POLARIZATION-ENTANGLED QUANTUM KEY DISTRIBUTION OVER TELECOMMUNICATION FIBRES

by

SHI YICHENG

A THESIS SUBMITTED FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

CENTRE FOR QUANTUM TECHNOLOGIES

NATIONAL UNIVERSITY OF SINGAPORE

2022

Supervisor:
Professor Christian Kurtsiefer

Examiners:
Professor Valerio Scarani, National University of Singapore
Associate Professor Macro Tomamichel, National University of Singapore
Professor Eleni Diamanti, Sorbonne Université

Declaration

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Shi Yicheng

11 February 2022

Acknowledgments

First, I would like to thank my PhD supervisor, Prof. Christian Kurtsiefer, for his guidance during the past few years. His patience and passion will also inspire us. The same gratitude also goes to Prof. Alexander Ling who supervised the NUS-Singtel corporate laboratory, in which the majority of the work in this thesis was carried out.

I would also like to thank the fiber engineering team from Singapore Telecommunications Limited for arranging the deployed fiber links for this project. This glimpse into an important real-world infrastructure has been a valuable experience for me.

The project described in this thesis is a result of teamwork. Special thanks to Dr Hou Shun Poh, Dr James Grieve, Mr Soe Moe Thar, Mr Tan Jyh Harng, and Ms Janet Lim for all the efforts we have put up together.

I would also like to thank Ms Brenda Chng, Dr Shen Lijiong, Dr Lee Jianwei and Dr Mathias Seidler who are/were members of S-Fifteen Instruments Pte. Ltd. for all the valuable discussions and logistic support. I wish them all the best for their future endeavors in the industry sector. Also to all the members of the CQT quantum optics group, thank you for the valuable time spent together and for all the knowledge and experience I have gained from the past few years.

Last but not least, I would like to thank my dear wife and my family, for their support over the years.

Contents

Abstract

Quantum Key Distribution (QKD) offers an alternative solution to the key exchange problem in symmetric cryptography, which traditionally can only be solved utilizing trusted couriers or public key schemes. Practical QKD can be implemented to secure communication between two parties provided an optical channel exists between them.

In metropolitan areas, existing telecommunication fibers can be used as QKD optical channels without imposing significant overhead cost on the current infrastructure. However, operating QKD over fibers can be challenging. Single photons, or an approximation thereof, need to be generated at telecommunication windows around 1310 nm or 1550 nm where fibers show low loss. Photons at these wavelengths are harder to detect compare to those at visible wavelengths; Transmission of quantum states, especially entangled polarization state of photons through long fibers is also non-trivial due to fiber dispersion and polarization effects. As a result, polarization entangled photon are rarely used in fiber QKD, despite being easier to implement compared to other schemes.

This thesis summarizes my studies on various technical aspects of entanglement-based QKD at telecommunication wavelengths, which involves generation and detection of polarization entangled photons at telecom O-band (1310 nm), as well as techniques for distributing entangled photons over long telecom fibers. These efforts eventually lead to an implementation of polarization-entangled QKD over a deployed fiber, demonstrating that QKD can be integrated into existing telecommunication fibers using polarization-entangled photons.

In this work, photon pairs are generated around 1310 nm using type-0 spontaneous parametric down-conversion (SPDC) and the entangled state is prepared through a linear beam displacement interferometer. The spectral bandwidth of photons are filtered down to about 20 nm to mitigate fiber polarization-mode dispersion.

At telecommunication wavelengths, detection of single photons is carried out with Indium Gallium Arsenide (InGaAs) avalanche photodetectors (APDs) which are sensitive at telecom wavelengths. As real devices, these detectors have vulnerabilities which may lead to side channels exploitable by an eavesdropper. We investigate one such vulnerability known as the breakdown flash in InGaAs APDs, whereby

the detectors emit photons upon detection events. We provide an estimation of the breakdown flash probability as well as characterized its spectral property. While the APD breakdown flash may potentially lead to attacks on a QKD system, we show that it can be prevented by applying spectral filtering [1].

Another challenge we face is the transmission of entangled photon pairs. When transmitted through long fibers, the timing correlation of photon pairs is significantly degraded due to chromatic dispersion. This makes it difficult to identify whether two photons are from the same pair, and eventually reduce the number of detection events that can be used for key generation. We show that this degradation in timing correlation can be alleviated by operating near the fiber zero-dispersion wavelength around 1310 nm, and further minimized via non-local dispersion cancellation [2].

Apart from dispersion, birefringence in the fiber also causes random rotations in photon polarization states, resulting in errors in QKD operation. We investigate the rate of polarization rotation in a deployed fiber and compensate this effect using a set of liquid crystal variable retarders as polarization controllers. The compensation scheme consists of a feedback loop which constantly seeks to minimize the quantum bit error rate with a stochastic minimization algorithm [3]. With this active compensation scheme, we demonstrate a stable QKD operation of 5.7 hours over a deployed 10 km fiber, with an average QBER of 6.4% and a final key rate of 109 bits/s [4].

List of Figures

List of Tables

Chapter 1

Introduction

Providing secure communication, that is allowing two parties to exchange secret information without any third parties knowing the content, has always been important to our society. The need for secure communication has led to the development of cryptography which studies the science of secret writing. On the other hand, cryptography is accompanied by the study of cryptanalysis which aims to break cryptographic methods and retrieve secrets.

As two co-evolving aspects of the field, constant rivalry exists between the development of secure communication protocols and techniques to break them. Although early breakthroughs in these fields arose mostly due to military/political demands, having secured communication in present days has become a necessity for everyone. Modern cryptography is based heavily on research in mathematics and computer science, which strives to design cryptographic schemes that are hard to break, but yet cost-effective enough to be adopted in practical systems.

1.1 From one-time pad to public-key encryption

One of the goals of cryptography is to come up with a practical communication scheme that is "information-theoretic secure". This cryptographic concept was first introduced by Shannon [5], which is used to describe a cryptographic system that is secure even against a third-party adversary with an unlimited amount of computational resources.

Contrary to what many people might think, there exists a simple encryption scheme that is information-theoretic secure, despite this being a very strong statement on communication security. This scheme is called the One-Time Pad (OTP)

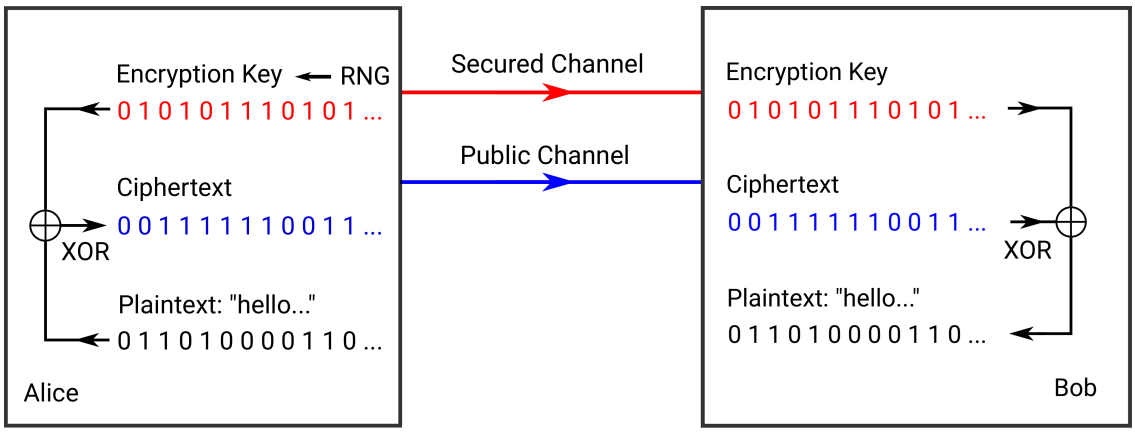

Figure 1.1: An illustration of the one-time pad protocol with keys distributed through a secure channel. In this scenario, all the information is encoded in binary. The symmetric encryption key is provided by a random number generator (RNG) to ensure that the content of the key is not predictable. Encryption/decryption is carried out by performing a bitwise XOR operation between plaintext/ciphertext and the key.

encryption and was invented in 1917 by Vernam [6]. Carrying out encryption and decryption using OTP is computationally simple: if one party named Alice wants to send a secret message to another party Bob using OTP to secure the communication, both parties just need to go through the following steps (also shown in Fig. 1.1):

1. Alice and Bob first agree on a shared encryption key in advance. In a binary context, this key is simply a string of bits that must be random and secret. The length of the key must equal the length of the message, which is also referred to as the plaintext.

