal of this attack highlighted the importance of, first, the need for a close collaboration between the experimental and theory

communities of quantum communication and, second, the development of security proofs with realistic assumptions.

1.3 QKD implementations

The development of QKD has lead to different kind of encodings and protocols [10, 11]. There are also commercial QKD systems [12, 13, 14] which are capable of distributing key over a distance of ∼100 km. Newer protocols are designed to avoid as many assumptions as possible about implementations. This provides higher security. At the same time efforts to extend achievable distances and secret key rates are made both theoretically and experimentally. QKD can be implemented using an optical fiber as a quantum channel or through free space. This thesis will focus on implementations in optical fiber. Innovative QKD implementations focus on having the following characteristics:

1. High secret key rates.
2. Straightforward integration of QKD systems into existing infrastructure of communication networks.
3. Secure implementations. Loopholes in the implementation should be known or avoided.
4. The secret key can be distributed for long distances (100 km -300 km)

In this thesis we address points 1, 2 and 3 for QKD implementations in a real world environment. We also address experimentally the possibility of improving other cryptographic protocols with quantum mechanics.

The need for high secret key rates becomes evident when one recalls that, in the one-time pad, the length of the secret key must be the same as the length of the private message that needs to be transmitted. Ideally, key rates in QKD should match bit rates in existing

communication systems (10-100 gigabits per second). So far, secret key rates in QKD are limited by hardware, specifically by single photon detectors, and channel loss. However, one must also foresee potential bottlenecks in QKD systems originating at various steps of the key distribution process. This requires studies that analyze the performance of a QKD system at different stages of the secret key distribution procedure. An analysis of the scalability of secret keys is presented in chapter 5. This analysis is done to optimize the entire key distribution process and to locate bottlenecks that can originate in high speeds systems.

In addition to commercial systems, there have also been several demonstrations of quantum networks [15, 16, 17, 18] over dedicated fiber links. A quantum network consists of dedicated optical fibers that interconnect individual parties, each with a QKD system. In order to distribute a private message between two parties of the network, current quantum networks establish pairwise secret keys, used to encode, decode, and again encode a message while being transmitted from one node to the next. These networks work under the assumption that every party involved in the network can be trusted as they have full access to the message. However, for some applications, the assumption of trusted parties in quantum networks may not be acceptable. Additionally, the economical expense required to have dedicated optical fibers make mandatory the use of existing optical networks. In order to integrate QKD into existing optical fiber networks we study tools that can be added to QKD systems in order to facilitate this integration (see chapter 4). The tools also include the capability to control parameters relevant in a network scenario. Additionally, the possibility of all-optical routing of quantum information is explored to avoid assumptions about trusted parties.

Implementations of QKD must be studied thoroughly before claiming information theoretic security. In particular, one must locate loopholes of security due to experimental imperfections or side-channels through which information about the key is leaked. An example of a side-channel is the occurrence of multiple photons (hence forward referred to as

"multi-photon" pulses) in attenuated pulses emitted by a laser, a commonly used source in QKD[2]. Multi-photon pulses can be exploited by Eve by intercepting one of the photons and extracting information about the key [9]. Another example is the optical access that Eve can have to Alice's and Bob's laboratory through the quantum channel that connects them. Nothing prevents Eve from sending signals into their laboratories and the devices used in the implementation [19, 20]. The eavesdropper can gain information about the key through the back reflected light. It is therefore important to develop protocols that exclude side-channels based on fundamental physical laws. A recently proposed protocol takes advantage of entangling measurements, or Bell state measurements (see chapter 2) in order to distribute a secret key. The benefit of this protocol is that detector side channels are automatically closed, if they are operated by the eavesdropper. The implementation of this protocol over deployed fiber is presented in chapter 6.

The extensive work on QKD has been proven successful, both theoretically and experimentally. While QKD between two parties has received by far the most attention, there are other kinds of cryptographic protocols that are also commonly employed for secure communication. An interesting question is whether other cryptographic protocols can also benefit from quantum mechanics. This question is addressed in chapter 8 for private queries, an application of the cryptographic primitive known as oblivious transfer. In oblivious transfer, Bob wants to learn a bit from a collection of bits in Alice's possession. However, Bob does not want to reveal which bit he is interested in and at the same time, Alice does not want to reveal the entirety of the bits in her possession. In chapter 8 we present the implementation of quantum private queries over deployed fiber. This required the development and implementation of error correction to fulfill the requirements of noise and loss tolerance of cryptographic protocols implemented in the real world.

[2]Attenuated laser pulses are commonly used in QKD implementations to replace single photon sources.

1.4 This thesis

The application of quantum physics in areas such as cryptography can be beneficial, since innovative or improved protocols can be developed. In particular, for key distribution the use of quantum mechanics brings the possibility of having information theoretic secure protocols that are also possible to implement with current technology. The development of QKD systems that are capable of working optimally over real world conditions is necessary. Furthermore, the study and implementation of other cryptographic protocols assisted by quantum mechanics is a natural extension of the field. The implementation of cryptographic protocols like quantum private queries over the real world is necessary to trigger the development of security proofs for this protocol, as it has been shown that improved performance can be achieved when quantum systems are employed.

This thesis is concerned with real world implementations of QKD systems and quantum private queries. In order to have a better understanding of this work I give a brief introduction to quantum mechanics and QKD in chapters 2 and 3, respectively. The QKD systems are used to study the tools that can be developed to integrate QKD in existing networks (chapter 4) and locate potential restrictions that will limit key rates in high speed systems when improved technology is available (chapter 5). A new QKD protocol called measurement-device independent QKD was demonstrated as well (chapter 6). This protocol requires the implementation of a Bell-state measurement, which was implemented for the first time over deployed fiber. The possibility for a highly efficient Bell state measurement is studied in chapter 7. Finally I present the first implementation of quantum private queries over deployed fiber in chapter 8. The thesis is also supplemented with appendices. Appendix A gives a detailed description of the error correction protocol used throughout this thesis. Appendix B gives a brief description of two of the most important security proofs developed for QKD. Appendix C describes in detail the applications of quantum communication that employ Bell state measurements. Appendix D contains the supplementary material of the

implementation of the measurement-device independent QKD system (chapter 6). Finally, appendix E contains the supplementary information to the quantum private queries work (chapter 8).

The work contained within this thesis was done in collaboration with: Xiaofan Mo, Philip Chan, Allison Rubenok, Josh Slater and Raju Valivarthi. I always participated in the measurement process and setup of experiments however; my specific contributions are adressed in the following chapters, in which these developments are described using published paper supplemented by short introductions.

Chapter 2

Elements of quantum cryptography

In this chapter I introduce some of the fundamental quantum concepts used in QKD. For more complete discussions refer to [10, 11, 21].

2.1 Introduction

The classical unit of information is the bit, it can take the values 0 or 1 and it can be identified with the state of a classical system ("on-of"). In the quantum counterpart the unit of information is the quantum bit or *qubit*. A qubit can be implemented using a two-level quantum system; that is to say a system described by two orthogonal basis states. In mathematical terms, the state of a qubit is a normalized vector in a two-dimensional complex vector space with an inner product $\langle\psi|\psi\rangle = 1$. Unlike classical bits, qubits can also be in a *linear superposition* of the basis states: $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where α and β are complex numbers that satisfy $|\alpha|^2 + |\beta|^2 = 1$

Qubit states can be represented graphically by vectors on what is known as a Bloch sphere, see figure 2.1. The convention is to represent the states $|0\rangle$ and $|1\rangle$ in the poles of the sphere. In this representation any states lying on opposite sides of the sphere are orthogonal and form a basis. Any point on the surface of the sphere, i.e. vector length of 1, corresponds to a *pure state*. The coefficients α and β of a general qubit state can be parametrized as $cos(\theta/2) \equiv \alpha$ and $e^{i\phi}sin(\theta/2) \equiv \beta$,

$$|\psi\rangle = cos\Big(\frac{\theta}{2}\Big)\,|0\rangle + e^{i\phi}sin\Big(\frac{\theta}{2}\Big)\,|1\rangle\,. \tag{2.1}$$

The states for which $|\alpha| = 1/\sqrt{2}$ and $|\beta| = 1/\sqrt{2}$ lie on the equator of the sphere.

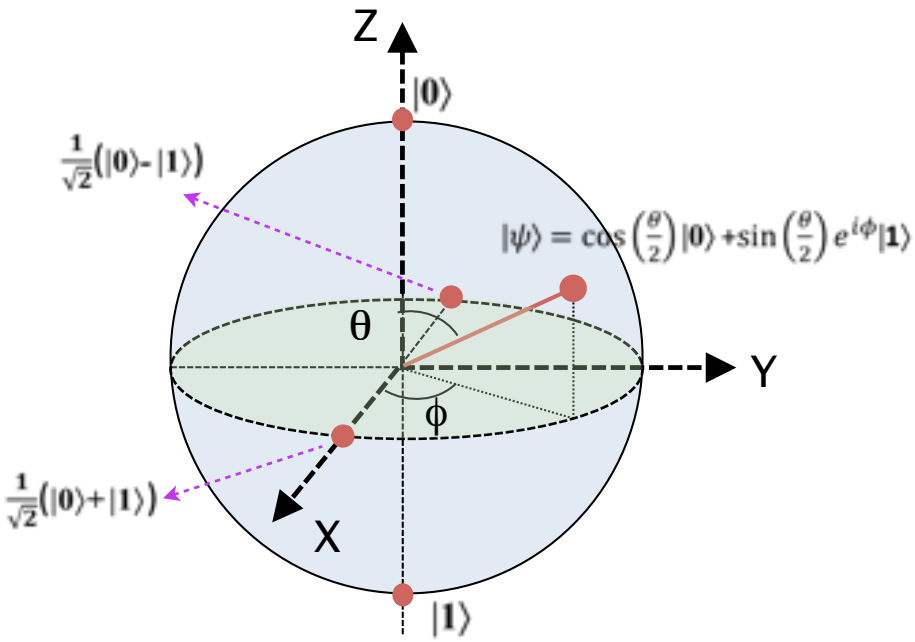

Figure 2.1: Representation of a qubit on a Bloch sphere. An arbitrary qubit $|\psi\rangle$ is represented by a point on the sphere defined by the angled θ and ϕ. The states $|0\rangle$ and $|1\rangle$ are represented on the poles of the sphere. The states $(|0\rangle + |1\rangle)/2$ and $(|0\rangle - |1\rangle)/2$ lie on the equator of the sphere, specifically on the X axis of the sphere.

2.2 Qubit preparation

There are different ways to create qubits. Any degree of freedom belonging to a two-level quantum system can be used. The most relevant to this thesis are photons, which give rise to the so-called photonic qubits. Different degrees of freedom of the photon can be used to encode information, in this thesis we restrict ourselves to polarization and timing of the photon, to form polarization and time-bin qubits respectively.

When using polarization, the two orthogonal basis states are $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$ where H and V refer to the horizontal and vertical polarization of the photon, respectively. Moreover, a pair of linear superpositions of the basis states are defined, for example, by the diagonal polarization states:

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \tag{2.2}$$

and

$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle), \tag{2.3}$$

in which the states $|+\rangle$ and $|-\rangle$ also form a basis.

In the case of time-bin qubits, the orthogonal basis states are $|e\rangle \equiv |0\rangle$ and $|l\rangle \equiv |1\rangle$, where e and l label the creation time of the photon '*early*' or '*late*'. If the time separation between early and late states is longer than the coherence time of the photon then the two different time windows, or time-bins, are well defined. If the photon is in a coherent superposition of the two temporal $|e\rangle$ and $|l\rangle$ modes we can obtain the superposition states:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|e\rangle + |l\rangle), \\ |-\rangle &= \frac{1}{\sqrt{2}}(|e\rangle - |l\rangle). \end{aligned} \tag{2.4}$$

2.3 Qubit measurement

Another difference between bits and qubits is the measurement process and result. When a classical bit is measured it outputs one of two values, '0' or '1', according to the value that the bit has.

A measurement on a qubit is different since measuring a qubit is only an attempt to determine its state. When a quantum state $|\psi_i\rangle$ is measured, its state is projected (projection measurement) onto the subspace $|m\rangle\langle m|$, where $|m\rangle$ is a label of the possible results of the measurement. The probability of projecting onto $|m\rangle$ is given by:

$$p = |\langle m|\psi_i\rangle|^2. \tag{2.5}$$

This means that the result of the measurement depends on the basis chosen to measure the qubit. For example if the state to be measured is $|\psi\rangle = |0\rangle$ and we measure it in the basis $\{|0\rangle, |1\rangle\}$ then it is projected onto the state $|0\rangle$ 100% of the time. However, if the state to be measured is $|\psi\rangle = |0\rangle$ and we measure it in the basis $\{|+\rangle, |-\rangle\}$ then it is projected onto the state $|+\rangle$ only with probability $p = |1/\sqrt{2}|^2 = 50\%$. Note that, when the basis states

are $|+\rangle$ and $|-\rangle$, then the state $|0\rangle$ can be expressed $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$. In quantum mechanics a measurement on a qubit disturbs or modifies its state and the quantum state resulting from the measurement is the new state after the measurement.

Bennet and Brassard realized that they could use this fundamental property of quantum states for cryptographic purposes. If the eavesdropper tries to obtain information about the qubits while they are in transmission she must measure them. However, when performing the measurement she changes the quantum state if the basis she chooses to measure is not the same in which the qubit was prepared in, leaving a trace or creating an error that Alice and Bob can detect. In addition, it is fundamentally impossible for Eve to measure a single qubit in two different bases simultaneously.

2.4 Entanglement

If one considers two bits, then the four possible states of the bits are 00, 01, 10 and 11.

In the case of two qubits, the quantum state of the two independent qubits A and B is represented as:

$$|\psi_A\rangle \otimes |\psi_B\rangle \equiv |\psi_A\psi_B\rangle\,. \tag{2.6}$$

As they are separable, these states are known as product states. When each of the quantum states are a superposition of two orthogonal basis states, the product is written as:

$$\begin{aligned} |\psi_A\psi_B\rangle &= (m\,|0_A\rangle + n\,|1_A\rangle) \otimes (m'\,|0_B\rangle + n'\,|1_B\rangle) \\ &= M\,|0_A0_B\rangle + N\,|0_A1_B\rangle + P\,|1_A0_B\rangle + Q\,|1_A1_B\rangle\,, \end{aligned} \tag{2.7}$$

in which the coefficients M, N, P, Q are given by the multiplications mm', mn', nm' and nn' respectively. The states $|0_A0_B\rangle$, $|0_A1_B\rangle$, $|1_A0_B\rangle$, $|1_A1_B\rangle$ form a basis for two-qubit states.

However, there are two-qubit states states that cannot be written as a product state of their individual systems. An example of this kind of states is the following:

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle). \tag{2.8}$$

When the quantum state shown above is measured, the value obtained from the measurement on one particle is correlated to the value of the measurement obtained on the second particle. The outcome of the first measurement is completely random, however the outcome of the second is always correlated. These are known as quantum correlations. As an example, if one of the bits is measured in the basis $\{|0\rangle, |1\rangle\}$, the measurement outcome can be $|1\rangle$ with probability 1/2 or $|0\rangle$ with probability 1/2. When the second particle is measured, the outcome value is completely correlated.

Quantum states that cannot be written as a product state of their individual systems are entangled states. An important set of two-qubit entangled states are the Bell states:

$$\begin{aligned} \left|\phi^+\right\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\ \left|\phi^-\right\rangle &= (|00\rangle - |11\rangle)/\sqrt{2} \\ \left|\psi^+\right\rangle &= (|01\rangle + |10\rangle)/\sqrt{2} \\ \left|\psi^+\right\rangle &= (|01\rangle - |10\rangle)/\sqrt{2}. \end{aligned} \tag{2.9}$$

There are relevant facts about Bell states: 1) Bell states form a basis for two-qubit states. 2) Bell states show quantum correlations, as explained for equation 2.8. Quantum correlations can be used to establish a secret key between two distant parties, as proposed by Ekert [6]. It is possible to perform measurements that project the state of two qubits into a Bell state, i.e. entangling of two photons. These are called Bell measurements, see chapter 7.

Entangled states play an important role in quantum communication as they have useful applications that cannot be reproduced with classical systems, including quantum teleportation and entanglement swapping, see appendix C.

2.5 No-cloning theorem

An important property of quantum states is that they cannot be cloned (or copied). To demonstrate this property assume we have an unknown qubit $|\psi\rangle$ that we want to copy onto

a second qubit with initial pure state $|0\rangle$. The initial state of the two qubits is: $|\psi\rangle \otimes |0\rangle$. Let U_c denote the unitary operator performing the cloning

$$U_c(|\psi\rangle \otimes |0\rangle) \rightarrow |\psi\rangle \otimes |\psi\rangle \,. \tag{2.10}$$

The same holds for an orthogonal quantum state $|\phi\rangle$:

$$U_c(|\phi\rangle \otimes |0\rangle) \rightarrow |\phi\rangle \otimes |\phi\rangle \,. \tag{2.11}$$

However, if the state we want to copy is an arbitrary superposition of $|\psi\rangle$ and $|\phi\rangle$, such as $\alpha\,|\psi\rangle + \beta\,|\phi\rangle$, from the linearity of quantum mechanics we will obtain:

$$\begin{aligned} U_c((\alpha\,|\psi\rangle + \beta\,|\phi\rangle) \otimes |0\rangle) &= \alpha U_c(|\psi\rangle \otimes |0\rangle) + \beta U_c(|\phi\rangle \otimes |0\rangle) \\ &= \alpha\,|\psi\rangle \otimes |\psi\rangle + \beta\,|\phi\rangle \otimes |\phi\rangle \end{aligned} \tag{2.12}$$

Which differs from the desired result:

$$U_c((\alpha\,|\psi\rangle + \beta\,|\phi\rangle) \otimes |0\rangle) \rightarrow (\alpha\,|\psi\rangle + \beta\,|\phi\rangle) \otimes (\alpha\,|\psi\rangle + \beta\,|\phi\rangle). \tag{2.13}$$

The no-cloning theorem states that it is impossible to create a perfect copy of an uknown quantum state. The no-cloning theorem, in combination with quantum measurements underpins the security of QKD.

2.6 Shannon entropy

Finally, I would also like to give a brief introduction to some concepts introduced by Claude Shannon in 1948 regarding information[1] [23]. The theory developed by Shannon has many applications, including secure communication, one of the goals of QKD. The key step taken by Shannon was to mathematically define information. He was interested in several questions: What is information? How do we measure information? How can we efficiently encode information? Can we send information in a reliable way over a noisy channel?

[1] The following paragraphs follow [22] closely.

Information is related to the amount of uncertainty in a situation of choice. Shannon used entropy as a measure of information and expressed the result of the measurement in bits. A bit is defined as the average amount of information that is obtained when tossing a fair coin. Information is quantified using random variables that describe the situation of choice. A discrete random variable is composed of a finite set of elements or symbols x that take value from the set X. Each value x is taken with probabilities $p(X = x) \equiv p(x)$. The elements $p(x)$ of the probability distribution satisfy $p(x) \geq 0 \ \forall x$ and $\sum_x p(x) = 1$. For example, the outcome of a fair coin toss can be $X = \{heads, tails\}$. The outcomes occur with probabilities $p(heads) = p(tails) = 1/2$. Information is additive. This means that the information obtained from two independent random variables is the sum of the information obtained from each random variable. If the probability distribution is not uniform, then the information received from each outcome is different. The information learned from knowing the outcome x is $-log_2 p(x)$ bits. Shannon entropy (or entropy) is the average information given by

$$h(X) = -\sum_i p(x_i) log_2 p(x_i). \tag{2.14}$$

If $p = 1/2$ then $h(X) = 1$ bit, if $p = 0, 1$ then $h(X) = 0$ bits.

The first application of entropy is the possibility to model information sources using random variables. In this case a set of outcomes is associated with a probability distribution. If a source outputs bit strings with nonuniform distribution of 1s and 0s, the messages can be compressed to shorter strings without loosing information. Shannon's channel coding theorem states that the maximum compression of a random variable X is given by the entropy $h(X)$.

In many situations, relationships between random variables are of interest. For example, in the context of QKD, what can we say about the message by seeing the encoded message. In this case we use the joint entropy $h(X, Y)$ of a pair of random variables X and Y with a

joint probability distribution $p(x, y)$. The joint entropy is defined as

$$h(X, Y) = -\sum_x \sum_y p(x, y) log(p(x, y)). \tag{2.15}$$

The joint entropy satisfies $h(X, Y) \leq h(X) + h(Y)$ with the equality only holding for independent variables.

It is possible to also define a conditional entropy, which express the lack of knowledge on X provided we know Y averaged over all possible realizations of Y:

$$\begin{aligned} h(X|Y) &= -\sum_x p(x) h(Y|X) \\ &= -\sum_x p(x) \sum_y p(y|x) log(p(y|x)) \\ &= -\sum_x \sum_y p(x, y) log(p(y|x)). \end{aligned} \tag{2.16}$$

The conditional entropy can be used to describe a binary symmetric channel in which the input and output sets are $\{0, 1\}$. This kind of channel is used to model a noisy channel, see appendix A.

Finally, we can describe the mutual information. Let X and Y be two random variables with join probability distribution $p(x, y)$. The information that Y gives about X is:

$$I(X : Y) = h(X) - h(X|Y), \tag{2.17}$$

if $I(X : Y) > 0$, the two variables X and Y are at least partially correlated and knowing (or measuring) one yields information about the other. Similarly, the information that X gives about Y is $I(Y : X) = h(Y) - h(Y|X)$. The mutual information measures the average reduction in uncertainty about X that results from learning the value of Y or vice versa, the average amount of information that X conveys about Y. Note that if X and Y are independent then $h(X|Y) = h(X)$ and $I(X : Y) = 0$, that is Y does not give any information about X. Shannon found that it is possible to reliably send information over noisy channels. The communication is possible if error correction protocols are implemented, in which the

rate of additional amount of information needed for correction is given by $h(Y|X)$. This rate is relevant for Alice and Bob as the quantum channel is a noisy channel and error correction mechanisms must be implemented at some point of the key distribution process, see chapter 3.

All the elements introduced so far are used in QKD and other cryptographic protocols. In the following chapter I will introduce QKD and highlight how the quantum properties introduced in this chapter are used to obtain information theoretic security.

Chapter 3

Quantum key distribution

Quantum bits can be implemented in two-level systems including ions, atoms, or photons. However, the advantages of photons over the other systems are easy to identify. First, photons do not interact with matter easily, hence it is possible to use optical fibers that present high transmission (very low loss) for long distances. Photons are easy to manipulate because there are many existing communication elements used to produce and control light. These communication elements are low cost, robust and reliable, and perfect to implement QKD. Finally, an extensive network of optical fiber is already deployed throughout the world.

There are also elements of QKD that are critical and hence common to every implementation, regardless of the protocol or encoding chosen. In the following paragraphs I will present the common elements to QKD implementations needed to obtain a secret key. I will also describe a hacking attack that exploits a loophole common to most of reported implementations and two possible solutions to the attack.

3.1 Assumptions

There are some assumptions made by Alice and Bob for secure key distribution [24]. I have only listed the common assumptions in QKD systems as specific implementations may differ on the assumptions made depending on the protocol implemented.

- The eavesdropper is restricted by quantum physics.
- Alice's and Bob's laboratories are perfectly isolated. This means that only information that is intended to leave the laboratory does so.
- Alice and Bob have access to trusted sources of random number generators.

- Alice and Bob share an authenticated classical channel (see section 3.3). This means that the messages transmitted through the classical channel cannot be changed by the eavesdropper without Alice and Bob noticing so.

- The devices at Alice and Bob have no internal memory. This means that there is no correlation between different uses of the devices.

3.2 Quantum and classical channel

Since Alice and Bob want to communicate, a communication channel between them is necessary. They share a public quantum channel through which quantum signals can be transmitted (e.g. an optical fiber or free space). The eavesdropper can modify or tamper with the signals transmitted through this channel. However, Alice and Bob can also exchange classical communication through a second public channel called a *classical channel*. This channel has been authenticated, see section 3.3. An eavesdropper can listen to the information transmitted through the classical channel but cannot change the signals sent through it without being noticed by Alice and Bob.

3.3 Authentication

QKD requires Alice and Bob to authenticate all communication taking place through the classical channel. This communication includes the process of sifting, error correction, and privacy amplification, explained in section 3.5. To do authentication they must share a small secret key before implementing QKD. For this reason QKD is sometimes referred to as quantum key growing. The small amount of secret key could initially be established by meeting personally, or formed by a small portion of a previous key distribution session between Alice and Bob.

Authentication is well studied in classical cryptography and it can be performed in an

information theoretic secure form. In order to do authentication, Alice and Bob use the shared secret key to choose a *hash function*, g, from a family of hash functions. Hash functions are used in order to map their message to the authenticated shorter secret message known as a *tag*. The tag is computed as $T = g_K(m)$, in which m is the message to be authenticated and K is the initial secret key. Alice sends to Bob a composite message $M = (m, T)$. Bob obtains the information and computes his own tag with the message received by Alice. If Eve tampered with the communication the tag that Bob obtains from his computation will be different. When performing authentication, if Alice receives the correct tag from Bob and vice versa, then they know that the eavesdropper has not changed the message.

3.4 Qubit exchange

Once a quantum channel has been established, Alice sends her qubits to Bob. In the following paragraphs I describe the BB84 protocol, however any QKD protocol can be implemented at this stage. The BB84 protocol uses four different quantum states belonging to two mutually unbiased bases and encoded into individual photons. Mutually unbiased bases are bases chosen such that the inner product between any two basis states belonging to different bases is the same. The quantum basis states used can be: $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, in which $|\pm\rangle = (|0\rangle \pm |1\rangle)/2$. The quantum states $|0\rangle, |+\rangle$ are associated to the bit value '0' and the states $|1\rangle, |-\rangle$ are associated to the bit value '1'. Alice randomly selects one of the four states and sends it to Bob, keeping a record of the qubit emitted. Upon receiving the qubit, Bob must randomly select one of the two bases to measure the state. That is, he must choose between distinguishing states $|0\rangle$ and $|1\rangle$ or $|+\rangle$ and $|-\rangle$. It is fundamentally impossible to make a measurement that can distinguish all four states. Next, Bob announces to Alice via the classical channel which of the emitted photons he detected. Alice discards all bits that are associated to the photons that Bob did not detect. At this stage, Alice and Bob share a

string of bits known as a *raw key.*

3.5 Post-processing

In the next step, Alice and Bob must communicate through the classical channel to compare their choice of basis preparation and basis measurement for each qubit. Alice and Bob discard all the events of the key that originate from having chosen different basis to prepare and measure the qubits as there will be no correlation between their bit values for these cases. This process is known as *sifting* and at the end of it Alice and Bob have strings of bits which can be expressed as vectors $\vec{\alpha}$ and $\vec{\beta}$, called *sifted key.* Only the events in which their basis choices coincide can lead to strings for which they know each of the bit values are the same.

After the sifting process Alice's and Bob's key strings should be completely correlated, i.e. contain identical bit values. However, either due to eavesdropping or noise there will be errors, and Alice and Bob must execute classical error correction, to reconcile their data. Note that for security purposes, all errors are attributed to Eve and determine her information about the key. In order to perform error correction, Alice and Bob must exchange additional information about their bit strings through the classical channel. For detailed information about the error correction procedure refer to appendix A.

At the end of error correction Alice and Bob share an error-free key that is a string of random bits. However, the additional information sent over the classical channel in order to perform error correction could be used by Eve to obtain information about the key. For this reason it is necessary for Alice and Bob to reduce their key to a secret key via privacy amplification. Using the same family of 2-universal hash functions used in channel authentication, Alice and Bob use a hash function to compress the error free key. By compressing the key, the information that the eavesdropper knows about the key is reduced to an arbitrarily small amount of information. 2-universal means that the probability that two different strings x_1

and x_2 (e.g. Alice's key and Eve's key respectively) have the same value is one over the number of possible key strings. For a 1000 bit key, the probability is 2^{-1000}.

Once privacy amplification is performed Alice and Bob share a string of completely correlated bits that is known only to them. The secret key can then be used for one-time pad encryption.

3.6 Photon number splitting attack and countermeasures

As the secret key generation rate is a key figure of QKD implementations, attenuated laser pulses are typically employed. This is done to overcome the low generation rates of single photon sources. The attenuated laser pulses used in QKD systems have mean photon numbers less than 1. These attenuated laser pulses are weak coherent pulses with randomized phase and are described by the Poissonian distribution

$$P_\mu(n) = \sum_n \frac{e^{-\mu}\mu^n}{n!}, \tag{3.1}$$

in which n indicates the photon number and μ indicates the mean photon number. As can be seen from equation 3.1 there is a non-zero probability of obtaining pulses that contain multi-photons. These multi-photon events can be exploited by an eavesdropper to perform a photon number splitting attack [9]. In this attack Eve measures the number of photons in the optical pulse.If the optical pulse only contains one photon then Eve blocks it. If the optical pulse contains more than one photon, then the eavesdropper keeps one of the photons and sends the rest to Bob. The eavesdropper can keep the "stolen" qubits until post-processing, during which she can listen to the communication between Alice and Bob. Eve learns the basis choice for each qubit and performs the respective measurements on the qubits she has, therefore learning all the information about the key without being caught.

3.6.1 Decoy states

The photon number splitting attack reveals why multi-photon events are not secure for QKD. Alice and Bob must obtain the secret key from single photons only as the eavesdropper cannot split them or eavesdrop on them without leaving a trace. The decoy state protocol [25, 26, 27] allows to identify, in an efficient way, how much key originates from individual photons and their associated error rate, needed to quantify the security of the key as shown in the paragraphs below and appendix B.

Alice, who has the source, must produce optical pulses for which she randomly chooses different mean photon numbers, e.g. μ, ν_1, ν_2. The change of mean photon number can be implemented with an optical attenuator. The optical pulses emitted by Alice belong to different Poissonian distributions $(P_\mu(n), P_{\nu 1}(n), P_{\nu 2}(n))$, depending on the mean photon number chosen. After the transmission of all the optical pulses has taken place, Alice and Bob communicate to sort the sifted key bits according to the mean photon number they belong to. For a given Poissonian distribution, the probability that Alice emits a pulse with n photons and Bob detects it is:

$$Q_n = Y_n \frac{\mu^n e^{-\mu}}{n!}, \tag{3.2}$$

and the sum over all the Q_n is known as the gain and it is given by:

$$\begin{aligned} Q_\mu &= \sum_n^\infty Y_n \frac{\mu^n e^{-\mu}}{n!}, \\ &= \sum_n^\infty Y_n P_\mu(n). \end{aligned} \tag{3.3}$$

In equations 3.2 and 3.3 the term Y_n is the conditional probability that Bob detects the pulse provided the source emitted n photons. The point of the decoy state protocol is that this conditional probability, Y_n is the same for any optical pulses belonging to any of the Poissonian distributions, that is, it is independent of the mean photon number chosen by Alice:

$$Y_n(\mu) = Y_n(\nu_1) = Y_n(\nu_2). \tag{3.4}$$

When the eavesdropper intercepts a pulse, she can obtain the number of photons in the pulse, however she cannot know which Poissonian distribution the pulse belongs to. This is important as for each mean photon number we have an equation like 3.3. The quantities Q_μ, Q_{ν_1} and Q_{ν_2} are measured, and P_μ, P_{ν_1}, P_{ν_2} are chosen by Alice, the only parameter left open is Y_n. Since there are three different mean photon numbers, we can write the following system of equations:

$$\begin{aligned} Q_\mu e^\mu &= Y_0 + \mu Y_1 + \frac{\mu^2 Y_2}{2!} + \frac{\mu^3 Y_3}{3!} + ..., \\ Q_{\nu_1} e^{\nu_1} &= Y_0 + \nu_1 Y_1 + \frac{\nu_1^2 Y_2}{2!} + \frac{\nu_1^3 Y_3}{3!} + ..., \\ Q_{\nu_2} e^{\nu_2} &= Y_0 + \nu_2 Y_1 + \frac{\nu_2^2 Y_2}{2!} + \frac{\nu_2^3 Y_3}{3!} + ... \end{aligned} \tag{3.5}$$

As stated in paragraphs above, optical pulses that contain more than one photon are insecure. Only pulses that contain single photons should be used to distill a secret key. Therefore it is possible to find the value Y_1 from the system of equations 3.5. The work by H.-K. Lo and cooworkers [27] proved that it is enough to implement two decoy states (ν_1, ν_0) in addition to the signals states (μ) to find an efficient lower bound of Y_1.

A similar analysis can be performed to find the upper bound of the error rate of single photon events using:

$$e_\mu = \sum P_\mu(n) Y_n e_n, \tag{3.6}$$

in which e_μ is the error rate measured by Alice and Bob for the optical pulses with mean photon number μ, and e_n is the error rate for n-photon signals.

The secret key generation rate for a QKD system implementing the BB84 protocol is given by equation [28]:

$$S = Q_1[1 - h_2(e_1)] - Q_\mu h_2(e_\mu). \tag{3.7}$$

Alice and Bob can measure Q_μ and e_μ, H_2 is the Shannon entropy, and through the decoy state protocol they can lower bound Q_1 and upper bound e_1, leading to a secure bound of the secret key generation rate.

3.6.2 SARG protocol

There is an alternative solution to the photon number splitting attack. The solution consists of implementing a different QKD protocol called SARG [29]. The SARG protocol assumes the implementation of QKD with weak coherent pulses. It employs the BB84 states, however, the difference stands in the association of states and bits. In this case Alice encodes the bit value in the basis rather than in the quantum state: the Z basis ($\{|0\rangle, |1\rangle\}$) corresponds to bit 0 and X basis ($\{|+\rangle, |-\rangle\}$) corresponds to bit 1. Therefore, the two values of a classical bit are encoded into pairs of non-orthogonal states, which are not possible to unambiguously discriminate. Bob chooses to measure between the two bases with probability 1/2, exactly as in the BB84 protocol. In BB84, during the sifting procedure Alice announces what basis she used to encode the quantum state. In the SARG protocol the basis are kept secret as they are associated to a bit value. Instead, Alice announces two states: the state she emitted and one of the states belonging to the other basis, and does so in random order. Bob can determine which state was sent by Alice only if he measures an orthogonal state to the ones announced by Alice, as a projection onto this state discards perfectly one of the states announced. For example, assume Alice emits the state $|0\rangle$ and announces $\{|-\rangle, |0\rangle\}$. If Bob chooses to measure in the X basis and obtains as a result $|+\rangle$ then he knows Alice could not have sent the state $|-\rangle$, and therefore concludes that Alice sent the state $|0\rangle$. Eve can implement a photon number splitting attack and obtain a photon from multi-photon pulses. However, the states that Alice announces are non-orthogonal and Eve cannot unambiguously distinguish what state was sent. Although the SARG protocol was initially intended to overcome the photon number splitting attack, in this thesis it was used to implement quantum private queries, see chapter 8. The remaining of the thesis is composed of the published papers about implementations of QKD and quantum private queries. The concepts presented in chapter 2 and this chapter are use throughout the rest of this thesis.

Chapter 4

Implementation of quantum frames in a QKD system

Since its proposal, quantum key distribution (QKD) has been subject of vast experimental and theoretical research [10, 11]. QKD systems consist of point-to-point links in which the sender (typically referred to as Alice) is directly connected to the receiver (typically referred to as Bob) through a quantum channel. Point-to-point QKD has been demonstrated up to a distance of ≈250 km over optical fiber [30] and free space for distance of 144 km [31] and some QKD systems have already been commercialized [12, 13, 14]. However, the implementation of QKD in a over dedicated point-to-point fashion links contrasts with the networks employed in the majority of current classical communications.

An important development in QKD, which started in 2003, is the integration of point-to-point QKD systems into networks, i.e. to create quantum networks, in which multiple users are interconnected and quantum information can be distributed among any pair of users. The integration of QKD systems into a quantum network requires the ability of the QKD system to communicate and control parameters that are relevant in such network setting. Examples of these control parameters are: routing information (sender and receiver identification), quantum link establishment, timing information, protocol and encoding information for interconnection of varying QKD systems, etc.

To date, several quantum networks have been demonstrated, including the cities of Boston (DARPA network) [18], Vienna (SECOQC network) [17], Hefei [16], and Tokyo [15]. The quantum networks are composed of many users interconnected via dedicated or reconfigurable point-to-point links. In a network, a link connects neighbouring locations denominated nodes. The secret key is distributed using trusted nodes or by means of optical switches that allow reconfigurable links between the users.

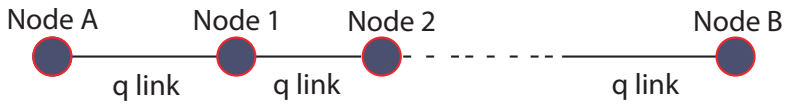

Figure 4.1: Illustration of a simplified quantum network. The distribution of a secret key from node A to node B is made in a *hop-by-hope* mode where node A encrypts the secret key using a session key (k_1) via one-time pad and sends the encrypted information to node 1 through the quantum link (q link). Node 1 decrypts the information and re-encrypts it using a second session key (k_2), and sends it to node 2. The process continues in a hop-by-hop mode until the secret key reaches node B.

The network in Vienna and Tokyo incorporated the trusted node method. The distribution of a secret key from node A to node B is performed in the following way: node A encodes the secret key, k_s, via the one time pad using a session key, k_1, and distributes the message to the adjacent node 1. Node 1 decrypts the secret key and re-encrypts it using one-time pad encryption and a second session key, k_2, and sends the encrypted key to its adjacent node. The process, typically referred to as *hop-by-hop*, continues until the secret key reaches node B. The advantage of this network scheme is the ability to distribute a secret key over an unlimited distance using existing technology. However, this scheme only works if all intermediate nodes between Alice and Bob can be trusted as they will have full information on the secret key. It is important to emphasize that in the Vienna and Tokyo networks the routing problem was solved at the software level. Once the trusted node receives the secret key, it is decrypted and transferred to dedicated hardware (e.g. PC) located in the node, where it is managed. An algorithm determines the routing path to follow. The key is then re-encrypted with another session key and sent towards the adjacent node specified by the routing algorithm.

The network in Boston [18] incorporated optical elements in its nodes that do not perform any measurement (e.g. optical switches) and instead allow the qubits to be routed from Alice to Bob. The advantage of the approach followed in the Boston network is that trusted nodes are not required. The disadvantage of this approach, however, is that the optical loss between each node limits this kind of network to metropolitan areas ($\sim$50 km). The Boston network

included 10 nodes with quantum systems, 8 of the nodes are connected with fixed links, and the other two nodes are connected through a 2×2 optical switch (optical switch with four input-output combinations). This network employed a combination of the hop-by-hop method described above and routing of optical signals via the optical switch to distribute a secret key between node A and node B.

The successful demonstration of early quantum networks is expected to lead to the development of larger quantum networks. For economical reasons, large quantum networks would take advantage of existing optical networks. These optical networks consist of optical fibers and include optical elements like switches or multiplexers that allow for routing of optical signals. The integration of QKD systems into these optical networks require routing quantum signals at the optical level, i.e. without having to send the entire key to dedicated hardware to process it and determine the path for routing. Instead, the receiver address information is dynamically communicated to the optical switch as soon as the message arrives to a node and the routing path changes according to the information received.

In this chapter we proposed a tool for existent QKD systems that will allow them to route quantum signals and communicate additional control parameters facilitating the integration of QKD systems into optical networks. I will present work we have done on developing a QKD system that is capable of, in principle, routing quantum signals. The system implements the BB84 protocol and makes use of polarization encoding and decoy states, and it operates through fiber deployed across the city of Calgary. The system features *quantum frames*, which, inspired by the Ethernet protocol, consist of alternating sequences of high-intensity pulses and faint pulses. The high-intensity pulses include classical control information and so they are labeled classical control frames. A classical control frame allows for a platform for tasks related to establishing a link for QKD in a network environment. It comprises:

- Routing information: Sender and receiver identification are encoded in the frame. It enables building a reconfigurable quantum network, where it is

possible to change the route between Alice and Bob within the network. For example, if a denial of service attack is present for a chosen path it is then possible to reroute the qubits through another path.

- Clock synchronization: timing information is included for qubit time-tagging (i.e. a time label attached to the detection of each qubit). Any timing variation due to a change in the fiber length of the quantum channel that could disrupt clock synchronization is automatically compensated because the quantum frames are transmitted through this channel.

- Channel stabilization: the quantum frames are used to implement a polarization compensation system. This compensation is needed because of time-varying birefringence in the quantum channel (fiber link between Alice and Bob) which causes polarization changes of the photons transmitted through the fiber. The polarization information is included in the quantum frames. The quantum frames are transmitted to the receiver through the quantum channel and the polarization information contained is analyzed at the receiver. The compensation system adjusts feedback mechanism according to the polarization information received in order to compensate for the changes induced by the fiber. The implementation of the compensation system using the quantum frames allow for a long-term operation of the system, as demonstrated in our work. In fact, the compensation system can be extended to other degrees of freedom and adapted for QKD systems that employ different kind of encoding [32].

Our proof-of-principle demonstration shows the suitability of quantum frames for QKD systems. We have demonstrated that our scheme facilitates the establishment of a quantum channel, allowing for timing and channel stabilization. Additionally, by implementing quantum frames, it is straightforward to add routing capabilities, bringing QKD systems closer

to network integration.

This work was done in collaboration with Xiaofan Mo and Philip Chan. Even though part of the work follows from studies done during my Masters degree, the components of the system presented here required to be characterized and a number of improvements were implemented, which was done during my PhD. I contributed to this study in the following stages: I characterized the optical components that form the system and assembled the system. I also adjusted the system for its deployment to perform measurements in a real world environment. I performed the measurements with the system presented in the manuscript. I developed the program to calculate the secret key generation rate of the system for different mean photon number and taking into account the use of decoy states. I also contributed by writing part or the entirety of sections 1-7 and 9 of the manuscript presented below.

4.1 Proof-of-concept of real-world quantum key distribution with quantum frames

I Lucio-Martinez[1], P Chan[2], X Mo[1,4], S Hosier[3] and W Tittel[1]

1.- Institute for Quantum Information Science and Department of Physics and Astronomy, University of Calgary, 2500 University Drive NW, Calgary T2N 1N4, Alberta, Canada

2.- Advanced Technology Information Processing Systems Laboratory and Department of Electrical and Computer Engineering, University of Calgary, 2500 University Drive NW, Calgary T2N 1N4, Alberta, Canada

3.- Applied Research and Innovation Services and School of Information and Communications Technologies, Southern Alberta Institute of Technology, 1301 16th Ave. NW, Calgary T2M 0L4, Alberta, Canada

Abstract

We propose a fibre-based quantum key distribution system, which employs polarization qubits encoded into faint laser pulses. As a novel feature, it allows sending of classical framing information via sequences of strong laser pulses that precede the quantum data. This allows synchronization, sender and receiver identification and compensation of time-varying birefringence in the communication channel. In addition, this method also provides a platform to communicate implementation specific information such as encoding and protocol in view of future optical quantum networks. We demonstrate in a long-term (37h) proof-of-principle study that polarization information encoded in the classical control frames can indeed be used to stabilize unwanted qubit transformation in the quantum channel. All optical elements in our setup can be operated at Gbps rates, which is a first requirement for a future system delivering secret keys at Mbps. In order to remove another bottleneck towards a high rate system, we investigate forward error correction based on low-density parity-check codes.

4.1.1 Introduction

Based on the particular properties of single quantum systems, quantum key distribution (QKD) promises cryptographic key exchange over an untrusted, authenticated public communication channel with information theoretic security [4, 33]. Significant academic [10, 11] and industrial effort [12, 13, 34] has been devoted to the development of point-to-point (P2P) QKD systems based on attenuated laser pulses or entangled photons, and the first fully functional prototype of a quantum cryptographic network consisting of pre-established P2P links in a trusted node scenario has recently been demonstrated [17] (see also [18]). Furthermore, various proof-of- principle demonstrations of quantum teleportation and quantum memory (see [35, 36] and references therein) have been reported, which will eventually allow building of fully quantum enabled networks [37, 38], e.g. for perfectly secure communication in settings with un-trusted nodes and over large distances [39, 40].

Despite these remarkable achievements, the building of a reconfigurable real-world QKD network still requires significant progress, even when limiting quantum communication to qubits encoded into faint laser pulses and to entangled qubits. Among the issues to be solved is the necessity to route quantum data from any sender to any receiver. The possibility to use active optical switches to send quantum information to different users has first been demonstrated in 2003 [41]. However, the question regarding the addition of sender and receiver addresses to the quantum data (which is not required in pre-established P2P links) has, to the best of our knowledge, never been addressed. Beyond routing, another requirement for quantum networks is path stabilization between sender and receiver, i.e. to ensure that carriers of qubits prepared at Alices arrive unperturbed at Bobs. This includes control of the properties of the quantum channel, e.g. birefringence in an optical fibre, and the establishment of a common reference frame at Alices and Bobs, e.g. a direction or a precise time-difference, depending on the property chosen to encode the qubit [42]. Current P2P QKD systems are either of the plug and play type and automatically stabilize the quantum

channel [43, 44], or achieve unperturbed quantum communication by adding from time to time short sequences of classical control information [45]. However, neither method allows communication of the properties that are important in reconfigurable networks, including sender and receiver address, or the specific QKD protocol or the type of qubit encoding chosen[1].

In this paper, we propose the use of quantum frames (Q-frames) as a flexible framework for sensing, communicating and controlling the parameters relevant in a QKD network setting. Our approach is sufficiently flexible to accommodate for current and future quantum technology or applications, including technology from different vendors, which is important in view of open quantum networks. We demonstrate the suitability of our solution for QKD with polarization qubits over a 12 km real-world fibre optic link.

This article is organized as follows: in section 4.1.2, we present the general idea of Q-frames. We then discuss the principle QKD setup (section 4.1.3), and give further details of key components (section 4.1.4). After presenting the properties of our fibre optics link (section 4.1.5), we describe the QKD field tests and discuss the results (section 4.1.6) and then elaborate briefly on some issues related to the security of the key establishment (section 4.1.7). In section 4.1.8, we present the status of our classical post processing, required to distil a secret key, specifically the possibility of hardware implementation of one-way error correction. We present our conclusions in section 4.1.9.

4.1.2 Q-frames

To add control functionalities to the communication between Alice and Bob, we propose supplementing the quantum data (e.g. qubits) with classical control frames (C-frames). The C-frames, encoded into strong laser pulses, alternate with the quantum data and a pair of

[1]Note that this information can also be sent through another (classical) channel. However, given that control information for channel stabilization has to be sent in any case (except for auto-compensating systems such as the plug and play system), it is natural to consider sending the network relevant control information through the quantum channel as well.

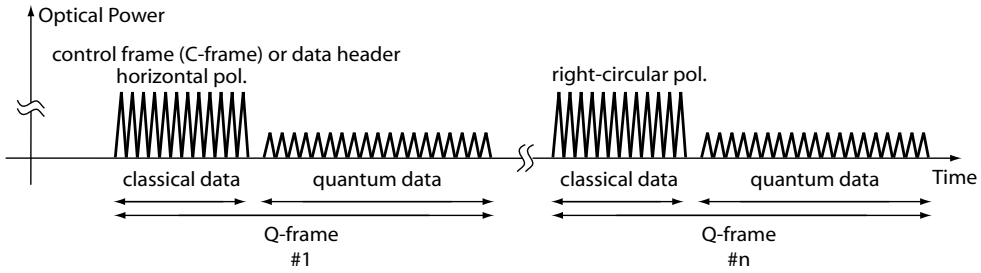

Figure 4.2: Quantum framing with alternating classical C-frames (inspired by the Ethernet protocol) and quantum data. In the here reported implementation, subsequent C-frames encode different polarization states (horizontal, vertical and circular), each one used to independently stabilize one particular set of polarization qubit basis states.

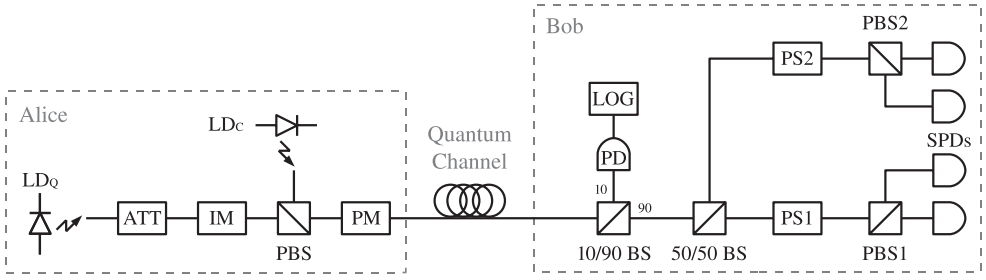

Figure 4.3: Schematic of our QKD system.

classical/quantum data forms a Q-frame (see figure 4.2). The C-frame allows synchronizing sender Alice and receiver Bob, facilitates time-tagging and provides a platform to communicate sender and receiver address (for routing or packet switching) plus implementation specific information such as encoding (e.g. polarization or time-bin qubit [42]) and protocol (e.g. BB84 [4], decoy state [25, 26, 27], or B92 [7]). This is interesting in view of open, reconfigurable networks comprising different QKD technologies.

The classical information in our implementation is encoded into specific polarization states, allowing assessment and compensation of time-varying birefringence in the quantum channel. Note that the compensation scheme can easily be adapted to other QKD setups employing e.g. time-bin qubits, entanglement, or quantum repeaters. Furthermore, the C-frames can be used to assess channel loss, which may be important for routing.

4.1.3 Our QKD system

Our QKD system is based on polarization qubits and employs the BB84 protocol [4], supplemented with two decoy states [25, 26, 27]. It allows alternating sequences of strong and faint laser pulses, encoding classical data and quantum data, respectively. A simplified schematic of the QKD system is depicted in figure 4.3. Alice uses two laser diodes to generate the classical data (LDC) and the quantum data (LDQ). The pulses emitted from LDQ are first attenuated by an optical attenuator (ATT), and then sent through an intensity modulator (IM) to create signal and decoy states with different mean photon numbers. To create vacuum decoy states, no electrical pulses are sent to LDQ. The horizontally polarized faint pulses are then transmitted through a polarization beam splitter (PBS), and combined with the strong, vertically polarized pulses from LDC. All pulses are then sent to a polarization modulator (PM), where horizontal (H), vertical (V), right (R), or left (L) circular polarization states can be created.

Quantum and classical data are transmitted to Bob through a quantum channel. At Bob's end, 10% of the light is directed towards a fast photodetector (PD) followed by a logic device (LOG). The detector and the logic device, which were not implemented in our investigation, will read the information encoded in the classical data and take appropriate action, e.g. for clock synchronization, optical routing, or communication of protocol specific information used by Bob for the measurement and subsequent processing of the quantum data.

The remaining light is split at a 50/50 beam splitter (BS), and directed to two polarization stabilizers (PSs) (PS1 and PS2) followed by PBSs (PBS1 and PBS2) and single photon detectors (SPDs). PS1 ensures that horizontally polarized classical data, and hence qubits, emitted at Alices arrive unchanged at PBS1. Similarly, PS2 is set up such that right circular polarized classical data and qubits emitted at Alices always impinge horizontally polarized on PBS2. Since the transformation in the quantum channel is described by a unitary matrix

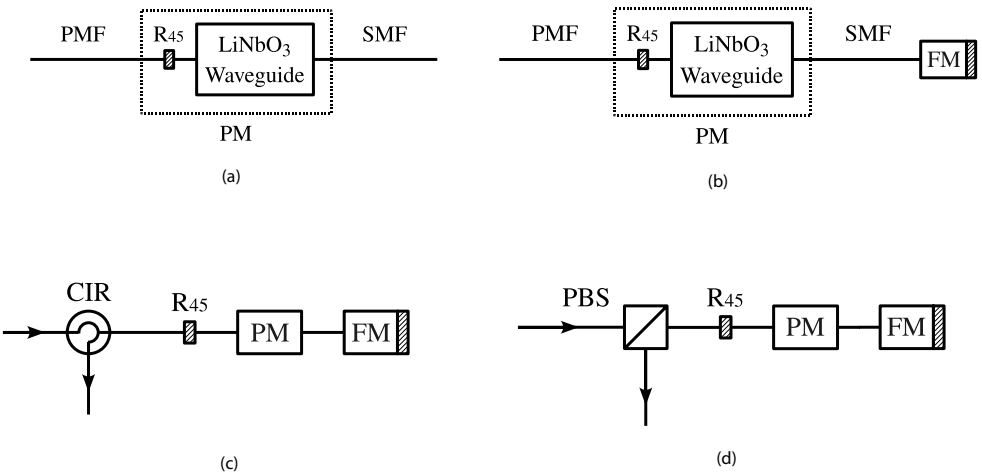

Figure 4.4: Schematics of (a) the one-way polarization modulator, (b) the basic unit, (c) the two-way polarization modulator based on the basic unit and (d) the two-way IM based on the basic unit.

(i.e. orthogonal states remain orthogonal), our stabilization scheme ensures that qubits prepared in H and V, or R and L states arrive horizontally and vertically polarized on PBS1 or PBS2, respectively. Hence, the two sets of PS, PBS and two SPDs both allow compensation of unwanted polarization transformations in the quantum channel, and projection measurements onto H, V, R and L, as required in the BB84 protocol. Note that our scheme does not prevent H and V created at Alices from arriving in an arbitrary superposition of H and V at PBS2 (similar for R and L at PBS1). However, these cases do not cause errors as they are eliminated during key sifting.

4.1.4 Polarization and IMs

One-way polarization and IM.

Initially, we used a commercial LiNbO3 phase modulator (PM) and a Mach-Zehnder IM in a one-way configuration to achieve fast polarization and intensity modulation. Figure 4.4(a) shows the schematics of the polarization modulator, i.e. a phase modulator with polarization maintaining input fibre (PMF) whose slow axis is rotated 45° (R45) with respect to the optical axis of the modulator waveguide, and standard single mode output fibre

(SMF). Hence, horizontally polarized input light, which propagates parallel to the slow axis of the PMF, is split into two components, where each one propagates along one axis of the waveguide. By applying a control voltage to the phase modulator, a phase shift is introduced between the two components, resulting in a polarization modulation.

Unfortunately, the phase modulator features significant polarization mode dispersion (PMD) for 500 ps long optical pulses resulting in a polarization extinction ratio (PER), i.e. the ratio between optical power in two orthogonal polarization states, of only 16 dB. Moreover, we found both the phase and IM to be temperature sensitive – a change of environmental temperature or heating caused by passing a current through the impedance matching resistance inside the modulators causes a variation of the polarization state, or the intensity level, of the output light. This would have a direct impact on the quantum bit error rate (QBER) and stability of our QKD system.