2. Alice encrypts the message by performing a bitwise XOR operation between the plaintext and the encryption key. She then sends the encrypted message (also called ciphertext) to Bob via a public channel.

3. After receiving the encrypted message, Bob uncovers the plaintext by applying a bitwise XOR operation between the ciphertext and the encryption key.

This scheme was proven to be information-theoretic secure by Shannon [5] in 1949. He analyzed the OTP protocol in the context of information theory,

and stated that the message encrypted with an OTP key has perfect secrecy: an adversary intercepting the ciphertext cannot gain any information on the content of the plaintext. As a result, eavesdropping on a one-time pad secured channel is considered impossible.

However, it is difficult to employ the OTP scheme in real life. The major limitation comes from the first step of the protocol: To encrypt a single message, one needs to consume an encryption key of the same length. New encryption keys therefore need to be constantly generated and distributed. As the ciphertext is transmitted over a public channel and is visible to adversaries, the secrecy of the message now relies on the OTP keys which need to stay secret during distribution.

Practically speaking, although the OTP scheme is information-theoretic secure, it merely migrates the task of secure communication into a different, yet still crucial task which is to distribute the encryption keys securely. The latter task is commonly referred to as the secure key distribution, and carrying out this task still requires having a secure channel which is typically a trusted courier. It should also be noted here that key distribution is a vital task not only to OTP, but in general to any symmetric encryption methods in which the same key is used for both encryption and decryption [1]. In symmetric encryption, the secrecy of the cryptographic system relies on the keys.

Public key encryption

As a result of this practical challenge, people turned to a different type of encryption scheme known as public-key encryptions [7]. In a public-key encryption scheme, two keys different in contents are generated by the receiver of the message. One of the keys, $\mathrm{K_s}$, stays secret with the receiver while the other key, $\mathrm{K_p}$, is typically derived from K_s and is delivered to the sender via a public channel.

The second key $\mathrm{K_p}$, also called the public key, is used by the sender as a parameter to determine a transformation $\mathrm{E_{K_p}}$ which converts the plaintext into ciphertext:

$$\mathrm{E_{K_p}}(\text{plaintext}) = \text{ciphertext}$$

[1] As such, these schemes are also called one-key encryption schemes. Similarly, the public-key schemes are sometimes known as two-key schemes.

Upon receiving the ciphertext from the public channel, the receiver uses the secret key (or private key) K_s to set up the decryption transformation D_{K_s} of ciphertext and recovers the message:

$$D_{K_s}(\text{ciphertext}) = D_{K_s}(E_{K_p}(\text{plaintext})) = \text{plaintext}$$

For public-key schemes, the public key and ciphertext are both transmitted through the public channel and a secured channel is thus not required.

As the encryption and decryption transformations (E_{K_p} and D_{K_s}) are determined by the public and secret keys K_p and K_s, a secure public-key protocol therefore requires that the process of deriving of a public key from a secret key shall be computationally infeasible. To put is simple, a function that computes K_p from K_s:

$$K_p = f(K_s)$$

should be easy to compute (so that public-key generation can be done efficiently), but its reverse:

$$K_s = f^{-1}(K_p)$$

should be extremely difficult to compute. In this way, the secret key can stay secret and the public-key scheme is secure.

Unlike the OTP scheme, the security of a public-key encryption protocol relies on irreversibility in the public-key generation, and much effort has been put into finding and proving practical mathematical processes that are hard to reverse. The most famous example of such a process is the factorization of large integers, a problem upon which many of the important public-key encryption schemes are based on. Some of the famous public-key encryption methods that utilize this problem include RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm) and ECDSA (Elliptic Curve Digital Signature Algorithm) [8–10]. These cryptographic methods (as well as their many derivatives) are widely adopted in information security systems in modern days.

It is worth noting that the symmetric key and public key schemes are often used in combination. One example is the Diffie Hellman key exchange algorithm, which uses a public key protocol to distribute keys between the senders and receivers [7]. These keys are then used to establish secure communication via a symmetric key protocol,

thus eliminating the need for a secure communication channel for key distribution. However, the security of such an algorithm still relies on the computational complexity of a public-key scheme.

1.2 Securing key distribution using quantum mechanics

Crossovers between the fields of computational science, cryptography, and quantum physics occur after the 1970s and gave birth to two intriguing interdisciplinary fields, which are later recognized as quantum computation and quantum cryptography. Two important results emerged from these fields and caused an impact on the study of both public-key encryptions and symmetric-key encryptions.

One of the results, from the field of quantum computation, was the discovery made by Peter Shor in 1994 that one can factorize large integers on a quantum computer much more efficiently compared to classical computers [11]. While the realization of a universal quantum computer is still in progress till the present day, the mere existence of such a quantum algorithm casts a shadow on the security of the public-key encryption schemes which are based on this mathematical task. This also triggers research interest in more fundamental questions like "What other problems are hard to solve by a classical computer but easier on a quantum computer?" and "Are there problems that are hard to solve even for a quantum computer?". These questions further lead to studies in quantum algorithms and post-quantum cryptography, which remain active in present days.

Another result, which dated 10 years earlier than Shor's algorithm, is the first complete Quantum Key Distribution (QKD) protocol proposed by Bennett and Brassard [12], which was based on even earlier ideas from Wiesner [13]. This protocol is later named "BB84" after its inventors, and it provided an alternative solution to the cryptographic task of key distribution in the case of symmetric encryption.

An example of the BB84 protocol using polarization states of photons is shown in Fig. 1.2. The sender, Alice, randomly prepares photons into one of 4 polarization states: H, V, +45, -45. The photons are sent to the receiver, Bob, who measures the polarization of photons randomly in one of two bases, namely H/V and +45/-45. Once the measurements are finished, Alice and Bob communicate over a public

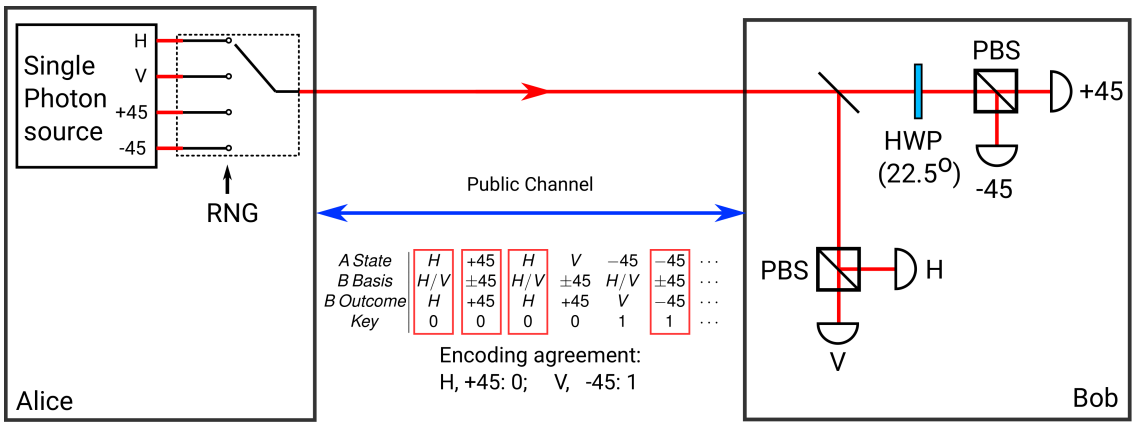

Figure 1.2: An illustration of the BB84 protocol: Alice randomly prepares a photon in one of the 4 polarization states (H, V, +45, -45) and sends it to Bob; Bob randomly measures the photon's polarization in one of two bases (H/V, +45/-45). After a series of measurements, Alice and Bob inform each other of the basis choices made for each generated/detected photon to establish a secret key. A Random Number Generator (RNG) is used to ensure randomness in state preparation.

channel and inform each other of the basis choices they made for each photon generation/measurement.

For photons that are prepared and measured under the same basis, key bits are derived from the state preparation choices and measurement outcomes on each side, respectively. Records of other photons that are processed under different basis are discarded. Through this sifting procedure, Alice and Bob each extracts a string of random bits whose length is about half of the number of detected photons. In an ideal case without the presence of an eavesdropper, the two strings are identical and can be used as encryption keys. However, in real QKD implementations, the sifted keys will contain a small fraction of erroneous bits, which are caused by detector dark counts and imperfections in the prepared polarization states. The ratio between the number of error bits and the total number of sifted keys is known as the Quantum Bit Error Rate (QBER), and is an important performance parameter of QKD systems. When the QBER is relatively low ($<\sim$11% [2]), the error bits can be eliminated through an error correction procedure between Alice and Bob.