The 'basic unit'

To overcome these problems, we designed a basic unit (see figure 4.4(b)) consisting of a phase modulator (PM) with 45° rotated input PMF and a Faraday mirror (FM) [46]. As explained below, this allows building stable polarization and IMs by means of a go-and-return configuration (the light travels twice and in orthogonal polarization states through the phase modulator). To explain how the basic unit works, we calculate the polarization evolution of light using Jones calculus:

$$\mathbf{J}_{out} = M_{BU} \cdot \mathbf{J}_{in}. \tag{4.1}$$

$\mathbf{J}_{in}$ and $\mathbf{J}_{out}$ denote the Jones polarization vectors of the input and output light, respectively, and M_{BU} is the polarization transformation matrix of the basic unit:

$$M_{BU} = \overleftarrow{M}_{\mathbf{PMF}} \cdot \mathbf{R}_{\mathbf{45}}^{\dagger} \cdot \overleftarrow{M}_{\mathbf{WG}} \cdot \overleftarrow{M}_{\mathbf{SMF}} \cdot \mathbf{FM} \cdot \overrightarrow{M}_{\mathbf{SMF}} \overrightarrow{M}_{\mathbf{WG}} \cdot \mathbf{R}_{\mathbf{45}} \cdot \overrightarrow{M}_{\mathbf{PMF}}. \tag{4.2}$$

$\mathbf{M_{SMF}}$, $\mathbf{M_{PMF}}$ and $\mathbf{M_{WG}}$ denote the polarization transformation matrices of the single mode

fibre, the polarization maintaining fibre and the waveguide, respectively, and the arrows on top of the matrices specify the direction of light propagation. FM denotes the effect of the Faraday mirror, and R_{45} characterizes the rotation between the polarization maintaining fibre and the waveguide. Assuming that one can neglect all temperature or mechanical stress mediated changes of the properties of the fibres and the waveguide between two subsequent passages of a pulse of light (around 10 ns in our setup), and that these elements do not feature polarization dependent loss, we have

$$\begin{aligned} \overleftarrow{M}_{\mathbf{PMF}} &= \mathbf{M}^{\dagger}_{\mathbf{PMF}}, \\ \overrightarrow{M}_{\mathbf{PMF}} &= \mathbf{M}_{\mathbf{PMF}}, \\ \mathbf{M}_{\mathbf{PMF}} &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi_{PMF}} \end{bmatrix} \end{aligned} \tag{4.3}$$

where $\mathbf{M}^{\dagger}$ stands for the adjoint matrix of M and ϕ_{PMF} is the phase shift caused by the birefringence of the polarization maintaining fibre. Furthermore, we have

$$\begin{aligned} \overleftarrow{M}_{\mathbf{SMF}} &= \mathbf{M}^{\dagger}_{\mathbf{SMF}}, \\ \overrightarrow{M}_{\mathbf{SMF}} &= \mathbf{M}_{\mathbf{SMF}}, \\ \mathbf{M}_{\mathbf{SMF}} &= \begin{bmatrix} \sqrt{a} & \sqrt{1-a}e^{i\alpha} \\ \sqrt{1-a}e^{i\beta} & -\sqrt{a}e^{i(\alpha+\beta)} \end{bmatrix} \end{aligned} \tag{4.4}$$

where M_{SMF} is the most general unitary matrix describing polarization transformations. The matrices of the waveguide are given by

$$\begin{aligned} \overrightarrow{M}_{\mathbf{WG}} &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i(\phi_m^{in}+\phi_e)} \end{bmatrix} \\ \overleftarrow{M}_{\mathbf{WG}} &= \begin{bmatrix} 1 & 0 \\ 0 & e^{-i(\phi_m^{out}+\phi_e)} \end{bmatrix} \end{aligned} \tag{4.5}$$

where ϕ_{in} and ϕ_{out} denote the phase shifts during the two subsequent passages of the light through the waveguide, as determined by the modulation voltage applied to the waveguide,

and ϕ_e refers to an additional, wavelength and polarization-dependent phase shift (leading to PMD).

The effect of the FM is to transform the polarization state of an arbitrary input state of light $\mathbf{J}_{in}$ with components j_1, j_2 into the orthogonal state [10]:

$$FM \cdot \mathbf{J_{in}} = FM \cdot \begin{bmatrix} j_1 \\ j_2 \end{bmatrix} = \begin{bmatrix} j_2^* \\ -j_1^* \end{bmatrix} = \mathbf{J_{in}^{\perp}} \tag{4.6}$$

Hence, from equation 4.6, we obtain the identity

$$\begin{aligned} FM \cdot M \cdot \mathbf{J_{in}} &= FM \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \mathbf{J_{in}} \\ &= \begin{bmatrix} D^* & -C^* \\ -B^* & A^* \end{bmatrix} \cdot FM \cdot \mathbf{J_{in}} \end{aligned} \tag{4.7}$$

and thus

$$\begin{aligned} M^{\dagger} \cdot FM \cdot M \cdot \mathbf{J_{in}} &= \begin{bmatrix} A & B \\ C & D \end{bmatrix}^{\dagger} \cdot FM \cdot \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \mathbf{J_{in}} \\ &= \begin{bmatrix} A^* & B^* \\ C^* & D^* \end{bmatrix} \cdot \begin{bmatrix} D^* & -C^* \\ -B^* & A^* \end{bmatrix} \cdot FM \cdot \mathbf{J_{in}} \\ &= (A^*D^* - B^*C^*) \cdot \mathbf{1} \cdot FM \cdot \mathbf{J_{in}} \\ &= det(M^*) \cdot \mathbf{J_{in}^{\perp}}, \end{aligned} \tag{4.8}$$

where M is an arbitrary two-by-two matrix, which may describe wavelength-dependent polarization rotations or polarization-dependent loss, and $\mathbf{1}$ is the two-by-two identity matrix. Equation 4.8 shows that any polarization transformation is compensated by the FM; the output polarization state $\mathbf{J_{out}}$ is always orthogonal to the input state $\mathbf{J_{in}}$, regardless of M.

Calculating the product of all matrices in equation 4.2, we obtain

$$M_{BU} = e^{-i(\phi_{SMF}+\phi_{PMF}+\phi_e+\phi'_m)} \cdot \begin{bmatrix} cos\Delta\phi_m & -ie^{i\phi_{PMF}} sin\Delta\phi_m \\ -ie^{-i\phi_{PMF}} sin\Delta\phi_m & cos\Delta\phi_m \end{bmatrix} \cdot FM, \tag{4.9}$$

where

$$\phi'_m = \frac{\phi_m^{in} + \phi_m^{in}}{2}$$
$$\Delta\phi_m = \frac{\phi_m^{out} - \phi_m^{in}}{2}$$
$$\phi_{SMF} = \pi - \alpha - \beta.$$

Accordingly, for a horizontal input state, we find

$$\begin{aligned}
\mathbf{J_{out}} &= M_{BU} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\
&= e^{-i(\phi_{SMF}+\phi_{PMF}+\phi_e+\phi'_m)} \cdot \begin{bmatrix} -ie^{\phi_{PMF}} sin\Delta\phi_m \\ cos\Delta\phi_m \end{bmatrix} \\
&= e^{-i(\phi_{SMF}+\phi_{PMF}+\phi_e+\phi'_m)} \cdot \begin{bmatrix} e^{i\phi_{PMF}} & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} -isin\Delta\phi_m \\ cos\Delta\phi_m \end{bmatrix}
\end{aligned} \tag{4.10}$$

Hence, owing to the use of an FM, the polarization and wavelength-dependent phase shift ϕ_e introduced by the waveguide impacts now on the global phase but does not lead to PMD any more. Furthermore, all (slow) modifications of the polarization modulation due to changes in temperature or mechanical stress of the SM and PM fibres are automatically compensated. The output polarization state thus only depends on the modulation of the waveguide ($\Delta\phi_m$) and the phase shift induced by the polarization maintaining fibre (ϕ_{PMF}).

Two-way polarization modulator

We complemented the basic unit to a polarization modulator by preceding it by a polarization maintaining circulator (CIR) that allows separating the input and output optical pulses (see figure 4.4(c)). By applying appropriate, short voltage pulses, which are synchronized with the propagations of the optical pulse, to the phase modulator, we can generate horizontal ($\Delta\phi_m = \pi/2$), vertical ($\Delta\phi_m = 0$), right-hand ($\Delta\phi_m = -\pi/4$), or left-hand circular

polarization ($\Delta\phi_m = \pi/4$) states. We point out that the existence of the phase introduced by the PM fibre, ϕ_{PMF}, makes circular polarization states unstable. However, note that the four generated polarization states always form two mutually unbiased bases, regardless of the value of this phase, as required for secure QKD. Furthermore, as the change in the polarization maintaining fibre is slow, it can be compensated by a PS at Bob, allowing for the establishment of a sifted key with a small QBER.

We obtained a PER of 20 dB for horizontal and vertical polarization states (limited by the light source used to test the polarization modulator), see figure 4.5, and of 15 dB for left and right circular polarization. We believe the reduced ratio to be caused by state-dependent PMD in the circulator, which will be replaced in the near future.

Two-way intensity modulator

Similarly, we built an intensity modulator by preceding the basic unit by a PBS, as shown in figure 4.4(d). The PBS reflects the vertical component of the impinging light. Hence, by varying the polarization state of the light at the output of the basic unit, we can vary the intensity of the vertical component at the output of the PBS.

The intensity extinction ratio, i.e. the ratio between the maximum and minimum intensity at the output of the PBS, exceeds 20 dB (see figure 4.6(a)). Moreover, as the phase, ϕ_{PMF}, does not impact on the output intensity, our modulator features an outstanding stability, as depicted in figure 4.6(b). This is important when implementing a decoy state QKD protocol, which relies on accurate preparation of average photon numbers per faint laser pulse.

4.1.5 The fibre link

Loss

The link consists of two single-mode dark fibres connecting laboratories at the University of Calgary (U of C) and the Southern Alberta Institute of Technology (SAIT), see figure 4.7.

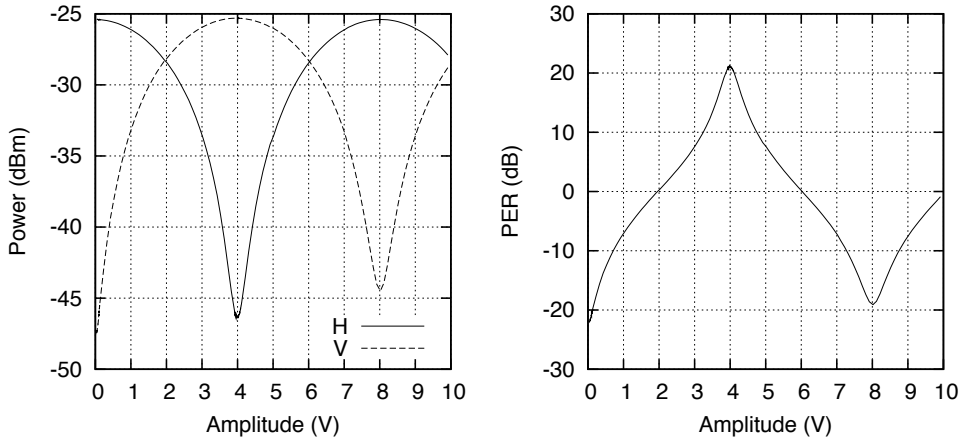

Figure 4.5: Test of the two-way polarization modulator. In the experiment, the light exiting the modulator was split by a PBS and the power was measured at the two outputs (H and V) as a function of the modulation voltage. The PER is defined as the ratio between the power in the two outputs.

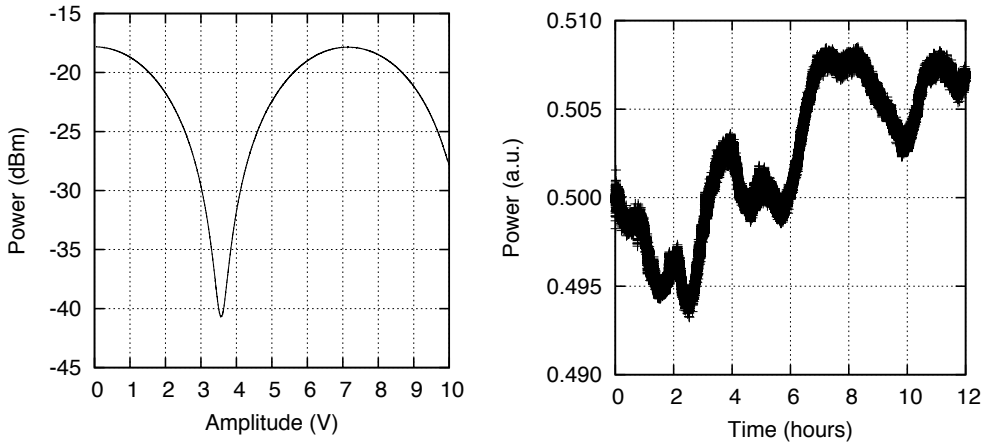

Figure 4.6: Tests of the two-way IM. Panel (a) shows the output power as a function of the applied voltage pulse to the phase modulator. The modulator features an extinction ratio of 23 dB. Panel (b) depicts the output power as a function of time. For this measurement, the output power was set to 50% of its maximum value. The total variation in 12 h is less than $\pm 1.5\%$. This is mostly determined by the power fluctuations of the laser diode, which we found to be 1.15% in 3 h (note that the latter can be further reduced using external power control).

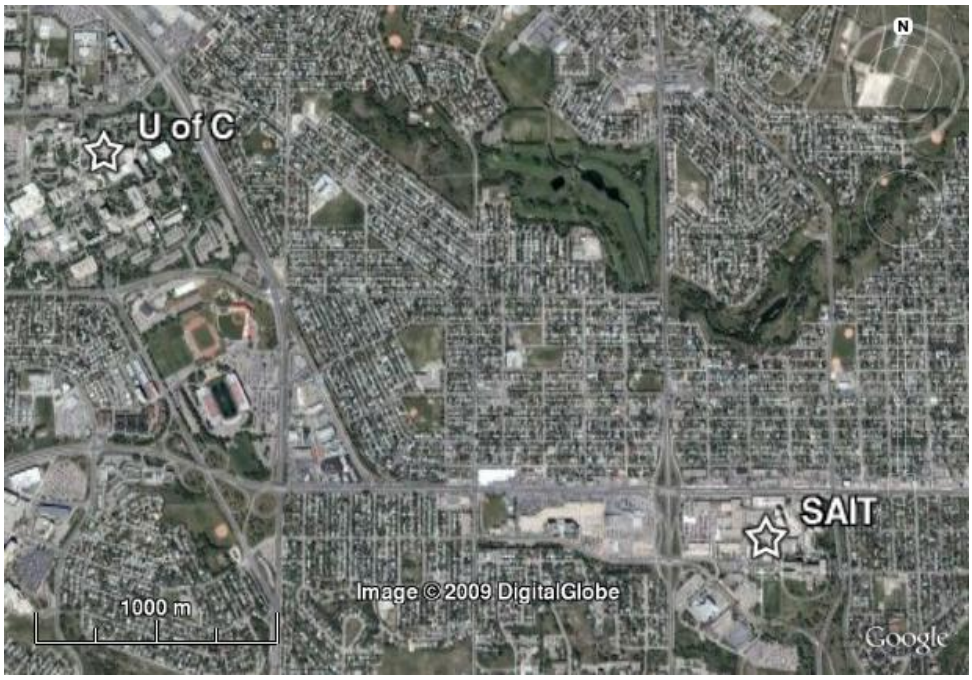

Figure 4.7: Satellite view of Calgary, showing the University of Calgary (U of C) and the Southern Alberta Institute of Technology (SAIT).

The fibres, which we refer to as channel 1 and channel 2, run through tunnels on the two campuses, and are buried or run through train tunnels in between the two institutions. They feature insertion loss of 7.8 and 6.5 dB, respectively. The fibre length is 12.4 km, while the straight line distance between the two laboratories is 3.3 km. A 1300 nm optical time-domain reflectometer (OTDR) with a 1 km dead zone eliminator was used to characterize the installed fibres. Figure 4.8 shows the measured OTDR traces. The figure clearly shows that the last several kilometres of fibre have bad connections, which result in high transmission loss in our system. The peaks at the distance of 1 km are induced by the core diameter mismatch between the tested fibre and the dead zone eliminator, where the latter one is a multi-mode fibre.

Polarization transformation

We experimentally studied the time evolution of polarization in the installed fibre. In the

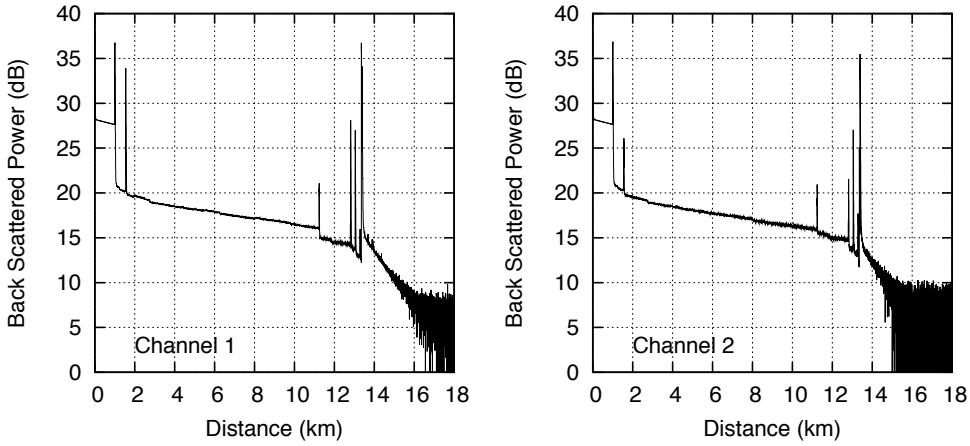

Figure 4.8: OTDR traces of the installed fibres. The horizontal axis denotes the distance measured from the laboratory at SAIT. The vertical axis denotes the logarithm of the ratio between the back scattered power detected by the OTDR and a reference power set by the instrument, where a higher value corresponds to more reflected power.

experiment, a stable polarized light source was launched into the fibre link, where channels 1 and 2 were looped at SAIT. We used a polarimeter to record Stokes parameters of the output light every second. Figure 4.9(a) presents the results of one week of continuous monitoring from 16 April 2008 to 24 April 2008. Figure 4.9(b) shows the temperature curve for the Calgary Airport during the measurement (data from Canada Environment Weather Office). Comparing figures 4.9(a) and (b), we observe a clear correlation between the variation of temperature and the fluctuation of polarization. This phenomenon is particularly obvious for the measurement from 19 April to 23 April, where we observe small polarization variation during night, and much more pronounced variations during day-time. Figure 4.9(c) is a zoom-in of the measurement on 19 April (around lunch time), where particularly rapid polarization fluctuations are observed. Even for this case, we find that the polarization is stable on a timescale of tens of seconds. This sets an upper limit to the duration of quantum data between consecutive stabilization cycles.

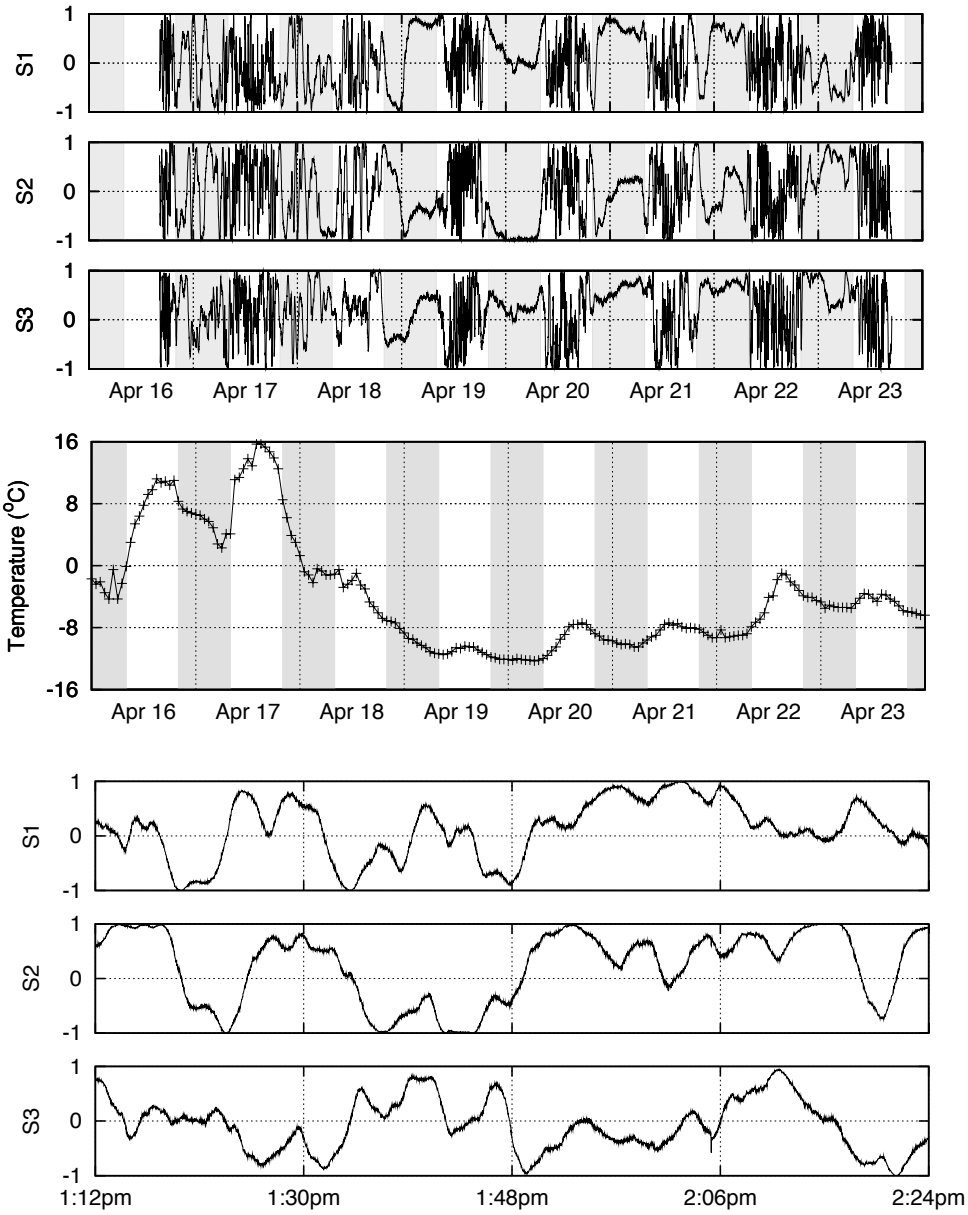

Figure 4.9: (a) Time evolution of Stokes parameters during a full week in 2008. The shaded regions indicate night-time from 8:00 p.m. to 8:00 a.m. (b) Temperature curve for Calgary. (c) Zoom of (a) around 19 April lunch time.

4.1.6 Field tests

Setup

A schematic of the complete experimental setup is shown in figure 4.10. A 10 GS s^{-1} function generator (FG1) with two independent outputs drives the quantum laser diode (LD_Q) and the classical laser diode (LD_C) via broadband RF amplifiers (APs). Both laser diodes produce horizontally polarized optical pulses with a duration of 500 ps and a repetition rate of 50 MHz. By adjusting the temperature, we could closely match the spectral properties of the two laser diodes. We obtained center wavelengths of 1548.07 nm and 1548.11 nm, and spectral widths (fullwidth at half-maximum (FWHM)) of 0.214 and 0.224 nm for LD_Q and LD_C, respectively. This is important to ensure that the polarization transformation sensed by means of the C-frames (generated with LD_C) equals the one experienced by the quantum data (generated with LD_Q).

The pulses from LD_Q, eventually encoding quantum data at different mean photon numbers, propagate through a two-by-two PBS and enter the IM, which is described in detail in section 4.1.4. To reduce their energy to the single-photon level, a fixed optical attenuator (ATT) is placed between the FM and the phase modulator (PM). Birefringence and polarization dependent loss of the attenuator are automatically compensated by the Faraday effect and therefore a stable attenuation is achieved. At the output of the PBS, the now vertically polarized weak laser pulses are combined with the horizontally polarized strong pulses from LD_C, which encode the C-frame, to form a complete Q-frame. Quantum and classical data are then sent through the polarization modulator, which is also presented in section 4.1.4. The intensity and the polarization modulator are driven by a function generator (FG2) with a pulse width of 4 ns. Note that the polarization maintaining circulator (CIR) that is part of the polarization modulator only allows horizontally polarized light to enter, while the pulses from LD_C and LD_Q impinge with orthogonal polarization. Therefore, we aligned the axes of the polarization maintaining fibre at the output of the PBS at 45° with respect to the axes

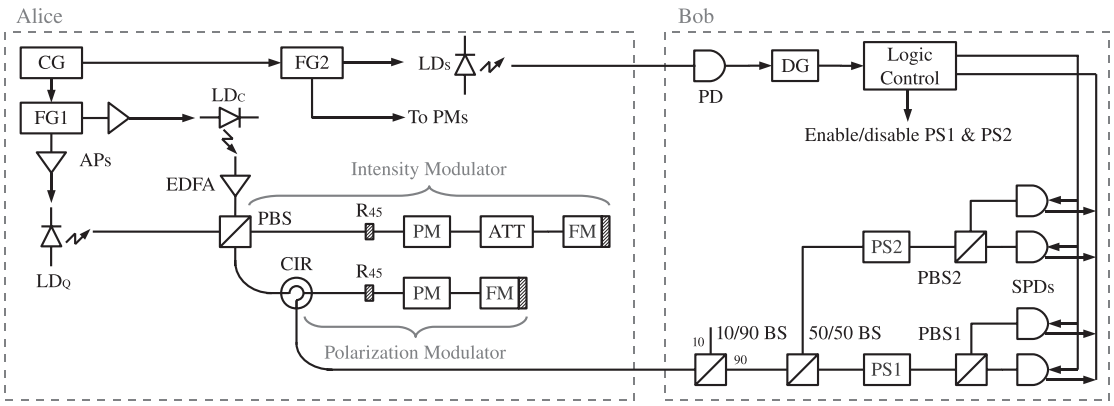

Figure 4.10: Schematic of the QKD setup.

of the polarization maintaining fibre at the input of the circulator. This alignment makes the circulator work with both directions of polarization, yet, at the expense of 3 dB loss. Finally, the polarization modulated data are forwarded to Bob through fibre channel 2.

Alice's electronic equipment is synchronized using a clock signal at 10 MHz from a clock generator (CG). Using a function generator, a laser diode (LD_S), a photodiode (PD) and a delay generator (DG), the clock signal (reduced to 1 MHz) is also transmitted to Bob, where it provides trigger signals for the SPDs, synchronized with the arrival time of the quantum data.

At Bob's side, 90% of the optical power encoded into each Q-frame is transmitted through a 10/90 BS and is then equally divided by a 50/50 BS. For each part, the C-frames are sensed by a PS (from General Photonics) to compensate for the polarization change in the transmission line, and the quantum data are detected by a measurement module consisting of a PBS and two InGaAs-based SPDs. The SPDs are triggered at 1 MHz, and operated with a gate width of 5 ns, a deadtime of 10 μs and a quantum efficiency of 10%.

In principle, the length of a C-frame is determined by the response time of the PS, which is 18 ms. However, due to the small duty cycle of the classical pulse sequence in the current implementation and the low transmission of the fibre link, the average power of the C-frame is below the detection threshold of the PS. To resolve this problem, we placed a polarization

maintaining erbium-doped fibre amplifier (EDFA) between LD_C and the PBS. The EDFA is turned off after each C-frame to avoid flooding the SPDs at Bob's with photons from amplified spontaneous emission. While the turn-off time is only tens of milliseconds (consistent with the radiative lifetime of population in the upper laser level), we found the turn-on time of the EDFA to be as long as 3 s, resulting in 5 s long C-frames. The length of quantum data is set to 2 s, according to the worst-case polarization stability of the fibre link, which is discussed in section 4.1.5. From this, we find that our setup currently limits the time for QKD to 30% of the operation time. Note, however, that the duty cycle of the classical pulse sequence can easily be increased by several orders of magnitude. In this case, the duration of a C-frame would be limited by the response time of the PS, and the time for QKD could exceed 99% of the system operation time.

Measurements

We performed a variety of measurements to assess the performance of our QKD system. For *2-detector measurements*, Alice repetitively creates sequences of Q-frames with polarizations HH, HL, HV, HR, LH, LL, LV, LR, VH, VL, VV, VR, RH, RL, RV and RR. The first letter indicates the polarization of the C-frame and the second one indicates that of the quantum data. Bob uses one measurement module to process the frames. The PS compensates the polarization transformation in the quantum channel for states belonging to the basis indicated by the first letter, i.e. linear or circular. For *4-detector measurements*, Alice modulates the polarization of the Q-frames in the more complicated order of HH, RH, VH, LH, RH, HH, LH, VH, HR, RR, VR, LR, RR, HR, LR, VR, HV, RV, VV, LV, RV, HV, LV, VV, HL, RL, VL, LL, RL, HL, LL and VL. Bob uses two measurement modules to process the Q-frames. The PS of one module is always activated for odd frame numbers and that of the other module is always activated for even frame numbers (see figure 4.2). In this way, the two measurement modules compensate polarization transformation for states encoded in

the linear, or the circular basis, respectively. We collect the number of trigger events and counts for all SPDs for each combination of polarization states and different mean number of photons per qubit. This allows calculating average QBERs and key generation probabilities (KGPs), where the KGP is defined as the probability of generating a sifted key bit from a qubit encoded into a weak signal state when Alice and Bob use the same basis:

$$\begin{aligned} \mathrm{QBER} &= \frac{P_{\mathrm{wrong}}}{P_{\mathrm{wrong}} + P_{\mathrm{correct}}}, \\ \mathrm{KGP} &= P_{\mathrm{correct}} + P_{\mathrm{wrong}}. \end{aligned} \tag{4.11}$$

The probabilities for correct (P_{correct}) and wrong sifted key bits (P_{wrong}) are obtained from experimental data by dividing the number of correct, or wrong, detection events by the number of trigger events. We assume that the probability for both detectors to click simultaneously can be ignored. In our setup, it was at least four orders of magnitude smaller compared to the probability for a single click. Note that in an actual implementation simultaneous clicks in two or more detectors have to be replaced by a randomly selected detection event [47, 48].

Assuming that the photon number per laser pulse satisfies a Poissonian distribution, P_{correct} and P_{wrong} can be calculated using

$$\begin{aligned} P_{\mathrm{correct}} &= 1 - \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} \left(1 - \frac{Y_0}{2}\right) (1 - t\eta a)^n \\ &= 1 - \left(1 - \frac{Y_0}{2}\right) e^{-\mu t \eta a}, \\ P_{\mathrm{wrong}} &= 1 - \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} \left(1 - \frac{Y_0}{2}\right) (1 - t\eta(1-a))^n \\ &= 1 - \left(1 - \frac{Y_0}{2}\right) e^{-\mu t \eta (1-a)}. \end{aligned} \tag{4.12}$$

$Y_0/2$ is the probability for a detector click without Alice sending a photon, which includes detection events due to dark counts and stray photons. We found this probability in our setup to be equivalent to the dark count rate. μ is the average photon number of the weak pulses at Alice's output, t is the overall transmission, which includes the fibre link and Bob's optical components, and η is the quantum efficiency of the SPDs. Finally, a describes the

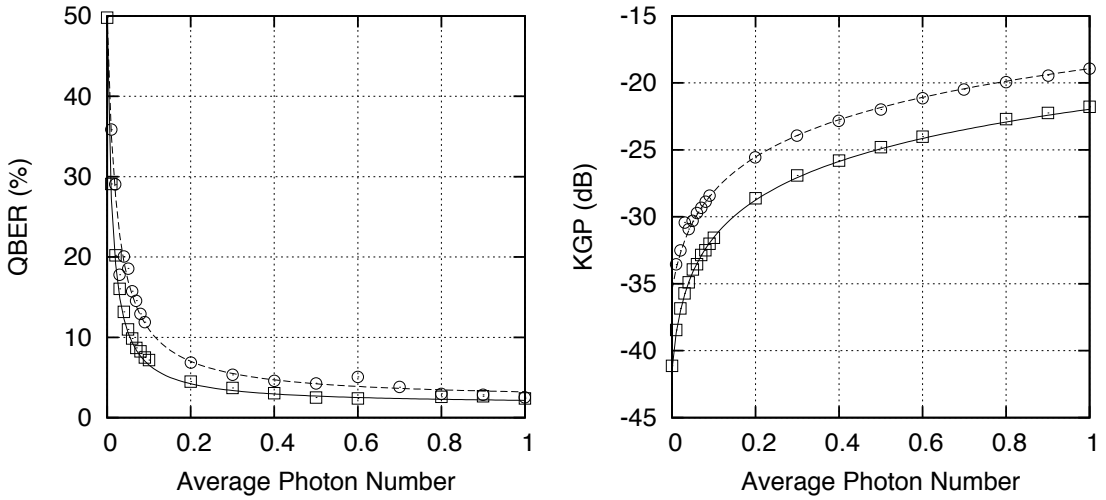

Figure 4.11: Average QBER and KGP (in dB) as a function of the mean photon number per weak laser pulse used to encode the polarization qubits. The squares and circles indicate the experimental results for the 2-detector and 4-detector measurements, respectively, and the solid and dashed lines are the corresponding theoretical predictions (no fit). Error bars (corresponding to one standard deviation) are smaller than the size of each experimental data point.

PER of the PBS, i.e. the probability for a horizontally polarized photon to be transmitted through the PBS, normalized to the probability to exit.

The experimental results of the measurements are summarized in figure 4.11, together with the theoretical predictions. Note that all parameters required to calculate the QBER and the KGP have been obtained through independent measurements. We see that the experimental values match the theoretical calculations very well. We also find that the average QBER of the 4-detector measurement is larger than that of the 2-detector measurement at the same mean photon number. This is due to an increased dark count probability of the two additional SPDs, and slightly worse alignment of the PS in the second measurement module. Furthermore, the 4-detector measurement features a higher KGP as no qubits are lost at the 50/50 BS. The individual data of the 4-detector measurement with an average photon number of 0.5 photons per pulse are listed in table 4.1.

Long-term stability of the system

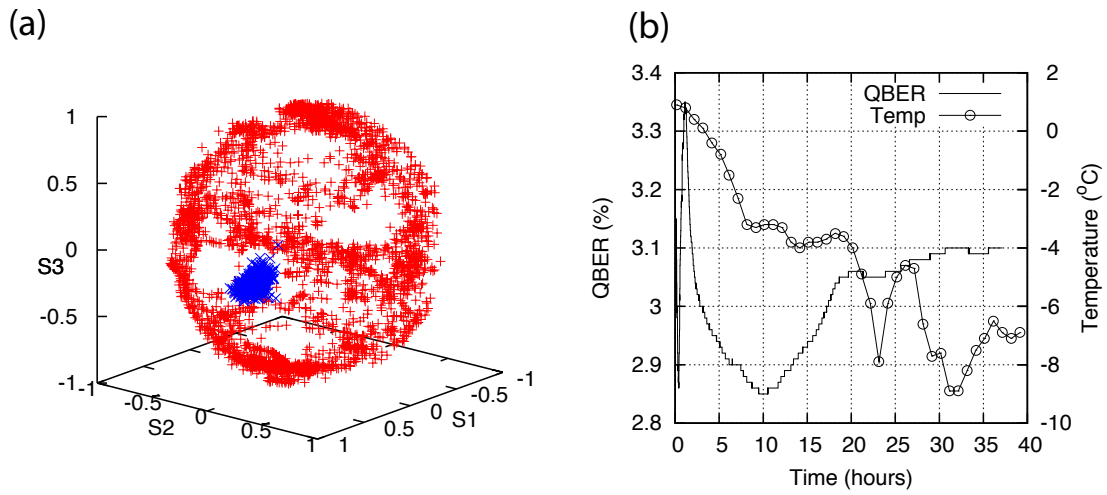

Figure 4.12: Results of the long-term measurement. (a) Stokes vectors of C-frames with (blue points) and without (red points) polarization stabilization. (b) Average QBER and temperature for the same time interval as a function of time.

To study the stability of the system, we performed a long time measurement over 37 h. In the measurement, Alice sends qubits encoded into weak laser pulses with an average photon number of 0.5, and Bob implements a 2-detector measurement using measurement module one. At the end of each C-frame, i.e. after stabilization, Bob records the polarization of the C-frame with PS1. Meanwhile, the PS (PS2) in the second measurement module monitors the polarization of the C-frame without polarization control. In figure 4.12(a), the red points indicate the Stokes vectors of the classical pulses measured by PS2, which are randomly distributed on the surface of the Poincaré sphere due to the time-varying polarization transformation in the transmission line. The blue points depict the measurements made by PS1, i.e. after polarization control. Even though the result slightly deviates from a single spot, which is expected in the ideal case, it clearly demonstrates the good long-term stability of our QKD system.

For a more quantitative analysis, we also recorded the evolution of the QBER over the same time interval, see figure 4.12(b). The temperature curve for the Calgary Airport (data from Canada Environment Weather Office) is shown as well. The QBER varies between 2.85% and 3.35% in over 35 h, and the variation is less than 0.1% in the last 15 h.

Table 4.1: Results of the 4-detector measurement with an average photon number of 0.5 photons per pulse, where pol indicates the polarizations of the Q-frames, det and trg are the number of photon detections and trigger events recorded by the SPDs, and prob is the detection probability (in dB). **Note added during thesis writing:* In the table the probability is calculated as $prob = -10log(det/trg)$. The difference in the trigger rate between detectors is due to different deadtimes for each of the detectors due to difference in the after-pulsing noise.

	SPD_1			SPD_2		
pol	det	trg	prob(dB)	det	trg	prob(dB)
HH	1569	13254716	39.27	37639	12504218	25.21
HV	39642	13381789	25.28	1922	13385381	38.43
RR	1243	13160359	40.25	35711	12443131	25.42
RL	41856	13521618	25.09	1979	13505244	38.34
VH	42567	12853157	24.80	950	12863193	41.32
VV	1569	13183509	39.24	34723	12454406	25.55
LL	41800	13514989	25.10	1841	13114840	38.53
LR	959	10908918	40.56	30270	10273810	25.31
	SPD_3			SPD_4		
pol	det	trg	prob(dB)	det	trg	prob(dB)
HH	37577	12468543	25.21	1050	12416198	40.73
HV	2121	12145604	37.58	35843	11410147	25.03
RR	35954	12409015	25.38	1605	12351662	38.86
RL	3222	12253689	35.80	36378	11541004	25.01
VH	2410	12817201	37.26	39290	12046285	24.86
VV	36215	12403829	25.35	925	12355805	41.26
LL	2751	12270811	36.49	36547	11534262	24.99
LR	29988	10247919	25.34	1149	10193024	39.48

4.1.7 Security issues

For any cryptographic system, be it of quantum or classical nature, it is important to carefully analyse the actual implementation for weak points that may compromise its principle security. Applied to QKD, these include deficiencies in the preparation of quantum data at Alice's that can be exploited by an eavesdropper to gain information about the sifted key. We refer to these kinds of attacks as *quantum state attacks*. Furthermore, Eve may also attempt to actively sense the classical devices that create or measure the quantum data, or try to actively impact on the interaction between quantum and classical systems to influence the outcomes of measurements. We refer to these kinds of attacks as *classical system attacks*.

Note that, once the deficiencies are found, it may be possible to eliminate them by devising a better optical setup, or to remove the corresponding amount of information that Eve may have obtained through additional privacy amplification [49]. Yet, we point out that loopholes may also arise from a careless implementation of privacy amplification, e.g. improper choice of Hash function, or of insufficient authentication of the classical channel. Finally, the size of the error corrected key has to be considered when calculating the appropriate amount of privacy amplification, i.e. to distil a secure key [50, 51].

In the following, we will briefly discuss our current optical setup in view of such weak points. Yet, a complete security analysis of our system is beyond the scope of this article, which is the introduction of Q-frames. Note that the existence of loopholes in a particular QKD setup breaks the unconditional security of this particular system, but does not disprove that QKD can, in principle, be information theoretic secure.

Quantum state attacks

The use of attenuated laser pulses, as opposed to pairs of entangled photons [10], entails the possibility that non-orthogonal qubit states (here encoded into the polarization degrees of freedom) may become distinguishable when taking into account other degrees of freedom

needed to fully describe the quantum data, e.g. frequency, temporal modes, or transverse modes. Obviously, in this case, the security offered by QKD would break down. We refer to these attacks as *quantum side channel attacks*. Furthermore, as the number of photons in the attenuated laser pulses is described by a Poissonian distribution, it may be possible for an eavesdropper to gain information based on *photon-number-splitting (PNS) attacks.*

Attacks exploiting quantum side channels.

In our QKD system, all four qubit states are produced by the same laser diode, which is triggered independently of the subsequent action of the polarization modulator or IM. Together with the polarization independent spectral transmission of both modulators and the attenuator, due to the use of the FMs, this ensures that correlation between polarization state and spectrum or temporal mode do not exist. However, we recall that the circulator (CIR) at the output of the polarization modulator adds basis dependent PMD, which manifests as a basis-dependent QBER. This may induce detectable temporal broadening of the photonic wave packets, i.e. may partially reveal the basis used for encoding the qubit. The circulator will be replaced in a future, improved setup. Furthermore, as the entire setup is built with (transverse) single mode optical fibres, correlation between polarization states and transverse modes, which may be present in a free space system, are ruled out.

PNS attacks and decoy states.

The use of faint laser pulses makes our system principally susceptible to PNS attacks, which were first mentioned in [52] and have been analysed thoroughly in [53, 9]. A possibility to remove the threat of the PNS attack is the use of so-called decoy states [25, 27, 26]. This allows establishing a conservative lower bound for the key that can be created from single photons emitted at Alice's, i.e. key that was not subject to the PNS attack. As described before, our setup has been devised to allow for the implementation of decoy states. In the

following, we will examine experimentally the accuracy with which the decoy state method allows bounding the size of the secret key.

With the GLLP method, the secure key rate per emitted faint pulse with mean photon number of μ is given by [28]

$$S \geq \frac{1}{2}\left[Q_1(1 - H_2(E_1)) - Q_\mu f(E_\mu) H_2(E_\mu)\right], \tag{4.13}$$

where the factor $\frac{1}{2}$ accounts for basis reconciliation, $H_2(x) = x\log_2(x) - (1-x)\log_2(1-x)$ denotes the Shannon entropy, Q_1, Q_μ, E_1 and E_μ specify the gains and error rates of signal states and single photons, respectively, and $f(E_\mu)$ is the error correction efficiency which is assumed to be 1.22 [54].

In the first analysis, we assume that no PNS attack took place during the measurement, which is a reasonable assumption. Using equations 4.12, we can estimate the gain and error rate for signal states with mean photon number μ:

$$\begin{aligned} Q_\mu &= P_{\text{correct}}(\mu) + P_{\text{wrong}}(\mu) \\ &= 2 - (1 - Y_0/2)(e^{-\mu t\eta a} + e^{-\mu t\eta(1-a)}), \\ E_\mu &= \frac{P_{\text{wrong}}(\mu)}{P_{\text{correct}}(\mu) + P_{\text{wrong}}(\mu)} \\ &= \frac{1 - (1 - Y_0/2)e^{-\mu t\eta a}}{2 - (1 - Y_0/2)(e^{-\mu t\eta a} + e^{-\mu t\eta(1-a)})}. \end{aligned} \tag{4.14}$$

Similarly, the gain and error rate for single photon pulses are given by

$$\begin{aligned} Q_1 &= \mu e^{-\mu}(2 - (1 - Y_0/2)(2 - t\eta)), \\ E_1 &= \frac{1 - (1 - Y_0/2)(1 - (1-a)t\eta)}{2 - (1 - Y_0/2)(2 - t\eta)}. \end{aligned} \tag{4.15}$$

Using equations 4.13–4.15 and taking into account the measured values for t, η, a and $Y_0/2$, we can calculate the secret key rate for different μ, see curve A of figure 4.13.

In the second analysis, which again relies on the assumption of fair loss, we use equation 4.14 to calculate the gains and error rates for the signal state with mean photon number μ and the decoy state with mean photon number ν of 0.1. To calculate the gain and error

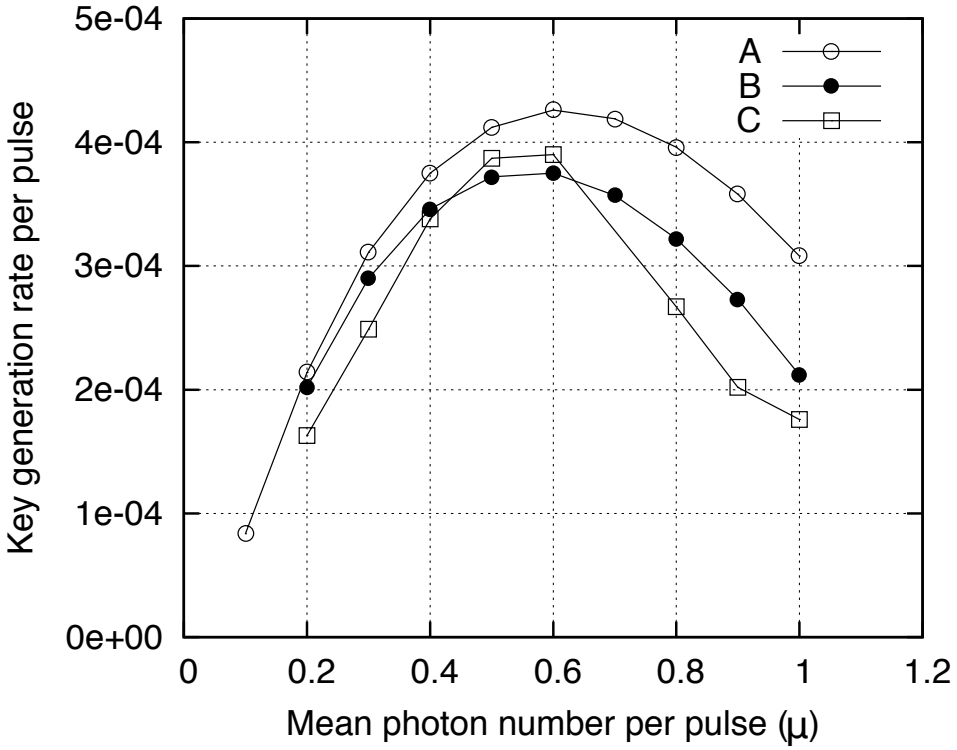

Figure 4.13: Comparison of secret key rates versus mean number of photons in the signal states. Curve A is the secret key rate calculated from the fraction of single photons emitted at Alices and assuming fair loss (i.e. assuming it is known that all loss is of technological origin and that there is no PNS attack). Curve B shows the secret key rate calculated via the decoy state method (using decoy states with mean photon number of 0.1 and vacuum states) and assuming fair loss. Curve C is the secret key rate obtained via the decoy state method using experimental data. All calculations assume an infinite sifted key length.

rate for single photon pulses, we use equations 34, 35 and 37 from [27]:

$$\begin{aligned} Q_1 \geq Q_1^{\nu,0} &= \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right), \\ e_1 \leq e_1^{\nu,0} &= \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^{L,\nu,0}\nu}, \\ Y_1 \geq Y_1^{L,\nu,0} &= \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2} Y_0\right). \end{aligned} \tag{4.16}$$

The resulting secret key rate follows from equation 4.13. It is shown in curve B of figure 4.13.

Finally, we calculate the secret key rate using the experimentally measured gain and error rates for signal and decoy states, as opposed to the previous case where they were calculated. The gain and error rate for single photons are estimated as before using equations 4.16. The result is plotted in curve C of figure 4.13. Note that the measurement does not rely on the fair loss assumption.

Comparing the three different curves, we find that the rates estimated from the decoy state method (curves B and C) is somewhat smaller than the one plotted in curve A. This is natural as the decoy state method with decoy states of finite photon mean number only yields a conservative lower bound [27]. As an example, for $\mu = 0.6$, we find the secret key rate (curves B and C) to be roughly 10% worse than the secret key rate given in curve A. We also find a reasonably good agreement between the rates estimated and measured using the decoy state method (curves B and C, respectively). We attribute the remaining discrepancy to a systematic error in the estimation of the single photon gain Q_1, resulting from a slightly wrong estimation of the transmission in the link, quantum efficiency of the detectors, or error rate due to wrongly received photons. Factors like fluctuations in the mean photon number could also have an effect. This systematic error also affects the estimation of the single photon error rate E_1. Furthermore, curves B and C show that the secret key rate in our QKD system is maximized for signal states with a mean number of photons of $\mu \approx 0.6$. This value agrees with estimations in [27] when taking into account the actual values for dark count rates, transmission, detector quantum efficiency and error rate caused by wrongly received photons. Indeed, we calculate $\mu_{\text{opt}} = 0.62$, in very good agreement with

our experimental results.

To finish this discussion, we emphasize that the secret key rate in an actual implementation of an information-theoretic secure QKD session must be calculated using the decoy state method used in the third analysis and must not rely on assumptions about fair loss in the quantum channel.

Other deficiencies.

We have noted that each faint pulse that encodes a qubit is preceded by another faint pulse, originating from a reflection on the PBS that is part of the IM (see section 4.1.4). Note that the number of photons in both pulses is comparable. Obviously, for our assessment of the eavesdropper's information to be correct, we have to make sure that this pulse, which also transits through the polarization modulator, does not encode any polarization information. Therefore, we have carefully adjusted the electrical trigger signal for the polarization modulator such that it only acts on the faint pulse, and not on the spurious one.

Classical system attacks

Trojan Horse attacks: As in any QKD system, regardless of whether it employs one-way or two-way quantum communication, appropriate measures have to be implemented to protect against Trojan Horse attacks [19]. In these attacks, the eavesdropper injects light through the optical fibre into Alice's or Bob's preparation or measurement device, respectively, and analyses the back reflection, which may reveal information about the quantum state created at Alice's or the measurement basis to be used at Bob's. In both cases, the security of the key distribution would be compromised as Eve either knows the state, or knows in which basis to perform an intercept resend attack without creating errors. In our QKD system, given the static setup at Bob's, Trojan Horse attacks have to be considered only at Alice's. Towards this end, a polarization independent optical isolator and a spectral filter that absorbs all

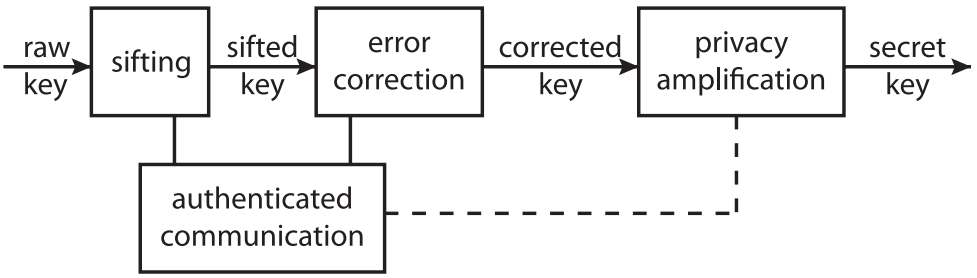

Figure 4.14: Classical post-processing steps.

wavelengths not blocked by the isolator should be placed at the output of Alice's.

Time-shift attacks: In a time-shift attack [55, 56, 57] the eavesdropper exploits the fact that the detection efficiency of different detectors may, for a given arrival time of a photon, be different. It may thus be possible for an eavesdropper to bias the detection probabilities by actively time-shifting the arrival time of photons and thereby acquire information for each photon if it was detected in a detector that codes for a bit value 0, or 1. This attack, which is possible in our current system, can be overcome if Bob randomly rotates the polarization state of each incoming qubit by 0 or $\pi/2$, thereby de-correlating a detection in a particular detector with a particular bit value. This can be done by placing a rapidly variable $\lambda/2$ waveplate in between the PS and the PBSs, at the expense of rendering Bob's setup 'active', i.e. vulnerable to Trojan Horse attacks (which then have to be protected against, as discussed above).

4.1.8 Classical post-processing

Once the quantum part of the QKD protocol is finished, Alice and Bob must perform a series of classical steps to go from the raw key to the secret key used for encryption [10]. The steps required are shown in figure 4.14. In addition to sifting, error correction is used to ensure that Alice and Bob have an identical key despite any errors that occur. Privacy amplification is then used to eliminate any information Eve has obtained about the key, whether through eavesdropping on the quantum channel or on the classical communication used for error

correction. These steps must also make use of authenticated communication to prevent Eve from performing a man-in- the-middle attack. Of these steps, error correction is expected to become the bottleneck in the QKD system once higher raw key rates are achieved. The Cascade protocol [7] that was originally developed for QKD is not suitable for high key rates as it requires many rounds of communication between Alice and Bob and is computationally expensive [58].

Low-density parity-check (LDPC) codes

LDPC codes were originally developed by Gallager in the 1960s [59] for classical communications, but their potential performance has only been recently been discovered [60]. LDPC codes for QKD differ slightly from those used in the classical case as the parity information is transmitted over a separate classical channel [58].

A LDPC code is defined using an $m \times n$ parity check matrix, H, consisting of zeros and ones. While either Alice's or Bob's sifted key may be considered the 'correct' key for the purpose of error correction, this discussion will use Alice's sifted key, the n bit column vector $\boldsymbol{\alpha}$, i.e. one-way, forward error correction. Alice computes a parity vector as follows:

$$\boldsymbol{p} = H\boldsymbol{\alpha} \pmod 2, \tag{4.17}$$

where the number of bits m in the parity vector is lower bounded by Shannon's noisy coding theorem; $m = nH_2(\text{QBER})$ with Shannon Entropy H_2. Thus, p_i indicates whether the sifted key bits indicated by the ones in the ith row of H contain an even ($p_i = 0$) or odd ($p_i = 1$) number of ones. Alice transmits $\boldsymbol{p}$ to Bob, whose task is to determine $\boldsymbol{\alpha}$ using H, $\boldsymbol{p}$, his sifted key, $\boldsymbol{\beta}$, and an initial estimate of the QBER. This estimate can be based on a characterization of the quantum channel or on the QBER from previous executions of the protocol. In order to recover $\boldsymbol{\alpha}$, Bob uses a process known as belief propagation to refine his initial probabilities for the entries of $\boldsymbol{\alpha}$ based on $\boldsymbol{\beta}$ and the QBER. Note that in the following discussion, Bob has full knowledge of his key vector, $\boldsymbol{\beta}$, but his knowledge of the Alice's key

Table 4.2: Results for $r_{\alpha j=1}(i,j)$.

j	β_j	$P_0(j)$	$P_1(j)$	$r_{\alpha j=1}(i,j)$ for $p_i - 0$	$r_{\alpha j=1}(i,j)$ for $p_i - 1$
1	1	0.1	0.9	0.82	0.18
2	1	0.1	0.9	0.82	0.18
3	0	0.9	0.1	0.18	0.82

Table 4.3: Results for $P_0'(j)$ and $P_1'(j)$ values.