[2]This bound on QBER is obtained from the QKD security proof given by Shor and Preskill [14], which was based on the work of Mayer [15]. In their security model, in which no assumptions is placed on the capability of an eavesdropper, secret keys can only be generated when the system QBER is less than 11%.

Unlike classical key distribution protocols which either rely on trusted couriers or the complexity of mathematical functions in public-key schemes, the security of a QKD protocol is derived from the no-cloning theorem in quantum mechanics, which states that an unknown quantum state cannot be perfectly duplicated [16]. In theory, eavesdropping on a QKD channel is impossible because one cannot intercept and resend the photons while keeping a perfect copy of all the quantum states. With the presence of an eavesdropper who performs intercept and resend on all the photons, Alice and Bob will quickly notice an increase of QBER to about 25% in the established keys and thus deduce the existence of the eavesdropping attempt.

Following the BB84 protocol, other QKD protocols were proposed such as SARG04 [17] and decoy-state protocol [18], allowing QKD systems to be implemented with weak coherent pulses instead of true single photon sources. For practical QKD applications, the key extraction procedure was formalized by introducing error correction together with privacy amplification [19]. A long list of works on the security proofs of QKD protocols can also be found [14, 20–22], in which security models were carefully constructed with assumptions made on various QKD systems parameters. Within the models of these works, several QKD protocols were rigorously proven to be information-theoretic secure.

QKD with entangled photons

The BB84 protocol and many of its practical derivatives are often categorized as "prepare&measure" protocols, due to the fact that these protocols require one party to prepare quantum states and send to the other party to measure. This was complemented by the invention of entanglement-based protocols, which was proposed in 1991 by Ekert (E91) and one year later by Bennett, Brassard, and Mermin (BBM92) [23, 24]. In particular, the BBM92 protocol is considered an entanglement-based version of the traditional BB84 protocol. The BBM92 protocol will be the basis of work in this thesis.

An example of the BBM92 protocol is illustrated in Fig. 1.3. Unlike a prepare&measure scheme, Alice and Bob both receive photons from a polarization-entangled photon pair source. In this example, a photon pair from this source is

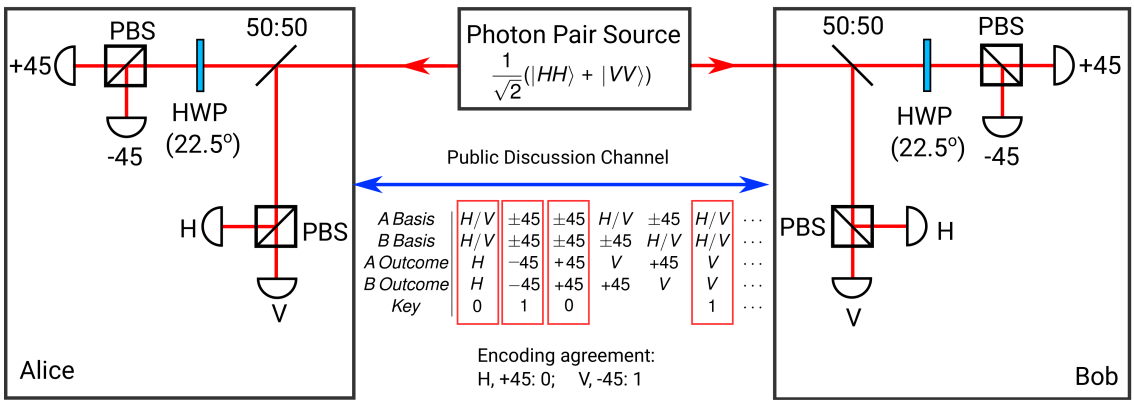

Figure 1.3: An illustration of the BBM92 protocol: An entanglephoton pair source distributes photons to Alice and Bob. The photon pairs are prepared in a polarization entangled state $\frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$, and are randomly measured in one of two bases (H/V, +45/-45) on both sides. The measurement results between Alice and Bob are correlated and can be used to establish a secret key composed of random bits.

prepared with an entangled state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$

Alice and Bob both randomly measure the polarization of each photon in one of two bases in the same way as Bob did in a BB84 protocol. In the H/V basis, the measurement outcomes between Alice and Bob will be correlated: they will find both photons to be either horizontally or vertically polarized, as indicated by the two components $|HH\rangle$ and $|VV\rangle$ of the $|\Phi^+\rangle$ state.

This correlation in polarization remains when the other set of measurement basis, namely the +/- (short for +45°/-45°) basis is used. This can be easily illustrated by expressing the state $|\Phi^+\rangle$ in the +/- basis:

$$\begin{aligned}
|H\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\
|V\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \\
&= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)
\end{aligned}$$

whereby the $|++\rangle$ and $|--\rangle$ components suggest that same polarization outcomes will emerge between Alice and Bob when both photons are measured under the +/-

basis. With a set of measurement outcomes obtained, Alice and Bob communicate over a public channel to exchange their basis choices. Measurement outcomes are sifted, leaving those bits that correspond to measurements conducted in the same basis. Key bits are then derived from the sifted measurement results on both sides.

It was argued that entanglement-based protocols are equivalent to prepare&measure protocols [24]. However, differences between the two types remain when practical issues are considered. For prepare&measure protocols, a trusted random number generator (RNG) is always required during the state preparation process. This is however not necessary for entanglement-based protocols where randomness emerges from the measurement process itself.

Practical implementations of prepare&measure protocols commonly use weak coherent pulses due to the technical difficulties in building a true single photon source. The Poissonian photon number distribution in these pulses leads to a potential photon number splitting attack [25, 26], which needs to be mitigated by using new protocols such as the decoy-state scheme [18]. Entanglement-based protocols do not rely on a true single photon source and have fewer possible side channels than typical prepare&measure protocols. This makes entanglement-based QKD less vulnerable to attacks in practical scenarios [27].

1.3 Implementations of Quantum Key Distribution

After the proposition of QKD in 1984, it didn't take long for people to realize the feasibility of QKD in practical implementations, given that technologies for generating and detecting single photons were already available. As mentioned in the previous section, strongly attenuated light pulses from lasers are commonly used in prepare&measure protocols as an approximation of true single photons [26]. Sub-Poissonian photon sources, while being technically challenging, also receive lots of research attention [28]. In entanglement-based implementations, photon pairs are typically generated by spontaneous parametric downconversion (SPDC) process in crystals with optical nonlinearity [29].

Detection of single photons was first achieved utilizing photomultipliers [30], which is later replaced by the more efficient and robust avalanche photodiodes

(APDs) [31] till present days. More recent developments in cryogenic technologies also enable single photon detection using devices such as superconducting nanowire detectors [32, 33] and superconducting transition-edge sensors [34] which offer excellent performances in efficiency.

Experimental demonstrations were first reported in the early 90s [30, 35, 36] over short optical fibers in a lab environment, with information encoded into the polarization of light. Many more experimental implementations followed in later years to cover longer distances using free-space links with telescopes, long optical fibers, and satellite-ground optical links [37–42]. Apart from the transmission channel, one can also use different degrees of freedom of light to encode quantum information. Apart from a photon's polarization state which is the earliest encoding scheme [30], other possibilities were explored such as the time of arrival of photons (time bin) [43], quadrature components of coherent light [44, 45] and more.

While QKD can in principle be achieved using any type of encoding over either free space or optical fiber links, this combination is not arbitrary in practical implementations. Although the polarization states of photons are easy to prepare and manipulate, polarization QKD is usually only implemented over free-space optical links which have a negligible amount of dispersion and polarization effect at its transmission window [46]. Optical fiber channels, on the other hand, are more frequently reported utilizing time bin encoding [47] instead of polarization, which is limited by the properties of optical fibers. These two types of implementations are usually associated with different usage scenarios in which free-space QKD (in particular, satellite QKD) provides long-distance services while fiber QKD covers small metropolitan areas utilizing existing telecom infrastructure.

Polarization encoding QKD over Telecom Fiber

Although polarization of light is easier to manipulate compared to other degrees of freedom of photon, polarization encoding is not a common choice for fiber QKD implementation [47]. Unlike the atmosphere, a long optical fiber possesses a non-negligible amount of dispersion and birefringence, which makes it difficult to transmit a photon over a long distance without altering the polarization state or increasing the discrepancy in arrival time.

When propagating through a fiber, a random rotation [3] is applied to the polarization state of photons. This rotation is partially due to the fiber's routing geometry, as well as the birefringence in the fiber core which causes different phase velocities of orthogonal polarization states. To make things worse, this rotation is time dependent and is affected by changes in temperature and mechanical stress. If not compensated, this random rotation results in alteration in the prepared polarization state and therefore causes errors.

Dispersion effects of fiber cause more problems when entanglement-based QKD protocols are implemented. In such systems, photons are generated from nonlinear processes in an optical crystal which can have a large spectral bandwidth (tens of nanometers is not unusual). These wideband photons are susceptible to both polarization mode dispersion (PMD) and chromatic dispersion (CD) during propagation in fiber. A fiber link with a large PMD value can act as a depolarizing channel for photons and cause degradation in entanglement [48, 49]. On the other hand, chromatic dispersion reduces the timing correlation between a pair of photons, which makes coincidence identification more difficult.

While these limitations make optical fibers unattractive to serve as quantum channels, especially for polarization-entangled QKD, they can be carefully mitigated using different polarization compensation and dispersion cancellation techniques [2, 3]. It is the goal of this thesis to demonstrate the feasibility of implementing a polarization entanglement-based QKD over a deployed telecom fiber, using entangled photon generated and detected at telecom O-band (1310 nm).

[3] The word "rotation" used here refers to one that happens in the Poincaré sphere, which includes elliptical and circular polarizations as well.

Thesis Outline

This thesis describes a polarization-entangled quantum key distribution system implemented over a deployed telecom fiber, as well as several aspects related to the advancement of this implementation.

Chapter 2 discusses the basic elements of such a system which is the generation and detection of polarization-entangled photon pairs at telecom wavelength. The first part of the chapter describes an entangled photon pair source based on type-0 spontaneous parametric down-conversion (SPDC) that produces photon pairs at the telecom 0-band (1310 nm). Detection of single photons at this wavelength is accomplished with Indium Gallium Arsenide (InGaAs) avalanche photodetectors. An overview of these detectors is given in the second part of this chapter.

In Chapter 3 we report an interesting effect in the APDs known as the breakdown flash, which could lead to potential side-channel attacks on the QKD systems if not dealt with. This effect, which is light emission from the recombination process in the detector itself was first observed in Silicon APDs. We confirmed that the InGaAs APDs suffer the same effect, and performed a subsequent measurement to determine the optical spectrum of the breakdown flash. We show that this flash is wideband and can be easily suppressed via spectral filtering [1].

In Chapter 4 we focus on the optical fiber which serves as the tranmission channel for our polarization entangled photons. We will discuss the chromatic dispersion effects of optical fibers, which is one of the major limitations for implementing entanglement based QKD. We show that fiber chromatic dispersion can significantly degrade the timing correlation of the photon pairs when sent over long distances, and this degradation can be compensated in principle using non-local dispersion cancellation [2].

Chapter 5 describes a full QKD setup implemented over a deployed, 10 km telecom fiber. While similar to a typical QKD system that follows the BBM92 protocol, we introduced an extra setup to perform polarization compensation to counter the fiber birefringence effect [3]. We demonstrate stable QKD operation for a period of 5.7 hours with a mean Quantum Bit Error Rate (QBER) of 6.3% and final key rate of 109 bits/s [4].

Chapter 2

Generating and Detecting Entangled Photon Pairs in the Telecom O-band

Although QKD can in principle be realized with any two-level quantum systems, utilizing photons, which are energy quanta of light, is the only practical choice as they are able to stay coherent over long distance transmissions. Unlike other particles, photons can be distributed to distant parties through free space links or optical fibers without too much loss of encoded information. There also exists various degrees of freedom in photons that be exploited to encode quantum information, such as polarization [50] and arrival time (time-bin) [43].

The choice of photon wavelength in QKD is another important consideration that is mainly dictated by the transmission spectrum of the quantum channel. For QKD over free-space links, a number of spectral bands are available ranging from 665 nm to 1680 nm, which correspond to wavelengths with low absorption in the atomsphere [46]. Over this large range, low-loss windows around 670 nm and 785 nm are two preferred choices as photons at these wavelengths can be efficiently detected using single photon detectors based on silicon [51–53]. While the transmission loss in free space depends on various parameters such as wavelengths, altitude, and atmospheric turbulence, attenuation below 0.1 dB/km can be achieved [41, 51, 53].

There are fewer wavelength choices available when transmitting photons in telecommunication fibers. Fig. 2.1 shows the attenuation spectrum of Corning's SMF-28, which is a standard single-mode fiber used in telecommunication networks [54]. There are two wavelengths in this spectrum that exhibit relatively low attenuation and are located around 1310 nm ($\sim$0.34 dB/km) and 1550 nm

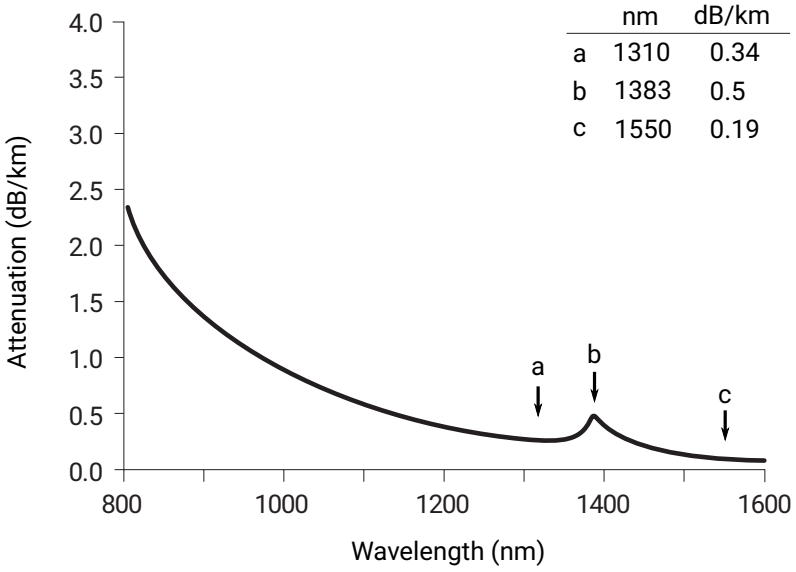

Figure 2.1: Attenuation spectrum of a typical SMF-28 fiber. There are two commonly used transmission windows located at 1310 nm (a) and 1550 nm (c), separated by a high loss peak around 1383 nm (b) caused by hydroxyl (OH^-) ion absorption. This figure is adapted from reference [54].

($\sim$0.19 dB/km). Transmission windows around these wavelengths are commonly recognized as the "O-band" (1260 nm-1360 nm) and "C-band" (1530 nm-1565 nm) in the telecommunication industry [1]. Out of the two, the C-band is the most commonly used window for long-haul communications (hundreds to thousands of kilometers) due to low transmission loss as well as the availability of good fiber amplifiers based on erbium [56].

In contrast, the telecom O-band is higher in loss, which limits the transmission distance to tens of kilometers without the aid of fiber amplifiers. However, this distance is sufficient for QKD to cover a metropolitan area such as the city of Singapore. An additional property of merit for the O-band is that the chromatic dispersion effect around 1310 nm is relatively small compared to the C-band, which eliminates the need of having chromatic dispersion-shifted fibers [57]. Due to these considerations, the work in this thesis is focused on QKD at O-band.

Fortunately, technologies for generating and detecting entangled photons around this wavelength have been long available. In this chapter, I will give an overview of our photon source at the O-band, as well as the single photon detectors for detecting

[1] "O" and "C" respectively stand for "Original" and "Conventional" [55].

these near-infrared photons. The photon source and detectors are the basic devices that enable us to implement QKD over a deployed fiber.

Following this, the chapter is naturally split into two sections. The first section describes a polarization-entangled photon pair source based on spontaneous parametric downconversion (SPDC), which generates photon pairs in the O-band (degenerate wavelength at 1316 nm) and prepares the polarization entanglement state via a linear beam displacement interferometer. The second section gives an overview of the Indium Gallium Arsenide (InGaAs) avalanche photodetectors (APDs) used for detecting single photons at O-band, as well as a summary of various characterization techniques for these detectors.

2.1 Polarization Entangled Photon Pairs at Telecom O-band

Photon pairs can be generated by many physical processes such as cascaded emissions in atomic ensembles [58] and nonlinear processes in optical crystals [59]. The most commonly used process is known as spontaneous parametric downconversion (SPDC), which is a nonlinear process in optical crystals that converts a high-energy pump photon into two daughter photons with the same total energy.

The SPDC process was first observed early in the late 1960s [29, 60]. These generated photon pairs are found to be highly correlated in time and are used to explore non-classical interference effects on a single photon level [59, 61]. Correlated photon pairs from SPDC were then utilized to efficiently prepare polarization-entangled states [62] and became widely adopted in experiments where photon entanglement is required. Even until the present day, SPDC remains the basis for most of the reported entangled-photon sources.