$r_{\alpha j=1}(1,j)$	$r_{\alpha j=1}(2,j)$	$r_{\alpha j=1}(3,j)$	$q_{\alpha j=0}(j)$	$q_{\alpha j=1}(j)$	$P_0'(j)$	$P_1'(j)$
0.82	0.82	0.82	0.0006	0.4963	0.0012	0.9988
0.18	0.82	0.82	0.0027	0.1089	0.0238	0.9762
0.18	0.18	0.82	0.0121	0.0239	0.3361	0.6639
0.18	0.18	0.18	0.0551	0.0052	0.9131	0.0869

vector, $\boldsymbol{\alpha}$ is probabilistic. For example, suppose row i of H is a parity check on three bits received by Bob, $\beta_1 = 1$, $\beta_2 = 1$ and $\beta_3 = 0$, where the expected QBER is 10% (chosen to prevent very small numbers in this example). The probability that a key bit α_j is zero or one based on the received values and the QBER are denoted $P_0(j)$ and $P_1(j)$, respectively. For each of his bits β_j , Bob assumes that $\alpha_j = 1$ and computes $r_{\alpha_j=1}(i,j)$, which denotes the probability that the parity check i is satisfied ($p_i = \alpha_1 + \alpha_2 + \alpha_3 \pmod 2$) given this assumption. Alternatively, $r_{\alpha_j=1}(i,j)$ may be viewed as the probability that $\alpha_j = 1$ given the value of p_i and what is known about the other bits of $\boldsymbol{\alpha}$ involved in the ith parity check. For example, $r_{\alpha j=1}(i,1)$ may be computed as follows:

$$r_{\alpha_j=1}(i,1) = \begin{cases} P_0(2)P_1(3) + P_1(2)P_0(3), & \text{for } p_i = 0, \\ P_0(2)P_0(3) + P_1(2)P_1(3), & \text{for } p_i = 1. \end{cases} \tag{4.18}$$

As can be seen in table 4.2, the probability that the bits retain their received value is high when $p_i = 0$ since this is consistent with the received values of $\boldsymbol{\beta}$. If instead $p_i = 1$, a high probability for bit flips is obtained since each row assumes that the received values for the other bits are likely to be correct. This information is useful when combined with the results of other parity checks.

After doing these computations for each row of H, Bob uses the information from all the

parity checks involving a particular key bit β_j to compute new values of $P_0^{'}(j)$ and $P_1^{'}(j)$. If the jth key bit is involved in three parity checks, Bob computes $q_{\alpha_j=0}(j)$ and $q_{\alpha_j=1}(j)$, which represent the probability that α_j is zero or one, respectively, based on β_j and the QBER, and that all parity checks involving α_j are satisfied:

$$q_{\alpha_j=0}(j) = P_0(j) r_{\alpha_j=0}(1,j) r_{\alpha_j=0}(2,j) r_{\alpha_j=0}(3,j), \tag{4.19}$$

$$q_{\alpha_j=1}(j) = P_1(j) r_{\alpha_j=1}(1,j) r_{\alpha_j=1}(2,j) r_{\alpha_j=1}(3,j), \tag{4.20}$$

where $r_{\alpha_j=0}(i,j) = 1 r_{\alpha_j=1}(i,j)$. Since valid results must be consistent with all parity checks, $P_0^{'}(j)$ and $P_1^{'}(j)$ are obtained by normalizing $q_{\alpha_j=0}(j)$ and $q_{\alpha_j=1}(j)$. For example, consider $\beta_j = 1$, implying $P_0(j) = 0.1$ and $P_1(j) = 0.9$ as shown in table 4.3. Even if one parity check suggests there is an error in this example, the confidence that $\beta_j = 1$ (i.e. β_j was received correctly) still increases. With all three parity checks suggesting a bit flip is necessary, a high confidence is obtained that the received value of β_j is incorrect. With two parity checks suggesting a bit flip is required, the result does not significantly favour either result.

Bob can then select the most likely value for each bit to form $\boldsymbol{\beta}^{'}$, and compute $\boldsymbol{p}^{'} = H\boldsymbol{\beta}^{'} (\mathrm{mod}\ 2)$. If $\boldsymbol{p}^{'} = \boldsymbol{p}$, the protocol is finished. Otherwise, additional iterations of the protocol are performed. With the additional modification that Bob also computes conditional probabilities, $P_0^{'}(i,j)$ and $P_1^{'}(i,j)$, to use inequation 4.18 during subsequent iterations, this procedure is generalized as the sum-product algorithm [58, 60].

Hardware LDPC decoding

Interest in LDPC codes stems not only from their potential to perform near the Shannon limit. Since the computations for each parity check and each key bit are independent, the structure of the sum-product algorithm lends itself to parallel computation. This makes sum-product decoding of LDPC codes well suited for high speed implementation in custom hardware or in reconfigurable devices such as Field Programmable Gate Arrays (FPGA) [61].

However, floating-point computations are expensive in terms of the amount of logic required. Thus, it is desirable to implement LDPC decoding using fixed-point arithmetic (equivalent to integer arithmetic) with as few bits as possible to represent the values. In initial simulations of fixedpoint decoding, we found that the primary obstacle for a small bit length was the very small values obtained for the probabilities. This problem manifested as divide by zero errors during the normalization since both $q_0(j)$ and $q_1(j)$ had rounded to zero. We overcome this limitation by modifying the algorithm to set any occurrences of zero in the $q(j)$ values to the smallest possible nonzero value.

A LDPC code was designed with a 1200×4000 parity check matrix using parameters similar to [58](QBER = 3%, parity checks on 20 key bits. Note that this QBER also reflects our experimental results, see section 4.1.5). It has been shown that having the key bits take part in a variable number of parity checks results in better performance [62]. Thus, H has a fixed number of ones in each row, known as the row weight, and a variable number of ones in each column, known as the column weight. The method presented in [62] was used to determine the column weights by applying a well-known optimization technique with the constraints ensuring that the design criteria (QBER and code rate) are met. In place of the arbitrary cost function in [62], we use a function reflecting the computational complexity. Our code was simulated over 40 iterations, with the number being selected based on tests that showed very little improvement beyond this point. The results in figure 4.15 show that 24-bit fixed-point and floating-point have very similar decoding performance.

Using VHDL (a hardware description language) code generated in Matlab, we are able to create code for parallel implementations of sum-product decoding for arbitrary values of H. While a Register Transfer Level (RTL) simulation of the 1200×4000 LDPC code is possible, a fully parallel implementation is not possible at this time. A 60×200 LDPC code with a row weight of 12 that is capable of operating at 50MHz was synthesized using the Artisan 3.0 logic cell library for 0.18 μm CMOS technology (several generations behind state of the

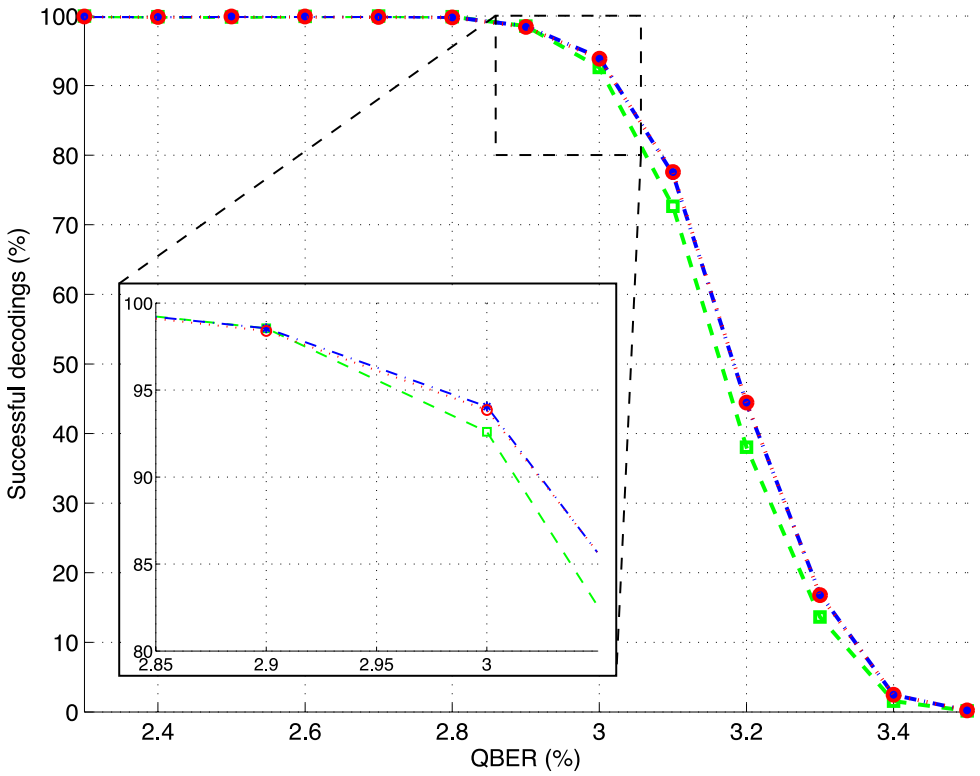

Figure 4.15: Simulation of the 1200 × 4000 LDPC code using 16-bit fixed-point ($- - \square$), 24-bit fixed-point ($- \cdot - , *$) and floating point ($\cdot \cdot \cdot \cdot \cdot , \circ$). The inset shows the region where the performance begins to drop in more detail.

Table 4.4: Simulation results for 60 × 200 LDPC decoding.

QBER (%)	Success rate (%)	Mean iterations	Sifted key rate (Mb s^{-1})
2.5	99.00	4.1070	52.9319
3.0	91.65	8.6785	25.0494
3.5	69.80	17.9455	12.1146

art). This code uses 12-bit arithmetic and requires 46 clock cycles (0.92 μs) per iteration of the algorithm. Simulation results for the performance of this code with a maximum of 40 iterations are given in table 4.4. The design contains 1,860,429 cells with a total cell area of approximately 47.24 mm^2.

Attempts to synthesize a larger LDPC code using the current VHDL code have failed as the synthesis tool does not have sufficient memory to complete the process. The size of the design also suggests that a 1200×4000 code would be impractical to implement (as a comparison, a processor is typically of the order of 100 mm^2, including interconnect).

However, larger codes are preferred because they experience less variance from the mean QBER and perform better relative to the Shannon limit.

It is important to note that we obtained these results without using any advanced techniques to reduce the size of the design. More efficient multiplier designs or the use of alternative number systems such as the multidimensional logarithmic number system (MDLNS) [63] have the potential reduce the hardware required to perform the computations. Larger block sizes could also be achieved using the partially parallel implementations proposed in [64], where efficient schedules are used rather than updating all probabilities at once, reducing the number of computations done in parallel, while mitigating the cost in terms of the run time.

4.1.9 Conclusion and outlook

We have proposed a novel, fibre-based QKD system employing polarization encoding and Q-frames, and have demonstrated in a long-term (37 h) QKD proof-of-principle study that polarization information encoded in the classical C-frames can indeed be used to stabilize unwanted qubit transformation in the quantum channel. All optical elements in our setup can be operated at Gbps rates, which is a first requirement for a future system delivering secret keys at Mbps. In order to remove another bottleneck towards a high rate system, we are investigating forward error correction based on LDPC codes [59, 60]. Work on the implementation of a system that distributes a quantum key, building on the here presented proof-of-concept demonstration, is under way.

4.1.10 Acknowledgements

The authors gratefully acknowledge discussions with Xiongfeng Ma. This work is supported by General Dynamics Canada, Alberta's Informatics Circle of Research Excellence (iCORE), the National Science and Engineering Research Council of Canada (NSERC), QuantumWorks, Canada Foundation for Innovation (CFI), Alberta Advanced Education and Technol-

ogy (AET), CMC Microsystems and the Mexican Consejo Nacional de Ciencia y Tecnologa (CONACYT).

Chapter 5

Analyzing QKD system performance

An important figure of merit of a QKD system is its secret-key rate for given loss in a quantum channel between two users. Significant effort has been dedicated to maximizing the secret key rate when implementing QKD systems. Obtaining secret-key rates of giga bits per second (Gbps) is an important milestone towards matching bit rates of classical communication systems [65]. To date, QKD systems can generate secret key at rates of $\sim$ 1 mega bits per second (Mbps) for a distance of 20 km between users [66]. In order to increase the secret-key generation rate of a QKD system further, it is important to investigate its performance and identify bottle necks, which could originate at different stages of the secret key distribution process.

The steps that take part in the distribution of a secret key between Alice and Bob and that must be optimized are: 1) raw key establishment, 2) sifting, 3) error correction, 4) privacy amplification. Steps 2, 3 and 4 are known as post-processing operations. Here, I will highlight the data processing and necessary communication between Alice and Bob that occurs during each step.

To achieve high secret-key rates, the first requirement is to achieve a high raw-key rate, which requires having a high qubit generation rate at the source and a high detection rate at the receiver. To generate a qubit the following is required: Alice does a random selection of the basis and qubit state in which the qubits are prepared. Both choices of basis and qubit state must be recorded. At the receiver side, Bob must also record the random measurement basis choice, the detector that registers each photon, as well as the time the detection happens. The bit values obtained by Alice and Bob after this process is known as *raw key*. Alice and Bob need to process the raw key to obtain a secret key. The processing of

the raw key is done using an authenticated classical channel between Alice and Bob.

During sifting, Alice and Bob communicate the bases selected to prepare and measure each bit that forms the raw key, keeping only the events in which both bases coincide. At the end of this process they each have a *sifted key*. In an ideal implementation, the bits belonging to the sifted keys would be perfectly correlated. In a real implementation, however, inevitable errors will result in differences between the two keys. The differences between Alice's sifted key and Bob's sifted key are eliminated through error correction. It has been shown that an efficient method for error correction is through the use of so called low-density parity check (LDPC) matrices as it only requires one-way communication between Alice and Bob [58]. In LDPC error correction, Alice tells Bob parity information (whether there is an even or an odd number of bits with value one) about her sifted key. Bob, in turn, compares the parity bits calculated from his own sifted key, through a previously agreed-upon parity check matrix, with the information he receives from Alice. The information that Bob receives from Alice allows him to find the errors in his sifted key and correct them such that, at the end of the process, his error-corrected key is identical to Alice's. After error correction, Alice and Bob share an error-corrected key (identical string of random bits). For detailed information about LDPC based error correction refer to appendix A.

Finally, to remove any information Eve may have obtained during transmission of quantum data as well as of classical error correction, a process known as privacy amplification is performed. During privacy amplification, Alice and Bob compress their error-corrected keys to a shorter key via a hash function (i.e. a function that maps a string of bits to a shorter string of bits). By using hash functions, the probability that Eve's compressed key is the same as Alice's and Bobs's is very small (in fact, the probability is $1/2^n$ where n is the number of bits in the compressed key). Following privacy amplification, Alice and Bob share a secret key.

In this chapter I present a paper in which we carry out a time-cost analysis of the secret

key establishment in our QKD system. The system implements the BB84 protocol with decoy states (see chapter 3) and quantum frames (see chapter 4) and is clocked at 100 MHz. This system is described in detail in 4. All post-processing is implemented via software. This work quantifies the scalability of the sifted and error corrected key as a function of the raw key rate of our system. The study takes into account the data generation, collection, and processing steps that Alice's and Bob's systems must accomplish during sifting and error correction. We show that in our implementation, data processing is a limiting component to reach higher secret key rates. From this investigation we state the necessary improvements for future QKD systems in order to maximize the secret key rate. Through the quantification of this processes we highlight the importance of moving to hardware-based post-processing and processing of data in a parallel fashion.

This work was done in collaboration with Xiaofan Mo, Philip Chan, Chris Healey and Steve Hosier. I contributed to this study in the following stages: I was responsible for the integration and test of drivers to control the optical components of the system. I carried out measurements. In this system a home-made single photon detector was employed. I characterized the detector and integrated it in the system to perform the high speed measurements. Sections 1 and 2 of the manuscript that follows were written by myself and I was involved throughout the editing process.

5.1 Time-cost analysis of a quantum key distribution system clocked at 100 MHz

X. F. Mo[1], I. Lucio-Martinez[1], P. Chan[2], C. Healey[1], S. Hosier[3], W. Tittel[1]

1. Institute for Quantum Information Science, and Department of Physics and Astronomy, University of Calgary, Calgary, Alberta, T2N 1N4, Canada

2. ATIPS Labs, Department of Electrical and Computer Engineering, University of Calgary, Calgary, Alberta, T2N 1N4, Canada

3. Southern Alberta Institute of Technology, Calgary, Alberta, T2M 0L4, Canada

Abstract

We describe the realization of a quantum key distribution (QKD) system clocked at 100 MHz. The system includes classical post-processing implemented via software, and is operated over a 12 km standard telecommunication dark fiber in a real-world environment. A time-cost analysis of the sifted, error-corrected, and secret key rates relative to the raw key rate is presented, and the scalability of our implementation with respect to higher secret key rates is discussed.

5.1.1 Introduction

Quantum Key Distribution (QKD) takes advantage of the peculiar quantum properties of single photons to distribute secret keys [4, 10, 11]. When implemented correctly [67, 56, 68, 69], QKD, in combination with the One-Time Pad, allows two distant parties to communicate in an information-theoretic secure way over an untrusted but authenticated channel.

A QKD system requires a quantum and a classical channel to distribute quantum information, here in form of quantum bits (qubits), and classical information, respectively. To obtain a secret key, a QKD system must complete the following steps: 1) Generation, faithful transmission, and measurement of qubits, yielding the *raw key*. 2) Sifting of the raw key,

i.e. comparison of the bases used by the sender and receiver to generate and detect each individual qubit. This is done over the classical channel. Only detection events where the bases match are kept, resulting in the *sifted key*. 3) Error correction. The purpose of this step is to remove all errors in the sifted key due to a noisy channel or eavesdropping. This procedure requires communication over the classical channel. It yields information about the quantum bit error rate (QBER) of the sifted key and results in the *error-corrected key*. 4) Privacy amplification. The final step in QKD shortens the error-corrected key and thereby removes all information that Eve might have obtained while eavesdropping. The result is the *secret key*. Furthermore, all classical communication required for the establishment of the secret key has to be authenticated to corroborate the identity of the authorized parties and to avoid a man-in-the-middle attack.

For given loss in the quantum channel, the relevant figure of merit characterizing a QKD system is the secret key rate. Significant effort has been devoted over the past several years to increase this rate [70, 71, 72]. However, with a few notable exceptions reporting actual rates up to 1 MHz [15, 17], the secret key rate is often calculated from the sifted key rate assuming a reasonable efficiency for error correction as compared to the Shannon limit [54], and taking into account a reduction of the error-corrected key during privacy amplification [28]. While this leads to a rate that has some predictive power, it states an upper bound that can only be attained if qubits are distributed continuously, key sifting, error correction and privacy amplification can keep up with the rate at which the raw key is obtained, and if the memory of the processor(s) in use can cope with the amount of data involved. These conditions may be difficult to satisfy in an actual system, in particular in the case of systems clocked at high rates.

In this paper we analyze the performance of our QKD system in view of a high secret key rate. The goal of the analysis is to determine the limitation on the key rate based on the time-cost of each of the steps mentioned above. We also propose improvements that we will

pursue in the near future. The bottlenecks revealed in this analysis, while obtained using our QKD system, are likely to be relevant for other implementations as well. Hence, we believe that this study will help other research groups to develop high-rate QKD systems.

5.1.2 Our QKD System

Hardware

Our test took place between the Quantum Cryptography and Communication Research Laboratory (QCCRL) at SAIT, where Alice is placed, and the Quantum Cryptography and Communication (QC2) Laboratory at the University of Calgary (UofC), where Bob is located. As usual, Alice and Bob denote the sender and receiver of quantum data, respectively. The transmission loss of the communication channel, a 12 km-long standard telecommunication fiber featuring many splices, is 6.5 dB. Our QKD system is fiber-based, implements the BB84 protocol supplemented with two decoy states [11, 25, 26, 27] to detect photon number splitting attacks [53, 9], and employs polarization encoding. Furthermore, it is characterized by the use of quantum frames, which consist of alternating sequences of high-intensity laser pulses (forming classical control frames) and faint laser pulses (encoding quantum data), see figure 5.1. The classical control frames contain frame number and polarization information; the latter is used to assess and compensate time-varying birefringence in the communication channel [73]. The frames also contain information for clock synchronization and, in view of future integration into network environments, sender and receiver address to allow for routing.

Figure 5.2 shows a schematic of the optical and electronic components of our QKD system; a more detailed description of the optical part is given in [73]. Optical pulses of 500 ps duration and 1550 nm wavelength are generated by the *quantum laser diode* and are attenuated using a variable attenuator (ATT). To create the required signal and two decoy states, we use an intensity modulator (IM), generating weak pulses of light with mean photon numbers of μ, 0.2μ, 0.01μ, respectively (the fixed relation between these three values

is due to the way the attenuator and intensity modulator are used to generate loss). To encode the required polarization states, $\pm$ 45^o linear polarized, and right- and left-circular polarized states, we use a polarization modulator (PM). Both modulators are configured to ensure passive compensation of temperature-dependent birefringence and polarization mode dispersion. On the receiver side, a photodiode is placed behind a 90/10 beamsplitter; it allows detecing the strong optical pulses, generated by the *classical laser diode*, that form the control frames. Next, a 50/50 beamsplitter is placed to randomly select one of the two polarization bases for qubit measurement. Per basis, a voltage-controlled polarization controller (PC) and an optical detector (a low-bandwidth powermeter in the current system, not shown) are used to compensate for time-varying polarization changes in the transmission line. This procedure relies on feedback from the classical control frames.

Polarization compensation executes whenever the QBER exceeds a certain threshold (between 3% and 4.5%, setup dependent). We have previously shown that the polarization stability over our real-world fiber link can vary greatly over time [73]. Thus, for this feedback to work, the QBER must be updated sufficiently often, i.e. error correction must run on sifted key bits collected over a sufficiently short time[1]. In this case the feedback will ensure that the QBER is kept low when the channel is unstable (then generating only a small amount of raw key bits), while allowing key generation to run without interruption over several minutes during extended periods of stability. The time needed for polarization compensation is determined by the reaction time of the powermeter, which limits the number of detectable voltage changes per second to one.

Qubit detection is either accomplished using four commercially available single photon detectors (SPDs) gated at 1 MHz, or using one high-rate, home-made detector [74] that utilizes the self-differencing technique [75, 76] and allows photon detection up to 100 MHz. Note that qubit generation is clocked at 100 MHz in both cases. Currently, our QKD system

[1]In the current setup, the number of sifted key bits to be processed in one execution of error correction is fixed to 10 kb. The time required to collect this data is setup dependent.

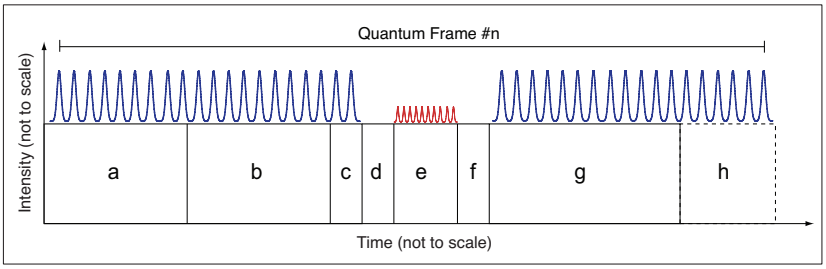

Figure 5.1: Structure of the quantum frames. a: generation of bit and basis information to encode qubits; b: data transfer; c: generation of the classical control frame; d: deadtime, e: generation and transmission of quantum data (qubits); f: deadtime, g: processing time, h: time for polarization control (when required).

is vulnerable to fake-state attacks [68], but preventive measures against detector vulnerabilities and potential loopholes arising from control information being sent between Alice and Bob [68, 69] or high-rate operation [77] will be implemented in the near future.

Software

All data is transferred via National Instruments digital I/O cards into or out of the CPUs with the following specifications; Alice: AMD 64 X2 Dual Core 4600+, 2.4 GHz, 2 GB RAM, WinXP 32-bit; Bob: Intel Core2 Quad CPU Q8300, 2.5 GHz, 4 GB RAM, Windows Vista 32-bit. Our system uses Field Programmable Gate Arrays (FPGAs) to control all active components. The clock rate, 100 MHz, is limited by the rate with which electronic signals are currently generated by the FPGA and can be transmitted to, and converted by our home-made drivers that control the laser diodes and modulators. However, the optical components can generate qubits at a maximum rate of 980 MHz. Our system also includes classical post-processing (sifting, error correction and privacy amplification) implemented via software. Error correction is performed using low-density parity check codes (LDPC) [59, 60, 58], and privacy amplification founds on Toeplitz matrices [78].

Our QKD software is responsible for frame generation (Alice), data acquisition (Bob), key sifting, error correction, controlling polarization compensation, and writing collected data to the hard drives. The classical communication required for these tasks is performed using a

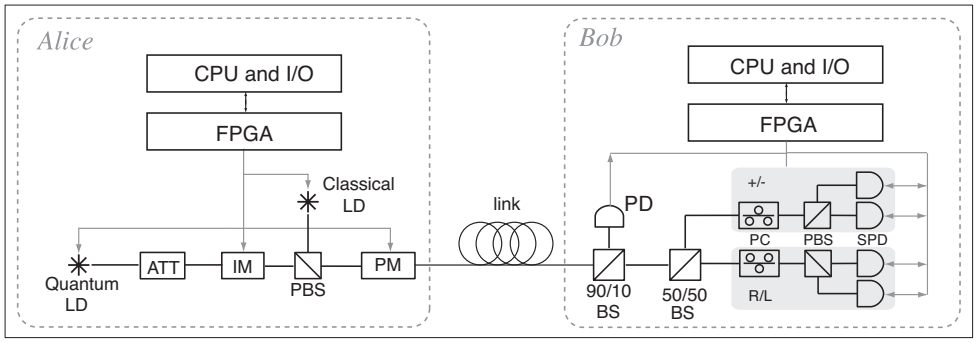

Figure 5.2: Schematics of the optical and some electronic components of our QKD system. LD: laser diode; ATT: attenuator; IM: intensity modulator; PBS: polarization beam splitter; PM: phase modulator; BS: beam splitter; PD: photo diode; PC: polarization controller; SPD: single photon detector; CPU: central processing unit (personal computer); FPGA: field programmable gate array; I/O: input/output interface. See text and [73] for more details.

TCP/IP connection established between the two computers over the public Internet. Each of the post-processing tasks can run independently, and both Alice and Bob run their tasks on one computer each. The data gathered by the system is analyzed later on a computer with an Intel i5 CPU 760 @ 2.8GHz, where decoy state analysis and privacy amplification is performed.

The software is implemented primarily in National Instruments LabVIEW, with more time-intensive tasks being implemented in C++ libraries that are called as appropriate by the LabVIEW code. These libraries may execute in parallel with any LabVIEW code that is not directly involved in controlling their execution. Hence, as more than one task may be executing at the same time, the elapsed times that we measure for processing tasks do not necessarily represent the required execution time. In particular, some tasks such as polarization compensation are not computationally intensive, but currently require significant time for the hardware to act. During this time, computationally intensive tasks such as error correction may execute if there is data available to be processed.

5.1.3 System Performance

To determine the performance of our QKD system, we increase the raw key rate from 0.2 to 120 kbps, and monitor the sifted and error-corrected key rates. As we will argue below, the secret key rate is simply related to the error-corrected rate by a factor described in [28]. As an example, the reduction assuming a QBER of 2.6%, μ=0.5 photons per pulse (with Poissonian photon number distribution), and no PNS attack is 23.5% (see also [73]).

In a first set of experiments, we employ four commercial single photon detectors gated at 1 MHz. This effectively limits the clock rate of our QKD system to the same value. To change the raw key rate, we vary μ between 0.40 and 7.0 photons per pulse. Given the loss of 6.5 dB in the quantum channel, a detector efficiency of $\sim$10%, as well as additional attenuation of $\sim$3.5 dB in Bob's device, this yields raw key rates between $\sim$0.2 and 4.8 kbps. This calculation also takes into account that quantum data is sent only during $\sim$10% of the system operation time; this is further discussed below. While this procedure does not deliver secret keys for large values of μ (e.g. $\mu > 1$), it does allow us to gauge how the system responds in the event of large raw key rates. However, we point out that there is a limit to this procedure. Indeed, as μ increases, the probability that multiple detectors detect photons simultaneously also increases. This leads to larger processing requirements as only one, randomly selected detection is kept for subsequent steps [48]. In turn, this leads to an underestimation of the sifted key, and hence error-corrected key rates (this effect was, however, not noticeable for $\mu \leq 7$).

To obtain higher raw key rates, we perform a second set of measurements using a single, home-made SPD [74] that is gated at 100 MHz. We vary μ from 0.30 to 20 photons per pulse. Obviously, using only one detector does not allow distributing a secret key. Nevertheless, this setup allows increasing the raw key rate, and hence assessing the system performance in the event of large rates. More precisely, it delivers one quarter (i.e. 2.24 to 121 kbps) of the raw key rate we expect in a fully implemented QKD system with four high-rate detectors

while providing a similar QBER. All key rates listed below and in figure 5.3 refer to the actually detected (not extrapolated) rates.

Figure 5.1 shows the execution flow and frame structure in our system from Alice's perspective. This perspective was chosen since Alice's timing currently limits the maximum frame rate. First, the state of all qubits within a quantum frame is determined by a software-based pseudo-random number generator (a, 225 ms). Note that this solution is temporary - our final QKD system will employ true (if possible quantum) random number generators for improved security; this will be discussed in section 4. This data is then transferred to a digital I/O card (b, 225 ms), which, along with an FPGA, controls our hardware. These devices generate the classical control frame (c, 960 ns), which includes a frame number, control information for polarization compensation, and a sender and receiver address that will be used for quantum packet routing in future work. The header is followed by a deadtime (d, 50 ms), after which the qubits are generated and transmitted (e, 100 ms). A second deadtime (f, 50 ms) follows. These deadtimes exist to avoid accidentally exposing the single photon detectors to strong light, which is generated at all times outside of the deadtimes and 'qubit time' (e). The second deadtime is followed by an idle time for the hardware, which is used by the computer for software post-processing and data logging (g, 55-130 ms, depending on the raw key rate). This time is determined by when the processor becomes available to generate the data for the next quantum frame. In particular, when the error rate has exceeded a certain threshold, the overall idle time is extended and then also comprises compensation for time-varying birefringence of the communication channel (h, averaging to 140 ms per frame). To summarize, qubits are transmitted on average during 100 ms out of 845-920 ms, i.e. during 10.9-11.8% of the system operation time.

The sifted and error corrected key rates obtained over the total system operation time are shown in figure 5.3 as a function of the raw key rate. From figure 5.3 we see that the error-corrected key rate peaks at 33.488 kbps at a raw key rate of 69.720 kbps, and that the

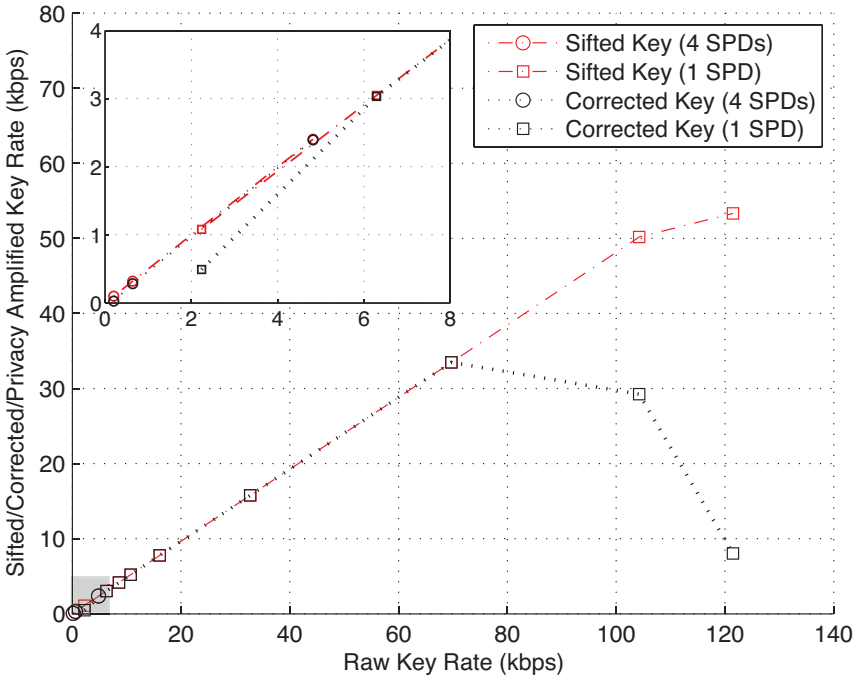

Figure 5.3: Sifted and error corrected key rates as a function of the raw key rate. The inset shows the shaded area in more detail.

sifted key rate does no longer increase linearly with respect to the raw key rate once the latter exceeds 114.160 kbps. This is due to the fact that the post-processing software is run on the same computers as the data generation and collection software, and once processing resources are at their limit, the error correction, and subsequently key sifting, will get less execution time than is required to process all available data. To show the impact of this effect, error correction was run independently with simulated data, yielding a maximum error-corrected key rate of 53.213 kbps at an average QBER of 3.5%. This average QBER is consistent with what is experienced during operation of the QKD system with the four commercial single photon detectors and $\mu = 1$. The QBER obtained using the high-rate detector is lower due to a better ratio between detection efficiency and dark count probability. In addition, the QBER decreases as μ is increased since the higher detection rates make dark counts less significant. Thus, the 33.488 kbps rate obtained in the actual system is due to limited computational resources. Similarly, we also conclude that the sifted key rate is affected by

process competition.

We have also performed the decoy state analysis (according to the methodology described in [27]) on the data recorded by our QKD system to establish the maximum amount of information that may have leaked to an eavesdropper. The execution time to process the data collected over 15 hours (enough to ignore finite key effects [79, 80]) was found to be less than a minute, and is thus negligible. Privacy amplification using the Toeplitz matrix approach has also been shown to require insignificant computational time if a number theoretic transform is used [15, 78]. Hence, the time required to establish and remove the eavesdropper's information does not need to be considered in our time-cost analysis. In addition, authenticated communication is needed for all classical post-processing steps to prevent a man-in-the-middle attack [81]. Yet, the impact of authentication on the secret key rate is negligible as well. Indeed, authentication of Gbps messages in real-time has been reported [82, 83].

5.1.4 Proposed Improvements

The secret key rate of our QKD system can be improved by increasing the proportion of time spent transmitting quantum data. Three simple modifications to our close to sequential execution of tasks stick out. First, the deadtimes (d, f) can be shortened. In principle, these times can be less than a millisecond. However, as our system is still under development, we have chosen to maintain a large safety margin in case changes are made that alter the relative timing at the sender and receiver. Second, we write more information to the hard drives than is necessary to perform decoy state analysis, privacy amplification, and authentication. This increases the hardware idle time (g), but allows for a thorough analysis of the system. The secret key rate can thus be improved by writing only necessary information to file, or by replacing our current approach with a more efficient method of data transfer. Third, the powermeters used for polarization compensation have a response time on the order of a second, and multiple measurements are required to determine the necessary adjustments to

the polarization controller. As such, the polarization compensation time (h) can be reduced to a few ms by using fast photodetectors in conjunction with a fast polarization controller.

In addition, we note that the 100 ms time interval for qubit transmission in each frame (e) is determined by the clock rate of 100 MHz and by the available memory in the digital I/O card, which allows generating 10^7 qubits per frame. This limitation is present in our system for both detector setups, as Alice's system generates qubits at 100 MHz even when the detector gate rate is limited to 1 MHz. While reducing Alice's clock frequency in the case of the commercial detectors would bring the time used for qubit transmission much closer to 100% of the system operation time, this would ideally provide only a 8-9 fold increase in the raw key rate. In comparison, using the fast detector provided more than a 60 fold increase in raw key rate. In the case of the fast detector setup, it is possible to add more memory to the I/O card. However, this would result in a proportional increase in the time required for the data preparation (a), data transfer (b), and key sifting plus error correction (g) steps. This suggests that the following needs to be explored: a faster interface to the computer, faster random number generation, as well as more efficient post-processing, for instance using dedicated hardware that may also take care of authentication.

As used in QKD, LDPC encoding is not computationally intensive, requiring only a series of parity calculations [58]. Decoding, however, is an iterative process that uses the received data, parity information, and an initial estimate of the error rate (derived from previous executions of the protocol) in order to compute better estimates of the probability that each bit is in error [59, 60]. This iterative process ends successfully when the most likely result for the corrected data is consistent with the parity information, and failure is declared if a set maximum number of iterations is reached without meeting this condition. In order to improve the throughput of the error correction in our system, two approaches are possible. The computations required for LDPC decoding algorithm are well suited to parallel implementations. Thus CPU utilization can be improved in our software implementation

by taking advantage of this fact. Moreover, LDPC decoding is well suited to hardware implementation [84], and performing the decoding using specialized hardware, whether in an FPGA or custom integrated circuit, can yield error-corrected key rates of Mbps error-corrected key rates, as we have shown in [73]. It should also be noted that the error correcting code used in our experiment was originally designed for use with the commercial detectors. Since these detectors only provide a small key rate, a short block length of 10^4 bits was used for the LDPC code in order to evaluate the QBER, and hence provide feedback to initiate the polarization control procedure in a timely fashion. The block length of the code can be increased significantly when using fast detectors, leading to better performance relative to the Shannon limit. This, in turn, translates to a higher secret key rate since less information is revealed to the eavesdropper in this process.

Similarly, one should investigate hardware-based key sifting. In particular, executing sifting, error correction, privacy amplification and authentication within the same FPGA would avoid time-consuming data transfer into and out of a CPU.

Another concern in our current implementation is the generation of random qubit states using a software-based, pseudo-random number generator. For a secure system, a true (possibly quantum) random number generator (RNG) is required. A lot of progress has been obtained over the past years, and the highest rate for a quantum RNG reported to date is 50 Mbps [85]. Hence, two RNGs operated in parallel would suffice for our current system as only $\sim 10^6$ qubits are generated per second, and each qubit is determined by six random bits with uniform distribution of zeros and ones[2]. Yet, to improve the clock rate to 1 GHz, or the fraction of time during which qubits are generated, or both, the amount of RNGs that have to be operated in parallel would constitute a major challenge. Nevertheless, given recent progress in high-rate single photon detectors [76], better quantum RNGs may

[2]Two bits are required to determine each polarization state, and four bits allow a random choice of vacuum, decoy and signal states with the desired distribution. Furthermore, some randomness is required for privacy amplification. Note that no random numbers are required at the receiver end due to the passive basis choice

become available in the near future and allow for high-rate QKD. Another possibility, which would already constitute a significant improvement over pseudo-random numbers, is the use of physical (non-quantum) RNGs for which Gbps rates have been reported [86].

5.1.5 Conclusions

We have demonstrated a QKD system that implements the BB84 protocol supplemented with decoy states and quantum frames. The system executes software-based key sifting and error correction in real-time over a real-world fiber optic channel. We have done a time-cost analysis of all steps required in the generation of a secret key, and proposed improvements to our current implementation. Furthermore, we have analyzed the scalability of the sifted, error corrected and privacy amplified key rate with respect to the raw key rate, finding them to be determined by the sequential execution of the different steps in the key distribution protocol. Consequently, all processes that take significant time despite optimization have to be executed parallel to the distribution of qubits using dedicated, possibly custom hardware. Ignoring communication time, transmission loss and detector efficiency, the secret key rate would then be limited by the clock rate and the detector gate rate, i.e. 100 MHz in our current implementation with high-rate detectors.

Acknowledgements

The authors thank V. Kiselyov for technical support. This work is supported by General Dynamics Canada, Alberta's Informatics Circle of Research Excellence (iCORE, now part of Alberta Innovates Technology Futures), the National Science and Engineering Research Council of Canada (NSERC), QuantumWorks, Canada Foundation for Innovation (CFI), Alberta Advanced Education and Technology (AET), and the Mexican Consejo Nacional de Ciencia y Tecnología (CONACYT).

Chapter 6

Modelling and implementing a measurement-device-independent QKD system

Quantum key distribution promises information theoretical security; this means security can be proven without assumptions about the computational power of the eavesdropper and for any eavesdropper bounded only by the laws of quantum physics. Security proofs of QKD are, however, typically done under certain assumptions about the devices used to perform QKD. Some of these assumptions are difficult to fulfil in experimental implementations and QKD systems can be subject to hacking attacks in which Eve exploits the leakage of information about the key through un-monitored side-channels.

To date, a number of proposals and demonstrations of possible side-channel attacks exist [9, 19, 68, 55, 87]. Different attacks target different vulnerabilities of QKD implementations. In the following paragraphs I will describe the most relevant side-channel attacks and possible countermeasures. The first attack is the photon-number splitting attack [9], which was explained in detail previously in chapter 3. This attack can be implemented if the source has a non-zero probability of emitting optical pulses that contain more than one photon (e.g. sources that use weak coherent pulses at the single photon level), instead of perfect single photons, as is the case in the majority of QKD systems. The photon-number splitting attack can be overcome if the decoy state protocol is implemented [25, 26, 27], for details see chapter 3.

A second attack is the so-called Trojan-horse attack [19]. In this attack Eve probes Alice's system by sending high intensity pulses into it. Eve can obtain information about the key through reflections from the optical elements of which Alice's system is composed of. This attack can easily be avoided by using an optical isolator, which is an optical element

that transmits light in only one direction. If the optical isolator is placed at the entrance of Alice's laboratory it would allow the transmission of optical pulses out of her system but would suppress the transmission of light directed towards the system.

Many proposed side-channel attacks exploit vulnerabilities of the single photon detectors used in QKD implementations [55, 68]. Note that single photon detectors are particularly exposed element of QKD implementations because external signals to Bob's laboratory, regardless of their origin[1], must always have an optical access to the photodiode where the detection occurs. Eve can take advantage of this optical access to send any kind of optical signals to Bob's system and attack it. The third side-channel attack I describe exploits the optical access to Bob's laboratory and it is called fake state attack. This attack consist of a combination of an intercept-resend attack and a blinding attack [88]. In the blinding attack Eve takes control of the single photon detectors by sending high intensity light to them. Single photon detectors are avalanche photodiodes (APD) that work in the so-called gated mode. In the gated mode the photodiode is reversed biased above breakdown voltage for a brief period of time, see figure 6.1a; this period of time is called gate. During the gate, the detector is sensitive to single photons impinging on the photodiode causing an electrical current through the device. This current gets amplified in an avalanche effect, producing a detection signal (also referred to as *detection event*). In order to suppress excess noise, the current avalanche is quenched by lowering the voltage below breakdown voltage. If Eve sends high intensity cw (continuous wave) light to the detector, it will lower the bias voltage causing it not to gate anymore (see figure 6.1b) and therefore the detector is no longer sensitive to single photon pulses. This attack is known as *blinding attack*. Although, at this point the avalanche photodiode cannot detect single photons, it is still sensitive to high intensity pulses and an electornic signal whose amplitude is proportional to power of the impinging light will be produced. Provided the amplitude exceeds a threshold in the subsequent electronic (generally including a threshold discriminator), a detection event

[1]These can be qubits emitted by Alice or high intensity pulses emitted by Eve.

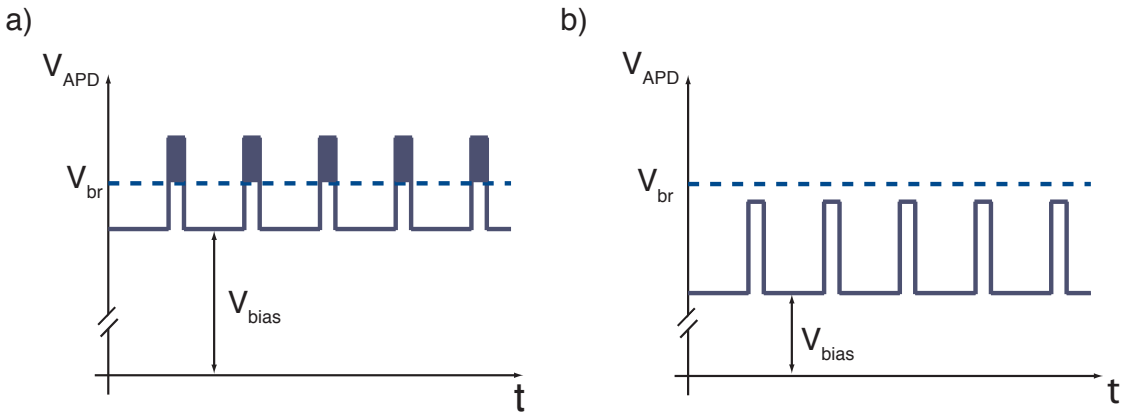

Figure 6.1: Voltage across avalanche photodiode. a) The avalanche photodiodes spend time biased under breakdown voltage (V_{br}); when they are gated above breakdown voltage the photodiode is sensitive to single photons. b) During the blinding attack, Eve sends high intensity light to the avalanche photodiode, reducing the bias voltage (V_{bias}). The detector is no longer gated and it is not sensitive to single photons. However it remains sensitive to high intensity pulses.

is produced. Eve can add high intensity pulses to the light used to blind the detectors to produce the detection events expected by Bob when the single photon detectors are operating in the expected mode. In a fake state attack Eve performs an intercept-resend attack and measures Alice's single photons in one of the two bases used to encode the qubits. Eve then sends high intensity pulses to Bob according to the result she obtained in her measurement. Eve can force Bob's detector to produce a detection event only if his basis choice is the same as Eve's, otherwise the optical power is split and the signal arriving to the detector is not strong enough to produce the detection event. With this attack Eve can learn Alice's and Bob's raw key without leaving a trace. Once Eve knows the raw key she listens to all the post-processing communication and processes her raw key accordingly to obtain the same secret key as Alice and Bob. The fake state attack has been demonstrated experimentally [68] and in view of the amount of information that Eve can obtain about the key it is the most threatening for current QKD systems. A countermeasure for this attack is to place an additional photodiode at the entrance of Bob's laboratory to monitor the input power to the detectors.

The fourth side-channel attack also takes advantage of single photon vulnerabilities; it is called time-shift attack. In this attack the eavesdropper exploits differences between the quantum detection efficiencies of the single photon detectors employed in an implementation. In a QKD system, the single photon detectors are gated simultaneously, however due to unavoidable variations between the electrical wiring or the optical path to the different detectors, the gate windows of the two detectors do not perfectly overlap. The mismatch of the two gate windows can be exploited by Eve if she uses an intercept resend attack in combination with a fake state attack using very short optical pulses. Eve can intercept Alice's qubit and measure it. She then adjusts the timing of the signal that she resends to Bob. By changing the arrival time of the optical signal to the detector she can change the probability of triggering one or the other detector provided she knows the gate window mismatch. As Eve controls if one of the two detectors triggers, and each detector has a bit value associated to it, Even can determine the bit values of Bob's key. This attack can be prevented if the detector gate is characterized carefully with a narrow optical pulse in order to obtain the gate features with the best resolution possible. Bob can also check the timing of the incoming pulses to his laboratory at random points of the key distribution process to detect the attack.

Note that, in general, once a side-channel attack is discovered it is typically possible to detect it or avoid it by improving the technology employed in the QKD implementation. However, one can never be sure that improved attack strategies of the eavesdropper are countered by improved technology of the legitimate users. An alternative to technological updates for every side-channel that is discovered is to develop more robust protocols that can guarantee the security of the distributed key despite the inevitable imperfections present in the devices used.

In 2011, Lo and co-workers [89] proposed a protocol that removes all possibilities for side-channel attacks that take advantage of single photon detector vulnerabilities. The protocol

is called measurement-device independent QKD. In this protocol a secret key is distributed between Alice and Bob through Charlie, a third untrusted party located between them. Alice and Bob each have a source of qubits. Each source produces equally probable, random and independent qubits chosen among the BB84 states. Alice and Bob send their qubits to Charlie. In turn, Charlie performs a Bell state measurement (BSM) on the pair of qubits he receives. The BSM projects both qubits onto one of the maximally entangled Bell states, (for more information about Bell state measurements refer to chapter 7 and appendix C). For instance, Charlie announces whenever the qubits have been projected onto the $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ state. Provided Alice and Bob used the same basis to prepare their qubits, they know that, for the announced events, they have bits with completely anti-correlated values. Subsequently, Alice and Bob can distil a secret key through classical post-processing. Note that Charlie is an untrusted third party and could easily perform a side-channel attack on the single photon detectors, which are in his possession. However, if Charlie performs a BSM it is fundamentally impossible for him to find out if Alice input a qubit encoded with a value of zero and Bob a value of one or vice versa - he only learns that Alice and Bob have anti-correlated values. Hence monitoring detection events does not provide Charlie with any information about the key because the protocol completely de-correlates the detection events from the bit value. Charlie could also try to fake detection events or cheat during the measurement process by not performing a BSM and instead executing another measurement that could give him information about the key. In this case, Charlie increases the QBER that Alice and Bob measure, therefore leaving a trace. In the MDI-QKD protocol, Charlie is effectively post-selecting projections onto maximally entangled states between Alice and Bob. Consequently, the protocol is equivalent to an entanglement based QKD system performed in a time-reversed manner, which has been proven to be secure [90].

Additionally, the MDI-QKD protocol is well suited to develop star type quantum networks. A star network consists of one central node to which all other nodes are connected. In

the quantum network Charlie would be located in the central node with the detectors needed to implement QKD and he would provide connections to any pair of users in the network that want to share a key. The benefits of this scenario are twofold: first, Charlie does not have to be a trusted node, second: the implementation of a star quantum network would require for only one node to be equipped with single photon detectors, which are typically the most costly devices in a QKD system.

This chapter contains two articles. The first article shows the development of a predictive model of a MDI-QKD system. The mathematical model predicts the performance of the system by taking into account imperfections in the devices employed. It reproduces the measurable parameters of the system such as quantum bit error rate as well as projection probabilities onto the $|\psi^-\rangle$ Bell state. The model also allows us to optimize the system performance as a function of the mean photon number emitted by the users, and allows us to identify limiting components of the system. This article also includes the experimental verification of the model.

In the second paper we added to the proof-of-principle demonstration the implementation of the decoy state protocol. In this proof-of-principle demonstration the mean photon number emitted by each source has been optimized via the mathematical model presented in the first paper of this chapter, allowing to optimize the secret key rate for each distance (or loss) between Alice and Bob. The proof-of-principle demonstration was done over deployed fiber in the city of Calgary and in a laboratory environment and it shows the possibility to perform a Bell state measurement with independently generated qubits travelling through deployed fibers featuring uncorrelated changes of polarization transmission times of the photons.

This work was done in collaboration with Allison Rubenok, Joshua Slater and Philip Chan. I contributed to these studies during the following stages: all measurements during the laboratory tests as well as over the deployed system across the city. I contributed to the location of implementation imperfections through different measurements and tests. I

also contributed to quantifying the imperfections in the implementation, some of which were possible to eliminate, this made possible to perform the demonstration at long distances. I contributed to the development of the model presented in the first paper. I contributed by writing sections 1, 2 and 3 of the first manuscript and taking part of the editing process as well as response to the referees for publication for both manuscripts.

6.1 Modeling a measurement-device-independent quantum key distribution system

P. Chan,[1,2] J. A. Slater,[1,3] I. Lucio-Martinez,[1,3] A. Rubenok,[1,3] W. Tittel[1,3]

[1]*Institute for Quantum Science & Technology, University of Calgary, Canada*

[2]*Department of Electrical & Computer Engineering, University of Calgary, Canada*

[3]*Department of Physics & Astronomy, University of Calgary, Canada*

Abstract

We present a detailed description of a widely applicable mathematical model for quantum key distribution (QKD) systems implementing the measurement-device-independent (MDI) protocol. The model is tested by comparing its predictions with data taken using a proof-of-principle, time-bin qubit-based QKD system in a secure laboratory environment (i.e. in a setting in which eavesdropping can be excluded). The good agreement between the predictions and the experimental data allows the model to be used to optimize mean photon numbers per attenuated laser pulse, which are used to encode quantum bits. This in turn allows optimization of secret key rates of existing MDI-QKD systems, identification of rate-limiting components, and projection of future performance. In addition, we also performed measurements over deployed fiber, showing that our system's performance is not affected by environment-induced perturbations.

6.1.1 Introduction

From the first proposal in 1984 to now, the field of quantum key distribution (QKD) has evolved significantly [10, 11]. For instance, experimentally, systems delivering key at Mbps rates [72] as well as key distribution over more than 100 km [30, 31] have been reported. From a theoretical perspective, efforts aim at developing QKD protocols and security proofs with minimal assumptions about the devices used [91]. Of particular practical importance

are two recently developed protocols that do not require trusted single photon detectors (SPDs) [89, 92]. One of these, the so-called measurement-device-independent QKD (MDI-QKD) protocol, has already been implemented experimentally [93, 94, 95, 87]. Hence, it is foreseeable that it will play an important role in the future of QKD, and it is thus important to understand the interplay between experimental imperfections (which will always remain in real systems) and system performance to maximize the latter.

In this work, we derive a widely applicable mathematical model describing systems that implement the MDI-QKD protocol. The model is based on facts about our [93], and other existing experimental setups [94, 95, 87], and takes into account carefully characterized imperfect state preparation, loss in the quantum channel, as well as limited detector efficiency and noise. It is tested by comparing its predictions with data taken with a proof-of-principle QKD system [93] employing time-bin qubits and implemented in a laboratory environment. Our model, which contains no free parameter, reproduces the experimental data within statistical uncertainties over three orders of magnitude of a relevant parameter. The excellent agreement allows optimizing central parameters that determine secret key rates, such as mean photon numbers used to encode qubits, and to identify rate-limiting components for future system improvement. In addition, we also find that the model accurately reproduces experimental data obtained over deployed fibers, showing that our system minimizes environment-induced perturbation to quantum key distribution in real-world settings.

This paper is organized in the following way: In section 6.1.2 we detail some of the side-channel attacks (i.e. attacks exploiting incorrect assumptions about the working of QKD devices) proposed so far and review technological countermeasures. In section 6.1.3 we briefly describe the MDI-QKD protocol, which instead exploits fundamental quantum physical laws to render the most important of these attacks useless. Our model of MDI-QKD systems is presented in section 6.1.4. This section is followed by an in-depth account of experimental imperfections that affect MDI-QKD performance and a description of how we characterized

them in our system (section 6.1.5). Section 6.1.6 shows the results of the comparison between modelled and measured quantities, and section 6.1.7 details how to optimize the performance of our MDI-QKD system using the model. Finally, we conclude the article in section 6.1.8.

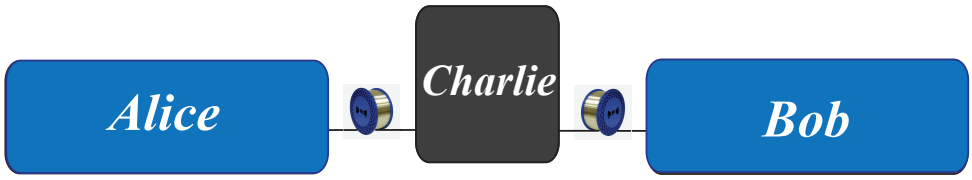

Figure 6.2: Schematics for MDI-QKD. Charlie facilitates the key distribution between Alice and Bob without being able to learn the secret key.

6.1.2 Side-channel attacks

A healthy development of QKD requires investigating the vulnerabilities of QKD implementations in terms of potential side-channel attacks. Side-channels in QKD are channels over which information about the key may leak out unintentionally. One of the first QKD side-channel attacks proposed was the photon number splitting (PNS) attack [9] in which the eavesdropper, Eve, exploits the fact that attenuated laser pulses sometimes include more than one photon to obtain information about the key. This attack can be detected if the decoy state protocol [25, 27, 26] is implemented. In the decoy state protocol, Alice varies the mean photon number per pulse in order to allow her and Bob to distill the secret key only from information stemming from single photon emissions. More proposals of side-channel attacks followed, including the Trojan-horse attack [20, 19], for which the countermeasure is an optical isolator [19], and the phase remapping attack [96], for which the countermeasure is phase randomization [96]. Later on, attacks that took advantage of SPD vulnerabilities were also proposed and demonstrated [56, 57, 97, 68]. For example, the time-shift attack [57] exploits a difference in the quantum efficiencies of the SPDs used in a QKD system. This attack can be prevented by actively selecting one of the two bases for the projection measure-

ment, as well as by monitoring the temporal distribution of photon detections [57]. Another example is the detector blinding attack [68] in which the eavesdropper uses high intensity pulses to modify the performance (i.e. blind) the SPDs. It can be detected by monitoring the intensity of light at the entrance of Bob's devices with a photodiode [68, 98, 99]. Nevertheless, due to its power, the blinding attack is currently of particular concern.

It is important to mention that open side-channels do not necessarily compromise the security of the final key if the information that Eve may have obtained through an attack is properly removed during privacy amplification. However, as technological fixes (as discussed above) or additional privacy amplification can only thwart known attacks, it is important to develop and implement protocols that use a minimum number of assumptions about the devices used to implement the protocol. An important example is the measurement-device-independent QKD protocol, which we will introduce in the next section.

6.1.3 The measurement-device-independent quantum key distribution protocol

The MDI-QKD protocol is a time-reversed version of entanglement-based QKD. In this protocol, the users, Alice and Bob, are each connected to Charlie, a third party, through a quantum channel, e.g. optical fiber (see Fig. 6.2). In the ideal version, the users have a source of single photons that they prepare randomly in one of the BB84 qubit states [4] $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$. The qubits are sent to Charlie where the SPDs are located. Charlie performs a partial Bell state measurement (BSM) through a 50/50 beam splitter and then announces the events for which the measurement resulted in a projection onto the $|\psi^-\rangle = 2^{-1/2}(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)$ state. Alice and Bob then publicly exchange information about the used bases (z, spanned by $|0\rangle$ and $|1\rangle$, or x, spanned by $|+\rangle$ and $|-\rangle$). Associating quantum states with classical bits (e.g. $|0\rangle, |-\rangle \equiv 0$, and $|1\rangle, |+\rangle \equiv 1$) and keeping only events in which Charlie found $|\psi^-\rangle$ and they picked the same basis, Alice and Bob now establish anti-correlated key strings. (Note that a projection of two photons onto $|\psi^-\rangle$ indicates that the two photons, if prepared in the same basis, must have been in

orthogonal states.) Bob then flips all his bits, thereby converting the anti-correlated strings into correlated ones. Next, the so-called *x-key* is formed out of all key bits for which Alice and Bob prepared their photons in the x-basis; its error rate is used to bound the information an eavesdropper may have acquired during photon transmission. Furthermore, Alice and Bob form the *z-key* out of those bits for which both picked the z-basis. Finally, they perform error correction and privacy amplification[10, 11] to the *z-key*, which results in the secret key.

The advantage of the MDI-QKD protocol over conventional prepare-and-measure or entangled photon-based QKD protocols is that, in the case of Charlie performing an ideal (partial) BSM as described above, detection events are uncorrelated with the final secret key bits. This is because a projection onto $|\psi^-\rangle$ only indicates that Alice and Bob sent orthogonal states, but does not reveal who sent which state. As a result, Charlie (or Eve) is unable to gain any information about the key from passively monitoring the detectors. Furthermore, a measurement that is different from the ideal BSM leads to an increased error rate and thus to a smaller, but still secret, key once privacy amplification has been applied. Notably, it does not matter wether the difference is due to experimental imperfections or to an eavesdropper (possibly Charlie himself) trying to gather information about the states that Alice and Bob sent by replacing or modifying the measurement apparatus. Hence, all detector side channels are closed in MDI-QKD.

In the ideal scenario introduced above, Alice and Bob use single photon sources to generate qubits. However, it is possible to implement the protocol using light pulses attenuated to the single photon level. Indeed, as in prepare-and-measure QKD, randomly varying the mean photon number of photons per attenuated light pulse between a few different values (so-called decoy and signal states) allows making the protocol practical while protecting

against a possible PNS attack [89, 100]. The secret key rate is then given by [89]:

$$S = Q_{11}^{z}\big(1 - h_2(e_{11}^{x})\big) - Q_{\mu\sigma}^{z} f h_2(e_{\mu\sigma}^{z}), \tag{6.1}$$

where h_2 is the binary entropy function, f indicates the error correction efficiency, Q indicates the gain (the probability of a projection onto $|\psi^-\rangle$ per emitted pair of pulses [2]) and e indicates error rates (the ratio of erroneous to total projections onto $|\psi^-\rangle$). Furthermore, the superscripts, x or z, denote if gains or error rates are calculated for qubits prepared in the x- or the z-basis, respectively. Similarly, the subscripts, μ and σ, show that the quantity under concern is calculated or measured for pulses with mean photon number μ (sent by Alice) and σ (sent by Bob), respectively. Finally, the subscript 11 indicates quantities stemming from detection events for which the pulses emitted by Alice and Bob contain only one photon each. Note that Q_{11} and e_{11} cannot be measured; their values must be bounded using either a decoy state method, or employing qubit tagging [9]. However, the latter yields smaller key rates and distances than the former.

Shortly after the original proposal [89], a practical decoy state protocol for MDI-QKD was proposed [100]. It requires Alice and Bob to randomly pick mean photon numbers between two decoy states and a signal state. One of the decoy states must have a mean photon number lower than the signal state, while the other one must be vacuum. A finite number of decoy states results in a lower bound for $Q_{11}^{x,z}$ and an upper bound for e_{11}^{x}, which in turn gives a lower bound for the secret key rate in Eq. (6.1). We will elaborate more on decoy states in section 6.1.7.

6.1.4 The model

Our model takes into account imperfections present in a typical QKD system. Regarding the sources, located at Alice and Bob, we take into account imperfect preparation of the quantum

[2]Note that a pulse does not necessarily contain one single photon. In particular, when considering attenuated light pulses, the number of photons in a pulse will, for example, follow the Poissonian distribution.

state of each photon. Furthermore, we consider transmission loss of the links between Alice and Charlie, and Bob and Charlie. And finally, concerning the measurement apparatus at Charlie's, we consider imperfect projection measurement stemming from non-maximum quantum interference on Charlie's beam splitter, detector noise such as dark counts and afterpulsing, and limited detector efficiency. See also [101] for another model describing MDI-QKD performance, but with a more restrictive set of imperfections and not yet tested against actual experimental data.

In the following paragraphs we present a detailed description of our model. It relies on the assumption of phase randomized laser pulses at Charlie's. While Alice and Bob generate coherent states in our proof-of-principle setup, this assumption is correct as the long fibres used to connect Alice and Bob with Charlie introduce random global phase variations (we will discuss the impact of the lack of phase randomization at Alice's and Bob's on the security of distributed keys in section 6.1.8). We note that, in order to facilitate explanations, we have adopted the terminology of time-bin encoding. However, our model is general and can also be applied to MDI-QKD systems implementing other types of encoding [95].

State preparation

In the MDI-QKD protocol, Alice and Bob derive key bits whenever Charlie announces a projection onto the $|\psi^-\rangle$ Bell state. We model the probability of a $|\psi^-\rangle$ projection for various quantum states of photons emitted by Alice and Bob as a function of the mean photon number per pulse (μ and σ, respectively) and transmission coefficients of the fiber links (t_A and t_B, respectively). We consider photons in qubit states described by:

$$|\psi\rangle = \frac{1}{\sqrt{1+2b^{x,z}}}\left(\sqrt{m^{x,z}+b^{x,z}}\,|0\rangle + e^{i\phi^{x,z}}\sqrt{1-m^{x,z}+b^{x,z}}\,|1\rangle\right) \tag{6.2}$$

where $|0\rangle$ and $|1\rangle$ denote orthogonal modes (i.e. early and late temporal modes assuming time-bin qubits), respectively. Note that $|\psi\rangle$ describes any pure state [3] and the presence of

[3]To the best of our knowledge, this assumption correctly describes all existing experimental implementa-

the $m^{x,z}$ and $b^{x,z}$ terms in Eq. (6.2), as opposed to using only one parameter, is motivated by the fact that they model different experimentally characterizable imperfections. In the ideal case, $m^z \in [0,1]$ for photon preparation in the z-basis (in this case, the value of ϕ^z is irrelevant), $m^x = \frac{1}{2}$ and $\phi^x \in [0,\pi]$ for the x-basis, and $b^{x,z} = 0$ for both bases. Imperfect preparation of photon states is modelled by using non-ideal $m^{x,z}$, $\phi^{x,z}$ and $b^{x,z}$ for Alice and Bob. The parameter $b^{x,z}$ is included to represent the background light emitted and modulated by an imperfect source. Furthermore, in principle, the various states generated by Alice and Bob could have differences in other degrees of freedom (i.e. polarization, spectral, spatial, temporal modes). This is not included in Eq. (6.2), but would be reflected in a reduced quality of the BSM, which will be discussed below.

Conditional probability for projections onto $|\psi^-\rangle$

A projection onto $|\psi^-\rangle$ occurs if one of the SPDs after Charlie's 50/50 beam splitter signals a detection in an early time-bin (a narrow time interval centered on the arrival time of photons occupying an early temporal mode) and the other detector signals a detection in a late time-bin (a narrow time-interval centered on the arrival time of photons occupying a late temporal mode). Note that, in the following paragraphs, this is the desired detection pattern we search for when modeling possible interference cases or noise effects. Also, note that we assume that Charlie's two single-photon detectors have identical properties. A deviation from this approximation does not open a potential security loophole (in contrast to prepare-and-measure and entangled photon based QKD), as all detector side-channel attacks are removed in MDI-QKD.

We build up the model by first considering the probabilities that particular outputs from the beam splitter (at Charlie's) will generate the detection pattern associated with a projection onto $|\psi^-\rangle$. The outputs are characterized by the number of photons per output port as well as their joint quantum state. The probabilities for each of the possible outputs to

tions. See section 5 for more information.

occur can then be calculated based on the inputs to the beam splitter (characterized by the number of photons per input port and their quantum states, as defined in Eq. (6.2)). Note that for the simple cases of inputs containing zero or one photon (summed over both input modes), we calculate the probabilities leading to the desired detection pattern directly, i.e. without going through the intermediate step of calculating outputs from the beam splitter. Finally, the probability for each input to occur is calculated based on the probability for Alice and Bob to send attenuated light pulses containing exactly i photons, all in a state given by Eq. (6.2). The probability for a particular input to occur also depends on the transmissions of the quantum channels, t_A and t_B. We note that this model considers up to three photons incident on the beam splitter. This is sufficient as, in the case of heavily attenuated light pulses and lossy transmission, higher order terms do not contribute significantly to projections onto $|\psi^-\rangle$. However, we limit the following description to two photons at most: the extension to three is lengthy but straightforward and follows the methodology presented for two photons.

Detector noise: Let us begin by considering the simplest case in which no photons are input into the beam splitter. In this case, detection events can only be caused by detector noise. We denote the probability that a detector indicates a spurious detection as P_n. Detector noise stems from two effects: dark counts and afterpulsing [102]. Dark counts represent the base level of noise in the absence of any light, and we denote the probability that a detector generates a dark count per time-bin as P_d. Afterpulsing is an additional noise source produced by the detector as a result of prior detection events. The probability of afterpulsing depends on the total count rate, hence we denote the afterpulsing probability per time-bin as P_a, which is a function of the mean photon number per pulse from Alice and Bob (μ and σ), the transmission of the channels (t_A and t_B) and the efficiency of the detectors (η) located at Charlie (see below for afterpulse characterization). The total probability of a noise count in a particular time-bin is thus $P_n = P_d + P_a$. All together, we

find the probability for generating the detection pattern associated with a projection onto the $|\psi^-\rangle$-state, conditioned on having no photons at the input, specified by "in", of the beam splitter, to be :

$$P(\left|\psi^-\right\rangle |0 \text{ photons, in}) = P(\left|\psi^-\right\rangle |0 \text{ photons, out}) = 2P_n^2, \tag{6.3}$$

Here and henceforward, we have ignored the multiplication factor (1-P_n) ~ 1[4], which indicates the probability that a noise event did not occur in the early time-bin (this is required in order to see a detection during the late time-bin assuming detectors with recovery time larger than the separation between the $|0\rangle$ and $|1\rangle$ temporal modes). Note that the probability conditioned on having no photons at the inputs of the beam splitter equals the one conditioned on having no photons at the outputs (specified in Eq. (6.3) by the conditional "out").

One-photon case: Next, we consider the case in which a single photon arrives at the beam splitter. To generate the detection pattern associated with $|\psi^-\rangle$, either the photon must be detected and a noise event must occur in the other detector in the opposite time-bin, or, if the photon is not detected, two noise counts must occur as in Eq. (6.3). We find

$$P(\left|\psi^-\right\rangle |1 \text{ photon, in}) = \eta P_n + (1-\eta) P(\left|\psi^-\right\rangle |0 \text{ photons, out}), \tag{6.4}$$

where η denotes the probability to detect a photon that occupies an early (late) temporal mode during an early (late) time-bin (we assume η to be the same for both detectors).

Two-photon case: We now consider detection events stemming from two photons entering the beam splitter. The possible outputs can be broken down into three cases. In the first case, both photons exit the beam splitter in the same output port and are directed to the same detector. This yields only a single detection event, even if the photons are in different

[4]Note that this approximation is, in general, not correct. However, in order to obtain the best performance from a QKD implementation, the noise level should be as low as possible, i.e. $P_n \sim 0$.

temporal modes (the latter is due to detector dead time. Note that as our model calculates detections in units of bits per gate, modeling a dead-time free detector is straightforward.). The probability for Charlie to declare a projection onto $|\psi^-\rangle$ is then

$$P(\left|\psi^-\right\rangle |2 \text{ photons, 1 spatial mode, out}) =$$
$$(1-(1-\eta)^2)P_n + (1-\eta)^2 P(\left|\psi^-\right\rangle |0 \text{ photons, out}). \tag{6.5}$$

In the second case, the photons are directed towards different detectors and occupy the same temporal mode. Hence, to find detections in opposite time-bins in the two detectors, at least one photon must not be detected. This leads to

$$P(\left|\psi^-\right\rangle |2 \text{ photons, 2 spatial modes, 1 temporal mode, out}) =$$
$$2\eta(1-\eta)P_n + (1-\eta)^2 P(\left|\psi^-\right\rangle |0 \text{ photons, out}). \tag{6.6}$$

In the final case, both photons occupy different spatial as well as temporal modes. In contrast to the previous case, a projection onto $|\psi^-\rangle$ can now also originate from the detection of both photons. This leads to

$$P(\left|\psi^-\right\rangle |2 \text{ photons, 2 spatial modes, 2 temporal modes, out}) =$$
$$\eta^2 + 2\eta(1-\eta)P_n + (1-\eta)^2 P(\left|\psi^-\right\rangle |0 \text{ photons, out}). \tag{6.7}$$

In order to find the probability for each of these three two-photon outputs to occur, we must examine two-photon inputs to the beam splitter. We note that it is possible for the two photons to be subject to a two-photon interference effect (known as photon bunching) when impinging on the beam splitter. As this quantum interference can lead to an entangled state between the output modes, the calculation must proceed with quantum mechanical operators. We consider three cases: two photons arrive at the same input of the beam

splitter, one photon arrives at each input of the beam splitter and the two photons are distinguishable, and one photon arrives at each input of the beam splitter and the two photons are indistinguishable. For ease of analysis, we first introduce some notation:

$$\begin{aligned} p^{x,z}(0,0) &\equiv (m_1^{x,z} + b_1^{x,z})(m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(0,1) &\equiv (m_1^{x,z} + b_1^{x,z})(1 - m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(1,0) &\equiv (1 - m_1^{x,z} + b_1^{x,z})(m_2^{x,z} + b_2^{x,z}) \\ p^{x,z}(1,1) &\equiv (1 - m_1^{x,z} + b_1^{x,z})(1 - m_2^{x,z} + b_2^{x,z}) \\ b_{norm}^{x,z} &\equiv 1 + 2b_1^{x,z} + 2b_2^{x,z} + 4b_1^{x,z} b_2^{x,z} \end{aligned} \tag{6.8}$$

where $b_{1,2}^{x,z}$ and $m_{1,2}^{x,z}$ are the parameters introduced in Eq. (6.2); the subscripts label the photon (one or two) whose state is specified by the parameters. Furthermore, $p^{x,z}(i,j)$ is proportional to finding photon one before the beam-splitter in temporal mode i and photon two in temporal mode j, where $i, j \in [0,1]$. Finally, $b_{norm}^{x,z}$ is a normalization factor.

First, considering the situation in which the two photons impinge from the same input on the beam splitter, one has the state

$$|\psi_{input}\rangle = \left(\frac{1}{\sqrt{1+2b^{x,z}}} \left(\sqrt{m^{x,z} + b^{x,z}}\ \hat{a}^\dagger(0) + e^{i\phi^{x,z}} \sqrt{1 - m^{x,z} + b^{x,z}}\ \hat{a}^\dagger(1) \right) \right)^{\otimes 2} |vac\rangle\,, \tag{6.9}$$

where $\hat{a}^\dagger(0)$ and $\hat{a}^\dagger(1)$ are the creation operators for a photon in the $|0\rangle$ or $|1\rangle$ state, respectively. Evolving this state through the standard unitary transformation for a lossless, 50/50 beam splitter, described by $\hat{a}^\dagger \to (\hat{c}^\dagger + \hat{d}^\dagger)/\sqrt{2}$ (where $\hat{c}^\dagger$ and $\hat{d}^\dagger$ are the two output modes of the beam splitter), one finds that with probability 1/2 the two photons exit the beam splitter in the same output port (or spatial mode) and with probability 1/2 in different ports. Furthermore, with probability $A = [p^{x,z}(0,0) + p^{x,z}(1,1)]/2b_{\text{norm}}^{x,z}$ we find the photons in different spatial modes and in the same temporal mode, and with probability $B = [p^{x,z}(0,1) + p^{x,z}(1,0)]/2b_{\text{norm}}^{x,z}$ we find the photons in different spatial and temporal

modes. By symmetry, we find the same result if the two photons arrive from the other input mode of the beam splitter.

Thus the probability that Charlie finds the desired detection pattern is:

$$\begin{aligned} & P(\left|\psi^-\right\rangle \text{ |2 photons, 1 spatial mode, in}) = \\ & \frac{1}{2} P(\left|\psi^-\right\rangle \text{ |2 photons, 1 spatial mode, out}) \\ + A \times P(\left|\psi^-\right\rangle & \text{ |2 photons, 2 spatial modes, 1 temporal mode, out}) \\ + B \times P(\left|\psi^-\right\rangle & \text{ |2 photons, 2 spatial modes, 2 temporal modes, out}). \end{aligned} \tag{6.10}$$

Second, consider the situation in which the two photons come from different inputs, and are completely distinguishable in some degree of freedom. This can be modelled by starting with the input state

$$\begin{aligned} |\psi_{input}\rangle \quad = & \frac{1}{\sqrt{1+2b_1^{x,z}}} \left(\sqrt{m_1^{x,z} + b_1^{x,z}}\ \hat{a}^\dagger(0) + e^{i\phi_1^{x,z}} \sqrt{1 - m_1^{x,z} + b_1^{x,z}}\ \hat{a}^\dagger(1) \right) \\ \otimes & \frac{1}{\sqrt{1+2b_2^{x,z}}} \left(\sqrt{m_2^{x,z} + b_2^{x,z}}\ \hat{b}^\dagger(0) + e^{i\phi_2^{x,z}} \sqrt{1 - m_2^{x,z} + b_2^{x,z}}\ \hat{b}^\dagger(1) \right) |vac\rangle \,, \end{aligned} \tag{6.11}$$

where $\hat{b}^\dagger$ is the creation operator for a photon in the second input mode of the beam splitter. One can then evolve the state with the beam splitter unitary described by $\hat{a}^\dagger \to (\hat{c}^\dagger + \hat{d}^\dagger)/\sqrt{2}$ (as before) and $\hat{b}^\dagger \to (-\hat{e}^\dagger + \hat{f}^\dagger)\sqrt{2}$, where $\hat{c}^\dagger$ and $\hat{e}^\dagger$ correspond to the same spatial output mode but with distinguishability in another degree of freedom, and similarly for the other spatial output mode described by $\hat{d}^\dagger$ and $\hat{f}^\dagger$. One finds the same result as for the previous case, described by Eq. (6.10):

$$\begin{aligned} P \quad & (|\psi^-\rangle \text{ |2 photons, 2 spatial modes, non-interfering, in}) \\ & = P(|\psi^-\rangle \text{ |2 photons, 1 spatial mode, in}) \\ & \equiv P(|\psi^-\rangle \text{ |2 photons, non-interfering, in}). \end{aligned} \tag{6.12}$$

The definition reflects that there is no two-photon interference in both cases.

Finally, consider the case in which the two photons impinge from different inputs are indistinguishable, and interfere on the beam splitter. This can be modelled by considering the same input state as in Eq. (6.11), but using a beam splitter unitary described by $\hat{a}^\dagger \rightarrow (\hat{c}^\dagger + \hat{d}^\dagger)/\sqrt{2}$ (as before) and $\hat{b}^\dagger \rightarrow (-\hat{c}^\dagger + \hat{d}^\dagger)/\sqrt{2}$. In this case, the probabilities of finding the outputs from the beam splitter discussed in Eqs. (6.5-6.7) depend on the difference between the phases $\phi_1^{x,z}$ and $\phi_2^{x,z}$ that specify the states of photons one and two, $\Delta\phi^{x,z} \equiv \phi_1^{x,z} - \phi_2^{x,z}$. Note that, due to the two-photon interference effect, finding the two photons in different spatial modes and the same temporal mode is impossible. We are thus left with the case of having two photons in the same output port (the same spatial mode), which occurs with probability $C = [p^{x,z}(0,0) + p^{x,z}(1,1) + 0.5(p^{x,z}(0,1) + p^{x,z}(1,0)) + \sqrt{p^{x,z}(0,1)p^{x,z}(1,0)}\cos(\Delta\phi^{x,z})]/b_{norm}^{x,z}$, and the case of having the photons in different temporal and spatial modes, which occurs with probability $D = [0.5(p^{x,z}(0,1) + p^{x,z}(1,0)) - \sqrt{p^{x,z}(0,1)p^{x,z}(1,0)}\cos(\Delta\phi^{x,z})]/b_{norm}^{x,z}$. This leads to

$$\begin{aligned} P(\left|\psi^-\right\rangle \text{ |2 photons, interfering, in}) = \\ C \times P(\left|\psi^-\right\rangle \text{ |2 photons, 1 spatial mode, out}) + \\ D \times P(\left|\psi^-\right\rangle \text{ |2 photons, 2 spatial modes, 2 temporal modes, out}). \end{aligned} \tag{6.13}$$

Aggregate probability for projections onto $|\psi^-\rangle$

Now that we have calculated the conditional probabilities of a detection pattern indicating $|\psi^-\rangle$ for various inputs to the beam splitter, let us consider with what probability each case occurs. This requires that we know the photon number distribution of the pulses arriving at Charlie's beam splitter from Alice and Bob, which can be computed based on the photon number distribution at the sources and the properties of the quantum channels. For the following discussion, we assume that the channels from Alice to Charlie, and from Bob to Charlie are characterized by the loss t_A and t_B, respectively, yielding pulses with number

distribution $\mathbb{D}$ and mean photon number, μt_A and σt_B, respectively. This is equivalent to assuming that no PNS attack takes place, which was ensured by performing experiments with the entire setup (including the fiber transmission lines) inside a single laboratory in which no eavesdropping took place during the experiments. We limit our discussion to the cases with two or less photons at the input of the beam splitter (but recall that the actual calculation includes up to three photons). Hence, the cases we consider and their probabilities of occurrence, P_O, are given by:

- 0 photons at the input from both sources: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 1 photon at the input from Alice and 0 photons from Bob: $P_O = \mathbb{D}_1(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 0 photons at the input from Alice and 1 photon from Bob: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_1(\sigma t_B)$
- 2 photons at the input from Alice and 0 photons from Bob: $P_O = \mathbb{D}_2(\mu t_A)\mathbb{D}_0(\sigma t_B)$
- 0 photons at the input from Alice and 2 photons from Bob: $P_O = \mathbb{D}_0(\mu t_A)\mathbb{D}_2(\sigma t_B)$
- 1 photon at the input from both sources: $P_O = \mathbb{D}_1(\mu t_A)\mathbb{D}_1(\sigma t_B)$

where we denote the probability of having i photons from a distribution $\mathbb{D}$ with mean number μ as $\mathbb{D}_i(\mu)$. For each of these cases, we have already computed the probability that Charlie obtains the detection pattern associated with the $|\psi^-\rangle$-state for arbitrary input states of the photons (as defined in Eq. (6.2)). When zero or one photons arrive at the beam splitter, Eq. (6.3) and Eq. (6.4) are used, respectively. In the case in which two photons arrive from the same source, Eq. (6.12) is used. Finally, in the case in which one photon arrives from each source at the beam splitter, Eq. (6.13) would be used in the ideal case. However, perfect indistinguishability of the photons cannot be guaranteed in practice. We characterize the degree of indistinguishability by the visibility, V, that we would observe in a closely-related Hong-Ou-Mandel (HOM) interference experiment [103] with single-photon inputs.

Taking into account partial distinguishability, the probability of finding a detection pattern corresponding to the projection onto $|\psi^-\rangle$ is given by

$$\begin{aligned} P(\left|\psi^-\right\rangle |2 \text{ photons, visibility } V, \text{ in}) = \\ VP(\left|\psi^-\right\rangle |2 \text{ photons, interfering, in}) \\ +(1-V)P(\left|\psi^-\right\rangle |2 \text{ photons, non-interfering, in}). \end{aligned} \tag{6.14}$$

Equations 6.3-6.14 detail all possible causes for observing the detection pattern associated with a projection onto the $|\psi^-\rangle$ Bell state, if up to two photons at the beam splitter input are taken into account. We remind the reader that all calculations in the following sections take up to three photons at the input of the beam splitter into account. To calculate the gains, $Q_{\mu\sigma}^{x,z}$, using these equations, we need only substitute in the correct values of μ, σ, t_A, t_B, $m^{x,z}$, $b^{x,z}$, and $\Delta\phi^{x,z}$ for the cases in which Alice and Bob both sent attenuated light pulses in the x-basis or z-basis, respectively. The error rates, $e_{\mu}^{x,z}$, can then be computed by separating the projections onto $|\psi^-\rangle$ into those where Alice and Bob sent photons in different states (yielding correct key bits) and in the same state (yielding erroneous key bits). More precisely, the error rates, $e_{\mu\sigma}^{x,z}$, are calculated as $e_{\mu\sigma}^{x,z} = p_{wrong}^{x,z}/(p_{correct}^{x,z} + p_{wrong}^{x,z})$ where $p_{wrong}^{x,z}$ ($p_{correct}^{x,z}$) denotes the probability for detections yielding an erroneous (correct) bit in the x (or z)-key.

6.1.5 Characterizing experimental imperfections

The parameters used to model our system are derived from data established through independent measurements. To test our model, the characterization of experimental imperfections in our MDI-QKD implementation [93] is very technical at times. It can be broken down into time-resolved energy measurements at the single photon level (required to extract μ, σ, $b^{x,z}$ and $m^{x,z}$ for Alice and Bob, as well as dark count and afterpulsing probabilities), measurements of phase (required to establish $\phi^{x,z}$ for Alice and Bob), and visibility measure-

ments. In the following paragraphs we describe the procedures we followed to obtain these parameters from our system.

Our MDI-QKD implementation

In our implementation of MDI-QKD [93] Alice's and Bob's setups are identical. Each setup consists of a CW laser with large coherence time, emitting at 1550nm wavelength. Time-bin qubits, encoded into single photon-level light pulses with Poissonian photon number statistics, are created through an attenuator, an intensity modulator and a phase modulator located in a temperature controlled box. More precisely, the intensity modulator is used to tailor pulse pairs out of the cw laser light, the phase modulator is used to change their relative phase, and the attenuator attenuates these pulses to the single-photon level. The two temporal modes defining each time-bin qubit are of 500 ps (FWHM) duration and are separated by 1.4 ns. Each source generates qubits at 2 MHz rate.

We emphasize that our qubit generation procedure justifies the assumption of a pure state in Eq. (6.2). Indeed, all photons, including background photons due to light leaking through imperfect intensity modulators, have to be generated by the CW lasers whose coherence times exceeds the separation between the temporal modes $|0\rangle$ and $|1\rangle$[5]. Note that in all experiments reported to date [93, 94, 95, 87] background photons always add coherently to the modes describing qubits, making our pure-state description widely applicable.

The time-bin qubits are sent to Charlie through an optical fiber link. The link consisted of spooled fiber (for the measurements in which Alice, Bob and Charlie were all located in the same laboratory) or deployed fiber (for the measurements in which the three parties were located in different locations within the city of Calgary). We remind the reader that all pulses arriving at Charlie's are phase randomized, due to the use of long fibers. Charlie

[5]The separation of photons into genuine qubit photons and background photons is somewhat artificial – as a matter of fact, there is no way to distinguish background photons from real photons. As already stated in section 4.1, the distinction is motivated by the need to write down a general expression for all emitted single-photon qubit states using parameters that can be characterized directly through experiments (these measurements are further described below).

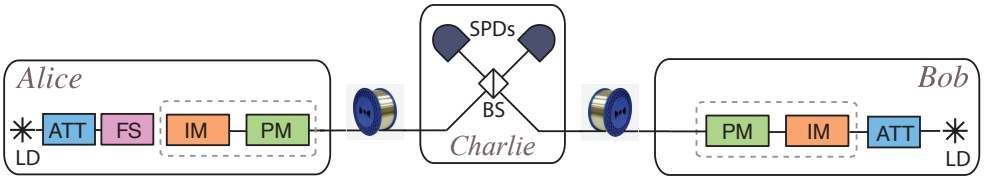

Figure 6.3: Time-bin qubits are created at Alice's and Bob's through a CW laser (LD), attenuator (ATT), and frequency shifter (FS) and temperature-controlled intensity (IM) and phase (PM) modulator. The projective measurements are done at Charlie's via a beam splitter (BS) and two single photon detectors (SPDs).

performs a BSM on the qubits he receives using a 50/50 beamsplitter and two SPDs. See Figure 6.3. Note that, in order to perform a Bell state measurement the photons arriving to Charlie must be indistinguishable in all degrees of freedom: polarization, frequency, time and spatial mode. The indistinguishability of the photons is assessed through a Hong-Ou-Mandel interference measurement [103]. As our system employs attenuated laser pulses, the maximum visibility we can obtain in this measurement is $V_{max} = 50\%$ (and not 100% as it would be with single photons) [104]. In our implementation the visibility measurements resulted in $V = (47 \pm 1)$, irrespective of whether they were taken with spooled fiber inside the lab, or over deployed fiber.

Time-resolved energy measurements

First, we characterize the dark count probability per time-bin, P_d, of the SPDs (InGaAs-avalanche photodiodes operated in gated Geiger mode [102]) by observing their count rates when the optical inputs are disconnected. We then send attenuated laser pulses so that they arrive just after the end of the 10 ns long gate that temporarily enables single photon detection. The observed change in the count rate is due to background light transmitted by the intensity modulators (whose extinction ratios are limited) and allows us to establish $b^{x,z}$ (per time-bin) for Alice and Bob. Next, we characterize the afterpulsing probability per time-bin, P_a, by placing the pulses within the gate, and observing the change in count rate

in the region of the gate prior to the arrival of the pulse. The afterpulsing model we use to assess P_a from these measurements is described below.

Once the background light and the sources of detector noise are characterized, the values of $m^{x,z}$ can be calculated by generating all required states and observing the count rates in the two time-bins corresponding to detecting photons generated in early and late temporal modes. Observe that $m^{z=1}$ for photons generated in state $|1\rangle$ (the late temporal mode) is zero, since all counts in the early time-bin are attributed to one of the three sources of background described above. Furthermore, we observed that $m^{z=0}$ for photons generated in the $|0\rangle$ state (the early temporal mode) is smaller than one due to electrical ringing in the signals driving the intensity modulators. Note that, in our implementation, the duration of a temporal mode exceeds the width of a time-bin, i.e. it is possible to detect photons outside a time-bin (see Figure 6.4 for a schematical representation). Hence, it will be useful to also define the probability for detecting a photon arriving at any time during a detector gate; we will refer to this quantity as η_{gate}.The count rate per gate, after having subtracted the rates due to background and detector noise, together with the detection efficiency, η_{gate} (η_{gate}, as well as η, have been characterized previously based on the usual procedure [102]), allows calculating the mean number of photons per pulse from Alice or Bob (μ or σ, respectively). The efficiency coefficient relevant for our model, η, is smaller than η_{gate}. Finally, we point out that the entire characterization described above was repeated for all experimental configurations investigated (the configurations are detailed in Table 6.2). We found all parameters to be constant in $\mu\sigma t_A t_B$, with the obvious exception of the afterpulsing probability.

Phase measurements

To detail the assessment of the phase values $\phi^{x,z}$ determining the superposition of photons in early and late temporal modes, let us assume for the moment that the lasers at Alice's and Bob's emit light at the same frequency. First, we defined the phase of Bob's $|+\rangle$ state

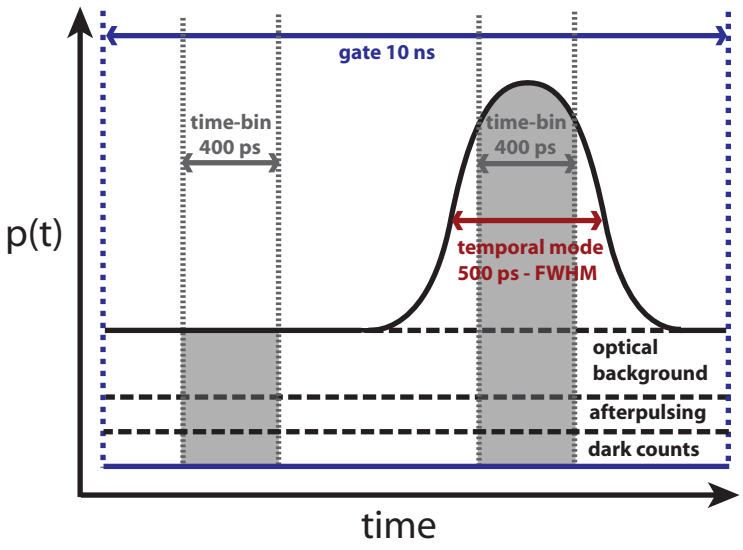

Figure 6.4: Sketch (not to scale) of the probability density p(t) for a detection event to occur as a function of time within one gate. Detection events can arise from a photon within an optical pulse (depicted here as a pulse in the late temporal mode), or be due to optical background, a dark count, or afterpulsing. Also shown are the 400 ps wide time-bins. Within the early time-bin only optical background, dark counts and afterpulsing give rise to detection events in this case. Note that the width of the temporal mode exceeds the widths of the time-bins.

to be zero (this can always be done by appropriately defining the time difference between the two temporal modes $|0\rangle$ and $|1\rangle$). Next, to measure the phase describing any other state (generated by either Alice or Bob) with respect to Bob's $|+\rangle$ state, we sequentially send unattenuated laser pulses encoding the two states through a common reference interferometer. This reference interferometer featured a path-length difference equal to the time-difference between the two temporal modes defining Alices and Bob's qubits. For the phase measurement of qubit states $|+\rangle$ and $|-\rangle$ (generate by Alice), and $|-\rangle$ generated by Bob), first, the phase of the interferometer was set such that Bob's $|+\rangle$ state generated equal intensities in each output of the interferometer (i.e. the interferometers phase was set to $\pi/4$). Thus, sending any of the other three states through the interferometer and comparing the output intensities, we can calculate the phase difference. We note that any frequency difference between Alice's and Bob's lasers results in an additional phase difference. Its upper bound for our maximum frequency difference of 10 MHz is denoted by ϕ_{freq}.

Measurements of afterpulsing

We now turn to the characterization of afterpulsing. After a detector click (or detection event, which includes photon detection, dark counts and afterpulsing), the probability of an afterpulse occuring due to that detection event decays exponentially with time. The SPDs are gated, with the afterpulse probability per gate being a discrete sampling of the exponential decay. This can be expressed using a geometric distribution: supposing a detection event occurred at gate $k = -1$, the probability of an afterpulse occuring in gate k is given by $P_k = \alpha p(1-p)^k$. Thus, if there are no other sources of detection events, the probability of an afterpulse occuring due to a detection event is given by $\sum_{k=0}^{\infty} \alpha p(1-p)^k$.

In a realistic situation, the geometric distribution for the afterpulses will be cut off by other detection events, either stemming from photons, or dark counts. In addition, the SPDs have a deadtime after each detection event during which the detector is not gated until

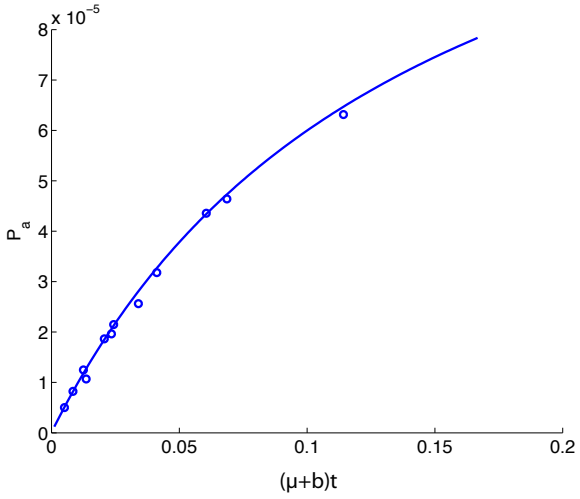

Figure 6.5: Afterpulse probability per time-bin as a function of the average number of photons arriving at the detector per gate.

$k \geq k_{dead}$ (note that time and the number of gates applied to the detector are proportional). The deadtime can simply be accounted for by starting the above summation at $k = k_{dead}$ rather than $k = 0$. However, for an afterpulse to occur during the k^{th} gate following a particular detection event, no other detection events must have occured in prior gates. This leads to the following equation for the probability of an afterpulse per detection event:

$$P(\text{a,det}) = \sum_{k=k_{dead}}^{\infty} (\gamma \times \upsilon \times \rho \times P_k) \tag{6.15}$$

where:

$$\gamma = (1 - \mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate})^{k-k_{dead}}$$

$$\upsilon = (1 - P_{d,gate})^{k-k_{dead}}$$

$$\rho = \prod_{j=k_{dead}}^{k-1} 1 - \alpha p(1-p)^j$$

$$P_k = \alpha p(1-p)^k \tag{6.16}$$

and $P_{d,gate}$ denotes the detector dark count probability per gate (as opposed to per time-bin), and $\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)$ expresses the average number of photons present on the detector during each gate as follows:

$$\mu_{\text{avg}}(\mu, \sigma, t_A, t_B) = \frac{(\mu + b_A)t_A + (\sigma + b_B)t_B}{2}, \tag{6.17}$$

where b_A and b_B characterize the amount of background light per gate from Alice and Bob, respectively, and the factor of $\frac{1}{2}$ comes from Charlie's beam splitter. The terms in the sum of Eq. (6.15) describe the probabilities of neither having an optical detection (γ), either caused by a modulated pulse or background light, nor a detector dark count (υ) in any gate before and including gate k, and not having an afterpulse in any gate before gate k (ρ), followed by an afterpulse in gate k (P_k). Equation (6.15) takes into account that afterpulsing within each time-bin is influenced by all detections within each detector gate, and not only those happening within the time-bins that we post-select when acquiring experimental data.

The afterpulse probability, $P_{a,gate}$, for given μ, σ, t_A and t_B can then be found by multiplying Eq. (6.15) by the total count rate

$$P_{a,gate} = (\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate} + P_{d,gate} + P_{a,gate})\, P(\text{a,det}). \tag{6.18}$$

This equation expresses that afterpulsing can arise from prior afterpulsing, which explains the appearance of $P_{a,gate}$ on both sides of the equation. Equation (6.18) simplifies to

$$P_{a,gate} = \frac{(\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)\eta_{gate} + P_{d,gate})\, P(\text{a,det})}{1 - P(\text{a,det})}. \tag{6.19}$$

Finally, to extract the afterpulsing probability per time-bin, $P_a(\mu, \sigma, t_A, t_B)$, we note that we found that the distribution of afterpulsing across the gate to be the same as the distribution of dark counts across the gate. Hence,

$$P_a(\mu, \sigma, t_A, t_B) = P_{a,gate}\frac{P_d}{P_{d,gate}}. \tag{6.20}$$

Fitting our afterpulse model to the measured afterpulse probabilities, we find $\alpha = 1.79\times10^{-1}$, $p = 2.90 \times 10^{-2}$, and $\frac{P_d}{P_{d,gate}} = 4.97 \times 10^{-2}$ for $k_{dead} = 20$. The fit, along with the measured values, is shown in Figure 6.5 as a function of the average number of photons arriving at the detector per gate $\mu_{\text{avg}}(\mu, \sigma, t_A, t_B)$.

A summary of all the values obtained through these measurements is shown in Table 6.1.

Table 6.1: Experimentally established values for all parameters required to describe the generated quantum states, as defined in Eq. (6.2), as well as two-photon interference parameters and detector properties.

Parameter	Alice's value	Bob's value
$b^{z=0} = b^{z=1}$	$(7.12 \pm 0.98) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$b^{x=-} = b^{x=+}$	$(5.45 \pm 0.37) \times 10^{-3}$	$(1.14 \pm 0.49) \times 10^{-3}$
$m^{z=0}$	0.9944 ± 0.0018	0.9967 ± 0.0008
$m^{z=1}$	0	0
$m^{x=+} = m^{x=-}$	0.4972 ± 0.011	0.5018 ± 0.0080
$\phi^{z=0} = \phi^{z=1} = \phi^{x=+}$ [rad]	0	0
$\phi^{x=-}$ [rad]	$\pi + (0.075 \pm 0.015)$	$\pi - (0.075 \pm 0.015)$
Parameter	Value	
$\lvert\phi_{freq}\rvert$ [rad]	< 0.088	
V	0.94 ± 0.02	
P_d	$(1.83 \pm 0.77) \times 10^{-5}$	
η_{gate}	0.2	
η	0.145	

6.1.6 Testing the model, and real-world tests

Comparing modelled with actual performance

To test our model, and to verify our ability to perform, in principle, QKD with deployed (real-world) fiber, we now compare the model's predictions with experimental data obtained using the QKD system characterized by the parameters listed in Table 6.1. We performed experiments in two configurations: inside the laboratory using spooled fiber (for four different distances between Alice and Bob ranging between 42 km and 103 km), and over deployed fiber (18 km). The first configuration allows testing the model, and the second configurations shines light on our system's capability to compensate for environment-induced perturbations, e.g. due to temperature fluctuations. For each test, three different mean photon numbers (0.1, 0.25 and 0.5) were used. All the configurations tested (as well as the specific parameters used in each test) and the results obtained are listed in Table 6.2. In Figure 6.6 we show the simulated values for the error rates ($e^{z,x}$) and gains ($Q^{z,x}$) predicted by the model as a function of $\mu\sigma t_A t_B$. The plot includes uncertainties from the measured parameters, leading to a range of values (bands) as opposed to single values. The figure also shows the experimental values of $e^{z,x}$ and $Q^{z,x}$ from our MDI-QKD system in both the laboratory environment and over deployed fiber.

Considering the data taken inside the lab, the modelled values and the experimental results agree within experimental uncertainties over three orders of magnitude. This shows that the model is suitable for predicting error rates and gains. In turn, this allows us to optimize performance of our QKD systems in terms of secret key rate (see section 6.1.7). In particular, the model allows optimizing the mean photon number per pulse that Alice and Bob use to encode signal and decoy states as a function of transmission loss, and identifying rate-limiting components.

Furthermore, the measurement results over deployed fibre are also well described by the same model, indicating that this more-difficult measurement worked correctly. The

Table 6.2: Measured error rates, $e^{x,z}_{\mu\sigma}$, and gains, $Q^{x,z}_{\mu\sigma}$, for different mean photon numbers, μ and σ (where $\mu = \sigma$), lengths of fiber connecting Alice and Charlie, and Charlie and Bob, ℓ_A and ℓ_B, respectively, and total transmission loss, l. The last set of data details real-world measurements using deployed fiber. Uncertainties are calculated using Poissonian detection statistics.

Fiber	$\mu = \sigma$	ℓ_A [km]	ℓ_B [km]	total loss l [dB]	$Q^x_{\mu\sigma}$	$Q^z_{\mu\sigma}$	$e^x_{\mu\sigma}$	$e^z_{\mu\sigma}$
	0.49(2)				$1.045(4) \times 10^{-4}$	$5.57(8) \times 10^{-5}$	0.272(2)	0.037(3)
Spool	0.254(9)	30.98	11.75	13.6	$3.20(2) \times 10^{-5}$	$1.47(3) \times 10^{-5}$	0.277(2)	0.040(4)
	0.101(4)				$4.84(6) \times 10^{-6}$	$2.72(6) \times 10^{-6}$	0.278(5)	0.073(6)
	0.49(2)				$3.92(2) \times 10^{-5}$	$2.02(1) \times 10^{-5}$	0.261(2)	0.046(1)
Spool	0.25(1)	40.80	40.77	18.2	$9.87(9) \times 10^{-6}$	$5.1(1) \times 10^{-6}$	0.270(4)	0.047(5)
	0.099(4)				$1.57(3) \times 10^{-6}$	$9.2(3) \times 10^{-7}$	0.281(9)	0.084(8)
	0.50(2)				$1.37(1) \times 10^{-5}$	$1.07(2) \times 10^{-5}$	0.275(3)	0.054(4)
Spool	0.24(1)	51.43	32.19	22.7	$3.73(4) \times 10^{-6}$	$3.01(8) \times 10^{-6}$	0.269(5)	0.071(7)
	0.100(6)				$6.0(1) \times 10^{-7}$	$4.07(9) \times 10^{-7}$	0.30(1)	0.103(7)
	0.50(5)				$4.96(4) \times 10^{-6}$	$2.94(3) \times 10^{-6}$	0.280(4)	0.068(3)
Spool	0.25(1)	61.15	42.80	27.2	$1.50(2) \times 10^{-6}$	$7.1(2) \times 10^{-7}$	0.282(7)	0.091(6)
	0.103(5)				$2.45(9) \times 10^{-7}$	$1.31(6) \times 10^{-7}$	0.28(2)	0.14(2)
	0.50(2)				$3.01(1) \times 10^{-4}$	$1.667(8) \times 10^{-4}$	0.273(2)	0.0362(7)
Deployed	0.26(1)	12.4	6.2	9.0	$8.78(6) \times 10^{-5}$	$5.01(4) \times 10^{-5}$	0.263(3)	0.043(1)
	0.100(4)				$1.45(2) \times 10^{-5}$	$7.3(1) \times 10^{-7}$	0.276(5)	0.055(3)

increased difficult across real-world fiber arises due to the fact that BSMs require incoming photons to be indistinguishable in all degrees of freedom (i.e. arrive within their respective coherence times, with identical polarization, and with large spectral overlap). As we have shown in [93], time-varying properties of optical fibers in the outside environment (e.g. temperature dependent polarization and travel-time changes) can remove indistinguishability in less than a minute. Active stabilization of these properties is thus required to achieve functioning BSMs and, in fact, three such stabilization systems were deployed during the MDI-QKD measurements presented here (more details are contained in [93]). That our measurement results agree with the predicted values of the model demonstrates that the impact of environmental perturbations on the ability to perform Bell state measurements is negligible (which is the same conclusion drawn in [93]).

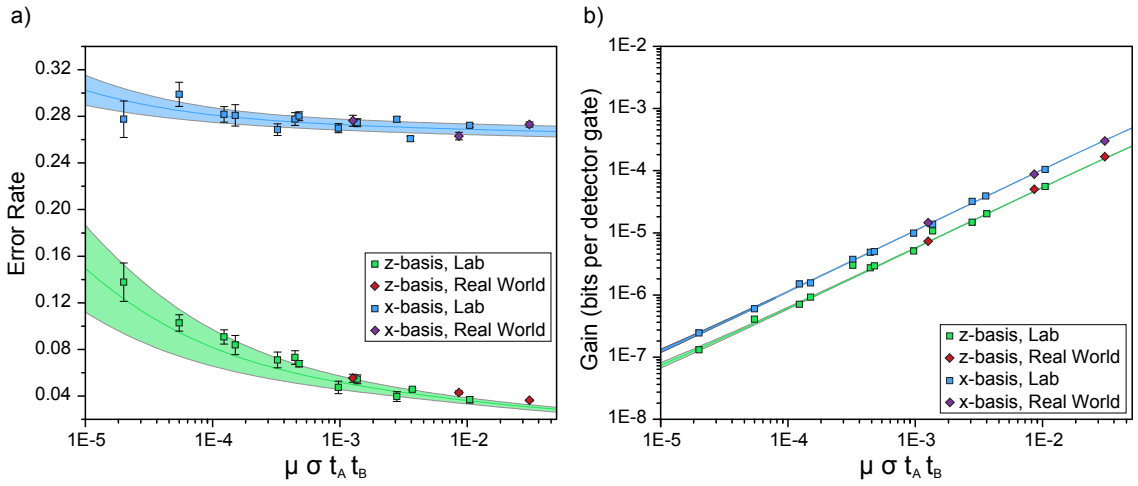

Figure 6.6: Modelled and measured results. Figure a) shows the plot for the error rates in the z-basis (green band) and in the x-basis (blue band) as a function of the mean photon number per pulse sent by Alice (μ) and Bob (σ) multiplied by the channel transmissions (t_A and t_B). Figure b) shows the plot of the gains as a function of $\mu\sigma t_A t_B$. The z-basis is shown in green and the x-basis is shown in blue. For both figures the results of the measurements done in the laboratory are shown with squares (blue or green) and the measurements done over deployed fiber are shown with diamond (red and purple). The difference in gains and error rates in the x- and the z-basis, respectively is due to the fact that, in the case in which one party sends a laser pulse containing more than one photon and the other party sends zero photons, projections onto the $|\psi^-\rangle$ Bell state can only occur if both pulses encode qubits belonging to the x-basis. The Bell state projection cannot occur if both prepare qubits belonging to the z-basis (we ignore detector noise for the sake of this argument). This causes increased gain for the x-basis and, due to an error rate of 50% associated with these projections, also an increased error rate for the x-basis.

6.1.7 Optimization of system performance

Decoy-state analysis

To calculate secret key rates for various system parameters, which allows optimizing these parameters, first, it is necessary to compute the gain, Q_{11}^{z}, and the error rate, e_{11}^{x}, that stem from events in which both sources emit a single photon. We consider the three-intensity decoy state method for the MDI-QKD protocol proposed in [100], which derives a lower bound for the secret key rate using lower bounds for $Q_{11}^{x,z}$ and an upper bound for e_{11}^{x}. Note that we assume here that the the only effect of imperfectly generated qubit states on the secret key rate that we consider here is that it increases the error rates (further considerations require advancements to security proofs, which are under way [100, 105]) increases of error rates.