2.1.1 Generating Correlated Photon Pairs

In the process of spontaneous parametric downconversion, a photon with relatively high energy (pump photon) propagates through an anisotropic optical crystal and is split into two photons with lower energies (signal and idler photons). The necessary condition for SPDC to take place is that the three participating photons obey the conservation of energy and momentum. While the conservation of energy is

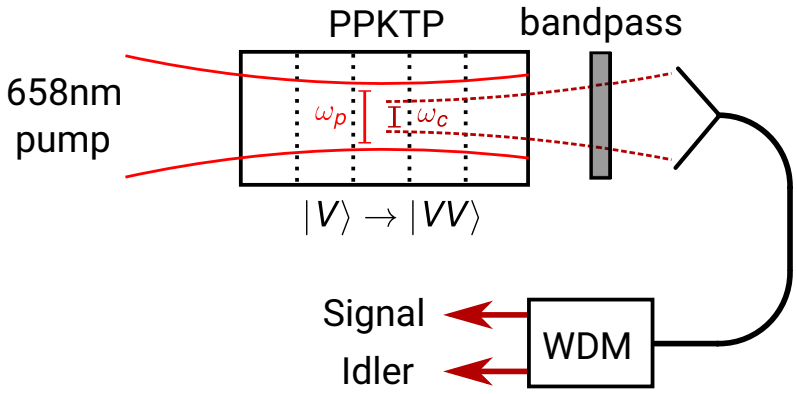

Figure 2.2: Simplified schematic of a correlated photon pair source. Pump light at 658 nm is converted to two photons degenerate at 1316 nm in a colinear configuration. The size of the beam spot (FWHM) for the pump light is $\omega_p = 112\,\mu$m, while the collection waist is $\omega_p = 57\,\mu$m. A wavelength division demultiplexer (WDM) is used to separate the signal and idler photons. With a vertically polarized pump photon, both signal and idler photons have vertical polarizations as well (type-0 phase matching).

always fixed with a given pump wavelength, the conservation of momentum, also call phase-matching, can be engineered by exploiting the anisotropic properties of the crystal. This typically refers to the different refractive indices along different directions, which can be continuously tuned by changing the temperature or rotating the crystal [63]. Another important way to enhance the efficiency of SPDC process is to periodically alternate the orientation of optical axes in a crystal, which effectively contributes additional momentum in the phase-matching condition [64]. This is typically referred to as quasi-phase-matching in a periodically poled crystal and has been commonly adopted in building SPDC sources.

Techniques for phase-matching have been extensively studied, with various types of anisotropic crystals with cutting angles commercially available to enable the implementation of such nonlinear optical processes at different wavelengths.

The correlated photon pair source in this work is realized through SPDC in a periodically poled potassium titanyl phosphate crystal (PPKTP, Raicol). The crystal is manufactured with a poling period of 16.775 μm and is designed for type-0 SPDC in which the down-converted signal and idler photons have the same polarization as the pump photon which is vertically polarized. To generate photons at the telecom O-band, the crystal is pumped with a grating stabilized laser at 658 nm

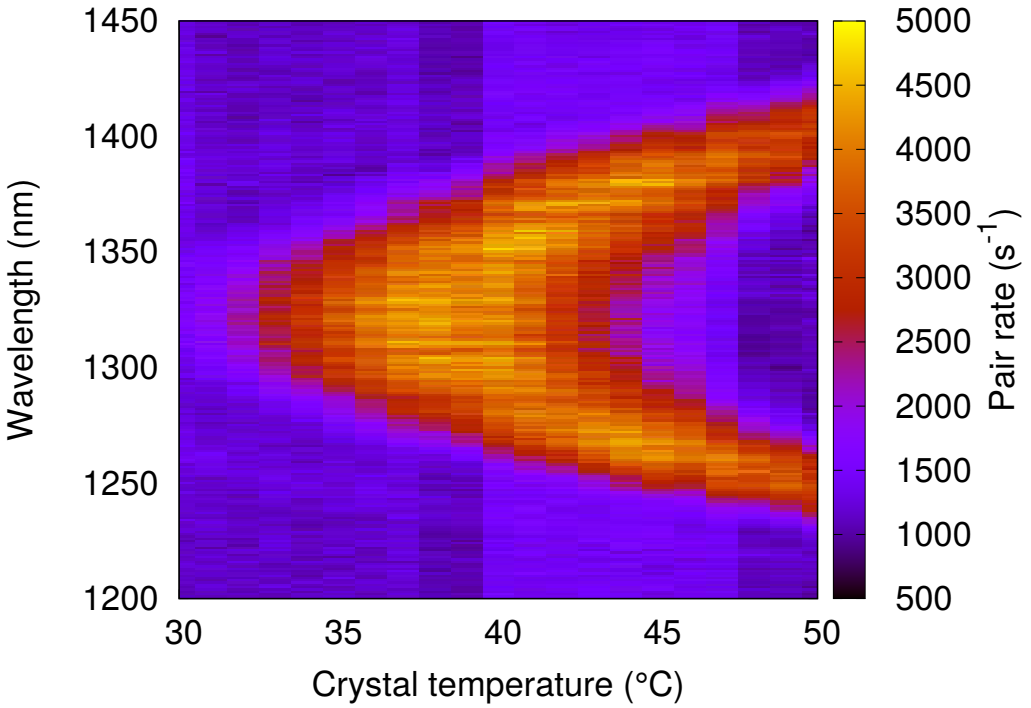

Figure 2.3: Measured SPDC spectrum as a function of crystal temperature. In this source setup, the PPKTP crystal temperature is stabilized at 40 °C where the signal and idler wavelengths are degenerate and the brightness is the highest.

(ONDAX Surelock) with a typical linewidth of 300 MHz. The resulting in degenerate wavelength of the down-converted photons is 1316 nm.

The spectral distribution of the down-converted photons is sensitive to the phase-matching condition in the PPKTP crystal, which is temperature-tuned in this case. Figure 2.3 shows a heat map representing the measured SPDC spectrum as a function of crystal temperature. With increasing crystal temperature, optimal phase-matching is achieved around 40 °C with the most number of signal and idler photons being generated and are degenerate in wavelength. The spectrum then bifurcates with a temperature above 44 °C where the down-converted photons become distinguishable by wavelength.

The correlated-photon pair source is therefore operated at a crystal temperature of 40 °C where the brightness is the highest. Following the work of Bennink [65] and Dixon [66], the pump and collection beam waist (FWHM) is set to be about 112 μm and 57 μm for optimal source efficiency. At this configuration we observed a pair rate as high as 57000 pairs/s/mW measured with two InGaAs single photon

detectors (IDQ220 from IDQuantique) at a pump power of 0.1 mW.

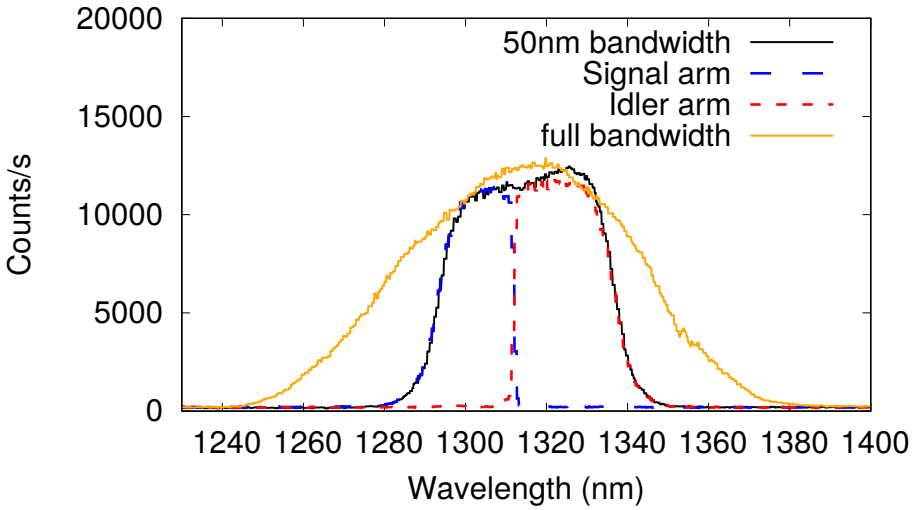

Figure 2.4: Spectrum of the Type-0 SPDC photons. The orange trace shows the full spectrum of the SPDC photons and the black trace indicates the 50 nm bandwidth defined by the bandpass filter applied. Signal (blue) and idler (red) photons are separated using a wavelength division demultiplexer edged at 1316 nm.