We denote the signal, decoy, and vacuum intensities by μ_s, μ_d, and μ_v, respectively, for Alice, and, similarly, as σ_s, σ_d, and σ_v for Bob. Note that $\mu_v = \sigma_v = 0$ by definition. This decoy analysis assumes that perfect vacuum intensities are achievable, which may not be correct in an experimental implementation. However, note that, first, intensity modulators with more than 50 dB extinction ratio exist, which allows obtaining almost zero vacuum intensity, and second, that a similar decoy state analysis with non-zero vacuum intensity values is possible as well [101]. For the purpose of this analysis, we take both channels to have the same transmission coefficients (that is $t_A = t_B \equiv t$), according to our experimental configuration, and Alice and Bob hence both select the same mean photon numbers for each of the three intensities (that is $\mu_s = \sigma_s \equiv \tau_s$, $\mu_d = \sigma_d \equiv \tau_d$, and $\mu_v = \sigma_v \equiv \tau_v$). Additionally, for compactness of notation, we omit the μ and σ when describing the gains and error rates (e.g. we write Q_{ss}^{z} to denote the gain in the z-basis when Alice and Bob both send photons using the signal intensity). Under these assumptions, the lower bound on $Q_{11}^{x,z}$ is given by

$$Q_{11}^{x,z} \geq \frac{\mathbb{D}_1(\tau_s)\mathbb{D}_2(\tau_s)\big(Q_{dd}^{x,z} - Q_0^{x,z}(\tau_d)\big) - \mathbb{D}_1(\tau_d)\mathbb{D}_2(\tau_d)\big(Q_{ss}^{x,z} - Q_0^{x,z}(\tau_s)\big)}{\mathbb{D}_1(\tau_s)\mathbb{D}_1(\tau_d)\big(\mathbb{D}_1(\tau_d)\mathbb{D}_2(\tau_s) - \mathbb{D}_1(\tau_s)\mathbb{D}_2(\tau_d)\big)}, \tag{6.21}$$

where the various $\mathbb{D}_i(\tau)$ denote the probability that a pulse with photon number distribution $\mathbb{D}$ and mean τ contains exactly i photons, and $Q_0^{x,z}(\tau_d)$ and $Q_0^{x,z}(\tau_s)$ are given by

$$Q_0^{x,z}(\tau_d) = \mathbb{D}_0(\tau_d)Q_{vd}^{x,z} + \mathbb{D}_0(\tau_d)Q_{dv}^{x,z} - \mathbb{D}_0(\tau_d)^2 Q_{vv}^{x,z}, \tag{6.22}$$

$$Q_0^{x,z}(\tau_s) = \mathbb{D}_0(\tau_s)Q_{vs}^{x,z} + \mathbb{D}_0(\tau_s)Q_{sv}^{x,z} - \mathbb{D}_0(\tau_s)^2 Q_{vv}^{x,z}. \tag{6.23}$$

The error rate e_{11}^x can then be computed as

$$e_{11}^x \leq \frac{e_{dd}^x Q_{dd}^x - \mathbb{D}_0(\tau_d)e_{vd}^x Q_{vd}^x - \mathbb{D}_0(\tau_d)e_{dv}^x Q_{dv}^x + \mathbb{D}_0(\tau_d)^2 e_{vv}^x Q_{vv}^x}{\mathbb{D}_1(\tau_d)^2 Q_{11}^x}, \tag{6.24}$$

where the upper bound holds if a lower bound is used for Q_{11}^x. Note that $Q_{11}^{x,z}$, $Q_0^{x,z}(\tau_d)$, $Q_0^{x,z}(\tau_s)$ and e_{11}^x (Eqs. (D.2-D.5)) are uniquely determined through measurable gains and error rates.

Optimization of signal and decoy intensities

For each set of experimental parameters (i.e. distribution function $\mathbb{D}$, channel transmissions and all parameters describing imperfect state preparation and measurement), the secret key rate (Eq. (6.1)) can be maximized by properly selecting the intensities of the signal and decoy states (τ_s and τ_d, respectively). Here we consider its optimization as a function of the total transmission (or distance) between Alice and Bob. We make the assumptions that both the channel between Alice and Charlie and the channel between Bob and Charlie have the same transmission coefficient, t, and that Alice and Bob use the same signal and decoy intensities. We considered values of τ_d in the range $0.01 \leq \tau_d < 0.99$ and values of τ_s in the range $\tau_d < \tau_s \leq 1$. An exhaustive search computing the secret key rate for an error correction efficiency $f = 1.14$ [15] is performed from 2 km to 200 km total distance (assuming 0.2 dB/km loss), with increments of 0.01 photons per pulse for both τ_s and τ_d. For each point, the model described in section 6.1.4 is used to compute all the experimentally accessible

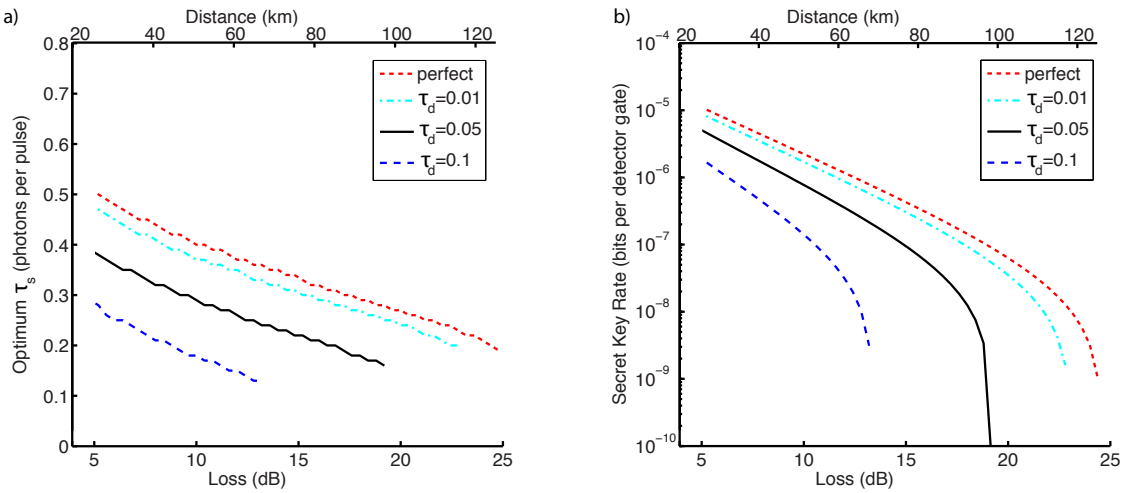

Figure 6.7: a) Optimum signal state intensity, τ_s, and b) corresponding secret key rate as a function of total loss in dB. The secondary axis shows distances assuming typical loss of 0.2 dB/km in optical fiber without splices. The optimum values for μ_s for small loss have to be taken with caution as in this regime the model needs to be expanded to higher photon number terms.

quantities required to compute secret key rates using the three-intensity decoy state method summarized in Eqs. (D.2-D.5).

In our optimization, we found that, in all cases, $\tau_d = 0.01$ is the optimal decoy intensity. We attribute this to the fact that τ_d has a large impact on the tightness of the upper bound on e_{11}^x in Eq. (D.5) (this is due to the fact that all errors in the cases in which both parties sent at least one photon, which increases with τ_d, are attributed to the case in which both parties sent exactly one photon). Figure 6.7 shows, as a function of total loss (or distance), the optimum values of the signal state intensity, τ_s, and the corresponding secret key rate, S, for decoy intensities of $\tau_d \in [0.01, 0.05, 0.1]$, as well as for a perfect decoy state protocol (i.e. using values of Q_{11}^z and e_{11}^x computed from the model, as detailed in the preceding section).

Rate-limiting components

Finally, we use our model to simulate the performance of the MDI-QKD protocol given

improved components. We consider two straightforward and modest modifications to the system: replacing the InGaAs single photon detectors (SPDs) with superconducting single photon detectors (SSPDs) [106], and improving the intensity modulation (IM). For various combinations of these improvements, the optimized signal intensities and secret key rates for $\mu_d = 0.05$ are shown in Figure 6.8. First, using state-of-the-art SSPDs in [106], the detection efficiency (η) is improved from 14.5% to 93%, and the dark count probability (P_d) is reduced by nearly two orders of magnitude. Furthermore, the mechanisms leading to afterpulsing in InGaAs SPDs are not present in SSPDs (that is $P_a = 0$). This improvement results in a drastic increase in the secret key rate and maximum distance as both the probability of projection onto $|\psi^-\rangle$ and the signal-to-noise-ratio are improved significantly. Second, imperfections in the intensity modulation system used to create pulses in our implementation contribute significantly to the observed error rates, particularly in the z-basis. Using commercially-available, state-of-the-art intensity modulators[6] allow suppressing the background light (represented by $b^{x,z}$ in general quantum state given in Eq. (6.2)) by an additional 10-20 dB, corresponding to an extinction ration of 40 dB. Furthermore, we considered improvements to the driving electronics that reduces ringing in our pulse generation by a factor of 5, bringing the values of $m^{x,z}$ in Eq. (6.2) closer to the ideal values. As seen in Figure 6.8, this provides a modest improvement to the secret key rate, both when applied to our existing implementation, and when applied in conjunction with the SSPDs. Note that in the case of improved detectors and intensity modulation system the optimized τ_s for small loss (under 10 dB) is likely overestimated due to neglected higher-order terms.

6.1.8 Discussion and conclusion

We have developed a widely applicable model for systems implementing the Measurement-Device-Independent QKD protocol. Our model is based on facts about the experimental setup and takes into account carefully characterized experimental imperfections in sources

[6]For instance, EOSpace sells intensity modulators with 50 dB extinction ratio.

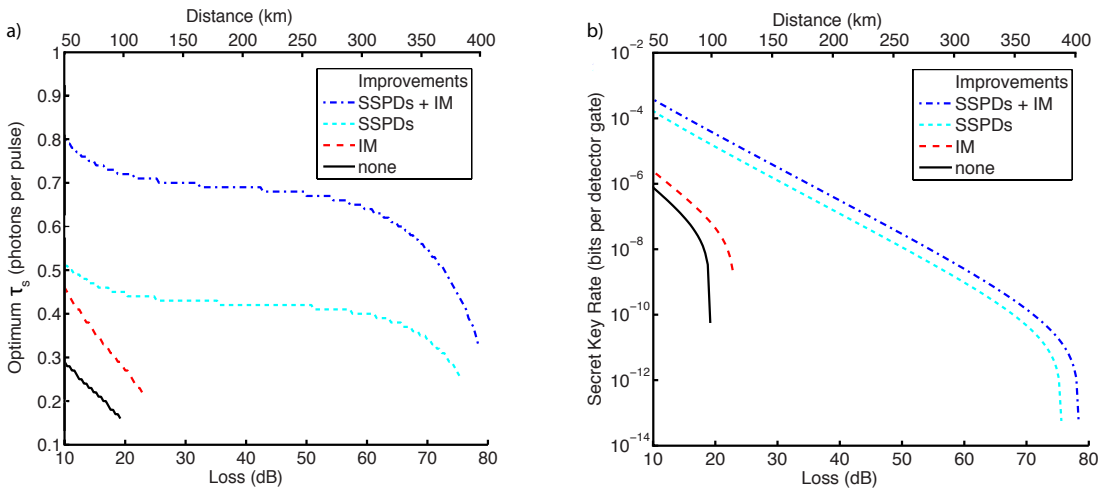

Figure 6.8: a) Optimum signal state intensity, τ_s, and b) corresponding secret key rate as a function of total loss in dB. The secondary axis shows distances assuming typical loss of 0.2 dB/km in optical fiber without splices. The optimum values for μ_s for small loss, are not shown as the model needs to be expanded to higher photon number terms in this regime.

and measurement devices as well as transmission loss. It is evaluated against data taken with a real, time-bin qubit-based QKD system. The excellent agreement between observed values and predicted data confirms the model. In turn, this allows optimizing mean photon numbers for signal and decoy states and finding rate-limiting components for future improvements. We believe that our model, which is straightforward to generalize to other types of qubit encoding, as well as the detailed description of the characterization of experimental imperfections will be useful to improve QKD beyond its current state of the art.

To finish, let us emphasize that tests of a model that describes the performance of a QKD system in terms of secret key rates has to happen in a setting in which eavesdropping can be excluded (i.e. within a secure lab and using spooled fibre) – otherwise, the measured data, which depends on the (unknown) type and amount of eavesdropping, may deviate from the predicted performance and no conclusion about the suitability of the model can be drawn. Interestingly, this implies that neither phase randomization, nor random selection of qubit states or intensities of attenuated laser pulses used to encode qubit states is necessary to test

a model, as their presence (or absence) does not impact the measured data. However, it is obvious that these modulations are crucial to ensure the security of a key that is distributed through a hostile environment. We note that in this article, all effects of imperfections in the system on the measured quantities are still attributed to an eavesdropper, and accounted for in the calculation of the secret key rate as well in the optimization of system parameters.

Acknowledgments

The authors thank E. Saglamyurek, V. Kiselyov and TeraXion for discussions and technical support, the University of Calgary's Infrastructure Services for providing access to the fiber link between the University's main campus and the Foothills campus, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI, AAET and the Killam Trusts.

6.2 Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks

A. Rubenok[1], 2, J. A. Slater[1], 2, P. Chan[1], 3, I. Lucio-Martinez[1], 2, W. Tittel[1,2]

1.- Institute for Quantum Science & Technology, University of Calgary, Canada.

2.- Department of Physics & Astronomy, University of Calgary, Canada

3.- Department of Electrical and Computer Engineering, University of Calgary, Canada

Abstract Several vulnerabilities of single photon detectors have recently been exploited to compromise the security of quantum key distribution (QKD) systems. In this letter we report the first proof-of-principle implementation of a new quantum key distribution protocol that is immune to any such attack. More precisely, we demonstrated this new approach to QKD in the laboratory over more than 80 km of spooled fiber, as well as across different locations within the city of Calgary. The robustness of our fibre-based implementation, together with the enhanced level of security offered by the protocol, confirms QKD as a realistic technology for safeguarding secrets in transmission. Furthermore, our demonstration establishes the feasibility of controlled two-photon interference in a real-world environment, and thereby removes a remaining obstacle to realizing future applications of quantum communication, such as quantum repeaters and, more generally, quantum networks.

Quantum key distribution (QKD) promises the distribution of cryptographic keys whose secrecy is guaranteed by fundamental laws of quantum physics[10, 11]. Starting with its invention in 1984[4], theoretical and experimental QKD have progressed rapidly. Information theoretic security, which ensures that secret keys can be distributed even if the eavesdropper, Eve, is only bounded by the laws of quantum physics, has been proven under various assumptions about the devices of the legitimate QKD users, Alice and Bob[33, 28]. Furthermore, experimental demonstrations employing quantum states of light have meanwhile resulted in

key distribution over more than 100 km distance through optical fiber[30] or air[31], QKD networks employing trusted nodes[15], as well as in commercially available products[12, 13].

However, it became rapidly clear that some of the assumptions made in QKD proofs were difficult to meet in real implementations, which opened side channels for eavesdropping attacks. The most prominent examples are the use of quantum states encoded into attenuated laser pulses as opposed to single photons [9], and, more recently, various possibilities for an eavesdropper to remote-control or monitor single photon detectors [56, 57, 68, 97]. Fortunately, both side channels can be removed using appropriately modified protocols. In the first case, randomly choosing between so-called signal or decoy states (quantum states encoded into attenuated laser pulses with different mean photon numbers) allows one to establish a secret key strictly from information conveyed by single photons emitted by the laser[25, 26, 27]. (We remind the reader that an attenuated laser pulse comprising on average μ photons contains exactly one photon with probability $P_1(\mu) = \mu e^{-\mu}$ [9].) Furthermore, the recently proposed measurement-device independent (MDI) QKD protocol[89] (for closely related work see [92]) additionally ensures that controlling or monitoring detectors, regardless by what means, does not help the eavesdropper to gain information about the distributed key. Note that, while the two most prominent side channels are removed by MDI-QKD, others remain open and have to be closed by means of appropriate experimental design (see appendix D).

The MDI-QKD protocol is a clever time-reversed version of QKD based on the distribution and measurement of pairs of maximally entangled photons[7]: In the idealized version, Alice and Bob randomly and independently prepare single photons in one out of the four qubit states $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle, |+\rangle, |-\rangle]$, where $|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)$. The photons are then sent to Charlie, who performs a Bell state measurement, i.e. projects the photons' joint state onto a maximally entangled Bell state[42]. Charlie then publicly announces the instances in which his measurement resulted in a projection onto $|\psi^-\rangle \equiv 2^{-1/2}\big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\big)$

and, for these cases, Alice and Bob publicly disclose the bases (z, spanned by $|0\rangle$ and $|1\rangle$, or x, spanned by $|\pm\rangle$) used to prepare their photons. (They keep their choices of states secret.) Identifying quantum states with classical bits (e.g. $|0\rangle, |-\rangle \equiv 0$, and $|1\rangle, |+\rangle \equiv 1$) and keeping only events in which Charlie found $|\psi^-\rangle$ and they picked the same basis, Alice and Bob now establish anti-correlated key strings. (Note that a projection of two photons onto $|\psi^-\rangle$ indicates that the two photons, if prepared in the same basis, must have been in orthogonal states.) Bob then flips all his bits, thereby converting the anti-correlated strings into correlated ones. Next, the so-called *x-key* is formed out of all key bits for which Alice and Bob prepared their photons in the x-basis; its error rate is used to bound the information an eavesdropper may have acquired during photon transmission. Furthermore, Alice and Bob form the *z-key* out of those bits for which both picked the z-basis. Finally, they perform error correction and privacy amplification[10, 11] to the *z-key*, which results in the secret key.

As in the entanglement-based protocol, the time-reversed version ensures that Eve cannot gain information by eavesdropping photons during transmission or by modifying the device that generates entanglement – either the source of photon pairs or the projective two-photon measurement, respectively – without leaving a trace[107, 90]. Furthermore, the outstanding attribute of the MDI-QKD protocol is that it de-correlates detection events (here indicating a successful projection onto the $|\psi^-\rangle$ Bell state) from the values of the *x*- and *z-key* bits and hence the secret key bits. In other words, all side channels related to the detection setup, regardless whether actively attacked or passively monitored, do not help Eve gain information about the secret key.

Unfortunately, the described procedure is currently difficult to implement for two reasons, first of which is the lack of practical single photon sources. However, it is possible to replace the true single photons by attenuated laser pulses of varying mean photon number (i.e. signal and decoy states, as introduced above), and to establish the secret key using information

only from joint measurements at Charlie's that stem from Alice and Bob both sending single photons[100]. This procedure results in the same security against eavesdropping as the conceptually simpler one discussed above. The secret key rate, S, distilled from signal states, is then given by[89]:

$$S \geq Q_{11}^{z}\big(1 - h_2(e_{11}^{x})\big) - Q_{\mu\sigma}^{z} f h_2(e_{\mu\sigma}^{z}), \tag{6.25}$$

where $h_2(X)$ denotes the binary entropy function evaluated on X, and f describes the efficiency of error correction with respect to Shannon's noisy coding theorem. Furthermore, Q_{11}^{z}, e_{11}^{x}, $Q_{\mu\sigma}^{z}$, and $e_{\mu\sigma}^{z}$ are gains (Q – the probability of a projection onto $|\psi^{-}\rangle$ per emitted pair of pulses) and error rates (e – the ratio of erroneous to total projections onto $|\psi^{-}\rangle$) in either the x- or z-basis for Alice and Bob sending single photons (denoted by subscript "11"), or for pulses emitted by Alice and Bob with mean photon number μ and σ (denoted by subscript "$\mu\sigma$"), respectively. While the latter are directly accessible from experimental data, the former have to be calculated using a decoy state method [89, 100] (see appendix D).

Second, a crucial element for MDI-QKD as well as future quantum repeaters and networks is a Bell state measurement (BSM). However, this two-photon interference measurement has not yet been demonstrated with photons that were generated by independent sources and have travelled through separate deployed fibers (i.e. fibers that feature independent changes of propagation times and polarization transformations). To implement the BSM one requires that these photons be indistinguishable, i.e. arrive simultaneously within their respective coherence times, with equal polarization, and feature sufficient spectral overlap. Yet, due to time-varying properties of optical fibers in a real-world environment, significant changes to photons' indistinguishability can happen in less than a minute, as depicted in Fig. 6.9. Furthermore, the carrier frequencies of the signals generated at Alice's and Bob's generally vary. These instabilities make real-world Bell state measurements without stabilization by means of active feedback impossible.

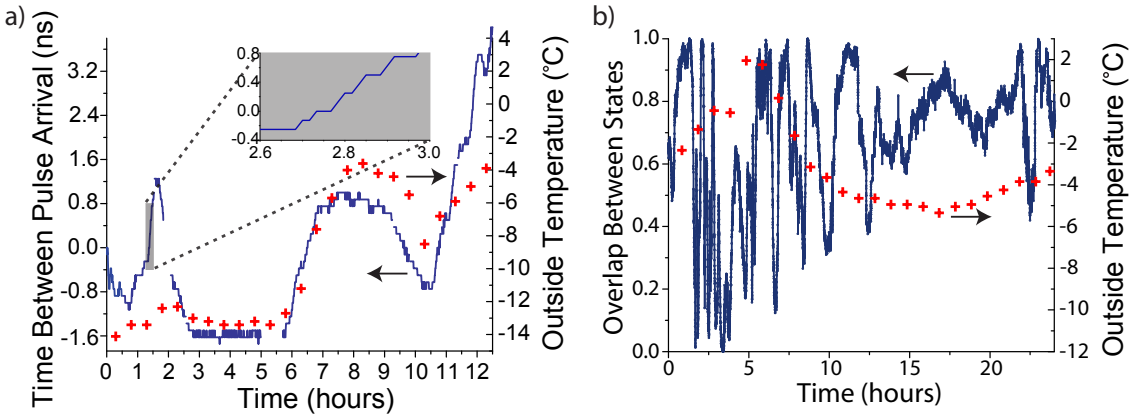

Figure 6.9: (a) Drift of differential arrival time. Variation of arrival time difference of attenuated laser pulses emitted at Alice's and Bob's after propagation to Charlie. (b) Variation in the overlap of the polarization states of originally horizontally polarized light (emitted by Alice and Bob) after propagation to Charlie. Both panels include temperature data (crosses), showing correlation between variations of indistinguishability and temperature. In addition, despite local frequency locks, the difference between the frequencies of Alice's and Bob's lasers varied by up to 20 MHz per hour (not shown).

Hence, to enable MDI-QKD and pave the way for quantum repeaters and quantum networks, we developed the ability to track and stabilize photon arrival times and polarization transformations as well as the frequency difference between Alice's and Bob's lasers during all measurements (for more information see appendix D). In order to ensure the indistinguishability of photons arriving at Charlie's and to allow, for the first time, Bell state measurements in a real-world environment, we developed and implemented three stabilization systems (see Fig. 6.10): fully-automatic polarization stabilization, manual adjustment of photon arrival time, and manual adjustment of laser frequency. Note that automating the frequency and timing stabilization systems is straightforward, particularly if the active control elements are placed in Charlie's setup.

We verified that we could indeed maintain the indistinguishability of the photons by frequently measuring the visibility, V_{HOM}, of the so-called Hong-Ou-Mandel dip[103] (a two-photon interference experiment that is closely related to a BSM). On average we found

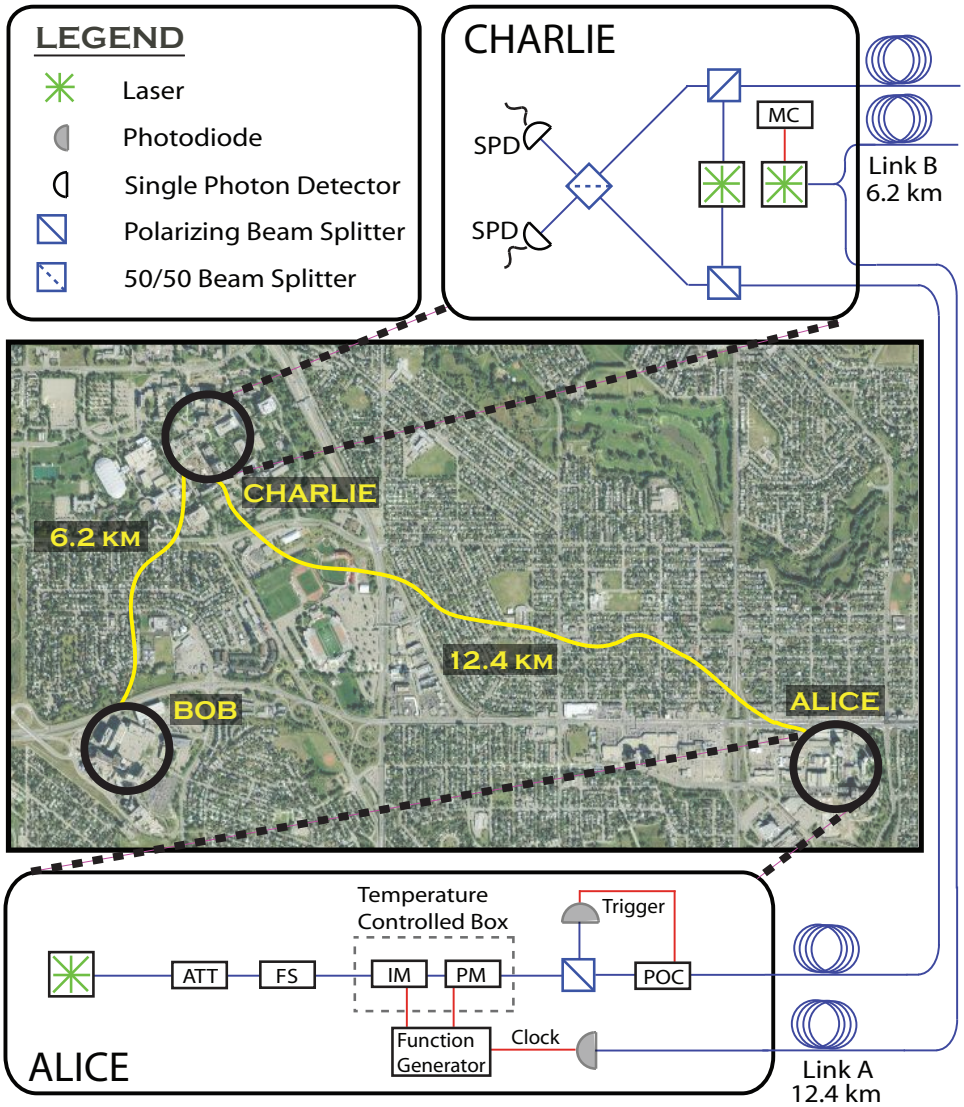

Figure 6.10: Aerial view showing Alice (located at SAIT Polytechnic), Bob (located at the University of Calgary (U of C) Foothills campus) and Charlie (located at the U of C main campus). Also shown is the schematic of the experimental setup. Optically synchronized using a master clock (MC) at Charlie's, Alice and Bob (not shown; setup identical to Alice's) generated time-bin qubits at 2 MHz rate encoded into Fourier-limited attenuated laser pulses using highly stable continuous-wave lasers at 1552.910 nm wavelength, temperature-stabilized intensity and phase modulators (IM, PM), and variable attenuators (ATT). The two temporal modes defining each time-bin qubit were of 500 ps (FWHM) duration and were separated by 1.4 ns. The qubits travelled through 12.4 and 6.2 km of deployed optical fibers to Charlie, where a 50/50 beam splitter followed by two gated (10 μs deadtime) InGaAs single photon detectors (SPD) allowed projecting the bi-partite state onto the $|\psi^-\rangle$ Bell state. (This projection occurred if the two detectors indicate detections with 1.4±0.4 ns time difference.) The MC, polarization controller (POC) and Alice's frequency shifter (FS) are used to maintain indistinguishability of the photons upon arrival at Charlie. These three feedback systems are detailed in appendix D. The individual setups for measurements using spooled fiber (arrangement (i)) are identical

Setup	Fiber	ℓ_A [km]	l_A [dB]	ℓ_B [km]	l_B [dB]	total length ℓ [km]	total loss l [dB]
1a	Spool	22.85	4.6	22.55	4.5	45.40	9.1
1b	Spool	30.98	6.8	34.65	6.9	65.63	13.7
1c	Spool	40.80	9.1	40.77	9.1	81.57	18.2
2	Deployed	12.4	4.5	6.2	4.5	18.6	9.0

Table 6.3: Length and loss (ℓ_A, l_A, ℓ_B, l_B) of the individual fiber links used to connect Alice and Charlie, and Charlie and Bob, respectively, for all tested setups. The table also lists the total length ℓ and total loss $l = l_A + l_B$ (in dB). The last line details measurements outside the laboratory with deployed fiber.

V_{HOM}=47±1%, which is close to the maximum value of 50% for attenuated laser pulses with a Poissonian photon number distribution[104], and thereby confirm that real-world two-photon interference is possible.

To assess the feasibility of MDI-QKD, we implemented a proof-of-principle demonstration of MDI-QKD using the decoy state protocol proposed by Wang[100]. This protocol requires that Alice and Bob choose between three different mean photon numbers: two non-zero values referred to as signal and decoy as well as vacuum. We performed our experiments over four different distances (henceforth referred to as setups) comprising two different arrangements (see Fig. 6.10): (i) Alice, Bob and Charlie are located within the same lab, and Alice and Bob are connected to Charlie via separate spooled fibers of various lengths and loss. (ii) Alice, Bob and Charlie are located in different locations within the city of Calgary, and Alice and Bob are connected to Charlie by deployed fibers of 12.4 and 6.2 km length, respectively. The fiber lengths and loss in each setup are listed in Table 1.

For each setup, we prepared all 4 combinations of Alice and Bob picking a state from the z-basis (i.e. $|\psi\rangle_{A,B} \in [|0\rangle, |1\rangle]$, where $|0\rangle$ and $|1\rangle$ denote time-bin qubits[42] prepared in an early or late temporal mode), and all 4 combinations of picking a state from the x-basis (i.e. $|\psi\rangle_{A,B} \in [|+\rangle, |-\rangle]$). Using a detailed model of our MDI-QKD system[108], we calculated the signal and decoy intensities that maximize the secret key rate produced by

the decoy-state method for each setup. For our decoy intensity we generated attenuated laser pulses containing on average $\mu = \sigma = 0.05 \pm 5\%$ photons and for our signal intensities we used a mean photon number between 0.25 and 0.5 (the optimal value depends on loss). For each of the four distance configurations listed in Table 1, and for each of the 16 pairs of qubit states, we performed measurements of all 9 combinations of Alice and Bob using the signal, decoy or vacuum intensity. We recorded the number of joint detections in which one detector indicated an early arriving photon (or an early noise count), and the other detector indicated a late arriving photon (or a late noise count), which, for time-bin qubits, is regarded as a projection onto the $|\psi^-\rangle$-state[42]. Depending on the observed detection rates, measurements took between 2 and 35 minutes. This data yields the gains, $Q^z_{\mu\sigma}$ and $Q^x_{\mu\sigma}$, and error rates, $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$, a subset of which is plotted in Fig. 6.11a. A complete list of gains and error rates is presented in appendix D.

We then computed secret key rates according to Eq. 6.25 after extracting Q^z_{11} and e^x_{11} using Wang's decoy state calculation[100] and assuming an error correction efficiency f=1.14[15]. As shown in Fig. 6.11b, all our measurements, both outside and inside the laboratory, and using up to 80 km of spooled fiber between Alice and Bob, output a positive secret key rate. Furthermore, using our model[108], we estimate that our setup allows secret key distribution up to a total loss of 18±4.8 dB, which is in agreement with our QKD results. Assuming the standard loss coefficient for telecommunication fibers without splices of 0.2 dB/km, this value corresponds to a maximum distance between Alice and Bob of 90±24 km. Note that moving from our proof-of-principle demonstration to the actual distribution of secret keys requires additional developments, which are detailed in appendix D.

In summary, we have demonstrated that real-world quantum key distribution with practical attenuated laser pulses and immunity to detector hacking attacks is possible using current technology. Our setup contains only standard, off-the-shelf components, its development into a complete QKD system follows well-known steps[15], and the extension to higher

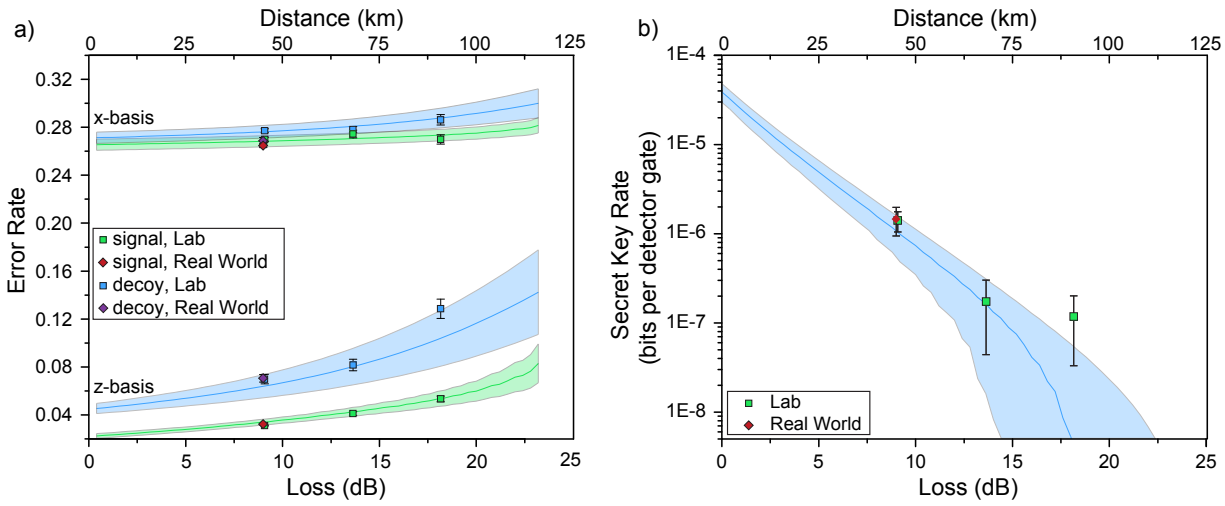

Figure 6.11: (a) Measured error rates $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ for Alice and Bob either both using signal intensity or both using decoy intensity as a function of total loss, $l = l_A + l_B$ (in dB). We note that every other combination of intensities used in the decoy-state analysis requires Alice or Bob (or both) sending vacuum, and thus the error rate is 50% and not plotted. (b) Experimentally obtained and simulated secret key rates as a function of total loss, $l = l_A + l_B$ (in dB), with $l_A \cong l_B$, for optimized mean photon numbers. Experimental secret key rates are directly calculated from measured gains and error rates using the decoy state method[100] (see appendix D for details). In both panels, the secondary x-axis shows distance assuming loss of 0.2 dB/km. Diamonds depict results obtained using deployed fibers (see Fig. 6.10a); all other data was obtained using fiber on spools. Uncertainties (one standard deviation) were calculated for all measured points assuming Poissonian detection statistics. We stress that the simulated values, computed using our model[108], do not stem from fits but are based on parameters that have been established through independent measurements. Monte-Carlo simulations using uncertainties in these measurements lead to predicted bands as opposed to lines (for more details see appendix D).

key rates using state-of-the-art detectors [109, 106] is straightforward. We also point out that MDI-QKD is well suited for key distribution over long distances, and we expect that further developments will rapidly push the separation between Alice and Bob beyond its current maximum of 250 km[30]. Finally, we remind the reader that the demonstrated possibility for Bell state measurements in a real-world environment and with truly independent photons also removes a remaining obstacle to building a quantum repeater, which promises quantum communication such as QKD over arbitrary distances.

Note added: We note that related experimental work has recently been reported in http://arxiv.org/abs/1207.0392 and http://arxiv.org/abs/1209.6178.

Acknowledgements

The authors thank E. Saglamyurek, V. Kiselyov and TeraXion for discussions and technical support, the University of Calgary's Infrastructure Services for providing access to the fiber link between the University's main campus and the Foothills campus, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of Alberta Innovates Technology Futures), CFI, AAET and the Killiam Trusts.

Chapter 7

Efficient Bell state measurement

A Bell state measurement (BSM) projects an arbitrary input state of two qubits onto the complete set of maximally entangled states, also known as the Bell basis:

$$\left|\psi^{\pm}\right\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}, \tag{7.1}$$
$$\left|\phi^{\pm}\right\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}.$$

In the simplest case, if the input state is one of the Bell states, only one measurement outcome is possible. If the input state is a completely mixed state the probability of projecting onto a given Bell state is 25%.

Bell state measurements are key elements in quantum communication and, in combination with other quantum resources (e.g. qubits and entanglement), are used to implement applications that are not possible to implement in classical communication systems. These applications include: measurement-device independent quantum key distribution [89]; quantum teleportation, i.e. the transfer of an unknown quantum state between two distant locations without having to transmit the carrier of the quantum state [110]; entanglement swapping, which is the teleportation of an entangled state [111] and superdense coding, which allows a party to communicate two bits of information in a single qubit [112]. For a detailed explanation of how the BSM plays a role on each of these applications refer to chapter 6 or appendix C.

All the listed applications can be implemented with single photon sources, attenuated laser pulses including decoy states or sources of entangled photons and linear optics. Unfortunately it has been shown that using linear optics and no auxiliary photons and the assumption of ideal detectors (including photon number resolving detectors) a perfect BSM is not possible. A perfect BSM means that the measurement outputs unambiguous and

deterministic results, i.e. all four Bell states can be distinguished and the measurement is successful in every trial. In fact, the success probability of the BSM, labeled as η_{BSM}, is limited to 50% [47]. This means that 50% of the time, the result will be inconclusive.

A BSM is typically implemented using a beam splitter with two output ports followed by optical elements and single photon detectors that allow the discrimination of orthogonal qubit modes, see figure 7.1. This scheme allows for the unambiguous identification of two Bell states. For example, a projection onto the state $|\psi^-\rangle$ is characterized by the output of the two photons in two orthogonal qubit modes ($|0\rangle$ and $|1\rangle$) and through the two different ports of the beam splitter. A projection onto the state $|\psi^+\rangle$ is characterized by the output of the two photons in two orthogonal qubit modes through the same port of the beam splitter. However, the states $|\phi^-\rangle$ and $|\phi^+\rangle$ will lead to the output of the two photons in the same mode and through the same output port of the beam splitter and hence can not be distinguished from each other. Similarly, if the states $|\phi^-\rangle$ and $|\phi^+\rangle$ can be unambiguously distinguished, the projection onto the states $|\psi^+\rangle$ and $|\psi^-\rangle$ give inconclusive results, etc. Thus, typical implementations of BSMs are restricted to a 50% success probability. A further limitation to the success probability arises from the quantum efficiency of the single photon detectors used to implement the measurement. This is because two single photon detectors must detect a photon simultaneously. As a result, the efficiency of a BSM scales as η_{det}^2, where η_{det} is the quantum efficiency of each detector. The typical efficiency of a commercial single photon detector for telecommunication wavelength is 15%. If these detectors are used to implement a BSM, then the success probability of the measurement cannot be larger than 1.1%. This means that if two qubits are incident on a Bell state measurement apparatus, only 1.1 percent of the time the qubits will be detected and the measurement outcome can be identified. Experimentally, the implementation of a perfect BSM (i.e. a measurement that identifies all four states and has a 100% success probability) is particularly appealing because of all the applications that can benefit from it. The identification of all four Bell states can

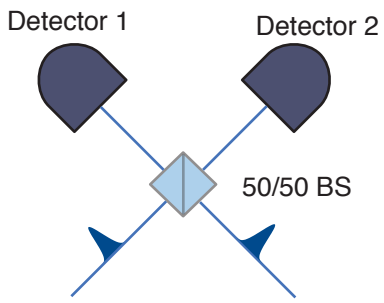

Figure 7.1: Typical Bell state measurement experimental setup. The figure shows a pair of photons incident on a 50/50 beam splitter (BS) followed by two single photon detectors (detector 1 and detector 2). This experimental setup is used to perform BSM on time-bin qubits. Polarization qubits require additional polarization beam splitters.

approach unit probability if auxiliary entangled photons are used, for more details refer to appendix C. A high success probability is achieved by employing single photon detectors with a high quantum efficiency.

When considering time-bin qubits, a typical implementation of a BSM consists of a beam splitter whose outputs are followed by two single photon detectors that can discriminate between different temporal modes, see figure 7.1. Note that in order to identify a $|\psi^+\rangle$ projection, the detection pattern is given by subsequent detections in both time-bins in a single detector, therefore the recovery time of the detector must be shorter than the time-bin separation of the qubit. However, typical single photon detectors do not have a sufficiently short recovery time to allow for the $|\psi^+\rangle$ projection and hence only the $|\psi^-\rangle$ state can be identified. As only one Bell state can be identified, the success probability of the BSM is reduced from 50% to just 25% for detectors with ideal quantum efficiency.

In this chapter I present work on the implementation of a BSM for time-bin qubits at telecommunication wavelengths in which the measurement can unambiguously identify the Bell states $|\psi^-\rangle$ and $|\psi^+\rangle$. The demonstration employs novel single photon detectors that feature small dead-times, which allows for the identification of the $|\psi^-\rangle$ and $|\psi^+\rangle$ Bell states. Additionally, the high quantum efficiency of the detectors, around 75% allows for a success probability that is 30 times greater than what has been previously demonstrated.

This work was done in collaboration with R. Valivarthi, A. Rubenok, P. Chan, F. Marsili, V. B. Verma, M. D. Shaw, J. A. Stern, J. A. Slater, D. Oblak and S. W. Nam. I contributed to these studies during the following stages: setup of single photon detectors, measurements and data analysis. I wrote the main manuscript of the paper and also contributed during its editing process.

7.1 Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors

R. Valivarthi[1,2], I. Lucio-Martinez[1,2], A. Rubenok[1,2,†], P. Chan[1,3], F. Marsili[5], V. B. Verma[4], M. D. Shaw[5], J. A. Stern[5], J. A. Slater[1,2], D. Oblak[1,2], S. W. Nam[4], W. Tittel[1,2]

1. Institute for Quantum Science and Technology, University of Calgary, Canada

2. Department of Physics and Astronomy, University of Calgary, Canada

3. Department of Electrical and Computer Engineering, University of Calgary, Canada

4. National Institute of Standards and Technology, USA

5. Jet Propulsion Laboratory, California Institute of Technology, USA

† *Present Address: School of Physics, HH Wills Physics Laboratory, University of Bristol, United Kingdom*

Abstract

We experimentally demonstrate a high-efficiency Bell state measurement for time-bin qubits that employs two superconducting nanowire single-photon detectors with short dead-times, allowing projections onto two Bell states, $|\psi^-\rangle$ and $|\psi^+\rangle$. Compared to previous implementations for time-bin qubits, this yields an increase in the efficiency of Bell state analysis by a factor of thirty.

7.1.1 Introduction

Bell state measurements (BSMs) play a key role in linear optics quantum computation and many quantum communication protocols, e.g. quantum repeaters [113], quantum teleportation [110], dense coding [112] and some quantum key distribution protocols [89]. A complete BSM allows projecting any two-photon state deterministically and unambiguously onto the set of four maximally-entangled Bell states, i.e.

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

and

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

Unfortunately, it has been shown that a complete BSM is impossible when using linear optics and no auxiliary photons: the probability for a BSM to succeed (henceforward referred to as efficiency, η_{BSM}) in the case of two photons in completely mixed input states (e.g. two photons that are members of different entangled pairs) is, in principle, limited to 50% [47]. The standard approach to Bell state analysis uses a 50/50 beam splitter followed by single-photon detectors that allow (possibly using additional external optical elements) discriminating between orthogonal qubit states $|0\rangle$ and $|1\rangle$ (see figure 7.2). This approach allows one to unambiguously project onto $|\psi^{-}\rangle$ and $|\psi^{+}\rangle$.

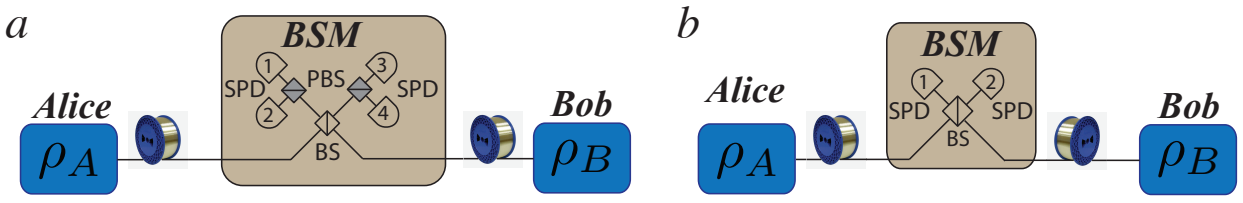

Figure 7.2: Experimental setup used to perform BSMs for a) polarization qubits and b) time-bin qubits. Density matrices ρ_A and ρ_B characterize the states of the photons emitted at Alice's and Bob's, respectively. Optical components: beam splitter (BS) and single photon detectors (SPD).

For instance, when implementing a BSM for polarization qubits, a projection onto $|\psi^{-}\rangle$ occurs if the two photons exit the beam splitter through two different ports and are detected in orthogonal polarizations, leading to detections in detectors 1 and 4, or detectors 2 and 3 (for an illustration see Fig. 7.2a). Furthermore, projections onto $|\psi^{+}\rangle$ happen if the two photons exit the beam splitter through the same port and, as before, are detected in orthogonal polarization states. This leads to detections in detectors 1 and 2, or detectors 3 and 4 (see Fig. 7.2a). Other coincidence detections correspond to projections onto product states

$|H\rangle|H\rangle \equiv |0\rangle|0\rangle$ and $|V\rangle|V\rangle \equiv |1\rangle|1\rangle$. Hence, this scheme allows achieving the maximum efficiency value of 50% if one considers single photon detectors with unity detection efficiency. Assuming realistic detectors with efficiency η_{det}, the BSM efficiency is reduced to

$$\eta_{BSM} = \frac{1}{2}\eta_{det}^2. \tag{7.2}$$

In addition to polarization, another widely used degree of freedom to encode qubits is time. In this case photons are generated in a superposition of two temporal modes $|early\rangle \equiv |0\rangle$ and $|late\rangle \equiv |1\rangle$ – so-called time-bin qubits. Time-bin qubits are particularly well suited for transmission over optical fiber (and thus generally encoded into photons at telecommunication wavelength), and have been used for a large number of experiments [43, 114, 115], including experiments that require projections onto Bell states [116, 117, 118, 93, 94]. BSMs with time-bin qubits generalize the scheme introduced above for polarization qubits: a projection onto the singlet $|\psi^-\rangle$ state occurs if one of the two detectors registers a photon in the early time bin and the second detector registers a photon in the late time bin (see Fig. 7.3b). On the other hand, a projection onto $|\psi^+\rangle$ happens if a detector registers one photon in the early time bin, and the same detector detects the second photon in the late bin (see Fig. 7.3c).

However, a problem arises if the detection of a photon is followed by dead-time during which the detector cannot detect a subsequent photon. For example, for commercial InGaAs-based single photon detectors (SPDs), which are widely used for quantum communication applications including BSM with time-bin qubits, this dead-time is typically around 10 μs[1]. This dead-time is necessary to suppress afterpulsing due to trapped carriers that are released after a detection and cause subsequent detection signals [120]. As the difference between early and late temporal modes has always been orders of magnitude smaller than the dead-

[1]To the best of our knowledge, the exceptions are [94], where frequency conversion and Si-APDs were employed, and [76, 119], where InGaAs-based SPDs with dead-times of 2 ns and 10 ns and quantum detection efficiencies of ≈10% have been reported. However, none of the last-mentioned detectors have been used for BSMs with time-bin qubits.

time of the employed detectors, commercial InGaAs SPDs have usually restricted BSMs with time-bin qubits to projections onto $|\psi^-\rangle$, reducing the maximum efficiency of the BSM from 50% to 25%. The only exception is [121], where the unambiguous projections onto three Bell states with theoretically maximum probability of 5/16≈31% was proposed and a proof-of-principle demonstration reported. Taking a typical detection efficiency for InGaAs SPDs of 15% into account, the highest efficiency of a BSM for time-bin qubits is currently thus only around 1%. This includes the demonstrations reported in [94, 76, 119] and [121].

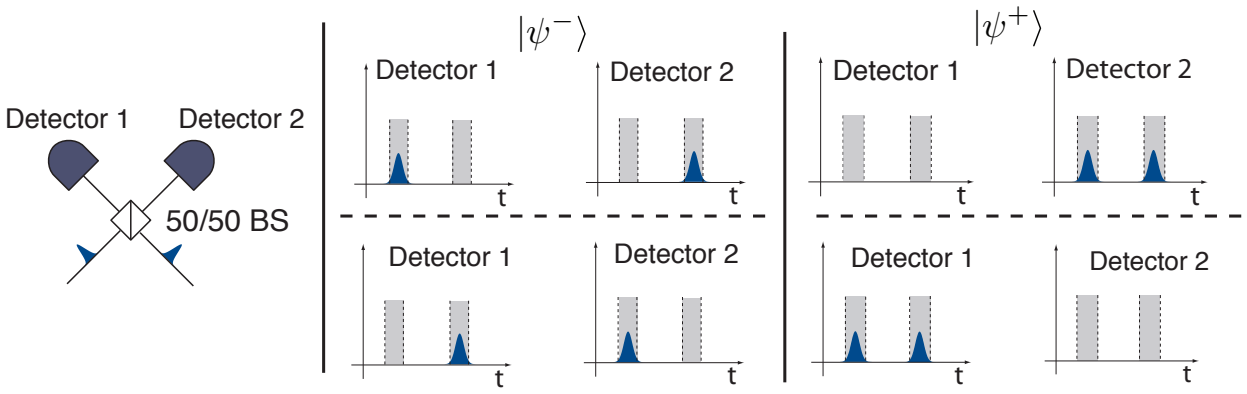

Figure 7.3: a) General setup for Bell state measurement for time-bin qubits using linear optics and single photon detectors (SPD). b) Detection pattern for projections onto $|\psi^-\rangle$ and (c) $|\psi^+\rangle$.

In this paper we present an efficient BSM for time-bin qubits encoded into telecommunication photons with projections onto the $|\psi^-\rangle$ as well as the $|\psi^+\rangle$ Bell state. Towards this end, we employ two superconducting nanowire single photons detectors (SNSPDs), which, in addition to short dead-times, feature system detection efficiencies of 76%. This leads to an increase of η_{BSM} by a factor of thirty compared to previous implementations, which is an important improvement in view of future applications of quantum information processing involving many BSMs, e.g. quantum repeaters.

The remainder of this article is structured as follows. In section 7.1.2 we describe the single-photon detectors employed to perform the measurements, and in section 7.1.3 we present the details of the experimental setup. The results of our measurements are presented

and discussed in section 7.1.4. Finally, in section 7.1.6, we present our conclusions and outlook.

7.1.2 Superconducting single photon detectors with short dead-times

Recent years have seen great progress in the development of single-photon detectors for telecommunication wavelengths. Arguably, the best detectors today are based on the transition of a superconducting nanowire into the resistive state [122], and many benchmark results have been reported with these SNSPDs. This includes dead-times as small as 10 ns [123, 124], and quantum efficiencies up to 93% at 1550 nm [106]. Furthermore, unlike InGaAs SPDs, which require gating, SNSPDs are inherently free running, show no afterpulsing, and feature very low dark count rates on the Hz level [106].

We employ SNSPDs that have been developed and fabricated at the National Institute for Standards and Technology (NIST) and the Jet Propulsion Laboratory (JPL). The detectors are based on one, or two mutually orthogonal, tungsten silicide (WSi) nanowire meanders (we refer to the two different detectors as detector 1 and 2, respectively – see Fig 7.4 a for a sketch of detector 2. The detector with two meanders features a detection efficiency that is highly insensitive to photon polarization [125], whereas the single meander version experiences up to 10% variation in efficiency at different polarizations. The two SNSPDs are mounted on an adiabatic diamagnetic refrigeration (ADR) stage inside a pulse-tube cooler, and are operated at a temperature around 800 mK. The setup for characterizing and operating the detectors is sketched in Fig. 7.4a. The SNSPDs are represented by a kinetic inductance L_k and load resistance R_l, which, in general, is equal to the impedance of the output coaxial cable. A sample of the detection signal is shown in Fig. 7.4b. The detector quantum efficiencies were measured at 1550 nm wavelength to be $77.5 \pm 0.7\%$ and $76.2 \pm 0.9\%$ for detectors 1 and 2, respectively.

To assess the detector dead-times, we illuminate the SNSPDs with weak continuous wave (cw) light and log the time Δt between subsequent detections, as illustrated in Fig. 7.4b.

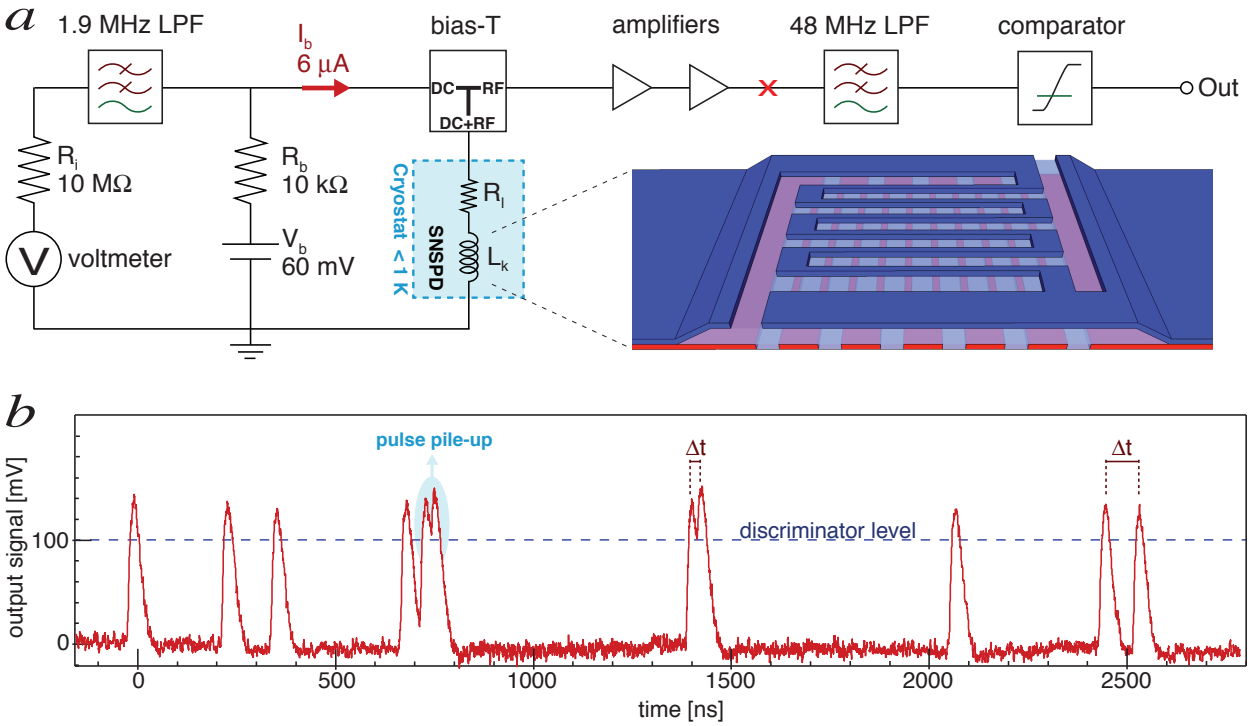

Figure 7.4: Detector setup and signal. a) Electrical diagram of the SNSPD setup. The $R_b = 10$ kΩ bias resistor translates the 60 mV bias voltage into a $I_b = 6$ μA bias current, which is directed to the superconducting detectors via the DC-port of the bias-T. The RF-port of the bias-T directs the photon detection signal through two amplifiers and a low-pass-filter (LPF) to a comparator, which generates a TTL output signal. The parallel connected voltmeter measures the voltage drop over the SNSPD and allows verifying that it is in the superconducting state. The panel also shows a sketch of an SNSPD consisting of two meanders. b) Single photon detection signals of detector 2 immediately after the amplifiers (marked by an x in figure a). A few detection inter-arrival times Δt are indicated for illustration.

Histograms of these inter-arrival detection times reveal the minimum time separation τ between detection events – during this time, the SNSPDs cannot detect another photon either because of the intrinsic time it takes the detector to return to its superconducting state or because of a pulse pile-up in which the signal does not cross the discriminator level between two consecutive incident photons and thus only the first detection event is registered. The measurements, with a 50 Ω coaxial cable attached to the detectors, shown in Fig. 7.5 by the solid lines, gives a dead-time τ on the order of 30 ns for detector 1 and 100 ns for detector 2. This dissimilarity of dead-time is due to the difference in kinetic inductance of

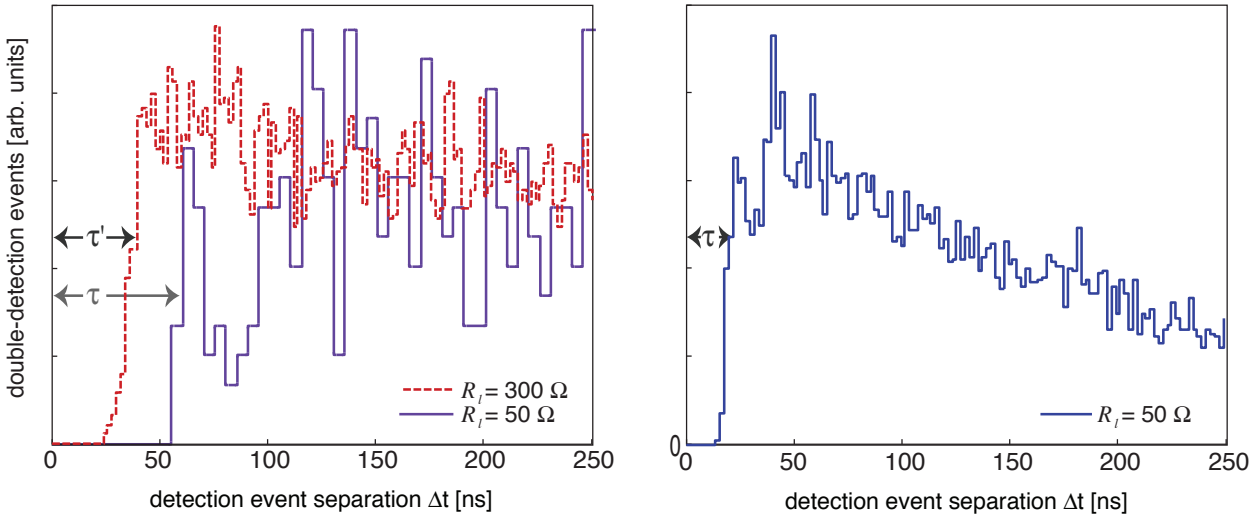

Figure 7.5: Detection dead-times. Histograms of detection inter-arrival times for SNSPD 1 and 2 in the left and right panel, respectively. Solid lines correspond to the setup with $R_l = 50\ \Omega$ (given by the impedance of the coaxial cable), while the dashed line shows the result when a $R_l = 300\ \Omega$ resistor is connected to detector 2 inside the cryostat. For R_l=50 Ω we find $\tau \approx 30$ ns for detector 1 and $\tau \approx 100$ ns for detector 2. The dead-time of detector 2 is reduced to around 40 ns when using R_l=300 Ω.

the detectors [123]. Hence, to allow projections onto the $|\psi^+\rangle$ state using detector 2, the time-bin separation would have to be on the order of 100 ns.

As argued above, it is desirable to reduce the SNSPD dead-time. Previous studies have shown $\tau \propto L_k/R_l$, and as the kinetic inductance is related to the inherent geometry and material properties of the SNSPD (which cannot be easily modified), we focus on increasing R_l as a means of reducing τ [126]. To that end we put a 300 Ω resistor in series with SNSPD detector 2. The resistors are regular ceramic surface-mount resistors and are connected to the SNSPDs after a 10 cm long coaxial cable. The resulting inter-arrival time statistics is plotted as a dashed line in Fig. 7.5. We see that the new dead-time of detector 2, τ', is significantly reduced to around 40 ns. One might conclude that an additional increase of the load resistance would further reduce the dead-time. However, we anticipate that with larger values of R_l the detector would begin to latch (i.e. not return to the superconducting state after the detection of a photon). This is supported by the observation that the factor of 6

increase in R_l only results in a factor of 2.5 decrease in the dead-time.

7.1.3 Experimental setup

Our experimental setup is similar to that described in [93]; it is depicted in Fig. 7.6: A stabilized cw laser emits polarized light at 1550 nm. The light is split by a polarization maintaining finer-optic beam splitter, and travels to two different stations, which we will refer to as Alice (A) and Bob (B). At each station, light is sent through intensity modulators that carve 0.5 ns long pulses, which, after appropriate attenuation, form time-bin qubit states encoded into laser pulses with mean photon number well below one. For instance, $|0\rangle$ corresponds to an attenuated laser pulse in an early temporal mode, $|1\rangle$ corresponds to a laser pulse in a late temporal mode, and $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ is generated by opening the intensity modulator twice in a row, generating photons in a coherent superposition of early and late temporal modes. The subsequent phase modulator allows applying a π phase shift to the late temporal mode, which results in generating $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. Qubits are created at a repetition rate of 5 MHz, and the two temporal modes are separated by 75 ns. Finally, each qubit (one generated at Alice's and one at Bob's) is sent through a polarization controller and 20 km of spooled fiber, which introduce random global phase shifts, and arrive at the Bell state analyzer where the BSM is performed using a beam splitter and two SNSPDs. Detection statistics is collected using a time-to-digital converter for various combinations of mean photon numbers per qubit generated at Alice's and Bob's, and is recorded on a PC.

It is important to recall that, for a BSM, the two photons impinging on the beam splitter must be indistinguishable in all degrees of freedom: polarization, arrival time, and frequency. Frequency indistinguishability is particularly important when working with $|\pm\rangle$ time-bin qubit states, as a frequency difference $\Delta\nu$ translates into a difference $\Delta\phi$ between the phases characterizing the superposition of the two time-bin qubit states according to $\Delta\phi = 2\pi\Delta\nu t_0$, where t_0 denotes the temporal separation between $|0\rangle$ and $|1\rangle$. While a constant phase difference (due to a constant frequency difference) can be compensated for during qubit

preparation, having time varying phase differences becomes problematic once the variation of the phase difference exceeds a few degrees. Consequently, the time-bin separation is not only constrained by the dead-time of the detectors, but also by the frequency stability of the light sources (assuming independent sources). For example, for our time-bin separation of t_0=75 ns, the two lasers must be frequency stable at least within ∼185 kHz over the duration of a measurement to keep the phase error under 5^o. Unfortunately, lasers with such frequency stability are currently not commercially available. To circumvent this problem, we used only one laser in our experiment, which allowed Alice and Bob to generate time-bin qubits with stable phase relation. Finally, to ensure indistinguishability in polarization and arrival time, we implemented feedback control as described in [93].

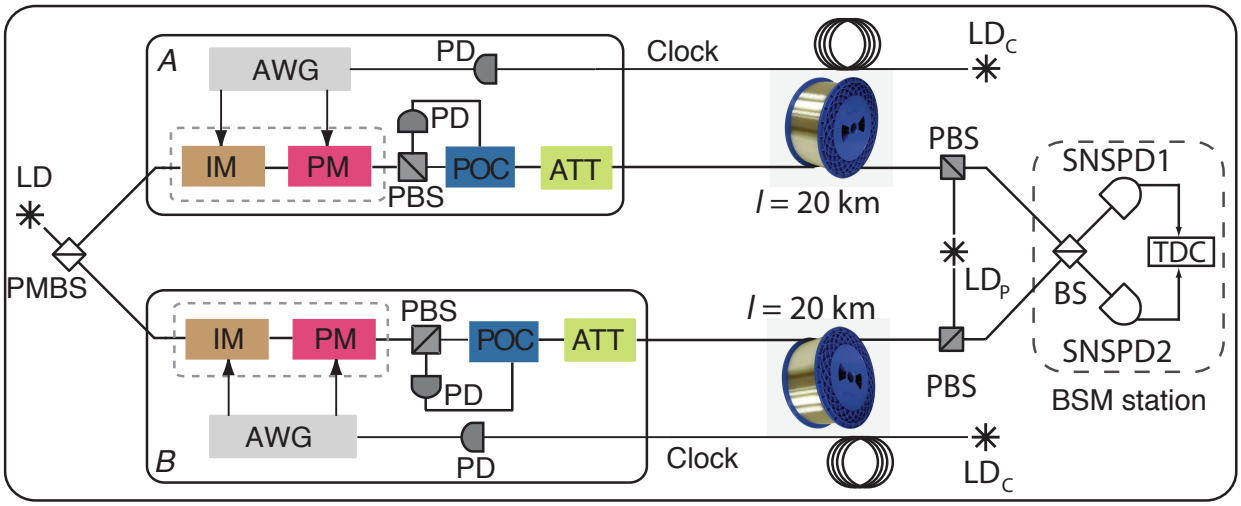

Figure 7.6: Schematic of the experimental setup employed for a BSM with time-bin qubits. LD, laser diode; PMBS, polarization maintaining beam splitter; IM, intensity modulator; PM, phase modulator; PBS, polarization beam splitter; POC, polarization controller; PD, photodiode; BS, beam splitter; AWG, arbitrary waveform generator; ATT, variable optical attenuator; SNSPD, superconducting nanowire single-photon detector. The lasers LD$_C$ and LD$_P$ are used for timing and polarization feedback control, respectively, which is further explained in [93].

7.1.4 Results

To characterize the reliability and efficiency of our Bell state analyzer, we work within the framework of the measurement-device-independent quantum key distribution (MDI-QKD) protocol [89], in which the establishment of an entangled channel by means of a BSM allows the establishment of correlated data. Conversely, the possibility to generate highly correlated bits using an MDI-QKD type setup allows one to draw conclusions about the quality of the BSM. To demonstrate efficient Bell state measurements with time-bin qubits, Alice and Bob prepare various combinations of qubit states, encoded into attenuated laser pulses with one out of three possible mean photon numbers (0.11, 0.05 and 0) and with both qubits belonging to the same basis (e.g. $|0\rangle_A|0\rangle_B$, $|0\rangle_A|1\rangle_B$, $|+\rangle_A|+\rangle_B$, $|-\rangle_A|-\rangle_B$, etc.), and send them to the Bell state analyzer. We define the z-basis to be spanned by $|0\rangle$ and $|1\rangle$, and the x-basis to be spanned by $|+\rangle$ and $|-\rangle$. For each combination of states and mean photon numbers, we record the number of projections onto $|\psi^+\rangle$ and $|\psi^-\rangle$.

7.1.5 Error rates

An important criterion for assessing the possibility for BSMs with time-bin qubits are error rates, which, for each basis and Bell state, are given by the number of erroneous projections (e.g. projections onto $|\psi^-\rangle$ if the two input states were identical) divided by the total number of projections onto that Bell state. Towards this end, qubits should be encoded into true single photons. As we use attenuated laser pulses instead, which feature Poissonian-distributed photon numbers, we use a decoy state protocol [100] to assess upper bounds e_{11} for the error rates that we would have measured had we used true single photon inputs. These rates are listed in table 7.1 below.

The results are close to ideal, in particular regarding the error rate for the z-basis, which exceeds the ideal outcome of 0% by only 0.44% and 0.80% for projections onto $|\psi^-\rangle$ and $|\psi^+\rangle$, respectively. This is a very good result, especially given that Alice and Bob are

Table 7.1: Bounded error rates e_{11}^z and e_{11}^x for two single photon inputs (one at Alice's and one at Bob's) with both photons prepared in the z and x basis, respectively. The rates are extracted from the measured data using a decoy state method [100].

Error rates	Projections onto $\|\psi^-\rangle$ (%)	Projections onto $\|\psi^+\rangle$ (%)
e_{11}^z	0.44±0.07	0.80±0.07
e_{11}^x	3.6±0.8	6.7±0.8

separated by 40 km of spooled fiber. The remaining errors are due to (almost negligible) background light leaking through Alice's and Bob's intensity modulators (featuring 50 dB extinction ratio) and detector dark counts (around 10 Hz, including detector counts due to blackbody radiation). For the x-basis, the error rates exceed the ideal outcome of 0% by 3.6% and 6.7% for the $|\psi^-\rangle$ and $|\psi^+\rangle$ projections, respectively. We attribute the increment in the error rates compared to those of the z-basis to phase errors occurring during the preparation of the $|-\rangle$-state, and to a poorer performance of the decoy state method, i.e. a larger gap between the bound on e_{11} and its actual value. The latter is due to errors in the raw data arising from multi-photon contributions (e.g. two photons arriving from Alice and zero photons from Bob) [93], which partially propagate into the calculated bound for e_{11}^x.

Efficiency

While error rates allow assessing if the BSM is functioning correctly, an equally important measure is the efficiency of the Bell state analyzer. As in the previous section, we use the decoy state protocol [100] to find a lower bound on the number of projections onto $|\psi^+\rangle$ and $|\psi^-\rangle$ that originate from the emission of single photons at Alice's and Bob's. The number of such projections per clock cycle, $Q_{11}^{x,z}$ (where x, z denotes the basis in which the qubits have been prepared), then allows us to calculate the BSM efficiency for each basis and Bell

state using

$$Q_{11}^{x,z} = P_1(\mu)P_1(\mu)t^2\eta_{BSM}^{x,z}. \tag{7.3}$$

Here, $P_1(\mu)$ refers to the probability of emission of a single photon per (Poissonian distributed) source, t denotes to the transmission between Alice or Bob and the Bell state analyzer, and $\eta_{BSM}^{x,z}$ is the basis-dependent efficiency of the BSM. The results for η_{BSM} are listed in table 7.2.

Table 7.2: Bell state measurement efficiencies extracted from measured data using a decoy state method [100].

Basis	Efficiency for projections onto $\|\psi^-\rangle$ (%)	Efficiency for projections onto $\|\psi^+\rangle$ (%)	Total efficiency (%)
z	13.6±0.2	14.5±0.2	28.1±0.4
x	14.5±0.4	15.3±0.4	29.8±0.8

We note, first, that the values for the total efficiencies per basis differ by only 1.7%, confirming that we can perform all projections with almost equal probability. In particular, this shows that the detectors have indeed fully recovered after 75 ns. Second, we find that the efficiency averaged over the x, y and z bases (where we made the physically motivated assumption that the efficiency in the y-basis, which we did not measure, equals the one measured in the x-basis), η_{BSM}, corresponds to that estimated using Eq.7.2 and taking into account the measured detector quantum efficiencies:

$$\begin{aligned} \eta_{BSM} &= \frac{1}{3}\big(\eta_{bsm,z} + 2\eta_{bsm,x}\big) = (29.3 \pm 0.4)\% \\ &\approx \frac{1}{2}\eta_{det}^2 = \big(29.5 \pm 0.4\big)\%. \end{aligned} \tag{7.4}$$

Furthermore, we point out that the efficiency is a factor of ≈ 30 higher than what has previously been obtained with time-bin qubits. Finally, we note that our average BSM

efficiency is only 2.3% below the theoretical maximum of 5/16≈31% (assuming detectors with 100% efficiency) achievable with previously implemented schemes [121].

7.1.6 Conclusions and Outlook

We have described and demonstrated how to perform efficient Bell state analysis with time-bin qubits using linear optics and no additional photons. By employing SNSPDs with short dead-times, it is possible to project not only onto the $|\psi^-\rangle$, but also onto the $|\psi^+\rangle$ Bell state. Together with the high quantum efficiency of the SNSPDs, this improved the efficiency of Bell state measurements with time-bin qubits from ≈1% to ≈29%, which falls only a few percent short of the previous theoretical maximum of 31%. Additionally, the low noise of the superconducting detectors yields a very small error rate.

Bell state measurements are key ingredients for applications of quantum information processing, including linear optics quantum computing, quantum repeaters, and measurement-device-independent quantum key distribution, and our results are interesting in view of improving (or allowing) implementations. However, to take full advantage of the increased efficiency, detector dead-times need to be decreased, for instance using detector arrays [127], to allow reducing the spacing between temporal modes used to encode time-bin qubits.

Acknowledgements

WT, JAS, PC, AR, RV, ILM and DO thank Neil Sinclair and Vladimir Kiselyov for discussions and technical support, and acknowledge funding by Alberta Innovates Technology Futures (AITF), the National Sciences and Engineering Research Council of Canada (NSERC), the US Defense Advanced Research Projects Agency (DARPA) Quiness Program under Grant No. W31P4Q-13-1-0004, and the Killam Trusts. VBV and SWN acknowledge partial funding for detector development from the DARPA Information in a Photon (InPho) program. Part of the research was carried out at the Jet Propulsion Laboratory,

California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

Chapter 8

Quantum private queries

Uncertainty in quantum mechanics has proven to be successful to achieve information theoretic security for key distribution. The question of whether security improvements to other 2-party cryptographic primitives[1] can be achieved with a quantum approach was raised some time ago. In this chapter, we will focus on an application of the oblivious transfer (OT) cryptographic protocol so called quantum private queries. It involves the interaction of two parties: a user and a database provider, who holds an N-element database. The user is interested in retrieving an element from the database without letting the database know which element was retrieved. On the other hand, the database is interested in keeping the database secret from the user and revealing only the element the user is interested in. Note that in this scenario the two parties (user and database) are adversaries and do not trust each other. This differs from the QKD scenario in which Alice and Bob trust each other and instead a third party, Eve, is considered the adversary.

Classically, the oblivious transfer protocol (or private queries) is performed either under the assumption of limited computational power of the adversary [128], or through third trusted parties (e.g. servers) [129]. Unfortunately, information theoretic security was proven impossible for the quantum version of oblivious transfer [130]. In the impossibility proof, the user and database are assumed to have unrestricted computational power, including the access to a quantum computer. The impossibility proof applies for a *perfectly concealing* protocol, i.e. the user only learns one element of the database and the database does not learn any information about what element the user learned. However, quantum oblivious transfer can offer practical degrees of security [131] if:

[1] These include secret sharing, coin flipping and bit commitment.

1. Non-perfect conditions are considered. For example if the user only learns probabilistic information about the database, or if the database can learn some information about the user's query.

2. A universal quantum computer is not available. This is a reasonable assumption since quantum computing is still in early stage of development.

Under these conditions, the quantum version of oblivious transfer has an advantage over its classical counterpart. Specifically, third trusted parties are not necessary to implement the protocol. Furthermore, there is no assumption needed on the classical computational power of the adversary.

Different protocols to implement quantum private queries have been proposed [131, 132, 133]. The security of all the suggested quantum protocols is based on cheating sensitivity, which means that the database can try to learn which element the user is interested in, but in doing so it can be caught cheating. The first quantum oblivious transfer protocol proposed [131] involves a user sending a quantum query or a decoy state to the database. The problem in this protocol is that due to inevitable loss in the quantum channel, the user has to send quantum states a number of times, giving the database a chance to use the loss to his advantage. Note that, just as for QKD, the requirements to make the quantum private queries protocol implementable in deployed systems are loss and channel noise tolerance. This protocol is neither loss nor noise tolerant, hence it is not a viable option for real world use.

Subsequent oblivious transfer protocols [132, 133] had a different approach to the problem of quantum private queries. In these protocols, the database and the user aim at sharing an oblivious key. The database knows the entire oblivious key and the user only knows n bits of it but the database does not know which bits the user knows. The N elements of the database are then encoded with the oblivious key and sent to the user, who is able to decode the number of elements n known from the oblivious key, see figure 8.1.

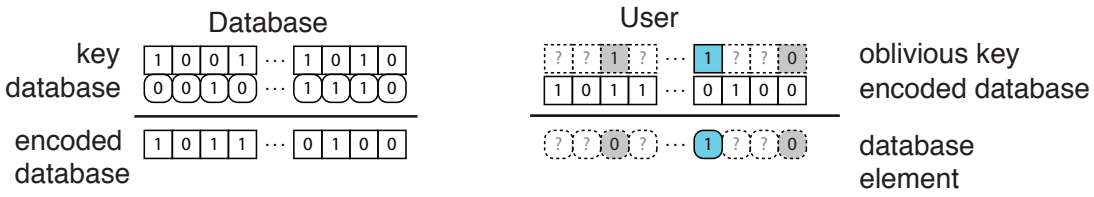

Figure 8.1: The left hand side of the picture shows how the database encodes the database elements using an oblivious key. The right hand side of the pictures shows the oblivious key of the user and the encoded database that the user receives. At the end of the protocol the user only knows with certainty few bits (blue color), while for the other bits the user only has partial information (gray color).

The database emits non-orthogonal quantum states in order to establish an oblivious key with the user. The quantum states are transmitted to the user who performs a measurement on them. The user then has to announce which states were received and measured, making the protocol loss tolerant. Note that the user does not have any information about the quantum states received, so there is no gain for him/her in lying about the results at this stage of the protocol. The use of non-orthogonal quantum states prevents the user from getting conclusive results in every measurement as deterministic and unambiguous state discrimination is fundamentally impossible in this case. From this point of the protocol the user does not give any feedback to the database until the oblivious key has been established. The uncertainty about the bit values that the user obtains from inconclusive measurements is propagated through the rest of the key in order to obtain the oblivious key. This protocol, however, does not consider the case of noisy channels. Hence, it can not be used in deployed systems.

In the work I present in this chapter, we developed an error correction protocol to make the previously introduced oblivious transfer protocol fault tolerant. This adds quantum private queries to the few communication protocols that are loss and noise tolerant. Furthermore, we also performed an experimental implementation of oblivious transfer with our error correction scheme to show its functionality. We also propose and analyze simple attacks that the database and the user can implement against each other. In addition, we emphasize

how the implementation of error correction contributes to the privacy of both the database and the user.

This work was done in collaboration with P. Chan, X.F. Mo, C. Simon and W. Tittel. I contributed to these studies in the following stages: modified the QKD system presented in chapters 4 and 5 in order to implement the oblivious transfer protocol, data measurement, discussions of data analysis and taking part of the editing process of the manuscript.

8.1 Performing private database queries in a real-world environment using a quantum protocol

Philip Chan[1], Itzel Lucio-Martinez[2], Xiaofan Mo[2†], Christoph Simon[2] & Wolfgang Tittel[2]

Institute for Quantum Science and Technology, and Department of Electrical & Computer Engineering,University of Calgary,

2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.

Institute for Quantum Science and Technology, and Department of Physics & Astronomy, University of Calgary, Canada,

2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada.

[†]Current address: Beijing Institute of Aerospace Control Devices, Quantum Engineering Center, China Aerospace Science and Technology Corporation, Beijing 100854.

Abstract In the well-studied cryptographic primitive 1-out-of-N oblivious transfer, a user retrieves a single element from a database of size N without the database learning which element was retrieved. While it has previously been shown that a secure implementation of 1-out-of-N oblivious transfer is impossible against arbitrarily powerful adversaries, recent research has revealed an interesting class of private query protocols based on quantum mechanics in a cheat sensitive model. Specifically, a practical protocol does not need to guarantee that database cannot learn what element was retrieved if doing so carries the risk of detection. The latter is sufficient motivation to keep a database provider honest. However, none of the previously proposed protocols could cope with noisy channels. Here we present a fault-tolerant private query protocol, in which the novel error correction procedure is integral to the security of the protocol. Furthermore, we present a proof-of-concept demonstration of the protocol over a deployed fibre.

Uncertainty in quantum mechanics can be used to provide security in cryptographic applications, allowing quantum cryptographic protocols to relax the typical assumptions

required for security (e.g. an adversary with limited computational power), or even avoid them altogether. The use of quantum information has proven extremely successful for key distribution,for which quantum key distribution (QKD)[4, 10, 11] can allow two parties to communicate over a public channel with information theoretic security (i.e. security against an adversary with arbitrarily powerful computational capability, including quantum computers). The application of quantum information theory to other cryptographic tasks is an interesting topic both because of the insight offered into capabilities of quantum versus classical information coding, and because of the possibility of developing new practical cryptographic protocols with improved security. Indeed, there are various proposals and experimental demonstrations of quantum cryptographic primitives such as secret sharing[134, 135], coin-flipping[4, 136, 137], bit commitment[138, 139], and oblivious transfer (OT)[131, 140, 141, 132, 133, 139].

When considering cryptographic protocols for deployment, a protocol must ultimately satisfy the following two criteria:

1. Security: The protocol must have a rigorous security analysis based on reasonable assumptions about the adversaries. A strong justification must exist for believing that these assumptions are true.

2. Implementability: The protocol must be implementable with existing technologies, and must function in the presence of loss and noise (which are inevitable in a realistic implementation).

However, initially proposed protocols often do not meet both requirements, and in particular often do not consider loss and/or noise in the quantum channel. Indeed, of the above mentioned protocols, only the bit commitment and OT protocols of ref. [141, 138, 139] are simultaneously loss- and noise-tolerant, and thus are candidates for real-world implementation.

In the case of oblivious transfer, it has been shown that if both parties possess a universal

quantum computer it is impossible to simultaneously guarantee that the user, Ursula, can reliably retrieve only a single element while ensuring that the database provider, Dave, has absolutely no knowledge of which element was retrieved[130]. However this does not mean a practical protocol cannot exist. First, note that the security criterion allows for reasonable assumptions about the computational capabilities of the dishonest party (e.g. restricting the adversary from having a universal quantum computer). Indeed, classical OT protocols also rely on one of two assumptions — that at least some fraction of the intermediaries used to perform the query are trustworthy[129, 142], or that the adversary has limited classical computational resources[128]. In particular, a quantum protocol has been proposed based on the assumption that the adversary has limited noisy quantum storage[141, 139] (which precludes the adversary from possessing a universal quantum computer). However, new developments (e.g. improvements in computational methods[143, 144] or in quantum memory[145, 146, 36, 147, 148, 149], respectively) may make these assumptions difficult to justify in the long term. Second, it may be acceptable in practice to relax security conditions of OT — that is, one can allow the user to learn more information from the database, and/or the database may be able to gain some information about the query. Several quantum protocols have been proposed in this vein based on a cheat sensitive model[131, 140, 132, 133], in which the database provider is kept honest by the possibility of being caught cheating. (This type of security can be sufficient if users wish to purchase information privately from a database who spends significant effort gathering and analyzing data, e.g. to make recommendations to investors, as the database must maintain a high quality of service[132].) In this setting, the protocol need not prevent the database from gaining any information about the user's query, hence protocols may exist in which the assumptions are easier to justify, or in which no assumptions are required at all. A brief comparison of the properties of the above mentioned protocols for OT and private queries, as well as the protocol we present in this work is given in Table 8.1, and we review these protocols in

further detail in appendix E.

Table 8.1: Comparison of the ability of various protocols for private queries to meet the two criteria for deployment (security and implementability). Note that the cheat sensitive security model may offer the possibility for security with no additional conditions since the impossibility proof [130] may not apply.

	Protocol	Security		Implementability	
		Security Model	Conditions For Which Security is Known to Hold	Loss-tolerant	Fault-tolerant
Classical information	computational[128]	standard	adversary has limited classical and quantum computational capability	N/A	N/A
	trusted[129, 142]	standard	trusted intermediaries are available	N/A	N/A
Quantum information	noisy-storage[141, 139, 150]	standard	parameters of the adversarys quantum memory (e.g. decoherence as a function of time) are known	yes	yes
	GLM[131]	cheat sensitive	no additional conditions	no	no
	QKD based[132, 133]	cheat sensitive	specific attacks discussed in refs. [132, 133]	yes	no
	our protocol	cheat sensitive	specific attacks discussed in this work	yes	yes

In this work, we propose a private query protocol based on the protocols of ref. [132, 133], retaining the advantages of those works while addressing the remaining obstacle to meeting the implementability criterion. This is accomplished using a novel error correction algorithm, in which the algorithm and its associated parameters are tailored to provide the desired level of security in the private query protocol. Furthermore, we note that the novel error correction procedure used to provide fault-tolerance also provides additional opportunities for Ursula to verify Dave's honesty, thus enhancing the cheat sensitive property of the protocol. Hence, we show that error correction is not simply necessary to meet the implementability criterion, but is integral to the security criterion as well.

8.1.1 Results

As in ref. [132, 133], we implement a cheat sensitive private query protocol based on the SARG04 Quantum Key Distribution (QKD) protocol[29]. The functionality of the protocol can be described as implementing probabilistic n-out-of-N OT — that is, Ursula will, on average, learn the value of $\bar{n}$ bits (where $\bar{n}$ is small) of the database with high confidence (for brevity, we often simply describe such bits as being known to Ursula). She will also have probabilistic knowledge of other bits of the database (i.e. she can guess their value with better than 50% probability). In this scheme, a private query on an N-bit database is made possible using an N-bit oblivious key (for simplicity, we consider each element of the database to be a single bit) generated by the quantum protocol, in which the goal is to ensure that Ursula knows, on average, $\bar{n}$ bits of the oblivious key, whose positions are unknown to Dave. In the following sections, we give a description of the protocol for generating an oblivious key and using it to perform private queries, give an overview of the error correction procedure, and then conclude with a brief discussion on security.

Description of the protocol.

A detailed description of the honest protocol for performing a private query is as follows (see

Figure 8.2 for a graphical representation of the protocol):

1. Dave generates two long strings of classical bits uniformly at random, and records their values. Each string should be $\approx \frac{kN}{t}$ bits in length, where k is a parameter determined by the previously agreed-upon error correction procedure (to be discussed later), N is the length of the database, and t is the transmission of the link between Ursula and Dave.

2. Dave uses each pair of classical bits generated above to choose a quantum state from a set of four previously agreed upon non-orthogonal states (shown in Figure 8.2), and prepares qubits accordingly. A random bit from the first string determines whether the state is prepared in the 0-basis (spanned by $|\psi_0\rangle$ and $|\phi_0\rangle$) or the 1-basis (spanned by $|\psi_1\rangle$ and $|\phi_1\rangle$), and the corresponding random bit in the second string determines whether the ψ or ϕ state in each basis is chosen. The first random string forms Dave's raw key, for which the bit values correspond to the bases in which he prepared the qubits.

3. Dave sends the qubits encoded into single photons to Ursula using a possibly lossy and noisy quantum channel.

4. Ursula makes projection measurements using either the 0- or 1-basis, chosen uniformly at random, and records the measurement bases and the results. Ursula publicly announces the cases in which she detected a photon, and Ursula and Dave both discard all the events in which Ursula failed to detect the photon. The protocol proceeds to the next step once Ursula has succeeded in detecting kN photons. Dave keeps the corresponding kN bits from his raw key to form his sifted key.

5. Dave publicly announces his second string of random bits (used to select whether he encoded the qubits into a ψ or ϕ state), which, combined with

knowledge from Ursula's measurements (and, for the moment, assuming a noiseless channel), allows her to conclusively identify whether the state was encoded in the 0- or 1-basis with probability $p_{\mathrm{c}} = \frac{\sin^2(\theta)}{2}$. Note that when Ursula's measurements yielded inconclusive results, which occurs with probability $p_{\mathrm{i}} = 1 - p_{\mathrm{c}}$, she gains probabilistic information about the basis. This information can be quantified by the probability that she incorrectly identifies the basis, $e_{\mathrm{i}} = \frac{\cos^2(\theta)}{1+\cos^2(\theta)}$. A noisy channel will affect the probabilities p_{c}, p_{i}, and e_{i}, as well as result in a non-zero error rate for conclusive measurements, denoted e_{c}. Like Dave, Ursula associates classical bit values to the quantum states based on the basis, and forms her sifted key using the most likely values of the bits given her measurement results.

6. Dave divides his sifted key into N k-bit blocks, and computes each bit of his oblivious key as the parity of the k bits in each block (the parity is 0 if an even number of the k bits is 1, and 1 otherwise). He publicly announces which bits form each block. In addition, according to a previously agreed upon error-correcting code, he also sends the parities of several subsets of the k bits to Ursula. Using this information, along with her sifted key and knowledge of whether the measurements were conclusive or inconclusive, Ursula computes the most likely value of each oblivious key bit, as well as the probability that this value is incorrect, denoted e_{k}. The error-correcting code is selected such that Ursula will only have a high confidence (or low e_{k}) in $\bar{n}$ bits on average, where $\bar{n}$ is typically a few bits. If Ursula does not learn any bits of the protocol (due to its probabilistic nature), the protocol must be restarted.

7. Ursula selects a shift value that aligns one of the bits she knows in the oblivious key to the bit in the database that she wants to know. She communicates this shift value classically to Dave, who applies the shift to his oblivious key, and

then uses it to encrypt the database using the one-time-pad[3]. He then sends the encrypted database to Ursula, who can only decrypt the bits for which she knows the corresponding oblivious key bit. If Ursula knows multiple bits of the oblivious key she will learn multiple bits of the database. However, the shift only allows her to select the location of a single bit of the database, with the remaining learned bits distributed randomly.

Error-correcting codes for private queries.

Let us now examine step 6 of the protocol in more detail. Our error correction procedure (see Supplementary Information for a full description) is inspired by syndrome decoding of error-correcting codes such as Hamming codes[151], which can operate on a few bits at a time. However, it is important to note that in the context of private queries error correction is integral to determining how much information Ursula learns about the oblivious key, creating unique requirements that made it necessary to investigate and design novel error-correcting codes and error correction procedures. In particular, the goal when designing an error-correcting code for private queries is not to simply maximize the probability of successful decoding as it is in standard communications applications. Rather, a specific success probability is desired in order to ensure that Ursula only learns a few bits of the oblivious key. Furthermore, to prevent Ursula from learning a large amount of probabilistic information about the remaining bits of the key, it is desirable to keep e_{k} as high as possible in those cases in which decoding does not succeed.

In addition there are two main technical differences between error correction in private queries and in communications. First, note that in order to recover the value of the oblivious key bit, Ursula need only determine the parity of the k-bits, and not the individual values of the k bits as would typically be the case for error correction. Hence, the error correction procedure seeks the most likely parity of the k-bit block, and successful decoding does not depend on having a high probability of identifying the correct values of the k-bit block as long

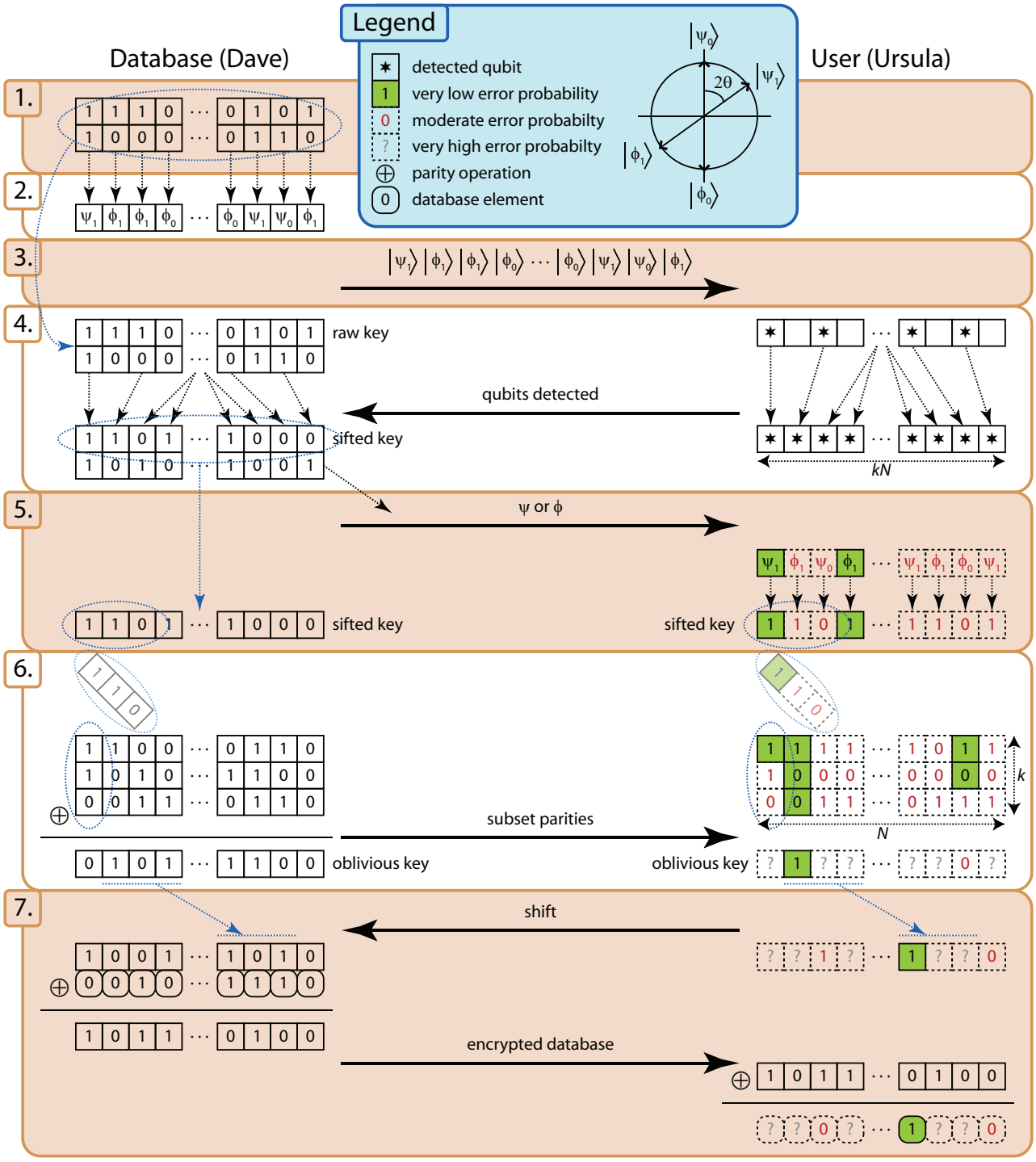

Figure 8.2: Graphical representation of the private query protocol. The steps indicated on the left margin correspond to the steps described in the text.

as it is possible to identify whether an even or odd number of errors occurred. Second, the input bits can be divided into those with low error rate (conclusive measurements), and those with very high error rate (inconclusive measurements). We note that it is the interaction of this latter property with the short block lengths used ($k \leq 10$) that allows uncertainty to be maintained after error correction, thereby limiting the amount of information that Ursula learns about the database.

The error-correcting codes used in this work are tailored based on the experimental parameters (i.e. conclusive and inconclusive probabilities, p_{c} and p_{i} and the associated error rates e_{c} and e_{i}) in order to achieve the goals discussed above. In order to quickly evaluate error-correcting codes, we define two thresholds, t_{U} and t_{D}. When $e_{\mathrm{k}} \leq t_{\mathrm{U}}$, Ursula considers the oblivious key bit to be known. When $e_{\mathrm{k}} \leq t_{\mathrm{D}}$, Dave considers Ursula to have significant partial information about that bit. These thresholds should be selected based on the requirements of the application. In this work, we use $t_{\mathrm{U}} = 10^{-3}$ and $t_{\mathrm{D}} = \frac{1}{3}$. In order to reduce the probability of error in Ursula's oblivious key bit below her threshold (i.e. $e_{\mathrm{k}} \leq t_{\mathrm{U}}$), the error correction process must sufficiently reduce e_{k} when her quantum measurements succeeded in obtaining a large amount of information about the k bits (i.e. when most or all measurements were conclusive). However, the error correction will also reduce e_{k} if several measurements were inconclusive. Hence, the error rate for inconclusive measurements, e_{i}, is of particular importance to the fraction of bits for which $e_{\mathrm{k}} \leq t_{\mathrm{D}}$. With this in mind, a smaller angle between states (characterized by θ as shown in Figure 8.2) has, in addition to those benefits noted in ref. [133] (i.e. reduced quantum communication, improved database security, and better control over the number of bits Ursula learns), the benefit of reducing the partial information from inconclusive measurements. However, there is a trade-off between these benefits and the fact that the error rate for conclusive measurements is also increased due to a reduced signal-to-noise ratio, making it more difficult to achieve $e_{\mathrm{k}} \leq t_{\mathrm{U}}$. A detailed description of the selection of our error-correcting codes is given

in the Supplementary Information.

Security of the protocol.

Let us now discuss how the steps in the above protocol contribute to security, beginning with a discussion of user privacy. User privacy is protected by the cheat sensitive property of the protocol, which allows a dishonest database to be detected. This property stems from step 4 of the protocol as Ursula randomly selects between two possible (non-commuting) measurements and does not announce which measurement she performed. Her security thus stems from the complementarity principle as her interpretation of her measurement results is dependent on her choice of measurement basis, with the protocol designed such that the classical bit value she assigns to each result is perfectly correlated with her basis choice (see step 5 and the Supplementary Information for more details). In the case that Dave is honest (and for the moment, assuming a noiseless system), Ursula's classical bit values for conclusive measurements will also be perfectly correlated with the classical bit values Dave used to select which quantum states he encodes. If Dave is dishonest, and supposing he can send a state such that Ursula's measurement is conclusive regardless of which measurement basis she chooses (a realistic attack is analyzed in the Supplementary Information), Ursula's interpretation of her measurements remain unchanged, hence her classical bit values are still perfectly correlated to her choice of basis. Since this choice is never revealed to Dave, he does not know which bit value she obtains. This leads to the cheat sensitivity in the protocol, as the dishonest database may be detected during error correction (since he sends parity values uncorrelated with Ursula's classical bit values), or after completion of the protocol since he may send incorrect query results. Furthermore, note that the error correction procedure in step 6 only involves one-way communication from Dave to Ursula, hence Dave gains no information regarding the results of the error correction procedure.

On the other hand, Ursula's limited knowledge about the oblivious key stems from the

superposition principle in quantum mechanics. Specifically, note that in step 2 Dave prepares qubits in non-orthogonal states, and that Ursula can thus not deterministically distinguish between these states. As such, Ursula's measurements only give her limited information, even after Dave reveals some information about which state he sent in step 5. Furthermore, note that Ursula must declare which bits were lost during transmission (or detection) in step 4, prior to receiving classical information indicating whether a ψ or ϕ state was sent. This makes the protocol loss-tolerant while ensuring that Ursula cannot choose which bits to keep based on whether her measurements were conclusive or inconclusive, even if she uses a heralded quantum memory to delay her measurements until after step 5. Note that in step 6, Ursula does have the ability to restart the protocol if the results are unfavorable as Dave cannot verify whether she indeed learned no bits of the oblivious key. However, choosing an error-correcting code such that $\bar{n}$ is a few bits ensures that the probability for Ursula to not know any bits is very low, and allows Dave to abort the protocol after a small number of declared failures by Ursula (preventing her from repeatedly declaring failure until she obtains a very favorable result).

Furthermore, a dishonest user may gain an advantage by deviating from the honest protocol. It has been shown that Ursula could perform an unambiguous state discrimination (USD) measurement[152, 153] in order to slightly improve her probability of conclusive measurements, which allows her to learn a few additional bits of the oblivious key[132]. However, this comes at the expense of gaining no information about the bit value (i.e. $e_{\mathrm{i}} = 0.5$) when the USD measurement gives inconclusive results. While this probabilistic information was not previously considered useful[132, 133], it is an important input to the error correction process. Thus, the effectiveness of this attack is reduced in the presence of error correction, and our analysis in the Supplementary Information shows that in some cases performing a USD measurement actually reduces the number of bits of the oblivious key that Ursula learns as compared to the honest measurements. Note that only individual USD measure-

ments have been considered, and coherent attacks (e.g. an optimized USD measurement on the k qubits that form each oblivious key bit) remain an interesting open question.

We also note that Ursula and Dave are adversarial in nature in the protocol, and thus may not cooperate when estimating the error rate in order to select an appropriate error-correcting code. An error-correcting code that is not well suited to the actual error rate in the system will either result in Ursula learning too few or too many bits of the oblivious key, but does not impact user security. Hence the database does not have any motivation to falsify the error rate, but the user would like the database to think the error rate is larger than it is in reality, leading to the selection of an error-correcting code that gives her more information. In our analysis (detailed in the Supplementary Information), we find that Dave can ensure that he has a reasonable level of security by determining the error rate of devices under his control (potentially by intentionally introducing noise) and selecting an error-correcting code accordingly. In addition, even if Ursula's devices introduce some additional error that Dave does not account for in his security analysis, the protocol is still successful for her.

Experimental and simulated performance of our protocol.

We performed an experimental demonstration of private queries over a 12.4 km fiber link between the University of Calgary and SAIT Polytechnic, using our BB84[4] QKD system[73] (with a small modification to the hardware to set $\theta = 35.6^\circ \pm 0.49^\circ$ — all other differences between our protocol and BB84 QKD are in the classical post-processing). Our experimental setup is shown in Figure 8.3 (see ref. [73] for a detailed description). Note that our demonstration uses weak coherent pulses rather than single photons, and hence database privacy requires the assumption that Ursula is not able to exploit pulses containing multiple photons (adapting the protocol for weak coherent pulses, e.g. using decoy states as in QKD[25, 26, 27, 154], remains an open question, and we discuss this possibility further

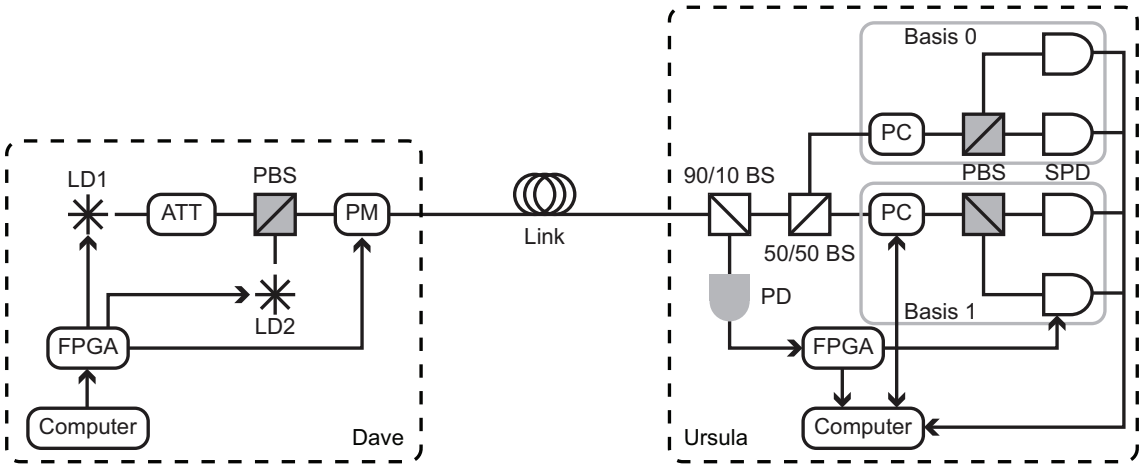

Figure 8.3: Diagram of the experimental setup. The database (Dave) uses a computer and field-programmable gate-array (FPGA) to control the generation of polarization qubits via an attenuated laser diode (LD1 and ATT) and polarization modular (PM). Quantum frames[73] (sequences of strong light for timing and stabilization) are generated by a second laser diode (LD2) and merged using a polarizing beam-splitter (PBS). Light is transmitted from Dave to Ursula through a 12.4 km dark fiber link with 4.5 dB loss between SAIT Polytechnic and the University of Calgary. Ursula splits off 10% of the incoming light (90/10 BS) to a photodiode (PD) used to detect the quantum frames. The 50/50 BS is used to passively select a random measurement basis. The apparatus for each basis consists of a polarization controller (PC), a PBS, and two single photon detectors (SPD) to make the projection measurement. Upon detecting a quantum frame, Ursula's FPGA triggers the SPDs and initiates data collection by the computer, or polarization compensation, as appropriate.

in the Supplementary Information). We consider a database size of $N = 10^6$ and, based on measured error rates for our system, an error-correcting code with $k = 10$ was selected, thus requiring 10^7 measured qubits per query. Note that we did not consider $k > 10$ due to computational constraints when searching for the best possible construction of the error-correcting code. A total of 11 queries was performed using a mean number of photons per pulse of $\mu = 0.95 \pm 0.047$ to show that the protocol can function at the single photon level. In this setting, our system took approximately 4.5 hours to accumulate the 10^7 bits of data needed for one private query. In order to quickly collect statistics, we repeated the experiment with mean number of photons per pulse increased to $\mu = 9.5 \pm 0.47$, performing 104 queries. While the multi-photon emissions at this μ are likely to compromise the security of the protocol if Ursula monitors the pulses outside Dave's laboratory, this value corresponds to ~ 0.95 photons per pulse at the detectors, ensuring that multi-photon detection events do not skew the detection statistics. The measured parameters that determine the performance of the protocol are shown in Table 8.2 (note that the experimentally measured parameters at both mean photon numbers are the same to within one standard deviation), along with parameters for a theoretical simulation of what could be achieved using state-of-the-art detectors[106, 155]. These detectors allow for significantly reduced noise (they feature dark count rates ≈ 100 Hz), and, in the case of ref. [106], detection efficiencies up to 93%. With the improved signal-to-noise ratio, we select the parameters of the protocol to be $\theta = 25°$ and $k = 9$.

The experimental and simulated results for these codes are shown in Table 8.3. The simulated results corresponding to our experiment are derived from Monte Carlo simulations taking into account the variation in the parameters shown in Table 8.2. Figure 8.4 compares the distribution of the results over the 104 queries performed in the $\mu = 9.5 \pm 0.47$ case with the simulation results, showing good agreement between the two. Note that in both experimental cases, no errors were observed in the bits learned by Ursula (i.e. for which

Table 8.2: Parameters for the private query protocol as measured in our experiment with standard detectors, and simulated for low-noise detectors. The value of θ (including standard deviation) is measured using classical light. For the probabilities of conclusive measurements, p_c, and error rates for conclusive and inconclusive measurements, e_c and e_i, the standard error expected based on Poissonian counting statistics for the 10^7 bits in each query is negligible compared to the observed variations across the queries performed. The observed standard deviations are attributed to time-varying error in the alignment of the measurement bases at the receiver as a result of channel instability. Note that the measurement results for the $\mu = 9.5 \pm 0.47$ case show more variation in the parameters than for the $\mu = 0.95 \pm 0.047$ case due to short-term fluctuations that are averaged out by the long data collection time needed to acquire the 10^7 bits per query in the $\mu = 0.95 \pm 0.47$ case.

	standard detectors		low-noise detectors
μ (photons)	0.95 ± 0.047	9.5 ± 0.47	1
θ (°)	35.6 ± 0.49	35.6 ± 0.49	25
p_c (%)	16.1 ± 0.29	16.1 ± 0.93	9.22
e_c (%)	4.4 ± 0.59	4.6 ± 0.38	1.91
e_i (%)	41.24 ± 0.08	41.3 ± 0.64	45.12
k (bits)	10	10	9

$e_k \leq 10^{-3}$), with a total of 45 bits learned in 11 queries when $\mu = 0.95 \pm 0.047$ and 405 bits learned in 104 queries when $\mu = 9.5 \pm 0.47$.

In addition, our simulation results show that the primary obstacle to improving database security in the protocol is noise in the system, which can be greatly reduced by state-of-the-art single photon detectors. These detectors can also improve the rate at which queries can be performed by almost an order of magnitude because of their higher detection efficiencies. Further improvement of this rate is straightforward, as QKD systems can easily be adapted to perform this protocol. A state-of-the-art BB84 QKD system has shown that data can be accumulated at a rate of 10^6 to 10^7 bits per second, depending on the distance between Ursula and Dave[66]. For the parameters in our experimental demonstration, this would allow one private query to be performed every few seconds. The amount of data required can also be reduced by repeating a short oblivious key over a longer database and then applying a shift as before to allow Ursula to select the desired bit. This would allow queries to be performed more often, or equivalently, allow queries to be performed on a larger database in the same amount of time. However, this comes at the expense of database security, as the user is able

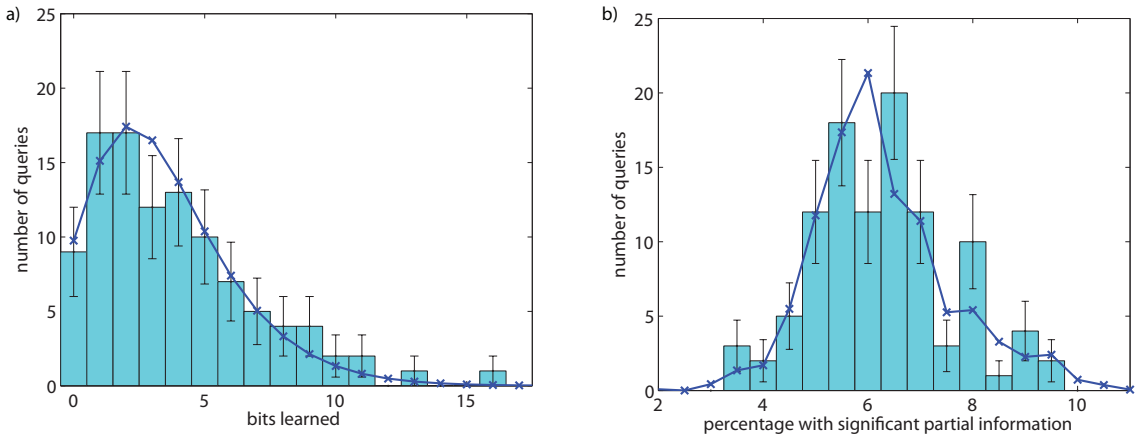

Figure 8.4: Histograms for the information gained by the user in the 104 queries performed in the $\mu = 9.5 \pm 0.47$ case. a) The number of bits learned by the user. b) The percentage of the database of which the user learns significant partial information. In both figures error bars for the experimental results represent one standard deviation assuming Poissonian counting statistics, and the blue crosses show the expected distribution obtained from Monte Carlo simulations.