The spectrum of the down-converted photons is measured with a grating monochromator and is shown in Fig. 2.4. Centered at 1316 nm, the full bandwidth of the down-converted photons is approximately 70 nm (yellow trace). The signal and idler photons are separated using a wavelength division demultiplexer (WDM) with a separation wavelength of 1316 nm. As will be discussed in later chapters, such a wide bandwidth makes the photons susceptible to both chromatic dispersion and polarization mode dispersion effects, which makes QKD implementations over long fibers infeasible. As a result, spectral filtering is required to narrow down the bandwidth of the generated photons. Under this consideration, a 50 nm bandpass filter is applied to limit the photon bandwidths which results in signal and idler photons of 20 nm and 24 nm, respectively (blue and red traces in Fig. 2.4).

2.1.2 Entangling the Photons

Both photons generated by type-0 SPDC are polarized along the vertical direction. This is denoted by $|VV\rangle$ using bracket notation. In order to create an entangled polarization state between the photons, we place the PPKTP crystal inside a linear beam-displacement interferometer [68]. In this configuration, the pump laser is

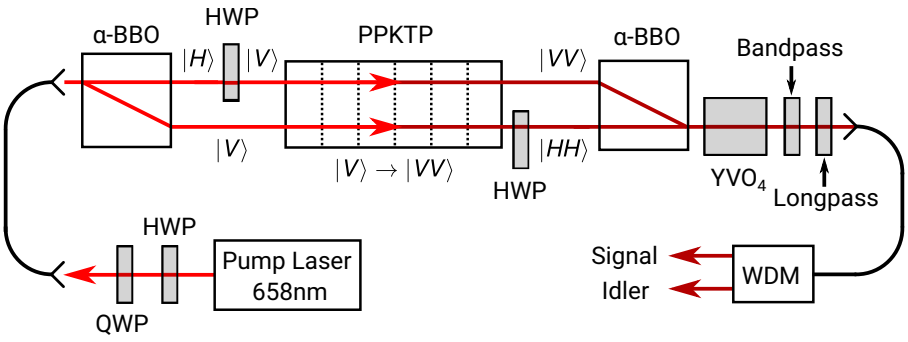

Figure 2.5: Experimental schematic of the entanglement source. The pump light is coherently distributed to two paths, each of which allows type-0 SPDC to take place inside the PPKTP crystal. For the downconverted photons, the polarization state in the lower path is rotated 90 degrees by a half-wave plate. The two paths are recombined to create an entangled state $\frac{1}{\sqrt{2}}(|HH\rangle + e^{i\Delta\phi(\lambda)}|VV\rangle)$. The wavelength dependence of the phase difference $\Delta\phi(\lambda)$ is minimized by inserting a piece of Yttrium Vanadate (YVO_4) crystal at the recombined path, resulting in a final $|\Phi^+\rangle$ output state[67].

split and recombined coherently, creating two possible paths in which SPDC can take place. Down-converted photon pairs with different two-photon states are produced within each path. The coherent recombination of these photons at the interferometer output produces a superposition of these states which eventually becomes a polarization-entangled state.

The experimental schematic of the entangled photon pair source is shown in Fig. 2.5. The 658 nm pump laser is guided to the crystal through a single mode fiber, with a half-wave plate (HWP) and a quarter-wave plate (QWP) controlling its polarization. The polarization of the pump light is set to +45 degrees before it enters a first α-Barium borate (α-BBO) crystal, which acts as a beam splitter for the linear displacement interferometer. This 9 mm α-BBO crystal has its optical axis oriented at 45° with respect to the horizontal direction and creates a spatial walk-off between the $|H\rangle$ and $|V\rangle$ component of the pump light. With pump light polarized at 45°, the transmitted path ($|H\rangle$) and the deflected path ($|V\rangle$) carry equal power and are separated by a walk-off distance of about 600 μm.

A half-wave plate at 658 nm changes the polarization of the transmitted pump light from $|H\rangle$ to $|V\rangle$. As a result, pump light in both paths is now vertically polarized and is subject to type-0 SPDC in the PPKTP crystal. The down-converted

photon pairs in both paths have a two-photon polarization state $|VV\rangle$. Similar to the pump light, another half-wave plate at 1316 nm converts the $|VV\rangle$ state of the down-converted photon pairs into $|HH\rangle$. The paths are then recombined using a second α-BBO crystal with 9.1 mm in length, preliminarily generating an entangled state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + e^{i\Delta\phi(\lambda)}|VV\rangle),$$

where $e^{i\Delta\phi(\lambda)}$ denotes a relative phase difference between the two generation paths. This phase difference is mainly due to the wavelength-dependent birefringence in the BBO crystal and can be compensated by introducing a 1.6 mm Yttrium orthovanadate crystal (YVO_4, a-cut) after the second α-BBO crystal [67].

The spectrum of the down-converted photons is further limited to 50 nm with a bandpass filter, while another long-pass filter (cut-off at 808 nm) is applied to block any leaked pump light. After a wavelength division demultiplexer which spectrally separates the signal and idler photons about the degenerate wavelength (1316 nm), the final two-photon state is the Bell state $|\Phi^+\rangle$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle).$$

2.1.3 Characterization of Polarization Entanglement

In order to verify the entangled state $|\Phi^+\rangle$ of generated photons pairs, we measured the polarization correlation between the signal and idler using a simple setup illustrated in Fig. 2.6. In this setup, both signal and idler photons propagate through a linear polarizer before being collected into two polarization-neutralized single mode fibers. The photons are eventually detected utilizing two single photon detectors which generate signals that are coincident in time. The number of coincidences between the two detectors is recorded with a counting device.

If the polarizers applied to signal and idler photons are set at angles θ_s and θ_i, respectively ($\theta_{\mathrm{s,i}} = 0$ corresponds to $|H\rangle$ polarization), the detection probability of a

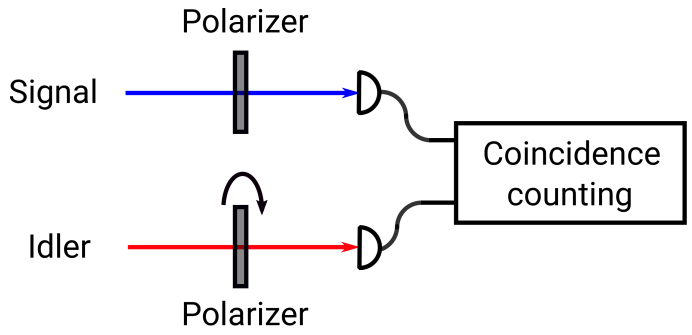

Figure 2.6: Setup for measuring the polarization correlation of the entanglement source in both H/V and D/A bases. The coincidence rate is measured with two half-wave plates (HWPs) and two polarizing beam splitters (PBSs) applied to the signal and idler photons. The HWP on the signal's side is kept at different polarization measurement settings (H, V, D, A) while the other HWP on the idler's side is scanned over 180 degrees.

photon pair follows the Malus's law:

$$\begin{aligned} P(\theta_{\mathrm{s}}, \theta_{\mathrm{i}}) &= |\langle \theta_{\mathrm{s}}, \theta_{\mathrm{i}} | \Phi^{+} \rangle|^2 \\ &= \frac{1}{2} |\langle \theta_{\mathrm{s}}, \theta_{\mathrm{i}} | HH \rangle + \langle \theta_{\mathrm{s}}, \theta_{\mathrm{i}} | VV \rangle|^2 \\ &= \frac{1}{2} |\cos(\theta_{\mathrm{s}} - \theta_{\mathrm{i}})|^2. \end{aligned} \tag{2.1}$$

For each measurement, the signal's polarizer angle is kept at one of four settings: $\theta_{\mathrm{s}} = 0°(\mathrm{H}), 90°(\mathrm{V}), +45°(\mathrm{D}), \text{and} -45°(\mathrm{A})$. At each setting, the idler's polarizer angle θ_{i} is scanned over 360 degrees. At each step, we record the number of detected coincidence events, which is proportional to the detection probability $P(\theta_{\mathrm{s}}, \theta_{\mathrm{i}})$.

Figure. 2.7 shows the measured polarization correlations in all four settings of the signal's polarizer angle. The measured coincidence rates as a function of idler's polarizer angle θ_i follow the sinusoidal functions described by Eq. 2.1. The quality of entanglement can be characterized by the visibility of the polarization correlations in different bases, which is defined as:

$$V = \frac{N_{\mathrm{max}} - N_{\mathrm{min}}}{N_{\mathrm{max}} + N_{\mathrm{min}}}, \tag{2.2}$$

where N_{max} and N_{min} represent the maximum and the minimum number of detected coincidences. The visibility calculated from 4 measurements at different polarizer settings are:

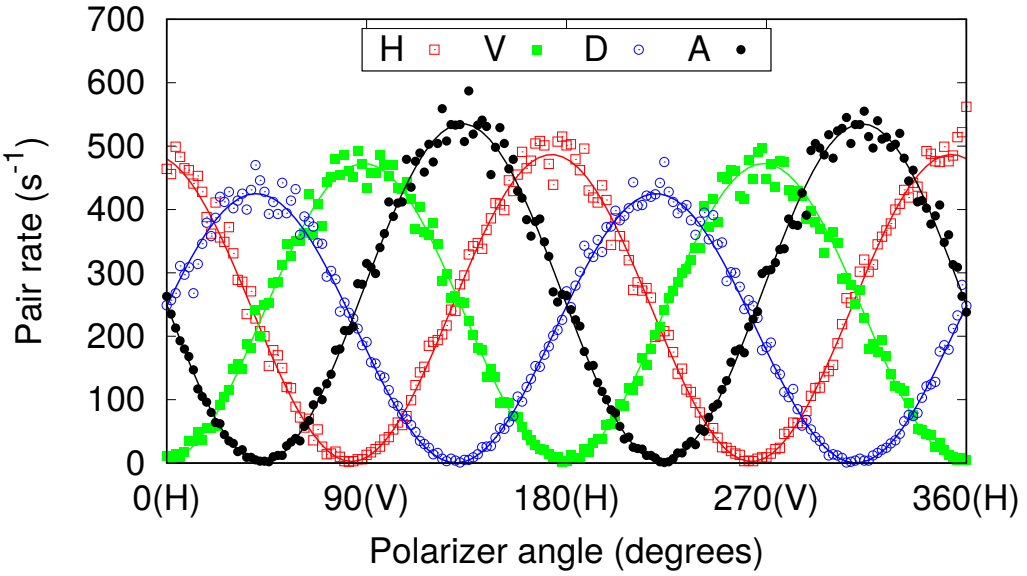

Figure 2.7: Polarization correlation in both H/V and D/A bases measured at the entanglement source. The coincidence rate is measured with two polarizers applied to the signal and idler photons. The polarizer on the signal's side is kept at different settings (H, V, D, A), while the other polarizer on the idler's side is scanned over 360 degrees.

Signal's Polarizer setting	H	V	+45°	-45°
Visibility	99±0.6%	98.9±0.7%	99.8±0.3%	99.4±0.5%

These high visibilities suggest that the source generates photon pairs with polarization states very close to the ideal $|\Phi^+\rangle$ state. The remaining difference between the visibility values and 100% is due to accidental coincidences (which account for about 0.3% of the visibility drop), and other optical errors caused by various polarization components and collection fibers.

2.2 Detecting single photons at telecom wavelengths

Besides a high quality entangled photon pair source, efficient detection of single photons is another important element in QKD. The technology of detecting light at single-photon level intensity predated quantum cryptography with the invention of photomultiplier tubes (PMTs) in the 1930s [69–71]. In a PMT, photons generate photoelectrons through the external photoelectric effect. The photoelectrons are

then accelerated in vacuum by electrical fields towards a nearby dynode where they trigger secondary emission and creates more free electrons. Such cascaded emissions results in high sensitivity of the PMT and therefore make it capable of single photon detection.

Photomultiplier tubes were used in some of the earliest experimental demonstrations of QKD [30] and are still being used in present days. However, these detectors are based on vacuum tube technology which is somewhat limited in terms of lifetime, reliability, and scalability [72]. Additionally, the quantum efficiencies of PMTs in the infrared wavelength region are relatively low. A competitive alternative, which is single photon detector based on solid-state devices, did not appear until the 1960s with the invention of Geiger-mode avalanche photodiodes (APDs) [31]. Also commonly referred to as single-photon avalanche diodes (SPADs), these detectors are typically manufactured from semiconductor materials such as Si (for visible photons), Ge, and InGaAs (for near-infrared photons). APDs achieve single photon detection through internal photoelectric effect amplified by impact ionization (avalanche effect) and offer higher detection efficiencies compare to PMTs especially for longer wavelengths [73] .

Recent advancements in superconducting technologies lead to more advanced options such as superconducting nanowire detectors [74] and superconducting transition-edge sensors [34]. While these detectors can offer excellent performance parameters such as low timing jitter [75] and high quantum efficiency [76] across a wide range of wavelengths, they need to be operated at a cryogenic temperature which significantly increases the cost of operation. As a result, APDs currently remains the most commonly used single photon detectors in practical applications, including this thesis.

2.2.1 Single Photon Detection with APDs

The solid-state structure of an APD is conceptually similar to that of a p-n junction (Fig. 2.8). A reverse bias (V_{bias}) higher than the junction breakdown voltage is applied to the cathode of the APD, making it operate in the so-called Geiger mode. This bias voltage is typically higher than 100 V for silicon APDs and 50 V for InGaAs APDs. The bias voltage causes a strong electrical field within the depletion

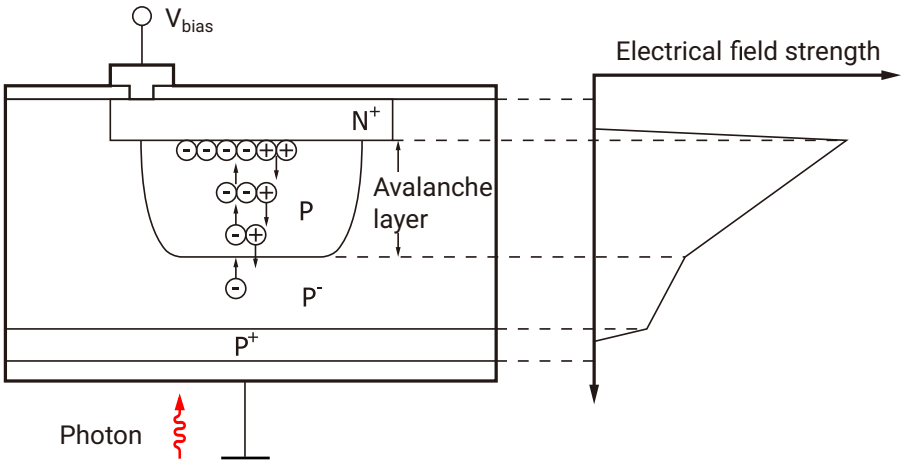

Figure 2.8: A simplified diagram illustrating the avalanche process in an APD. A high bias voltage is applied to the APD which creates a depletion region in the weakly doped P^- and P region. A single photon incident on the APD creates a free electron-hole pair, which then triggers an avalanche. The number of free charge carriers quickly multiplies in the avalanche layer and eventually forms a measurable amount of electrical current. This diagram is adopted from reference [77].

region of the P-N junction, which makes the device non-conductive in the absence of light.

Detection of a single photon in an APD begins with an internal photoelectric effect, which excites a valence electron to the conduction band of the p-n junction, generating a free electron-hold pair. These charge carriers accelerate in the electrical field and collide with atoms in the junction lattice to create more free electron-hold pairs as illustrated in Fig. 2.8. This process, called impact ionization, effectively amplifies the number of free charge carriers and creates a measurable amount of current (on the order of a few mA) which is converted to a voltage pulse across a load resistor (R_L in Fig. 2.9).

With an impinging photon triggering an avalanche current, the APD becomes conductive with the presence of free charge carriers across the junction. An APD at this state cannot detect subsequent photons until it is reinstated to the previous non-conducting state. This process, also called quenching, can be achieved by connecting a resistor R_q between the reverse bias and the cathode, as shown in Fig. 2.9. With the presence of this quench resistor, the avalanche current produces a voltage drop across the resistor which effectively lowers the APD reverse bias to

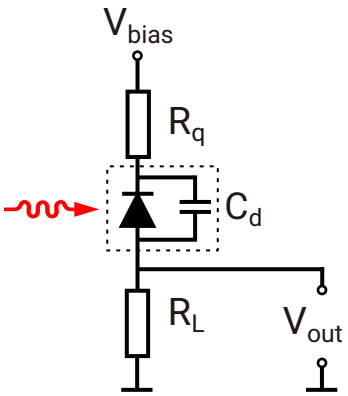

Figure 2.9: Schematic circuit diagram of an APD operated with the passive-quenching method. A high reverse bias voltage V_{bias} is applied to operate the APD in Geiger mode. In this mode, the APD is non-conductive with a high electrical field built across the depletion inside. After detecting a photon, the APD generates an avalanche current which is converted to a voltage pulse over a load resistor R_{L}. A quenching resistor R_{q} with a large resistance value is used to limit the avalanche current and reinstate the non-conducting state of the APD.

a level below the breakdown voltage. The avalanche current also decreases during this process until the APD becomes non-conductive again. The voltage at the APD cathode then slowly recovers towards V_{bias} with a small current flowing across R_{q} and charges the the APD junction capacitance C_{d} with a time constant $\tau_{dead} = R_{\text{q}}C_{\text{d}}$. This time constant represents the recovery time of an APD during which no photons can be detected, and is commonly referred to as the detection dead time.