Table 8.3: Experimental and simulated results for the quantum private queries. The following figures of merit are used: the average number of bits learned by the user per query, $\bar{n}$, the average proportion of the database where the user has significant partial information (i.e. $e_k \leq t_D$), $\bar{m}$, and the failure probability (i.e. that the user learns zero bits), P_0.

	$\mu = 0.95 \pm 0.047$		$\mu = 9.5 \pm 0.47$		low-noise
	experimental	simulated	experimental	simulated	simulated
$\bar{n}$ (bits)	4.1 ± 2.4	3.2 ± 1.1	3.9 ± 3.1	3.5 ± 1.9	4.35
$\bar{m}$ (%)	6.1 ± 0.25	6.1 ± 0.25	6.3 ± 1.4	6.3 ± 1.3	0.96
P_0 (%)	9.1 ± 9.1	8.8	8.7 ± 2.9	9.4	1.29

to learn additional bits for each repetition of the key (though not in locations of her choice, as only a single shift value is communicated). We also note that a modification to the protocol of ref. [132] has recently been proposed that reduces the amount of quantum communication required[156], however applying this modification to our protocol is not straightforward.

8.1.2 Discussion

We have proposed and demonstrated, over deployed optical fibres, a quantum protocol for private queries using the cheat sensitive model. This first demonstration of private queries in a real-world setting was made possible by the development of a protocol which integrates a

novel error correction procedure. Our analysis of this protocol has shown that error correction plays a pivotal role in the security, both in terms of controlling how much information the user learns, and in providing the ability for Ursula to detect a dishonest database. While our security analysis is currently limited to several specific attacks, it is important to note that the error correction should be viewed as an important tool for tailoring the amount of information learned by the user, and hence may be adaptable to a more general scenario where Ursula makes more powerful measurements. In this general view, database security stems from the fact that quantum mechanics allows a protocol to be designed where the user cannot extract full information about the quantum states sent, and error correction allows the extracted information to be processed into an oblivious key with the desired distribution of information for private queries. Furthermore, quantum mechanics allows such a private query protocol to be set up such that the correlation between Ursula and Dave's classical raw key bits is destroyed if Dave can control which bits of the oblivious key Ursula learns. Hence, the methods presented in this work should provide a strong basis for the further development of cheat sensitive quantum protocols.

8.2 Acknowledgements

The authors thank M. Jakobi, M.V. Panduranga Rao and C. Erven for useful discussions, V. Kiselyov for technical support, SAIT Polytechnic for providing laboratory space, and acknowledge funding by NSERC, QuantumWorks, General Dynamics Canada, iCORE (now part of AITF), AITF, CFI, and AAET.

Chapter 9

Conclusions and Outlook

9.1 Conclusions

This thesis has focused on the implementation of two different QKD protocols on two independent QKD systems as well as the implementation of the quantum private queries protocol, all of them over deployed fiber.

A first QKD system implementing the BB84 protocol allowed us to develop and test tools that, in principle, can be used to integrate any QKD system into existing optical-fiber networks. The same system is used to perform an analysis of the scalability of the key generation rate at different stages of the process of key distribution. From this study we found that a hardware based operation of sifting, error correction and privacy amplification must be implemented to improve the secret key generation rate.

The second QKD system implemented the recently proposed measurement-device independent QKD (MDI-QKD) protocol [89]. The benefit of the MDI-QKD protocol is that the detectors employed do not have to be trusted. This constitutes a huge advantage over prepare and measure QKD protocols as many hacking attacks exploit single photon detectors. As part of our MDI-QKD implementation, we demonstrated, for the first time, a Bell state measurement over deployed fiber. Additionally, novel single photon detectors were used to study the possibility of a high-efficiency Bell state measurement. Bell state measurements play an important role in a number of quantum communication applications (e.g. MDI-QKD, quantum repeaters, quantum teleportation). As Bell state measurements are limited to a 50% success probability for ideal detectors [47], the overall success probability of different applications that use Bell state measurements can benefit from the most efficient implementations available for these measurements.

Finally, the quantum private queries protocol was implemented using a modified version of our BB84 QKD system. An error correction protocol to make the protocol noise tolerant was developed and allowed us to demonstrate quantum private queries in the real world for the first time.

9.2 Outlook

One of the main goals of the quantum communication community is to establish quantum networks that can implement high speed quantum cryptography over existing infrastructure between many parties over long distances. Several quantum networks have been demonstrated, however, they operated over short distances and assumed that all of the nodes trusted each other. The quantum frames tool described in chapter 4 can potentially solve this problem by including routing information. Another potential solution is implement a "star-topology" network using MDI-QKD. In this network, only a central node requires single photon detectors (the most expensive devices in a QKD system) and would connect different parties within the network. The central node does not have to be trusted, due to the specific features of the MDI-QKD protocol.

Measurement-device independent QKD overcame potential security flaws associated with devices used for measuring in QKD systems. It is naturally highly desirable to extend this idea and create a QKD system that does not need to make assumptions about any of the devices used by Alice and Bob. Several such protocols, known as device independent QKD, have been proposed [91, 24]. These protocols rely on fundamental concepts of quantum mechanics like Bell inequalities to guarantee the security of the distributed key. Although an experimental implementation of device independent QKD in the real world has not been performed yet due to the large gap between the theoretical requirements and the experimental possibilities, significant effort is being directed towards making this gap smaller.

In current QKD implementations, the noise in single photon detectors places a limit on

the distance at which it is possible to distribute a secret key. The access to low noise and more efficient single photon detectors like the ones demonstrated recently [106] opens the possibility to implement QKD at longer distances (up to ∼300 km). However, for more than a few hundred kilometres distance better detectors do not suffice and it becomes necessary to use entanglement based QKD in combination with quantum repeaters [113]. The goal of a quantum repeater is to distribute entanglement over long distances. This is done by dividing the long quantum channel in smaller links, called elementary links. Two sources of entangled photons are found within each elementary link. Each source emits a pair of entangled photons. Using entanglement swapping, which makes use of Bell measurements, it is possible to distribute entanglement across the elementary link. Multiple elementary links can be concatenated in order to distribute entanglement across an arbitrary distance. The implementation of MDI-QKD is a first step towards a repeater as MDI-QKD requires the demonstration of a Bell state measurement with photons created independently. As such, the MDI-QKD scheme can easily be upgraded as the improved repeater technology becomes available. Quantum repeaters must also be supplemented with quantum memories, as the probability of simultaneously having entangled photons at the end of multiple elementary links is small. Currently, there is a lot of research done on quantum memories and implementation of quantum repeaters [113].

While many challenges still remain, the field of quantum communication continues to mature and move closer to being a powerful tool in real-world situations.

Bibliography

[1] R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).

[2] C. E. Shannon, Bell System Technical Journal **28**, 656 (1949).

[3] G. S. Vernam, Journal of the American Institute of Electrical Engineers **55**, 109 (1926).

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

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. of Cryptology **5**, 253 (1992).

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

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

[8] A. Muller, H. Zbinden, and N. Gisin, Nature **378**, 449 (1995).

[9] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

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

[11] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[12] idquantique, `www.idQuantique.com`.

[13] Magiq, `http://www.magiqtech.com/MagiQ/Home.html`.

[14] Quintessence, `http://www.quintessencelabs.com/`.

[15] M. S. et al., Optics Express **19**, 10387 (2011).

[16] T. C. et al., Opt. Exp. **18**, 27217 (2010).

[17] M. P. et al., New Journal of Physics **11**, 075001 (2009).

[18] C. Elliot *et al.*, Proceedings of SPIE **5815**, 138 (2005).

[19] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 6 (2006).

[20] A. Vakhitov, V. Makarov, and D. Hjelme, J. Mod. Opt **48**, 2023 (2001).

[21] M. A. Nielsen and I. I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[22] R. Safavi-Naeini, Information theoretic security course, Lecture notes, 2009.

[23] C. E. Shannon, The Bell System Technical Journal **27**, 623 (1948).

[24] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).

[25] W. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[26] X. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[28] D. Gottesman, H. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).

[29] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[30] D. Stucki *et al.*, New J. Phys. **11**, 075003 (2009).

[31] T. S.-M. et al., Phys. Rev. Lett. **98**, 010504 (2007).

[32] A. Rubenok, Quantum key disitribution with temporal mode encoding, Master's thesis, University of Calgary, 2011.

[33] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[34] Smartquantum, www.smartquantum.com.

[35] W. Tittel *et al.*, Laser Photonics Rev **4**, 244 (2009).

[36] K. Hammerer, A. S. Sorensen, and E. S. Polzik, arXiv **0807.3358** (2008).

[37] N. Gisin and R. Thew, Nature Photon. **1**, 165 (2007).

[38] H. J. Kimble, Nature **453**, 1023 (2008).

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

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

[41] P. T. et al., IEEE Photonics Technol. Lett. **15**, 1669 (2003).

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

[43] A. Muller *et al.*, Appl. Phys. Lett. **70**, 793 (1997).

[44] H. Zbinden *et al.*, Electron. Lett. **33(7)**, 586 (1997).

[45] Z. L. Yuan and A. J. Shields, Optics Express **13**, 660 (2005).

[46] M. Martinelli, Optics Communications **72**, 341 (1989).

[47] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[48] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[49] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[50] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[51] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).

[52] N. Gisin, B. Huttner, N. Imoto, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[53] M. Dušek, O. Haderka, and M. Hendrych, Opt. Commun. **169**, 103 (1999).

[54] G. Brassard and L. Salvail, Advances in Cryptology EUROCRYPT '93 (Berlin: sSpringer) **Vol. 765**, 410 (1994).

[55] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[56] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[57] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[58] D. Pearson, Quanutm Communication, Measurement and Computing **734**, 299 (2004).

[59] R. G. Gallager, IRE Transactions on Information Theory **8**, 21 (1962).

[60] D. J. C. MacKay and R. M. Neal, Electronics Lett. **33**, 457 (1997).

[61] B. Levine, T. R. Reed, and H. Schmit, IEEE Symp. on Field-Programmable Custom Computing Machines , 217 (2000).

[62] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, IEEE Trans. Inf. Theory **47**, 585 (2001).

[63] R. Muscedere, V. S. Dimitrov, and G. Jullien, Fourtieth Asilomar Conf. on Signals, Systems and Computers (ACSSC '06) , 921 (2006).

[64] E. Sharon, S. Litsyn, and J. Goldberger, IEEE Trans. Inf. Theory **53**, 4076 (2007).

[65] S. Koehl, A. Liu, and M. Paniccia, Optics Express **22**, 24 (2011).

[66] A. Dixon, Z. L. Yuan, J. Dynes, A. Sharpe, and A. J. Shields, Optics Express **16** (2008).

[67] B. Qi and et.al., Quant. Inf. Comp. **7**, 73 (2007).

[68] L. Lydersen *et al.*, Nature Photon. **4**, 686 (2010).

[69] N. Jain *et al.*, arXiv **1103.2327v2** (2011).

[70] K. J. Gordon *et al.*, Opt. Express **13**, 3015 (2005).

[71] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **92**, 201104 (2008).

[72] A. Dixon, Z. L. Yuan, J. Dynes, A. W. Sharpe, and A. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

[73] I. Lucio-Martinez, P. Chan, X.-F. Mo, S. Hosier, and W. Tittel, New Journal of Physics **11**, 095001 (2009).

[74] C. Healey, I. Lucio-Martinez, M. R. E. Lamont, X. F. Mo, and W. Tittel, arXiv **1105.3760** (2011).

[75] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **91**, 041114 (2007).

[76] A. R. Dixon *et al.*, Appl. Phys. Lett. **94**, 231113 (2009).

[77] D. J. Rogers, J. C. Bienfang, A. Nakassis, H. Xu, and C. W. Clark, New Journal of Physics **9**, 319 (2007).

[78] R. C. Agarwal and C. S. Burrus, Proceedings of the IEEE **63**, 550 (1975).

[79] P. Rice and J. Harrington, arXiv **0901.0013** (2009).

[80] R. Y. Q. Cai and V. Scarani, New Journal of Physics **11**, 045024 (2009).

[81] C.-H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).

[82] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, Umac: Fast and secure message authentication, in *Advances in Cryptology — CRYPTO' 99*, edited by M. Wiener, , Lecture Notes in Computer Science Vol. 1666, pp. 79–79, Springer Berlin / Heidelberg, 1999.

[83] B. Yang, R. Karri, and D. A. McGrew, Selected Areas in Communications, IEEE Journal on **24**, 1831 (2006).

[84] B. Levine, R. R. Taylor, and H. Schmit, IEEE Symposium on Field-Programmable Custom Computing Machines , 217 (2000).

[85] M. Fürst *et al.*, Optics Express **18**, 13029 (2010).

[86] T. H. et al., Optics Express **17**, 9053 (2009).

[87] Y.-L. T. et al., Phys. Rev. A **88**, 022308 (2013).

[88] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, Optics Express **19**, 23590 (2011).

[89] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[90] H. Inamori, Algorithmica **34**, 340 (2002).

[91] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[92] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[93] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[94] Y. L. et al., Phys. Rev. Lett. **111**, 130502 (2013).

[95] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, arXiv **1207.6345** (2012).

[96] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).

[97] L. Lydersen *et al.*, Opt. Express **18**, 27938 (2010).

[98] Z. L. Yuan, J. Dynes, and A. J. Shields, Nature Photon. **4**, 800 (2010).

[99] L. Lydersen *et al.*, Nature Photon. **4**, 801 (2010).

[100] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).

[101] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New Journal of Physics **15**, 113007 (2013).

[102] D. Stucki *et al.*, Journal of Modern Optics **48**, 1967 (2001).

[103] C. K. Hong, Z. Ou, and L. Mandel, Phy. Rev. Lett. **59**, 2044 (1987).

[104] L. Mandel, Phys. Rev. A **28**, 929 (1983).

[105] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, arXiv **1111.3413v4** (2013).

[106] F. Marsili *et al.*, Nature Photon. **7**, 210 (2013).

[107] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[108] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv **1204.0738** (2012).

[109] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, Appl. Phys. Lett. **96**, 071101 (2010).

[110] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[111] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[112] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[113] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys **83**, 33 (2011).

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

[115] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[116] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature **421**, 509 (2003).

[117] H. D. Riedmatten *et al.*, Phys. Rev. A **71**, 050302 (2005).

[118] J. J. et al., Nature Comm. **4**, 2386 (2013).

[119] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, Appl. Phys. Lett. **95**, 091103 (2009).

[120] J. Zhang, R. Thew, J.-D. Gautier, N. Gisin, and H. Zbinden, IEEE Journal of Quantum Electronics **45**, 792 (2009).

[121] J. van Houwelingen, A. Beveratos, N. Brunner, N. Gisin, and H. Zbinden, Phys. Rev. Lett. **96**, 130502 (2006).

[122] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Supercond. Sci. Technol. **25**, 063001 (2012).

[123] A. J. Kerman *et al.*, Appl. Phys. Lett. **88**, 111116 (2006).

[124] B. S. R. et al., Opt. Lett. **31**, 444 (2006).

[125] V. Verma, Appl. Phys. Lett. **101**, 251114 (2012).

[126] J. K. W. Yang *et al.*, IEEE Trans. on Appl. Supercond. **17**, 581 (2007).

[127] V. B. Verma *et al.*, Appl. Phys. Lett. **104**, 051115 (2014).

[128] Aiken Computation Lab, Harvard University Report No., , 1981 (unpublished).

[129] M. Naor and B. Pinkas, Advances in Cryptology - ASIACRYPT (2000).

[130] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).

[131] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **100**, 230502 (2008).

[132] M. Jakobi *et al.*, Phys. Rev. A **83**, 022301 (2011).

[133] F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, Optics Express **20**, 170253 (2012).

[134] M. Hillery, V. Buek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[135] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[136] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, Proc. 32nd annual ACM symp. Theory of computing STOKC '00 , 705 (2000).

[137] G. B. et al., Nat. Commun. **2**, 561 (2011).

[138] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nat. Commun. **3**, 1326 (2012).

[139] R. König, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).

[140] F. D. Martini *et al.*, Phys. Rev. A **80**, 010302 (2009).

[141] C. Schaffner, Phys. Rev. A **82**, 032308 (2010).

[142] C. Blundo, P. D'Arco, A. D. Santis, and D. Stinson, Journal of Cryptology **20**, 323 (2007).

[143] T. Kleinjung and et al, Proc. 30th annual conf. on Advances in cryptology, CRYPTO'10 , 333 (2010).

[144] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[145] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Nature Photon. **3**, 706 (2009).

[146] W. Tittel and et al., Laser Photonics Rev. **4**, 244 (2010).

[147] C. S. et al., Eur. Phys. J. D **58**, 58 (2010).

[148] P. S. et al, Science **332**, 1059 (2011).

[149] F. B. et al., arXiv **1306.6904** (2013).

[150] C. Erven *et al.*, arXiv **1308.5098** (2013).

[151] D. MacKay, *Information Theory, Inference, and Learning Algorithms* (Cambridge University Press, 2003).

[152] U. Herzog and J. A. Bergou, Phys. Rev. A **71**, 050301 (2005).

[153] P. Raynal, arXiv **quant-ph/0611133** (2006).

[154] S. Wehner, M. Curty, C. Shaffner, and H.-K. Lo, Phys. Rev. A **81**, 052336 (2010).

[155] Z. Y. et al., Rev. Sci. Instrum. **83**, 073105 (2012).

[156] M. V. P. Rao and M. Jakobi, Phys. Rev. A **87**, 012331 (2013).

[157] D. Mayers, Advances in Cryptology – Proceedings of Crypto '96 **1109**, 343 (1996).

[158] M. Dušek, N. Lütkenhaus, and M. Hendrych, Progress in Optics **49** (2006).

[159] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

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

[161] W. P. Grice, Phys. Rev. A **84**, 042331 (2011).

[162] Y.-H. Kim, S. P. Kulik, and Y. Shih, arXiv **0010046** (2000).

[163] F. Bussières, J. A. Slater, J. Jin, N. Godbout, and W. Tittel, Phys. Rev. A **81**, 052106 (2010).

[164] E. Woodhead and S. Pironio, arXiv **1209.6479** (2012).

[165] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).

[166] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).

[167] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A **86**, 022332 (2012).

[168] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

Appendix A

Error Correction

All QKD protocols developed so far require post-processing of the sifted key. The sifted key is the string of bits that originate from photons in which Alice and Bob have used the same basis to prepare and measure qubits. If Alice and Bob were using a perfect noiseless quantum channel, the bits in their respective sifted keys would be perfectly correlated. However, noise in the channel or eavesdropping can cause errors that translate into differences between Alice's and Bob's sifted keys. In order to obtain a secret key, Alice and Bob must first share perfectly correlated keys, which is achieved by the process of *error correction*.

To perform error correction, Alice and Bob use an authenticated classical channel, which is additional to the quantum channel. Alice sends information about her sifted key through the classical channel to Bob. In turn, Bob performs operations to his own sifted key according to the information received to match Alice's sifted key. Note that alternatively Alice could match her sifted key to Bob's, in which case Bob sends the error correction information to Alice.

A.1 Low-density parity check matrices

Throughout this thesis, error correction is performed using so called low-density parity check (LDPC) matrices [60, 58]. The benefits of LDPC matrices over alternative methods of error correction are: first, LDPC matrices require only one-way communication, which means that only one of the parties must transmit classical information to the other party in order to perform error correction. Second, LDPC matrices perform close to the Shannon limit for error rates of a few percent. Error rates that are typical in QKD implementations are on the order of one percent. This contrasts with classical communication systems in which

error rates are on the order of 10^{-6}. Performing close to the Shannon limit means that the amount of information that Alice has to send to Bob to perform error correction is close to the minimum amount of information necessary to correct errors in a channel as established by Shannon [23]. The amount of information needed to perform error correction is relevant because it has a direct impact on the secret key rate of the QKD system. This will be discussed in the paragraphs below.

The correlation between Alice's sifted bits and Bob's sifted bits are described using a binary symmetric channel: if the sender emits a bit 0, the receiver obtains a bit 0 with probability $1 - E$ and a bit 1 with probability E, where E is the probability of having a bit flip. A bit 1 emitted by the sender will arrive at the receiver with probability $1 - E$ as bit 1 and with probability E as 0. The channel is described mathematically by the following equations:

$$\begin{aligned} P(0|0) &= 1 - E \\ P(1|0) &= E \\ P(0|1) &= E \\ P(1|1) &= 1 - E. \end{aligned} \tag{A.1}$$

To perform error correction via LDPC matrices, Alice and Bob divide their sifted key into blocks (typically of ∼4000 bits). Alice uses a block of her sifted key, represented by a vector $\vec{\alpha}$, and an LDPC matrix $\mathbf{H}$ of dimensions $m \times n$ (in which $m < n$) to calculate a parity information vector $\vec{p}$ in the following way:

$$\vec{p} = \mathbf{H}\vec{\alpha}. \tag{A.2}$$

Alice sends the parity information to Bob through the classical channel. The matrix $\mathbf{H}$ consists of zeros and ones and it is constructed such that each row of the matrix contains a low number of non-zero elements (on average 5). The vector $\vec{\alpha}$ is an n-bit column vector, in which n indicates the size of the block employed. Each element p_i of the vector $\vec{p}$ indicates

Table A.1: Probability of each bit of Bob's sifted key to be 0 or 1.

bit j	$P_0(j)$	$P_1(j)$
1	0.05	0.95
0	0.95	0.05
1	0.05	0.95

if the sifted bits specified by the i^{th} row in the matrix $\mathbf{H}$ contain an even ($p = 0$) or odd ($p = 1$) number of ones.

In turn, Bob receives the parity information $\vec{p}$, knows the matrix $\mathbf{H}$ in advance and tries to reproduce vector $\vec{\alpha}$ by using his own sifted key $\vec{\beta}$ and taking into account the quantum bit error rate, so that:

$$\mathbf{H}\vec{\beta'} = \vec{p}, \tag{A.3}$$

in which $\vec{\beta'}$ is the corrected key and satisfies $\vec{\beta'} = \vec{\alpha}$. The quantum bit error rate can be estimated by disclosing a subset of the sifted key or from previous runs of the implementation.

For example, assume Bob and Alice share a sifted key consisting of three bits. Assuming Bob's three sifted bits are (1,0,1) and the quantum bit error rate is 5%, table A.1 shows the resulting probabilities $P_0(j)$ and $P_1(j)$. To do this Bob calculates the probability for each bit in his sifted key to be one ($P_1(j)$) or zero ($P_0(j)$)[1], taking into account $\vec{p}$ and the quantum bit error rate, e. Bob then uses the parity information about the relevant block of qubits he received from Alice, $\vec{p}$. Continuing with the example, for simplicity, lets assume that the parity vector that Bob receives consists of a single element $p = 0$ and it is the combination of the three sifted bits. The possible combinations of bit values with parity 0 are: (1,0,1), (1,1,0), (0,1,1), (0,0,0). Bob can then calculate the probability of each of those combinations based on the table A.1 (see table A.2).

In general the parity vector contains m elements. Bob uses the parity information involving a particular sifted bit to calculate the probability that he has the correct value for

[1]Note that $P_0(j) + P_1(j) = 1$.

Table A.2: Computation of the probability of occurrence for each combination of bits.

combination of bits	Probabilities
1,0,1	0.95*0.95*0.95 = 0.857
1,1,0	0.95*0.05*0.05= 0.002
0,1,1	0.05*0.05*0.95 = 0.002
0,0,0	0.05*0.95*0.05 = 0.002

that bit. The algorithm is repeated until the probability for each element is $0+\epsilon$ or $1-\epsilon$. If a predetermined number of rounds is reached and the probability for each element is not close to 0 or 1, then failure is declared. Therefore, the quantum bit error rate of a system is actually found after the error correction process is completed.

An important question to ask is: how much parity information does Alice have to send to Bob so that he can correct his sifted key? The rate of information from Alice to Bob is given by [23]:

$$I(A:B) = h_2(A) - h_2(B|A), \tag{A.4}$$

in which $h_2(A)$ refers to the Shannon entropy, $h_2(B|A)$ refers to the conditional entropy and $I(X:Y)$ is the mutual information between Alice and Bob, all defined in chapter 2. Since the message Alice sends to Bob is composed of bits 0 and 1 with uniform probability distribution, then

$$\begin{aligned} h_2(A) &= -p(0)log_2(p(0)) - (1-p(0))log_2(1-p(0)) \\ &= -\frac{1}{2}log_2\Big(\frac{1}{2}\Big) - \Big(1-\frac{1}{2}\Big)log_2\Big(1-\frac{1}{2}\Big) = 1. \end{aligned} \tag{A.5}$$

Calculating $h_2(B|A)$, we obtain:

$$\begin{aligned} h_2(B|A) &= -\sum_A p(A) \sum_B p(B|A) log_2(p(B|A)) \\ &= -p(0)\Big(p(0|0)log_2(0|0) + p(1|0)log_2(1|0)\Big) - p(1)\Big(p(1|1)log_2(1|1) + p(0|1)log_2(0|1)\Big) \\ &= -\frac{1}{2}\Big[(1-e)log_2(1-e) + elog_2(e)\Big] - \frac{1}{2}\Big[(1-e)log_2(1-e) + elog_2(e)\Big] \\ &= -(1-e)log_2(1-e) - elog_2(e) \\ &= h_2(e). \end{aligned} \tag{A.6}$$

Therefore,

$$I(A:B) = 1 - h_2(e), \tag{A.7}$$

in which e indicates the quantum bit error rate. Note that Alice sends the m parity bits through the classical channel, and Eve learns m bits per block due to error correction. Alice and Bob will only have $n-m$ secure bits left per block, in which n is the size of the block of sifted key. The rate of information transfer (number of information bits over total number of bits transmitted) is then $R = (n-m)/n$. For an ideal error correction code the number of parity bits that Alice needs to send to Bob are given by equation A.7:

$$\begin{aligned} \frac{n-m}{n} &= 1 - h_2(e), \\ m &= nh_2(e). \end{aligned} \tag{A.8}$$

The quantum bit error rate in the example given above was $e = 5\%$ and the block size considered was $n = 4000$ bits. The number of parity bits needed for error correction is at least $m = 1146$ bits.

As the name indicates, error correction allows Alice and Bob to remove all errors that originate from transmission of the qubits or due to eavesdropping. The implementation of error correction makes QKD noise tolerant, which is one of the requirements to execute a protocol in real-world conditions.

Appendix B

Security proofs

The first proposal of QKD was published in 1984 by Bennet and Brassard (BB84) [4]. The security of QKD is based on the fact that measuring a quantum system disturbs its state. An advantage of QKD over traditional key distribution[1] is the provable security of the key that Alice and Bob share before it is used to encode private information. Despite the intuition behind the security of QKD, a rigours mathematical proof showing its security was not given until 1996 by Mayers [157]. Since then, a variety of security proofs have been published for the BB84 protocol, and to a lesser degree for other QKD protocols. Each of these security proofs make a number of assumptions about things like the type of attack performed by the eavesdropper, whether the key is finite or infinite in size, the use of imperfect or perfect devices, etc. In this appendix I will give a brief definition of the types of attacks that an eavesdropper can perform against a QKD system. I will then sketch two different security proofs that assume infinitely long keys (i.e. keys composed of an infinite amount of bits).

B.1 Types of attacks

Attacks by an eavesdropper can be divided into three categories [158, 11]:

a) *Individual attacks*: the attacker Eve interacts with each qubit through independent auxiliary systems (probes). She then performs a measurement on each probe separately after the interaction. For individual attacks, it is assumed that Eve measures her probe before classical post-processing. This type of attack does not introduce correlations between the qubits.

b) *Collective attacks*: the attacker Eve interacts with each qubit with an independent

[1] Referred to as classical key distribution in the quantum information community.

probe, just as in individual attacks, but can also keep her probes in a quantum memory until the end of classical post-processing. At the end of classical post-processing Eve optimizes for her measurement taking into account additional information acquired during error correction and privacy amplification. This kind of attack does not introduce correlations between the qubits.

c) *Coherent attacks*: This is the most general attack Eve can perform on the qubits. A coherent attack can involve many variations, including the modification of the attack according to the result of intermediate measurements. In this case, Eve's probe interacts with all qubits which creates a high-dimensional quantum state, which Eve then measures. In this type of attack it is considered that Eve introduces correlations between the qubits.

B.2 Security proofs

Before 1999, security proofs that considered individual attacks had been developed, however, there is no reason to believe an eavesdropper will limit herself to individual attacks, hence a security proof that considered collective and coherent attacks was necessary. Triggered by the work of Mayers [157], Lo and Chau developed a QKD protocol based on entanglement distillation and proved its security against collective attacks [159]. Entanglement distillation is a process in which m pairs of maximally entangled states are obtained from a larger group, n, of partially entangled states. Lo and Chau's security proof makes use of the fact that, if Alice and Bob share maximally entangled pairs of photons, these photons can not be entangled with any other system such as Eve's probe. This is known as the monogamy of entanglement. Hence, if Alice and Bob obtain a string of bits from measurements on maximally entangled states, then the eavesdropper cannot have any information about their bit string. The problem with the protocol from Lo and Chau is that it calls for a quantum computer that performs entanglement distillation to ensure security, making it currently impractical.

B.2.1 Shor & Preskill, 2000

Shor and Preskill [33] proposed two modifications to the protocol by Lo and Chau in order to remove any requirement for a quantum computer and reduce it to BB84. They first modified Lo and Chau's protocol using the equivalence between entanglement distillation and quantum error correction [159]. One can see this equivalence in the goal of quantum error correction, which is to allow the transmission of n qubits with maximum fidelity from Alice to Bob through a noisy channel. Shor and Preskill's proof has the following assumption: the eavesdropper never introduces more than t errors per block of qubits. If Alice can encode her qubits in a t-error correcting code, then the errors can be corrected during decoding. Therefore, if an upper bound on t is placed by sampling the channel, it is possible to have a secure protocol. The steps to the first modified protocol by Shor and Preskill are the following[2]:

Lo-Chau protocol: first modification

1. Alice creates $2n$ entangled pairs, for example, in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

2. Alice randomly selects n of the $2n$ entangled pairs, the n pairs will serve as check bits for Eve's interference.

3. Alice selects a random $2n$-bit string b, and performs a Hadamard transform[3] on the second qubit of each pair for which b is 1.

4. Alice sends the second qubit of each pair to Bob. Bob receives the qubits and announces it.

5. Alice announces b and which n qubits serve as check bits.

6. Bob performs Hadamard on the qubits in which b is 1.

7. Alice and Bob each measure their n check qubits in the $|0\rangle$, $|1\rangle$ basis, and publicly share the results. If more than t of these disagree, they abort the protocol.

[2]The following description follows [21] closely

[3]The action of a hadamard transformation on the qubits $|0\rangle$ and $|1\rangle$ is $H|0\rangle = |+\rangle$ and $H|0\rangle = |-\rangle$. A Hadamard is unitary, $H^\dagger H = I$.

8. Alice and Bob perform entanglement distillation on the remaining n qubits, obtaining m nearly perfect entangled states (in which $m < n$).

9. Alice and Bob measure the m entangled pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Shor and Preskill noted that, the measurement Alice performs at step 7 can be performed at any time during the protocol. This is because her measurement does not change the state that Bob has. When Alice performs a measurement on her qubit, the entangled state is collapsed to a single qubit. Additionally, Shor and Preskill noted that an eavesdropper cannot tell the difference between a particle belonging to an entangled pair and a source emitting a completely mixed state. Recall that individual states of entangled particles are described by completely mixed states. This can be seen by examining the density operator of a Bell state (e.g.$|\phi^+\rangle$):

$$\rho^{AB} = \Big(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\Big)\Big(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\Big). \tag{B.1}$$

If we then trace out the first qubit, the reduced density operator for the second qubit is given by:

$$\begin{aligned} \rho^B &= tr_A\Big(\frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}\Big) \\ &= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 1|0\rangle + |0\rangle\langle 1|\langle 0|1\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \\ &= \frac{I}{2}, \end{aligned} \tag{B.2}$$

which is identical to the density matrix of a completely mixed state:

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{I}{2}. \tag{B.3}$$

In step 1, Alice can simply prepare n qubits $|0\rangle$ and $|1\rangle$ and n entangled states instead of $2n$ entangled states. Alice sends both, qubits and entangled photons to Bob in a random order. In this case Eve can not discriminate if Alice has sent a qubit or a photon belonging to an entangled state. From a practical point of view, Alice can prepare mixed states, which are

easy to implement. The mixed states can be used to distill a key between Alice and Bob while the entangled states are used as check qubits in order to verify the presence of Eve.

Additionally, the measurements Alice performs in steps 8 and 9 are equivalent to collapsing the n maximally entangled state into random qubits encoded in a random quantum error correction code. The qubits are transmitted to Bob and, while in transmission, they can flip (e.g. $|0\rangle \rightarrow |1\rangle$), known as bit flip or the relative phase between qubits can change (e.g. $|0\rangle + |1\rangle \rightarrow |0\rangle - |1\rangle$), known as phase flip, due to noise or eavesdropping. However, remember that the assumption is that the error rate is less than t and it can be fixed with a quantum error correction code. Thus, instead of sending n maximally entangled pairs, Alice can equivalently randomly choose an X ($|\pm\rangle = (|0\rangle \pm |1\rangle)/2$) or Z ($|0\rangle, |1\rangle$) basis encoding and a key k and encode the key in a quantum error correcting code and send Bob the encoded qubits. The encoding of a message, in the context of quantum error correction, is done by adding some redundant information to the message. In this approach, even if the information in the encoded message changes due to noise or eavesdropping, there will be enough redundancy in the encoded message such that it is possible to decode it (recover the message). In this way all the information in the original message is transmitted. The second modification to the protocol is the following:

Lo-Chau protocol: second modification

1'. Alice creates n random check bits, a random m bit string and two random n bit strings x and z. She encodes the key $|k\rangle$ in the so called Calderbank-Shor-Steane code ($CSS_{x,z}$) code.
2'. Alice randomly selects n positions (out of $2n$) and puts the check qubits in these positions and the encoded qubits in the remaining positions.
3. Alice selects a random $2n$-bit string b, and performs a Hadamard transform on the qubit for which b is 1.
4. Alice sends the qubits to Bob. Bob receives the qubits and publicly announces this fact.
5'. Alice announces b and x, z (used for decoding) and which n qubits are to provide check

bits.

6. Bob performs Hadamard on the qubits in which b is 1.

7'. Bob measures the n check qubits in the $|0\rangle$, $|1\rangle$ basis, and publicly share the results with Alice. If more than t of these disagree, they abort the protocol.

8'. Bob decodes the remaining n qubits from $CSS_{x,z}$

9'. Bob measures his qubits to obtain the shared secret key k.

A property of the quantum error correcting code (CSS code) used is that the error correction for bit flips is decoupled from the phase flip error correction. But Alice and Bob only measure in the Z basis ($|0\rangle, |1\rangle$) so they do not need information about phase errors, they only need to correct bit flips. Alice can send only bit flip decoding information. However, note that decoding, fixing bit flips and then measuring the Z basis is equivalent to performing classical error correction, in which the measurement is carried out first and the correction is performed afterwards. And in fact, this is exactly the BB84 protocol, in which the Hadamard operation, H, has been replaced by a random selection basis between X and Z. Shor and Preskill used this analogy to further modify their protocol and reduce it to the well known BB84 protocol.

BB84 protocol

1. Alice creates two 4n random bit strings a and b.

2. Alice creates 4n qubits, in which a determines the bit values, and b the bases Z or X.

3. Alice sends the 4n qubits to Bob.

4. Bob receives the qubits, measures either in the Z or X basis (chosen uniformly and at random), and announces that he received the qubits.

5. Alice announces b.

6. Alice and Bob perform key sifting and discard all events in which their bases do not match. This results in a 2n bit of sifted key.

7. Alice randomly selects n (or less) bits that serve as check bits, and announces the selection.

8. Alice and Bob calculate the QBER. If the error rate is too high (more thant t errors) they abort the protocol. Otherwise they share n bits.
9. Alice and Bob perform error correction and privacy amplification, leading to m secret bits.

The modification of the Lo and Chau's protocol and its reduction to the BB84 protocol allowed Shor and Preskill to prove the security of the BB84 protocol against coherent attacks. A figure of merit of any QKD protocol is its secret key rate. Shor and Preskill showed that the secret key rate for the BB84 protocol (assuming perfect single photons) is:

$$R = 1 - h_2(\delta) - h_2(\delta), \tag{B.4}$$

in which δ refers to the quantum bit error rate, $h_2()$ is the Shannon entropy, the second term refers to the eavesdropping performed during error correction (classical eavesdropping) and the third term refers to the eavesdropping done during transmission of the qubits (quantum eavesdropping). The equations can be rewritten as:

$$R = 1 - 2h_2(\delta), \tag{B.5}$$

in which the term $2h_2(\delta)$ is just the cost of privacy amplification.

B.2.2 Gottesman, Lo, Lütkenhaus and Preskill (GLLP), 2004

The security proof presented in the previous section applies in a scenario in which the devices used to implement QKD are perfect. The next relevant security proof for the BB84 protocol was developed by Gottesman, Lütkenhaus, Lo and Preskill and it is usually referred as the GLLP security proof [28]. The proof takes into account specific imperfections in the devices used in QKD implementations. Just as in the previous case, the security proof applies to infinitely long keys. The conditions under which this proof is done are:

- *Sources*: GLLP considered sources that emit weak, phase randomized, coherent states (instead of perfect single photons), which contain multi-photon

pulses with non-negligible probability. The multi-photon events can be used by an eavesdropper to perform a photon number splitting attack to obtain information about the key.

- *Detectors*: the authors considered basis-dependent detectors efficiencies. This means that the probability that a qubit is successfully detected depends on the basis in which the qubit is encoded.

Note that in this proof the flaws considered in the source or measuring devices are limited but it is also considered that the adversary controls the apparatus within that limit, (e.g. detector noise). The proof is developed around two kinds of qubits. Expected qubits or untagged qubits and tagged qubits. Tagged qubits are those that can reveal information to Eve, therefore they are not secure for QKD. Untagged qubits are secure for QKD. In BB84, qubits emitted by single photon sources are untagged, while weak coherent sources emit a fraction of qubits that can be tagged by Eve. When the fraction of tagged qubits and imperfect detectors are considered, the secret key rate for the BB84 protocol is:

$$R = (1 - \Delta) - h_2(\delta) - (1 - \Delta)h_2\Big(\frac{\delta}{1 - \Delta}\Big) \tag{B.6}$$

in which δ is the quantum bit error rate, Δ is the fraction of tagged qubits received by Bob. This fraction is given via the multi-photon probability of the source, p_{multi}, and the total signal detection probability for Bob, p_{exp}, as

$$\Delta = \frac{p_{multi}}{p_{exp}}. \tag{B.7}$$

Equation B.6 can be rewritten as:

$$R = Q_1[1 - h_2(e_1)] - Q_\mu h_2(e_\mu), \tag{B.8}$$

in which Q refers to the rate of qubits emitted by Alice and detected by Bob, e refers to the quantum bit error rate, the subscript 1 indicates optical pulses containing single photons

and the subscript μ indicates the mean photon number per pulse. From this security proof it is possible to show that, if one considers one-way classical communication between Alice and Bob, the upper bound of the error rate e_μ for the distribution of a secret key is 11%. Further developments of security proofs showed that the bound found for collective attacks also applies for coherent attacks [11].

Appendix C

Bell state measurements

C.1 Applications of quantum communication employing Bell state measurements

In the following paragraphs I will describe in detail the applications of quantum communication that employ Bell state measurements (BSM).

C.1.1 Quantum teleportation

Teleportation can be defined as the transmission of an unknown quantum state between two distant parties without transmission of the photon in which the unknown quantum state is encoded. To perform quantum teleportation, a pair of photons in one of the maximally entangled state are used, in this example I label these photons as B and C and I will use the state $|\psi^-\rangle$. The arbitrary quantum state $(\alpha\,|0\rangle_A + \beta\,|1\rangle_A$, where $|\alpha|^2 + |\beta|^2 = 1)$ to be teleported is encoded in a third photon, labeled photon A. Photon A and one of the entangled photons, for example photon B, are transmitted to a station where a BSM is performed, see figure C.1. The state of the three-qubit system is given by:

$$|\psi\rangle_{ABC} = (\alpha\,|0\rangle_A + \beta\,|1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|01\rangle_{BC} - |10\rangle_{BC}). \tag{C.1}$$

This can be rewritten by expressing photons A and B in the Bell basis:

$$\begin{aligned}|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\Bigg(&\left|\phi^+\right\rangle_{AB} \otimes (\alpha\,|1\rangle_C - \beta\,|0\rangle_C) + \left|\phi^-\right\rangle_{AB} \otimes (\alpha\,|1\rangle_C + \beta\,|0\rangle_C) \\ &- \left|\psi^+\right\rangle_{AB} \otimes (\alpha\,|0\rangle_C - \beta\,|1\rangle_C) - \left|\psi^-\right\rangle_{AB} \otimes (\alpha\,|0\rangle_C + \beta\,|1\rangle_C)\Bigg).\end{aligned} \tag{C.2}$$

We can see from equation C.2 that when a BSM is carried out, the initial quantum state from photon A is transmitted to photon C up to a bit flip, a π phase flip or a combination

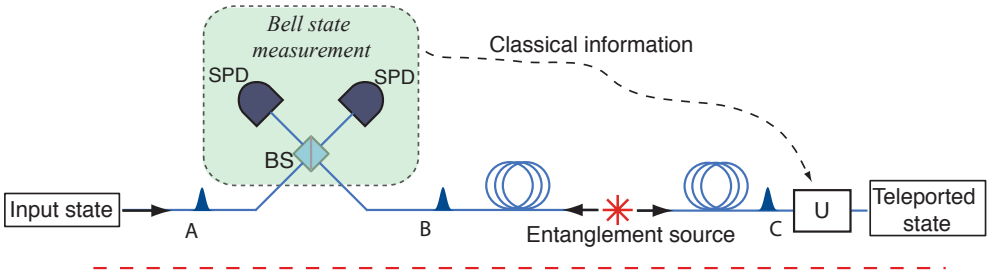

Figure C.1: Quantum teleportation. A photon A in a unknown quantum state is transmitted to a BSM setup, which consists of a beam splitter and a pair of single photon detectors (SPD). A source of entanglement produces a pair of photons labeled B and C. Photon B is sent towards the BSM, while photon C is sent towards a distant location to which the state of photon A is teleported.

of these two. In order to recover the original state from photon A, a unitary transformation of the state of photon C is necessary. These transformations are a phase flip (Z) or a bit flip (X), given by the Pauli matrices:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{C.3}$$

and,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{C.4}$$

respectively.

We can see from equation C.2 that the resulting state in photon C depends on the projection resulting from the BSM. The result of the BSM is transmitted to the photon C via a classical communication channel. This information determines which unitary transformation is needed to apply to photon C to recover the original quantum state from photon A. Note that the requirement to transmit classical information to recover the original quantum state prevents teleportation from transmitting information faster than the speed of light. It is also important to note that quantum teleportation does not violate the no-cloning theorem [160] as the target quantum state ($\alpha|0\rangle + \beta|1\rangle$) only exists in location C once the teleportation process is finished and all traces of the original state are removed from photon A.

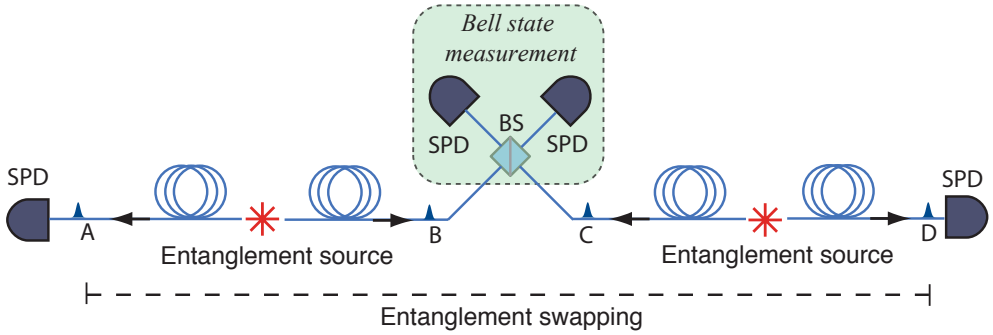

Figure C.2: Entanglement swapping. A source of entangled photons produces a pair of photons labeled A and B. A second source of entanglement produces photons C and D. Photons B and C are sent towards a central station where their joint state is projected onto a Bell state. Photons A and D are sent in opposite directions. The result of the BSM is transmitted to photons A and D. A unitary transformation can be applied to photon A or photon D. As a result, photons A and D are in the entangled state onto which photons B and C were projected. Note that without the unitary transformation photons A and D are also entangled, however, in a different state.

C.1.2 Entanglement swapping

Entanglement swapping is very similar to quantum teleportation in that it can be seen as the teleportation of entanglement. In entanglement swapping, two sources of entanglement separated by some distance produce two maximally entangled photon pairs. Photons A and B are produced by the first source, e.g. in state $|\psi^-\rangle$ while photons C and D are produced by the second source, e.g. in state $|\psi^-\rangle$. The state of the system is described by:

$$|\psi\rangle_{ABCD} = |\psi^-\rangle_{AB} \otimes |\psi^-\rangle_{CD} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) \otimes \frac{1}{\sqrt{2}}(|01\rangle_{CD} - |10\rangle_{CD}). \tag{C.5}$$

Photons B and C are transmitted to a central station where a BSM is performed while photons A and D are transmitted in opposite directions, see figure C.2.

A convenient basis change can be made to re-write equation C.5 as:

$$|\psi\rangle_{ABCD} = \frac{1}{2}\Big(|\psi^+\rangle_{AD} |\psi^+\rangle_{BC} - |\psi^-\rangle_{AD} |\psi^-\rangle_{BC} - |\phi^+\rangle_{AD} |\phi^+\rangle_{BC} + |\phi^-\rangle_{AD} |\phi^-\rangle_{BC} \Big). \tag{C.6}$$

From equation C.6 we can see that a BSM performed on photon B and C will result in an entangled state between photons A and D. Similarly to quantum teleportation the result

of the Bell state measurement is transmitted via classical communication towards photons A and D. A unitary transformation is applied to photons A and D according to the result of the Bell-state measurement. Photons A and D could be separated by a longer distance than the distance between the entanglement sources. Therefore entanglement swapping can be used to propagate entanglement through long distances [111].

C.1.3 Superdense coding

Assume that two parties, Alice and Bob, are far away from each other and they want to communicate. Superdense coding allows Alice to send two bits of information using only one qubit. This is possible if initially Alice and Bob agree on the correspondence between quantum state and pairs of bits, where the bits that can be transmitted are 00, 01, 10 and 11. If Alice and Bob begin by sharing one maximally entangled state, say $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, Alice can apply a unitary transformation of the form $U_A \otimes I_B$ to her qubit and then send her qubit to Bob. The transformation she applies to her qubit depends on the two bit values she wants to send in the following way:

$$\begin{aligned}
00 &: |\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \\
01 &: |\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}) \\
10 &: |\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}}(|10\rangle_{AB} + |01\rangle_{AB}) \\
11 &: |\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB})
\end{aligned} \tag{C.7}$$

After receiving Alice's qubit, Bob must perform a Bell state measurement in order to distinguish which of the four Bell states was sent and thus obtain the information about the classical bits transmitted [111].

C.2 Exceeding the 50% limit of a Bell state measurement

The efficiency of quantum communication applications relying on Bell state measurements is experimentally limited. The problem lies in the impossibility to unambiguously distinguish all four Bell states using only linear optics and no auxiliary photons [47], leading to inconclusive results in at least half of the measurements. The work presented in chapter 7 demonstrates the possibility to distinguish $|\psi^-\rangle$ and $|\psi^+\rangle$ for time-bin qubits and it was shown that, in order to obtain a BSM with a high success probability, it is necessary to employ highly efficient single photon detectors. In order to distinguish all four Bell states, different methods have been proposed [161, 162].

The evolution of the maximally entangled states through a 50/50 beam splitter which is described by the transformation:

$$a_{in} \rightarrow \frac{1}{\sqrt{2}}(a_{out} + b_{out}), \tag{C.8}$$

$$b_{in} \rightarrow \frac{1}{\sqrt{2}}(b_{out} - a_{out}), \tag{C.9}$$

is given by:

$$|\psi^+\rangle \rightarrow \frac{1}{2}(|0_a 1_a\rangle + |0_b 1_b\rangle), \tag{C.10}$$

$$|\psi^-\rangle \rightarrow \frac{1}{2}(|0_a 1_b\rangle - |1_a 0_b\rangle), \tag{C.11}$$

$$|\phi^+\rangle \rightarrow \frac{1}{2}(|0_a 0_a\rangle + |0_b 0_b\rangle + |1_a 1_a\rangle + |1_b 1_b\rangle), \tag{C.12}$$

$$|\phi^-\rangle \rightarrow \frac{1}{2}(|0_a 0_a\rangle + |0_b 0_b\rangle - |1_a 1_a\rangle - |1_b 1_b\rangle), \tag{C.13}$$

where the ket $|0\rangle$ and $|1\rangle$ indicate orthogonal modes used to encode the qubit states and the subscripts a and b indicate the output port of the beam splitter. From the first two expressions above, we can see that the evolution of the states $|\psi^+\rangle$ and $|\psi^-\rangle$ is characterized by orthogonal qubit modes at the output of the beam splitter through the same port for state $|\psi^+\rangle$ or in different ports for state $|\psi^-\rangle$. In the case of states $|\phi^+\rangle$ and $|\phi^-\rangle$ the output results in having the same mode for both qubits, leaving the beam splitter through the same output port. This makes the latter two states indistinguishable.

A proposal by Grice [161] uses interference in order to distinguish aditionally between the states $|\phi^+\rangle$ and $|\phi^-\rangle$. In this case, the BSM employs auxiliary photons that are in the maximally entangled state $|\phi^+\rangle$. The auxiliary photons are interfered with the state to be discriminated in a setup that employs four beam splitters, see figure C.3. In this scheme, the modes at the input of the four beam splitter setup undergo the following transformations:

$$\begin{aligned} a'_{in} &\rightarrow \frac{1}{2}(a_{out} + ib_{out} + ic_{out} - d_{out}), \\ b'_{in} &\rightarrow \frac{1}{2}(ia_{out} + b_{out} - c_{out} + id_{out}), \\ c'_{in} &\rightarrow \frac{1}{2}(ia_{out} - b_{out} + c_{out} + id_{out}), \\ d'_{in} &\rightarrow \frac{1}{2}(-a_{out} + ib_{out} + ic_{out} + d_{out}) \end{aligned} \tag{C.14}$$

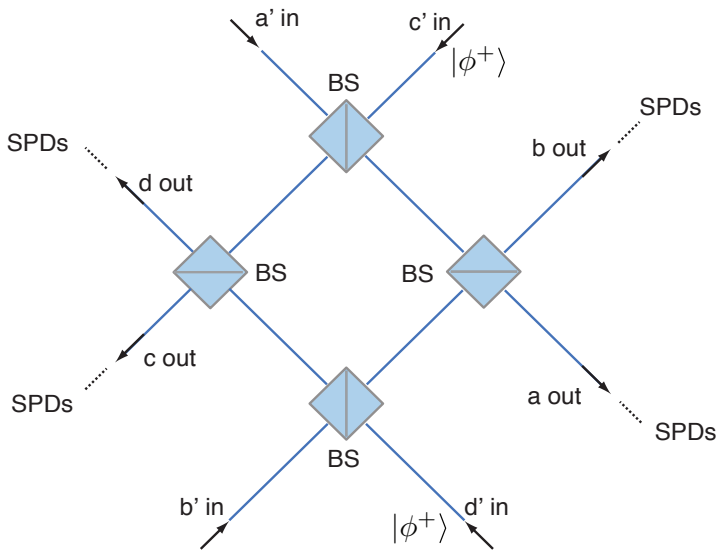

Figure C.3: Bell state measurement with auxiliary entangled photons. The figure shows the experimental setup for a BSM measurement that employs auxiliary entangled photons. The BSM is performed on the qubits in the ports labeled a'_{in} and b'_{in} while the auxiliary photons are input through the ports labeled as c'_{in} and d'_{in}.

where the subscripts $a'_{in}, b'_{in}, c'_{in}$ and d'_{in} label of the four input ports, and a, b, c and d label of the four output ports in the proposed setup, see figure C.3. The choice of the auxiliary state, $|\phi^+\rangle$, is to break the degeneracy observed in the single beam splitter setup for the states $|\phi^+\rangle$ and $|\phi^-\rangle$ with a state in a similar form. To illustrate the way this scheme works

I will present two examples using time-bin qubits, in which $|0\rangle$ represents the early temporal mode and $|1\rangle$ represents the late temporal mode. In the first example the input state is $|\phi^+\rangle_{a'b'}$ and the auxiliary state is $|\phi^+\rangle_{c'd'}$. The evolution of these two input states through the four beam splitter setup is:

$$\begin{aligned}
\left|\phi^+\right\rangle_{a'b'} \otimes \left|\phi^+\right\rangle_{c'd'} \;\rightarrow\; & \left|0_a^4\right\rangle + \left|0_b^4\right\rangle + \left|1_a^4\right\rangle + \left|1_b^4\right\rangle + \left|0_c^4\right\rangle + \left|0_d^4\right\rangle + \left|1_c^4\right\rangle + \left|1_d^4\right\rangle \\
& + \left|0_a^2 0_b^2\right\rangle - \left|0_a^2 0_c^2\right\rangle - \left|0_a^2 0_d^2\right\rangle - \left|0_b^2 0_c^2\right\rangle - \left|0_b^2 0_d^2\right\rangle \\
& + \left|1_c^2 1_d^2\right\rangle + \left|1_b^2 1_d^2\right\rangle + \left|1_a^2 1_b^2\right\rangle - \left|1_a^2 1_c^2\right\rangle - \left|1_a^2 1_d^2\right\rangle \\
& - \left|1_b^2 1_c^2\right\rangle + \left|0_c^2 0_d^2\right\rangle - \left|0_a^2 1_c^2\right\rangle - \left|0_a^2 1_d^2\right\rangle + \left|0_b^2 1_a^2\right\rangle \\
& + \left|0_a^2 1_b^2\right\rangle - \left|0_b^2 1_c^2\right\rangle + \left|0_b^2 1_d^2\right\rangle - \left|0_c^2 1_b^2\right\rangle - \left|1_a^2 0_c^2\right\rangle \\
& + \left|0_c^2 1_d^2\right\rangle - \left|1_a^2 0_d^2\right\rangle - \left|1_b^2 0_d^2\right\rangle + \left|0_d^2 1_c^2\right\rangle + \left|0_d^2 1_d^2\right\rangle \\
& + \left|0_a^2 1_a^2\right\rangle + \left|0_b^2 1_b^2\right\rangle, \qquad \text{(C.15)}
\end{aligned}$$

where the numerical superscript indicates the number of photons exiting through the port of the beam splitter in a given temporal mode. The expression C.15 shows two types of outcomes: either all the photons are in the same temporal mode (which is the case for the first 20 terms) or half of the photons are in the early temporal mode and the other half are in the late mode (rest of the terms).

In the second example the input state is $|\phi^-\rangle_{a'b'}$ and the auxiliary state is $|\phi^+\rangle_{c'd'}$. The

evolution of the two input states through the proposed setup is:

$$\begin{aligned}
\left|\phi^-\right\rangle_{a'b'}\left|\phi^+\right\rangle_{c'd'} \rightarrow\ & \left|0_a^4\right\rangle+\left|0_b^4\right\rangle+\left|0_c^4\right\rangle+\left|0_d^4\right\rangle-\left|1_a^4\right\rangle-\left|1_b^4\right\rangle-\left|1_c^4\right\rangle-\left|1_d^4\right\rangle \\
& -\left|1_a^2 1_c^2\right\rangle-\left|1_b^2 1_d^2\right\rangle+\left|0_a^2 0_b^2\right\rangle+\left|0_a^2 0_c^2\right\rangle-\left|0_a^2 0_d^2\right\rangle \\
& -\left|0_b^2 0_c^2\right\rangle+\left|0_c^2 0_d^2\right\rangle-\left|1_b^2 1_a^2\right\rangle+\left|1_a^2 1_d^2\right\rangle-2\left|1_c^2 1_d^2\right\rangle \\
& +\left|0_b^2 0_d^2\right\rangle+\left|1_b^2 1_c^2\right\rangle+|0_a 0_b 0_c 0_d\rangle-|1_a 1_b 1_c 1_d\rangle \\
& -\left|1_a 1_c 0_a^2\right\rangle-\left|1_b 1_d 0_a^2\right\rangle+\left|1_a 1_c 0_b^2\right\rangle-\left|1_b 1_d 0_b^2\right\rangle \\
& +\left|1_1 1_c 0_c^2\right\rangle+\left|1_b 1_d 0_c^2\right\rangle+\left|1_b 1_d 0_d^2\right\rangle+\left|0_a 0_c 1_a^2\right\rangle \\
& +\left|0_b 0_d 1_a^2\right\rangle+\left|0_a 0_c 1_b^2\right\rangle+\left|0_b 0_d 1_b^2\right\rangle-\left|0_a 0_c 1_c^2\right\rangle \\
& -\left|0_b 0_d 1_c^2\right\rangle-\left|0_a 0_c 1_d^2\right\rangle-\left|0_b 0_d 1_d^2\right\rangle
\end{aligned} \tag{C.16}$$

In both examples (equations C.15 and C.16), if all the photons exit in the same temporal mode the states $|\phi^+\rangle$ and $|\phi^-\rangle$ are indistinguishable. However, if the photons exist in both qubit modes, the two states ($|\phi^+\rangle_{a'b'}$ and $|\phi^-\rangle_{a'b'}$) are distinguishable by the total amount of photons in the outputs a and b, which is even for $|\phi^+\rangle_{a'b'}\otimes|\phi^+\rangle_{c'd'}$ (equation C.15) and odd for $|\phi^-\rangle_{a'b'}\otimes|\phi^+\rangle_{c'd'}$ (equation C.16). Therefore, the use of auxiliary entangled photons enables the recognition of states $|\phi^+\rangle$ and $|\phi^-\rangle$ 50% of the time. Simultaneously, the states $|\psi^+\rangle$ and $|\psi^-\rangle$ remain indistinguishable in this scheme. With this method the success rate of the BSM is thus increased from 50% to 75%. In this paper it was shown that, as the number of auxiliary entangled states is increased, the probability of discriminating all four Bell states can be made arbitrarily close to one. However, practically, this method also requires the generation of entangled photons (which is not an efficient process) and a larger number of photon number resolving detectors making it impractical given current technology.

Appendix D

Supplementary Information: Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks

A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel

Institute for Quantum Science & Technology and Department of Physics & Astronomy, University of Calgary, Canada

D.1 Ensuring Indistinguishability

In order to ensure the indistinguishability of photons arriving at Charlie's and to allow Bell state measurements in a real-world environment, we developed and implemented three stabilization systems (see Fig. 6.10 in the main text): fully-automatic polarization stabilization, manual adjustment of photon arrival time, and manual adjustment of laser frequency. Note that automating the frequency and timing stabilization systems is straightforward, particularly if the active control elements are placed in Charlie's setup.

The polarization stabilization system [73, 163] employed an additional laser (at Charlie's) and two polarization controllers (one at Alice's and one at Bob's). Every 10 s, Charlie disabled data collection for 0.5 s and sent high intensity, vertically polarized stabilization light to Alice and Bob. This light was detected by photodiodes at Alice's and Bob's, and used to trigger their commercially available polarization controllers (POCs), which were programmed to adjust the polarization of the stabilization light to vertical. This implies that Alice's and Bob's attenuated laser pulses, which were emitted horizontally polarized, both arrive horizontally polarized at Charlie's.

To stabilize the frequency difference between Alice's and Bob's lasers, Alice used a frequency shifter (FS) that employed a linear phase chirp via a serrodyne modulation signal applied to a phase modulator. Whenever the error rate in the *x-key* increased significantly, Charlie communicated the frequency difference after measuring the beat frequency by mixing their unmodulated and unattenuated laser outputs on the beam splitter. Adjustments, in the worst case, were required every 30 minutes to maintain the difference below 10 MHz.

To enable temporal synchronization, Charlie sent a master clock signal via a second set of fibers to Alice and Bob. Roughly every minute, Charlie measured the qubit arrival-time difference using his SPDs and high-resolution electronics and sent this information to Alice and Bob. They then adjusted their qubit generation times using function generators to apply a phase shift to the recovered master clock. This maintained the arrival-time difference under 30 ps.

D.2 Decoy-State Analysis

In MDI-QKD the secret key rate is given by

$$S \geq Q_{11}^{z}\big(1 - h_2(e_{11}^{x})\big) - Q_{\mu\sigma}^{z} f h_2(e_{\mu\sigma}^{z}), \tag{D.1}$$

where $h_2(X)$ denotes the binary entropy function evaluated on X, and f describes the efficiency of error correction with respect to Shannon's noisy coding theorem. Furthermore, Q_{11}^{z}, e_{11}^{x}, $Q_{\mu\sigma}^{z}$, and $e_{\mu\sigma}^{z}$ are gains (Q – the probability of a projection onto $|\psi^{-}\rangle$ per emitted pair of pulses) and error rates (e – the ratio of erroneous to total projections onto $|\psi^{-}\rangle$) in either the x- or z-basis for Alice and Bob sending single photons (denoted by subscript "11"), or for pulses emitted by Alice and Bob with mean photon number μ and σ (denoted by subscript "$\mu\sigma$"), respectively. While $Q_{\mu\sigma}^{z}$, and $e_{\mu\sigma}^{z}$ are directly accessible from experimental data, Q_{11}^{z}, e_{11}^{x} have to be bounded using a decoy state method

We use a three-intensity decoy state method for the MDI-QKD protocol [100] that derives a lower bound for Q_{11}^{x} and Q_{11}^{z} and an upper bound for e_{11}^{x}, to calculate a lower bound for the

secure secret key rate. We denote the signal, decoy, and vacuum intensities by μ_s, μ_d, and μ_v, respectively, for Alice, and Bob (note that $\mu_v = 0$ by definition). In our implementation Alice and Bob both select the same mean photon numbers for the three intensities and use channels of equal transmission. For compactness of notation, we omit the μ when describing the gains and error rates (e.g. we write Q^z_{ss} to denote the gain in the z-basis when Alice and Bob both send photons using the signal intensity). Under these assumptions, the lower bound on Q^x_{11} is given by

$$Q^x_{11} \geq \frac{P_1(\mu_s)P_2(\mu_s)\big(Q^x_{dd} - Q^x_0(\mu_d)\big) - P_1(\mu_d)P_2(\mu_d)\big(Q^x_{ss} - Q^x_0(\mu_s)\big)}{P_1(\mu_s)P_1(\mu_d)\big(P_1(\mu_d)P_2(\mu_s) - P_1(\mu_s)P_2(\mu_d)\big)}, \tag{D.2}$$

where the various $P_i(\mu)$ denote the probabilities that a pulse with Poissonian photon number distribution and mean μ contains exactly i photons, and $Q^z_0(\mu_d)$ and $Q^z_0(\mu_s)$ are given by

$$Q^x_0(\mu_d) = P_0(\mu_d)Q^x_{vd} + P_0(\mu_d)Q^x_{dv} - P_0(\mu_d)^2 Q^x_{vv}, \tag{D.3}$$

$$Q^x_0(\mu_s) = P_0(\mu_s)Q^x_{vs} + P_0(\mu_s)Q^x_{sv} - P_0(\mu_s)^2 Q^x_{vv}. \tag{D.4}$$

Similar equations are used to bound Q^z_{11} (we replace the superscript x by z). Finally, the error rate e^x_{11} can then be computed as

$$e^x_{11} \leq \frac{e^x_{dd}Q^x_{dd} - P_0(\mu_d)e^x_{vd}Q^x_{vd} - P_0(\mu_d)e^x_{dv}Q^x_{dv} + P_0(\mu_d)^2 e^x_{vv}Q^x_{vv}}{P_1(\mu_d)^2 Q^x_{11}}, \tag{D.5}$$

where the upper bound holds if a lower bound is used for Q^x_{11}. Note that $Q^{x,z}_{11}$, $Q^{x,z}_0(\mu_d)$, $Q^{x,z}_0(\mu_s)$ and e^x_{11} (Eqs. D.2-D.5) are uniquely determined through measurable gains and error rates.

Our analysis in [108] determined that lowering μ_d as much as possible maximizes secret key rate. In these experiments, we select $\mu_d = 0.05$ in order to obtain statistically significant data in a reasonable amount of time (see Suplementary Table D.1)

Table D.1: List of experimentally obtained error rates, $e^{x,z}_{\mu\sigma}$, and gains, $Q^{x,z}_{\mu\sigma}$, used to calculate the secret key rate in four different configurations. For each configuration we show the mean photon numbers for the signal and decoy states, μ_s and μ_d, employed by Alice and Bob. The vacuum state corresponds to a mean photon number of $\mu_v = 0$. We remind the reader that we omit the μ when writing the gains and error rates, writing only the subscript denoting the signal (s), decoy (d), or vacuum (v) state. We also indicate the lengths of fiber connecting Alice and Charlie (ℓ_A), Bob and Charlie (ℓ_B) and the total transmission loss (l). Finally, the computed secret key rate (S) is shown in bits per detector gate. Additionally, we measured $Q^{x,z}_{vv} = (7.1 \pm 0.30) \times 10^{-10}$ and $e^{x,z}_{vv} = 0.49 \pm 0.021$, which is applied to all distances.

Fiber	Spool	Z-basis				X-basis			
ℓ_A	22.85 km	Q^z_{ss}	$1.028(3) \times 10^{-4}$	e^z_{ss}	0.0311(4)	Q^x_{ss}	$1.95(1) \times 10^{-4}$	e^x_{ss}	0.270(2)
ℓ_B	22.55 km	Q^z_{sv}	$2.98(5) \times 10^{-6}$	e^z_{sv}	0.49(1)	Q^x_{sv}	$5.68(2) \times 10^{-5}$	e^x_{sv}	0.494(2)
Total loss l	9.1 dB	Q^z_{vs}	$1.78(4) \times 10^{-6}$	e^z_{vs}	0.47(1)	Q^x_{vs}	$5.77(2) \times 10^{-5}$	e^x_{vs}	0.507(2)
μ_s	0.396(4)	Q^z_{dd}	$1.89(3) \times 10^{-6}$	e^z_{dd}	0.070(4)	Q^x_{dd}	$3.40(1) \times 10^{-6}$	e^x_{dd}	0.277(2)
μ_d	0.050(1)	Q^z_{dv}	$1.05(6) \times 10^{-7}$	e^z_{dv}	0.47(3)	Q^x_{dv}	$8.76(8) \times 10^{-7}$	e^x_{dv}	0.511(5)
S	$1.4(4) \times 10^{-6}$	Q^z_{vd}	$9.24(5) \times 10^{-8}$	e^z_{vd}	0.48(3)	Q^x_{vd}	$8.59(9) \times 10^{-7}$	e^x_{vd}	0.503(5)

Fiber	Spool	Z-basis				X-basis			
ℓ_A	30.98 km	Q^z_{ss}	$1.67(1) \times 10^{-5}$	e^z_{ss}	0.041(2)	Q^x_{ss}	$3.57(3) \times 10^{-5}$	e^x_{ss}	0.274(3)
ℓ_B	34.65 km	Q^z_{sv}	$6.7(2) \times 10^{-7}$	e^z_{sv}	0.51(2)	Q^x_{sv}	$9.62(9) \times 10^{-6}$	e^x_{sv}	0.498(4)
Total loss l	13.7 dB	Q^z_{vs}	$4.4(2) \times 10^{-7}$	e^z_{vs}	0.48(2)	Q^x_{vs}	$9.32(7) \times 10^{-6}$	e^x_{vs}	0.499(4)
μ_s	0.279(6)	Q^z_{dd}	$6.0(1) \times 10^{-7}$	e^z_{dd}	0.082(5)	Q^x_{dd}	$1.192(7) \times 10^{-6}$	e^x_{dd}	0.278(2)
μ_d	0.050(1)	Q^z_{dv}	$4.7(4) \times 10^{-8}$	e^z_{dv}	0.47(4)	Q^x_{dv}	$3.08(7) \times 10^{-7}$	e^x_{dv}	0.50(1)
S	$1.7(1.3) \times 10^{-7}$	Q^z_{vd}	$4.0(4) \times 10^{-8}$	e^z_{vd}	0.41(4)	Q^x_{vd}	$3.03(7) \times 10^{-7}$	e^x_{vd}	0.50(1)

Fiber	Spool	Z-basis				X-basis			
ℓ_A	40.80 km	Q^z_{ss}	$5.57(6) \times 10^{-6}$	e^z_{ss}	0.053(2)	Q^x_{ss}	$9.87(9) \times 10^{-6}$	e^x_{ss}	0.270(4)
ℓ_B	40.77 km	Q^z_{sv}	$2.15(9) \times 10^{-7}$	e^z_{sv}	0.51(2)	Q^x_{sv}	$2.50(3) \times 10^{-6}$	e^x_{sv}	0.505(7)
Total loss l	18.2 dB	Q^z_{vs}	$1.88(8) \times 10^{-7}$	e^z_{vs}	0.49(2)	Q^x_{vs}	$2.95(4) \times 10^{-6}$	e^x_{vs}	0.501(6)
μ_s	0.251(6)	Q^z_{dd}	$2.66(6) \times 10^{-7}$	e^z_{dd}	0.129(8)	Q^x_{dd}	$4.49(4) \times 10^{-7}$	e^x_{dd}	0.286(4)
μ_d	0.050(1)	Q^z_{dv}	$2.8(2) \times 10^{-8}$	e^z_{dv}	0.52(4)	Q^x_{dv}	$1.25(4) \times 10^{-7}$	e^x_{dv}	0.51(1)
S	$1.2(8) \times 10^{-7}$	Q^z_{vd}	$2.2(2) \times 10^{-8}$	e^z_{vd}	0.45(4)	Q^x_{vd}	$1.22(3) \times 10^{-7}$	e^x_{vd}	0.51(1)

Fiber	Deployed	Z-basis				X-basis			
ℓ_A	12.4 km	Q^z_{ss}	$1.042(3) \times 10^{-4}$	e^z_{ss}	0.0323(6)	Q^x_{ss}	$2.020(8) \times 10^{-4}$	e^x_{ss}	0.265(2)
ℓ_B	6.2 km	Q^z_{sv}	$2.96(6) \times 10^{-6}$	e^z_{sv}	0.50(1)	Q^x_{sv}	$5.63(2) \times 10^{-5}$	e^x_{sv}	0.492(2)
Total loss l	9.0 dB	Q^z_{vs}	$1.87(4) \times 10^{-6}$	e^z_{vs}	0.52(1)	Q^x_{vs}	$5.10(2) \times 10^{-5}$	e^x_{vd}	0.512(2)
μ_s	0.402(2)	Q^z_{dd}	$1.82(2) \times 10^{-6}$	e^z_{dd}	0.071(3)	Q^x_{dd}	$3.35(2) \times 10^{-6}$	e^x_{dd}	0.269(3)
μ_d	0.050(1)	Q^z_{dv}	$1.15(6) \times 10^{-7}$	e^z_{dv}	0.53(3)	Q^x_{dv}	$8.5(1) \times 10^{-7}$	e^x_{dv}	0.502(6)
S	$1.5(5) \times 10^{-6}$	Q^z_{vd}	$8.4(5) \times 10^{-8}$	e^z_{vd}	0.49(4)	Q^x_{vd}	$8.5(1) \times 10^{-7}$	e^x_{vd}	0.501(6)

D.3 Secure key distribution using MDI-QKD

In this section we describe the assumptions underpinning secure key distribution in MDI-QKD as well as further technological and theoretical developments required for our current proof-of-principle demonstration to meet this goal. We note that any QKD system used to distribute secret key must be vetted against attacks arising from imperfections in its implementation[1]. Protection against such attacks requires the development of hardware that strives to be as ideal as possible, in conjunction with the development of security proofs that are able to take into account those imperfections that inevitably remain in any realistic implementation. (Such proofs would bound the information leaked to an eavesdropper, which, in turn, allows removing it by means of privacy amplification). Even for the heavily studied prepare-and-measure BB84 protocol, this is an area of ongoing research [164], and more needs to be done for the new MDI-QKD protocol. Yet, MDI-QKD constitutes a very important development in this context as it eliminates all potential attack strategies related to imperfections in the measurement apparatus, including arbitrary measurement-basis misalignment errors as well as detector attacks that have recently been shown to provide the eavesdropper full information about the key without leaving a trace [56, 57, 68, 97]. Remaining assumptions and required developments are:

1. **Quantum mechanics is correct and complete.** This assumption is generally believed to be true.

2. **Alice's and Bob's laboratories are private.** This assumption entails that no undesired signals, e.g. RF electromagnetic radiation, escape from Alice's and Bob's apparatus when working in normal conditions. Information gain through such passive observation can be avoided using appropriate shielding, which, as is standard in academic QKD implementations, we have not spent

[1] A notable exception is fully device independent QKD (DI-QKD) [91], which, however, is currently impossible to realize due to the need for a loophole free violation of a Bell inequality.

any particular effort on. Furthermore, the assumption implies that Eve cannot actively obtain information about the experimental settings, e.g. by sending a probe, such as light, into the laboratories using the fiber that connects Alice or Bob, respectively, with the outside world, and analyzing the back reflection. This is often referred to as a Trojan horse attack [10, 11]. And finally, Eve cannot actively influence Alice's or Bob's devices to modify their functioning. Protection against active attacks requires that the laboratories are isolated from signals sent by Eve, e.g. using optical isolators or attenuators. No such countermeasures were realized in our proof-of-principle demonstration. However, their implementation is straightforward, at least in what concerns attenuators and isolators [15]. We emphasize that there is no need to protect Charlie's laboratory; the MDI-QKD protocol ensures that it can even be run by the eavesdropper.

3. **Alice and Bob send phase-randomized attenuated pulses of light produced by a laser operated well above threshold.** This ensures that the generated light pulses are correctly described by the density matrix $\rho = \sum_n P_n(\mu) |n\rangle \langle n|$, where $P_n(\mu) = \frac{e^{-\mu}\mu^n}{n!}$ is the Poisson distribution with mean photon number μ, and $|n\rangle \langle n|$ denotes the density matrix of an n-photon Fock state. This condition is easily met by generating every light pulse using a laser diode triggered by a short electrical pulse. However, as we carve qubits out of a laser beam with large coherence time using an intensity modulator, it is not fulfilled in our setup (more precisely, subsequent pulses are coherent). Yet, we point out that the solution to our problem is well understood and has been implemented before [165]: it simply requires adding a phase modulator that randomizes the global phase of each qubit.

4. **The mean values of photons per pulse, as well as the encoded states**

are chosen randomly. No random choices have been implemented in our current proof-of-principle demonstration. Instead, we sent pulses with the same mean photon number and encoded the same qubit state during several minutes before changing the state or mean number. However, operating the phase and amplitude modulators that generate qubit states using adequate drivers connected to quantum random number generators is well understood [15], and meeting the requirement of random modulation is straightforward, though time consuming.

5. **Alice and Bob generate qubits in states that are sufficiently close to those that form two maximally conjugate bases.** These states were denoted in the main text as $|0\rangle$, $|1\rangle$, $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, respectively. This assumption may currently not be satisfied (see [108] for a detailed description of our experimental imperfections). For instance, considering states in different bases (for which the overlap should be 0.5), we find an average deviation of 0.074, and for different states in the same basis (for which we expect an overlap of zero), the average deviation is 0.013. According to the analyses in [100, 105] these overlaps, together with the current detector performance, are insufficient to securely distribute key. However, we point out that both proofs lead to very conservative bounds. For instance, the proof in [100] requires a state generation procedure that artificially increases error rates and applies non-tight bounds, and hence underestimates secure key rates. We believe that future investigations will rapidly improve proof techniques and yield higher secret key rates (and result in secret key in cases in which current proofs predict no secret key). Furthermore, we note that straightforward technological improvements allow reducing the maximum deviation from the ideal overlap values to around 1 part in 1000. For instance, this can be ac-

complished by reducing ringing in our pulse generation by a factor of 5, and using commercially-available, state-of-the-art intensity modulators that allow suppressing the background by an additional 10-20 dB (EOspace). In addition, using state-of-the-art detectors with 93% quantum efficiency and 1kHz noise [106] leads, according to simulation results with a theoretical model of MDI-QKD that we presented in [108], to secret key rates similar to or above the ones reported in the main document, even using the conservative approach in [100].

6. **Sufficiently weak correlations between qubit states and all degrees of freedom not used to encode the qubit.** In principle, the various states generated by Alice and Bob could have differences in other degrees of freedom (i.e. polarization, spectral, spatial, or temporal modes), which could open a security loophole [166] if not properly quantified and taken into account during privacy amplification. However, for MDI-QKD, the link between correlations with unobserved degrees of freedom and Eve's information gain is not yet clear. In particular, correlations are likely to degrade the visibility of the BSM, thus creating observable errors. The upper bound on Eve's information gain, possibly zero, can only be assessed using plausible arguments based on the actual implementation of the setup supplemented by careful measurements. For instance, in our implementation, the use of a single laser to generate all qubits states and of a single-mode fiber to transmit qubits from Alice, or Bob, to Charlie, respectively, makes it highly unlikely that correlation between states and photon spectra or spatial modes exist. Furthermore, careful programming of the function generator that generates all states through interaction with the same intensity modulator makes it very plausible that no temporal distinguishability is observable in our experiment. And finally, the polariza-

tion beam splitter at the exit of Alice's and Bob's laboratories ensures equal polarization of all time-bin qubit states.

7. **Appropriate classical post-processing of the sifted key, i.e. error correction and privacy amplification**. Note that while we have not implemented error correction, we have used a realistic estimation of the error correction efficiency [15] to determine the potential secret key rate of our system. Furthermore, we did not consider finite key size effects in our proof-of-principle demonstration (in other words, we assumed that we could run our QKD devices during an infinitely long time and produce an infinite amount of measured data), which, in the case of MDI-QKD, have so far only been investigated using an overly conservative approach [167].

8. **A short secret authentication key exists before starting QKD.** This key is used to authenticate the classical communication channel during error correction and privacy amplification. As we did not implement any of these post-processing steps, we did not need any pre-established secret key. In an actual implementation, this step can, for instance, be accomplished during a personal meeting between Alice and Bob.

We recall that some of the above topics are currently not as thoroughly studied for MDI-QKD as for prepare-and-measure QKD. However, the ability to close all side channels in measurement devices represents a significant step forward in closing the gap between theoretical security proofs and experimentally viable implementations. In particular, it has, for the first time, allowed for the development of security proofs in QKD that take arbitrary state generation and measurement errors into account, even though the efficiency of the current approaches can certainly be increased[2]. In addition, for actual key distribution, our

[2]In comparison, the only security proof for BB84 QKD dealing with arbitrary state generation errors at the source and arbitrary misalignment of the measurement bases is limited to individual attacks but does not apply to more powerful coherent attacks [164].

experimental implementation has to be improved along the lines discussed above. We leave these interesting and important topics for future investigations and emphasize that our work has focused on previously undemonstrated requirements for MDI-QKD, such as the Bell state measurement over deployed fiber, on improving the understanding of the capabilities and current limitations of our setup (including optimization and efficiency calculations of a decoy state analysis; for more information see [108]) and on experimental demonstrations of the protocol over various distances as well as over deployed, real-world optical fiber.

D.4 Discussion of error rates $e^{x,z}_{\mu\sigma}$

Let us briefly discuss the ideal case in which the quantum states encoded into attenuated laser pulses, as well as the projection measurements, are perfect. To gain some insight into how the difference in the error rates, $e^{x,z}_{\mu\sigma}$, arises[3], we consider only the most likely case that can cause the detection pattern associated with a projection onto $|\psi^-\rangle$ (this projection occurs if the two detectors indicate detections with 1.4±0.4 ns time difference). Specifically, we consider only the case in which two photons arrive at the beam splitter. Note that these photons can either come from the same person, or from different persons.

- z-basis: Assuming that Alice and Bob both prepare states in the z-basis, only photons prepared in orthogonal states can cause a projection onto $|\psi^-\rangle$. This implies that one photon has to come from Alice, and the other one from Bob (if generated by the same person, both photons would be in the same state). Hence, taking into account Bob's bit flip, Alice and Bob always establish identical bits, i.e. $e^z_{\mu\sigma}(\text{ideal}) = 0$.

[3]Note when two superscripts, each one denoting a different basis, are present on variables, (e.g. $e^{x,z}_{\mu\sigma}$, as above, or $Q^{x,z}_{\mu\sigma}$), this is a shorthand for, e.g. $e^z_{\mu\sigma}$ and $e^x_{\mu\sigma}$ – that is, the statement is valid for both the z- and x-bases. Note that variables may take different values for each basis, e.g. $e^z_{\mu\sigma} \neq e^x_{\mu\sigma}$. When this notation is used within an equation such as Eq. 6.2, then the equation may be written for either the z- or x-basis.

- x-basis: Assuming that both Alice and Bob prepare states in the x-basis, it is no longer true that only photons prepared in orthogonal states and by different persons can cause a projection onto $|\psi^-\rangle$. Indeed, if the two photons have been prepared by the same person, it is possible to observe the detection pattern associated with a projection onto $|\psi^-\rangle$. In this case, given that all detected photons have been prepared by either one or the other person, the detection does not indicate any correlation between the states prepared by Alice and Bob. In turn, this leads to uncorrelated key bits. Thus, $e^x_{\mu\sigma}$(ideal) is determined by the probability that one photon arrived from each person relative to the probability that two photons arrived from the same person. A detailed analysis for attenuated laser pulses with Poissonian photon number distribution, assuming an equal probability of photons arriving from either party, yields $e^x_{\mu\sigma}(\text{ideal}) = 1/4$.

Appendix E

Supplementary Information: Performing private database queries in a real-world environment using a quantum protocol

Philip Chan, Itzel Lucio-Martinez, Xiaofan Mo†, Christoph Simon, Wolfgang Tittel

1.- Institute for Quantum Science and Technology, and Department of Electrical & Computer Engineering, University of Calgary, Canada

2.- Institute for Quantum Science and Technology, and Department of Physics & Astronomy, University of Calgary, Canada

† *Current address: Beijing Institute of Aerospace Control Devices, Quantum Engineering Center, China Aerospace Science and Technology Corporation, Beijing 100854.*

E.1 Review of Oblivious Transfer and Private Queries

An ideal 1-out-of-N oblivious transfer protocol simultaneously guarantees that (a) that the user, Ursula, is able to retrieve a single element from the N-bit database, and (b) that the database provider, Dave, cannot gain any information about which element was retrieved. However, it has been shown that, assuming a universal quantum computer, if a protocol meets condition (b) then condition (a) implies that Ursula can access every element of the database[130]. As such, it is impossible for a protocol to implement ideal oblivious transfer without making assumptions in the security model. Alternatively, the class of protocols we refer to as private queries avoids the impossibility proof by implementing functionality similar to 1-out-of-N OT. Such protocols offer a reduced level of privacy up front, but this

reduction in privacy may allow secure protocols using assumptions that are easier to justify, or in which no assumptions are required at all. In this section, we briefly review protocols for oblivious transfer and private queries.[130]

In classical information theory, protocols for OT rely on one of two assumptions — that at least some fraction of the intermediaries used to perform the query are trustworthy[129, 142], or that the adversary has limited classical computational resources[128]. The former assumption can be difficult to assess, as one must both believe that the intermediaries will not collude with each other, and that their infrastructure is secured against attacks. The latter assumption is shared with today's public key cryptography infrastructure, and is hence well justified in the short term. However, in the long term, the security of such systems can be compromised by advances in algorithms (e.g. ref. [143]) or hardware such as a quantum computer[144].

A quantum 1-out-of-2 OT protocol has also recently been proposed using the noisy-storage model[139], where it is assumed that the dishonest party has a limited ability to store quantum information, and that the amount of information that can be faithfully stored decreases over time due to noise in the quantum memories (note that this protocol is loss- and fault-tolerant, as quantum memories are not required by the honest protocol). Since quantum memories are a basic component in a universal quantum computer, this assumption means that the proof that ideal OT is not possible[130] does not apply. Thus, perfect privacy is possible under this model, and this has indeed been shown in the protocol of ref. [141, 139]. An experimental demonstration of the protocol in [141] has also recently been performed[150], showing that it meets the implementability criterion. As with the classical OT protocols relying on assumptions about the adversaries computational capabilities, this assumption is well justified in the short term given current quantum memories. However, there is no fundamental principle limiting the adversaries ability to store quantum information, and recent advances in quantum memories[145, 146, 36, 147, 148, 149] threaten the validity of

this assumption in the long term.

The private queries approach to OT using cheat sensitivity was first proposed in ref. [131]. This protocol does not satisfy condition (b) above, since a dishonest database could gain complete information about which element Ursula retrieved. However, the protocol still offers security for Ursula as she has, in principle, the potential to detect Dave's attempt to gain information about her query, thus discouraging Dave from cheating. Note that condition (a) was also not satisfied, as a dishonest user could sacrifice her ability to verify Dave's honesty in order to obtain a small number of additional elements (although, this is not a significant loss of privacy for the database if N is large). An experimental proof-of-principle demonstration of this protocol was subsequently performed[140], however, as Dave could hide his attempts to cheat if there was significant transmission loss and/or errors in the quantum channel, the protocol is not practical under realistic conditions. Ref. [132] then proposed a probabilistic n-out-of-N OT protocol based on the SARG04 Quantum Key Distribution (QKD) protocol[29], which was then generalized[133]. This protocol allows Dave to gain information about Ursula's query, but only at the risk of introducing errors into the element Ursula retrieved, thereby allowing a dishonest database to be detected. The protocol also did not satisfy condition (a) above as Ursula gains probabilistic information about elements of the database she does not request. Interesting features of this protocol are the ability to tolerate loss in the channel, as well as the fact that it is simple to implement using existing QKD technology. However, noisy channels were left as an open question, preventing implementation of the protocol in realistic scenarios. Finally, our protocol proposed in this work represents the first cheat sensitive protocol to be both loss- and fault-tolerant, making it suitable for implementation in a realistic environment.

E.2 Quantum State Identification

In our protocol, the database provider, Dave, encodes each qubit into one of four randomly chosen quantum states, $|\psi_0\rangle$, $|\psi_1\rangle$, $|\phi_0\rangle$ or $|\phi_1\rangle$, as shown in Figure E.1. The user, Ursula, measures each qubit in either the 0-basis, spanned by $|\psi_0\rangle$ and $|\phi_0\rangle$, or the 1-basis, spanned by $|\psi_1\rangle$ and $|\phi_1\rangle$. After these measurements, Dave tells Ursula whether each qubit was encoded into one of the ψ states or one of the ϕ states. In order to demonstrate the state identification process, suppose Ursula measured in the 0-basis, and Dave declares that he sent one of the ψ states. If Ursula's measurement result was $|\phi_0\rangle$, she knows Dave could not have sent $|\psi_0\rangle$ as these two states are orthogonal. Hence Dave must have sent $|\psi_1\rangle$. This is a conclusive result, and occurs with probability $p_{\mathrm{c}} = \frac{\sin^2(\theta)}{2}$. Alternatively, if Ursula's measurement result was $|\psi_0\rangle$, she only knows that the state was more likely to have been $|\psi_0\rangle$ than $|\psi_1\rangle$. This is an inconclusive result, occurring with probability $p_{\mathrm{i}} = 1 - p_{\mathrm{c}}$. As the two potential states are associated with different classical bit values (as indicated by the subscripts), Ursula only gains probabilistic knowledge from this measurement result. This corresponds to an error rate of $e_{\mathrm{i}} = \frac{\cos^2(\theta)}{1+\cos^2(\theta)}$ in the ideal case (i.e. when no other sources of error are present).

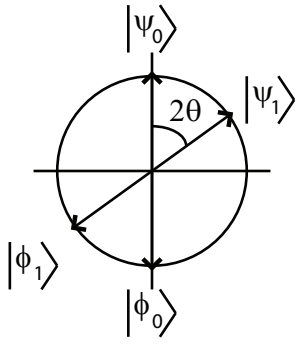

Figure E.1: Quantum states used in the private query protocol shown on a plane of the Bloch sphere.

Let us now examine how this state identification process leads to user privacy, considering first the honest protocol. In the above example where Dave sent one of the ψ states and

Ursula measures in the 0-basis, note that Ursula can only get a conclusive measurement result if Dave sent the $|\psi_1\rangle$ state. If Ursula instead measures in the 1-basis, she can only get a conclusive measurement if Dave sent the $|\psi_0\rangle$ state. Hence, for any given qubit that Dave sends, Ursula's choice of measurement determines whether a conclusive result is possible — she never gets a conclusive result if she measures in the same basis in which Dave encoded the qubit. Since she never reveals her choice of measurement basis to Dave, he cannot know which of her measurements gave conclusive results.

Now, let us consider the case in which Dave is dishonest. In this case, Dave wishes to break the correlation between Ursula's choice of measurement basis and the conclusiveness of her measurement results. Ideally, he would like to choose whether Ursula will get a conclusive or inconclusive measurement result, regardless of which measurement she makes. For ease of discussion, we assume here that Dave can send a quantum state that accomplishes this goal (we discuss a more realistic attack in Section E.5). Since Ursula is honest, she makes the same measurements as before, and interprets them assuming Dave is honest. In the above example, in which Dave declares he sent one of the ψ states, if Ursula measures in the 0-basis, she will either conclusively identify that Dave sent the $|\psi_1\rangle$ state, or inconclusively identify that Dave likely sent the $|\psi_0\rangle$ state. If she instead measured in the 1-basis, she will either conclusively identify that Dave sent the $|\psi_0\rangle$ state, or inconclusively identify that Dave likely sent the $|\psi_1\rangle$ state. Recall that the classical bit values that form the raw keys in the protocol are given by the basis of the state that Ursula believes Dave sent (and correspond to the subscripts in the ket notation). Thus, Ursula's raw key bits are anti-correlated with her choice of measurement basis for conclusive results, and correlated for inconclusive results. Hence, if Ursula's choice of measurement basis does not determine whether a measurement is conclusive, it instead determines her raw key bits. In this case, since she never reveals her choice of measurement basis, Dave cannot know her raw key bits. This leads to the cheat sensitivity in the protocol as the fact that Dave has no knowledge of Ursula's raw key

bits may be detected during error correction, and if not detected, results in incorrect query responses. A more detailed analysis of the cheat sensitivity is given in Section E.5.

E.3 Error Correction

We use a parity-based forward error-correcting code operating on k-bit blocks (corresponding to the k bits used to compute one oblivious key bit), where Dave sends the parity of several subsets of the k bits to Ursula. The construction of the code is normally described as a parity check matrix, denoted $\mathbf{H}$, and is known to both Ursula and Dave. The parity computation for the j^{th} oblivious key bit is then given by:

$$\vec{p_j} = \mathbf{H}\vec{d_j} \pmod 2 \tag{E.1}$$

where $\vec{p_j}$ is a vector of computed parity bits (which Dave sends to Ursula) and $\vec{d_j}$ is a vector containing the k bits that Dave uses to compute a single oblivious key bit. For each oblivious key bit, Ursula has a corresponding k-bit vector, $\vec{u}_j$, in which each bit stems from a conclusive or an inconclusive measurement that have, respectively, error rates of e_{c} and e_{i}. Ursula can estimate these error rates over the entire protocol by comparing the parities, $\vec{p}_j$, she receives from Dave and the parities she computes locally using $\vec{u}_j$. Using these error rates, Ursula's error correction procedure for each oblivious key bit is as follows:

1. Rule out those combinations of values for the k bits that are not consistent with the values for $\vec{p}_j$ received from Dave.

2. Divide the remaining possibilities into two sets — those that correspond to an oblivious key bit of 0, and of 1.

3. Based on the measurement results and estimated error rates, calculate the probability that each combination of values for the k bits is correct. The

set with the higher total probability determines the most likely value of the oblivious key bit.

4. Compute the probability of error in the oblivious key bit, e_{k}.

Note that Ursula can significantly reduce the computation required for error correction by performing this procedure only if almost all of the k bits were measured conclusively. In doing so, she only performs error correction if there is a possibility that the result will satisfy $e_{\mathrm{k}} \leq t_{\mathrm{U}}$.

The error correcting codes used in this work are given by:

$$\mathbf{H}_{35.6} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{E.2}$$

for $\theta = 35.6°$ and

$$\mathbf{H}_{25} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{E.3}$$

for $\theta = 25°$. They were selected using an exhaustive search of potential error-correcting codes for $k \leq 10$. The probability distribution for e_{k} is computed for each code based on the parameters in Table 2 of the main text, and the selected codes provide a low probability for $e_{\mathrm{k}} \leq t_{\mathrm{D}}$ (indicating a small amount of information leakage to Ursula) as well as a suitable probability for $e_{\mathrm{k}} \leq t_{\mathrm{U}}$ (ensuring that Ursula learns a few bits of the oblivious key on average). Note that both matrices are in reduced row echelon form (i.e. no 1's appear below

the leftmost 1 in any row). This is due to the fact that the possible k-bit vectors remaining after step 1 of the error correction process (i.e. consistent with the parity information received from Dave) are given by the possible solutions of the system of linear equations in Eq. E.1, hence any error correction codes that have the same reduced row echelon form behave identically in the error correction process. The search space was thus limited by only considering matrices in reduced row echelon form.

E.4 Requirements for security

The security of the experimental results presented in Table 3 and Figure 3 of the main text hold given that the dishonest party is limited to non-quantum attacks (e.g. an arbitrarily powerful classical computer, which would be sufficient to break computational protocols using classical information such as [128]). Furthermore, results for the security of the protocol against several quantum attacks are presented in the Section E.5. Note that these limitations on the attacks a dishonest party can perform are a result of the current security analysis of the protocol, and may not be required in general. It remains an open question as to what limitations on the dishonest party, if any, are required to achieve a sufficient level of security. Based on the attacks we have studied, we believe that at a fundamental level, the security of the protocol stems from the complementarity principle (protecting the user's security) and the superposition principle (protecting the database's security). In addition, we note that the error-correcting code in our protocol can be selected in order to provide less information to Ursula in order to compensate for an increased information gain from more powerful quantum measurements. Thus, it may be possible to adopt such measurements as the legitimate procedure for the user, provided that the measurements are feasible technologically.

We also note that the security results are valid only if certain requirements are met. These requirements are listed below, beginning with those that are required in general, followed by those that are imposed by the current security analysis:

1. Ursula's and Dave's laboratories are secure (i.e. no information leaves their laboratories except as specified in the protocol). (Required for any protocol.)

2. Quantum theory is correct and complete. (Required for any quantum protocol.)

3. The dishonest party is limited to the attacks covered in the current security analysis (see Section E.5).

4. In our experimental demonstration, it is also necessary to assume that the user is not able to take advantage of multi-photon pulses that result from using a source of weak coherent pulses. While this assumption can be avoided if Dave uses a single photon source, the implementation of weak coherent pulses is much simpler from a technological perspective. Thus, it is desirable for the protocol to be secure for weak coherent pulses without the need for additional assumptions. The decoy state techniques used in QKD [25, 26, 168] provide security against an adversary capable of exploiting multi-photon pulses. However, these techniques cannot be directly applied in cases where the two parties are adversarial, as is the case in private queries, and must be modified to account for the fact that the two parties need not be honest in the protocol [154]. However, it is not clear that the techniques in ref. [154] can be applied directly to our protocol. In particular, Ursula may gain an advantage by manipulating the aggregate statistics of the decoy state protocol by conducting an attack (e.g. by lying about detections) during a subset of the protocol while acting honestly for the remaining subset. Analyzing and adapting decoy state techniques for our protocol is thus an interesting open question. It may also be possible for Dave to base his estimate of the additional information that

may have been extracted from multi-photon pulses on a characterization of his source. Regardless of how Dave quantifies Ursula's information gain due to multi-photon pulses it can be accounted for by selecting an appropriate error-correcting code. If the information gain is sufficiently small, the protocol can provide a suitable level of database security while maintaining a high success probability for the user.

E.5 Cheating Strategies

In this section we discuss the attacks on individual qubits proposed in [132, 133]. The discussion below shows that the error correction step provides improved security for the protocol against these individual attacks. Optimization of error correction in view of coherent attacks remains an interesting open question, as does an analysis of fully general quantum attacks and an information theoretic treatment of our protocol. Furthermore, we comment on the issue of error rate estimation between adversarial parties. As example cases for these discussions, we consider the mean parameters (θ, p_{c}, e_{c}, and e_{i}) measured with $\mu = 0.95 \pm 0.47$ using standard detectors and the simulated parameters for low-noise detectors (see Table 2 in the main text). For the measured parameters, we do not consider the observed variances since they are specific to the system used to implement the honest protocol.

E.5.1 User Privacy

Let us first consider an attempt by the database to determine which piece of information Ursula is interested in. Recall that our protocol does not prevent a dishonest database from gaining some information about Ursula's query, but is cheat sensitive in that it gives Ursula the possibility of detecting such an attack. Performing the attack described below does not require any additional technology, as it simply requires Dave to send quantum states that

either maximize or minimize the probability, p_c, that Ursula will believe her measurement was conclusive [132]. In order to determine Ursula's query, Dave seeks to have Ursula learn only a single bit of the oblivious key whose position is known to him, thus he maximizes p_c for the k bits that form one oblivious key bit in an attempt to convince Ursula that she knows a particular bit of the oblivious key. He then minimizes p_c elsewhere in an attempt to prevent Ursula from knowing other bits in the oblivious key, in positions unknown to him. As noted in [133], Dave's ability to control p_c improves as the angle between the 0-basis and 1-basis, θ, is decreased, making the attack more powerful. However, in both cases (i.e. maximization or minimization of p_c), the quantum state Dave sends for this attack lies directly between either pair of ψ or ϕ states shown in Supplementary Figure E.1, and thus Ursula will associate a bit value to the measurement that is completely unknown to Dave. Hence, under this attack, Ursula receives a random bit value in response to her query, leading to the cheat sensitive property in [132, 133] (and in our protocol), in which incorrect query results will reveal Dave's dishonest behavior (i.e. over time, Dave will acquire a reputation of providing poor query results).

Furthermore, in our protocol the error correction steps provide additional opportunities for Ursula to verify Dave's honesty, both weakening the above attack as well as providing the possibility of detecting the weakened attack prior to Ursula revealing information about her query. Specifically, the consequence of Dave sending quantum states that minimize p_c (in order to prevent Ursula from knowing one or more bits of the oblivious key in random positions) is that Ursula's and Dave's sifted keys are completely uncorrelated (i.e. they have error rates $e_c = e_i = 50\%$). Additionally, since Dave has no knowledge of Ursula's sifted key, the parity bits, $\vec{p}_j$ (see Supplementary Eq. E.1), that he sends for error correction will be completely uncorrelated with the parity bits Ursula computes from her measurement results. This allows Ursula to detect a cheating database, and abort the protocol. While this severely restricts Dave's ability to ensure that Ursula does not know bits of the oblivious

key in random positions, it does not prevent him from attempting to convince Ursula that she knows a bit in a particular position of his choosing in addition to any bits she learns randomly (in this case, Dave is unsure if Ursula's query corresponds to the position where he conducted the attack, or to an unknown position that Ursula learned randomly). This is because Dave only needs to maximize p_{c} in k bits out of kN bits of the sifted key, which has a negligible effect on the overall error rates for large N. However, this attack has a limited success probability, and if it fails, it may fail in a way that is suspicious to Ursula, again allowing Ursula to abort the protocol (see below for a detailed example). Note that the above verifications occur after the error correction step, but before the shift value is communicated, thus Dave gains no information about Ursula's query if the protocol is aborted.

To illustrate the possibility for Ursula to detect an attempt by Dave to convince her that she knows a particular bit, we consider the parameters discussed above. For $k = 10$ and $\theta = 35.6°$, there is a 37.49% chance that Ursula will believe all k bits are conclusive given this attack. For $k = 9$ and $\theta = 25°$, this probability increases to 64.93%. However, for Dave to convince Ursula that she knows a particular bit of the oblivious key, it is not sufficient for her to believe that all k bits are conclusive, as the error correction procedure must also indicate that her measurement results are correct or correctable (i.e. the error correction procedure results in a error probability $e_{\mathrm{k}} \leq t_{\mathrm{U}}$, where we recall that we have selected $t_{\mathrm{U}} = 10^{-3}$ as the threshold below which Ursula considers a bit to be known). The attack thus becomes more difficult with error correction, since the database must also send parity information to Ursula that is consistent with her measurements. Since Dave's bit values are completely uncorrelated with Ursula's measured bit values, the parity information that Dave sends is essentially random, and Ursula is unlikely to find a low value for e_{k}. In the above examples, Ursula finds $e_{\mathrm{k}} \leq 10^{-3}$ with only 5.92% probability (for $k = 10$ and $\theta = 35.6°$) and 12.73% probability (for $k = 9$ and $\theta = 25°$), showing that this attack has a limited success probability. In addition, the case in which Ursula believes all k bits were

measured conclusively is of particular interest as it is very unlikely that she will find a large probability of error in the oblivious key bit after error correction, e_{k}, if the protocol was performed honestly. However, in the above attack, Dave must send parity information that is uncorrelated with Ursula's measurement results, leading to a large amount of uncertainty during Ursula's error correction process and resulting in a high probability of finding a large value for e_{k}. For example, when Ursula believes all k bits were measured conclusively, for $k = 10$ and $\theta = 35.6°$, she expects $e_{\mathrm{k}} \geq 0.15$ with 2.14% probability if Dave is honest, but this value increases to 40.63% given the above attack. For $k = 9$ and $\theta = 25°$, she expects $e_{\mathrm{k}} \geq 0.055$ with 0.71% probability when honest, and 65.63% with the attack. A large value for e_{k} if all k bits are measured conclusively can thus serve as an indication that Dave is attempting to cheat, and allows Ursula to abort the protocol. Furthermore, even if the protocol proceeds and Dave is cheating (e.g. because Dave, by chance, sent consistent parity information), Ursula's and Dave's oblivious key bits after error correction are still uncorrelated, as in the protocol of [132, 133]. This ensures that the cheat sensitive property of the protocols in [132, 133] discussed above is preserved in our protocol.

Generally speaking, we note that the additional benefits provided by the error correction procedure are relevant to other attack strategies as well. Ursula now has the ability to monitor the aggregate error rates in the system, allowing her to detect any attack by Dave that has a significant effect on the overall error rates. Furthermore, the need for the database to be able to send meaningful parity information during error correction provides an additional hurdle for attacks that cause Dave to lose information about Ursula's measurement results.

E.5.2 Database Privacy

On the other hand, a user attacking the protocol seeks to learn as many bits from the database as possible. One method of doing so is to store the photons from Dave in a quantum memory until after he reveals whether he sent a ψ or ϕ state, and then perform

an unambiguous state discrimination (USD) measurement [152, 153] to distinguish which of the two remaining states was sent. However, as Dave only reveals information about a quantum state after Ursula has declared that a photon has been detected, every photon that a dishonest Ursula declares as "detected" contributes to her sifted key. As such, any photon that Ursula declares as "detected" but subsequently fails to detect (e.g. because she could not identify when a photon was successfully stored in her quantum memory, or because of loss occurring after the declaration) results in bits in the sifted key of which Ursula has no knowledge. Successfully performing an USD attack thus requires a heralding signal indicating that a photon was successfully stored in the quantum memory, and the ability to recall the photon from the quantum memory with near 100% efficiency. For the following analysis, we assume a heralding signal in conjunction with a perfect quantum memory (i.e. one that introduces no error into the quantum states, and has 100% efficiency; a realistic quantum memory, such as those assumed in the noisy-storage model, would reduce the effectiveness of the attack), and that there are no other sources of loss that reduce the success probability of the USD measurement.

If Ursula is able to perform an USD measurement, this allows her to maximize the probability that the quantum measurements will give conclusive results. As shown in [132], the probability of conclusive results increases only slightly when performing USD measurements, resulting in the user only learning a few more bits than when making honest measurements. Furthermore, the advantage decreases as θ is decreased [133]. Additionally, in the presence of error correction, the advantage of performing an USD measurement further decreases. This is because the USD measurement gains no information from inconclusive results, essentially exchanging this information for an increased probability of obtaining a conclusive result. However, the partial information from inconclusive results is useful during error correction, and can even allow Ursula to know the value of the oblivious key bit in some instances in which not all measurements were conclusive. As such, error correction can reduce the

Table E.1: Comparison of simulation results for a user experiencing higher error rates than those used by Dave to select an error-correcting code. The columns labeled "all" show experimental results obtained using standard detectors ($\theta = 35.6°$, $k = 10$), or simulation results with improved detectors ($\theta = 25°$, $k = 9$), as taken from Tables 2 and 3 of the main text, and represent the actual results of the protocol as influenced by noise due to all imperfections. The columns labeled "source only" represent Dave's predicted results for the protocol, based on an error rate estimation considering only noise introduced by his source.

	$\theta = 35.6°$, $k = 10$		$\theta = 25°$, $k = 9$	
noise	all	source only	all	source only
p_c (%)	16.1	15.9	9.22	9.14
e_c (%)	4.4	2.5	1.91	1.38
e_i (%)	41.24	40.89	45.12	45.11
$\bar{n}$ (bits)	3.89	14.32	4.35	10.67
$\bar{m}$ (%)	6.03	6.69	0.96	0.93

effectiveness of the USD attack. Performing USD measurements when using the code with $k = 10$ and $\theta = 35.6°$ only increases the average number of bits the user knows from $\bar{n} = 3.89$ to $\bar{n} = 11.15$ — a rather small gain for a database of 10^6 bits. For the code using $k = 9$ and $\theta = 25°$, performing USD measurements actually decreases the average number of bits the user knows from $\bar{n} = 4.35$ to $\bar{n} = 1.00$. This decrease is due to the fact that at this smaller value of θ, the value of the partial information gained from inconclusive measurements outweighs the slightly improved probability for a conclusive measurement offered by the USD measurement. Note that these results are based on having the same error rate as for the honest measurements, which may not be a realistic assumption given that a different measurement apparatus is required. The issue of error rates differing from those used to select the error-correcting code is addressed separately below so as to isolate this effect from that of the USD measurement.

E.5.3 Error rate estimation

Finally, since Ursula and Dave have an adversarial nature in the private query protocol, accurately characterizing the error rate in the system in order to select an error-correcting

code is not straightforward. In particular, Ursula would like the database to believe that the error rate is higher than in reality, as Dave would then select an error-correcting code that gives her more information, allowing her to learn more bits from the database. To avoid this problem, Dave can determine the amount of information a user will learn from the protocol based solely on the error introduced by devices directly under his control. In fact, he can even choose to deliberately introduce additional noise in order to provide the desired level of database security. Additional imperfections in the system would cause the user to experience a higher error rate than Dave's estimate, leading to her learning fewer bits than the database predicts. To show that there is a regime that allows the protocol to succeed from the user's perspective while still providing good database security, we re-examine the error-correcting codes that we have considered thus far using the parameters shown in the columns labeled "source only" in Supplementary Table E.1, where noise in the system has been reduced compared to the original parameters in the main text (shown in the columns labeled "all"). Note that the effect of the lower noise observed by the database is not just a lower error rate in the conclusive measurements, e_{c}, in the "source only" columns — the other parameters are affected as well. The error rate for inconclusive measurements, e_{i}, is affected by the same noise sources as e_{c}, but the effect on e_{i} is smaller as the error for inconclusive measurements is dominated by uncertainty inherent in the quantum measurement. Hence, e_{i} in the "source only" columns is only slightly lower than in the "user" columns. The total number of conclusive results is reduced slightly as the number of conclusive results recorded due to noise events is lower. Hence, the probability of conclusive measurements, p_{c}, is lowered slightly in the "source only" columns. Supplementary Table E.1 also shows the results for the average number of bits learned by the user, $\bar{n}$, and the average proportion of the database for whic Dave considers Ursula to have significant partial information, $\bar{m}$, for the original parameters in the "user" columns, as well as for a lower error rate that can be used to select the error-correcting code in the "source only" columns. As can be seen,

the reduction in error rates does not result in a large increase in the potential amount of information gained by a user who experiences no additional error. Thus, it is possible for an error-correcting code that is selected based on local error rates to both provide the database with good security and allow the protocol to be successful for a user experiencing higher error rates.