APDs for infrared photons

For visible and near-infrared photons with wavelengths shorter than 1 μm, single photon APDs based on silicon deliver good performances. Commercial silicon APDs are widely available offering high efficiency ($\sim$50%) and low dark count rate ($<$1000 s^{-1}) [72, 78].

This is unfortunately not the case for single photons at telecommunication wavelengths that lay beyond the 1 μm mark. For photons around 1310 or 1550 nm, APDs based on a compound of Indium Gallium Arsenide and Indium Phosphide (InGaAs/InP) are more commonly utilized [2]. While linear mode APDs based on

[2] APDs made with germanium is also capable of near-infrared photon detection, but only up to about 1400 nm, therefore is less commonly used than InGaAs

InGaAs [3] have been present since the 1970s and are now widely adopted in the telecommunication industry, InGaAs devices operating in Geiger mode have not been reported until the late 1990s [79, 80]. Over the past two decades, more efforts have been devoted to optimizing the performances of single photon InGaAs APDs as well as commercialization of these devices [81, 82].

Despite the difference in material, the basic working principle of InGaAs APDs is the same as APDs based on silicon and can be operated with the same quenching circuit illustrated in Fig. 2.9. However, the performance of InGaAs APDs at their working wavelengths is generally inferior compared to the silicon detectors in the visible range. Difficulties in material engineering, as well as the smaller energy bandgap in InGaAs semiconductors, lead to higher dark count rates and after pulsing effects in InGaAs APDs, which gives a performance disadvantage to InGaAs APDs [83].

2.2.2 Methods for characterizating of APDs

In this thesis, we used a number of APDs from different suppliers which include both commercial modules and bare diodes. The performance of InGaAs APDs vary from unit to unit even when they are from the same manufacturer and therefore need to be characterized individually. We provide a summary of the different characteristics of InGaAs APDs as well as methods of characterizing them.

Dark counts

Even without the presence of light, an APD can still breakdown and subsequently generate pulses. These unwanted events are referred to as dark counts and are typically caused by thermal excitation or tunneling of valence electrons in the p-n junction [84]. In InGaAs devices, the probability of having a thermally triggered dark count is higher than in a silicon APD owning to a smaller energy bandgap between the valence band and conduction band. As a result, InGaAs APDs are commonly cooled to low temperatures during operation.

The dark count rate of an APD can be easily measured by covering the active area of the detector and simply counting the number of pulses per second. The

[3] An InGaAs/InP APD are sometimes informally referred to as just an InGaAs APD for simplicity. This is also partially because InGaAs is used as the absorption layer in such APDs where the photoelectric effect takes place.

InGaAs APDs in our setup is operated at a temperature of -50 °C and exhibit dark count rates typically between 5×10^3 and $3 \times 10^4\,\mathrm{s}^{-1}$.

Detection efficiency

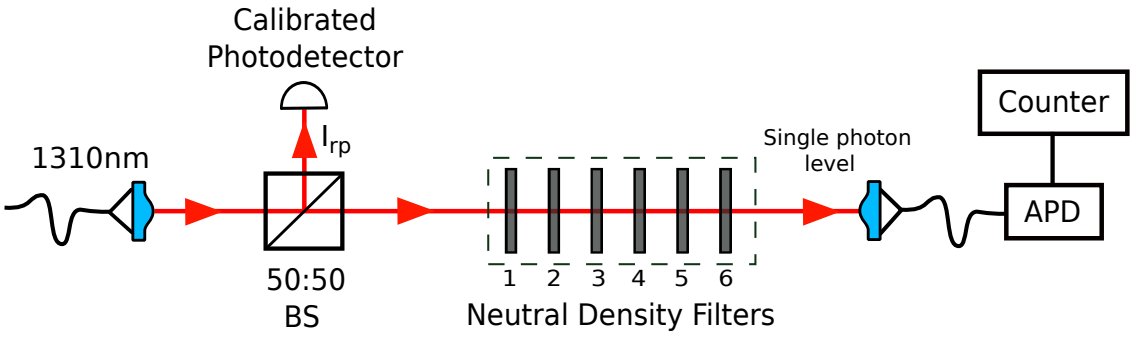

Figure 2.10: Setup for characterizing the efficiency of an APD. Light of a single-photon intensity level is prepared by strongly attenuating a 1310 nm laser with a series of neutral density filters. Half of the laser power is measured with a calibrated photodiode to provide a reference in optical power, which can be used to estimate the average number of photons in the attenuated laser. The detection efficiency is approximately the ratio between the detected number of photons and the estimated number of photons in the attenuated laser.

Detection efficiency is the overall probability of generating a pulse given a photon arrives at the APD. The efficiency η of an APD can be modeled as a product of three parameters: $\eta = \eta_\mathrm{c} \times \eta_\mathrm{q} \times P_\mathrm{a}$, in which η_c is the optical coupling efficiency to the detector, η_q is the quantum efficiency of the APD absorption layer, and P_a is the probability of triggering a detectable avalanche current given a photon is absorbed by the APD (avalanche probability) [85]. The optical coupling efficiency η_c and quantum efficiency η_q are generally fixed parameters that only depend on the optical setup (or diode packaging for fiber-pigtailed APDs) and material properties of the absorption layer, respectively. On the other hand, the avalanche probability P_a depends not only on the structure of an APD's absorption and avalanche layer but also on its operating parameters such as reverse bias voltage and temperature. Modeling an InGaAs APDs efficiency dependence can be non-trivial and has been investigated in several different works [86–88].

The detection efficiency of an APD can be experimentally characterized with the setup shown in Fig. 2.10. The measurement begins with a laser at 1310 nm

generating a fixed amount of optical power (e.g. around 100 μW), which is then divided by a 50:50 beam splitter. Half of the light is reflected and measured by a calibrated reference photodiode, generating a photocurrent of I_{RPD}. The other half of the light propagates through a series of neutral density (ND) filters which provides a high combined attenuation (e.g. 100 dB). Light is attenuated down to the single photon level by the ND filters and is detected with the APD under test.

The APD's detection efficiency η is estimated as the ratio between the corrected count rate $C_{\mathrm{measured}} - C_{\mathrm{dark}}$ (after subtracting the dark counts), and the number of photons per unit time in the attenuated laser C_{laser}:

$$\eta = \frac{C_{\mathrm{measured}} - C_{\mathrm{dark}}}{C_{\mathrm{laser}}}$$

The rate of photons in the attenuated lase C_{laser} can be calculated from the measured photocurrent I_{RPD}:

$$C_{\mathrm{laser}} = \frac{I_{\mathrm{RPD}}}{S} \times T \times \frac{1}{h\nu}$$

where S is the sensitivity of the reference photodiode, T is the combined transmission of the ND filters and $h\nu$ is the energy of a single photon at 1310 nm.

While this method of estimating the detection efficiency is conceptually simple, meticulous care is required when conducting the measurement. The reference photodiode needs to be carefully calibrated in order to provide accurate readings of optical power; the loss of each ND filter (as well as any other optical components) needs to be tested in advance and the optical coupling into the APD requires several adjustments to account for small walk-offs caused by the filters. As a result, setting up such a measurement can be challenging and time-consuming.

A complementary method is shown in Fig. 2.11 which instead allows comparing the ratio between the detection efficiencies of two APDs. This measurement uses a correlated photon source with a stable photon pair rate. One first measures the coincidence rate using APD1 and APD2, then replaces APD2 with APD3 and repeats the coincidence measurement. The ratio of detection efficiencies between APD2 and APD3 approximately equals the ratio between the two measured coincidence rates [4]:

$$\frac{\eta_{\mathrm{APD2}}}{\eta_{\mathrm{APD3}}} \approx \frac{R_{1,2}}{R_{1,3}}$$

[4]This is a good approximation when the measured accidental coincidence rate is much lower than the true coincidence rate.

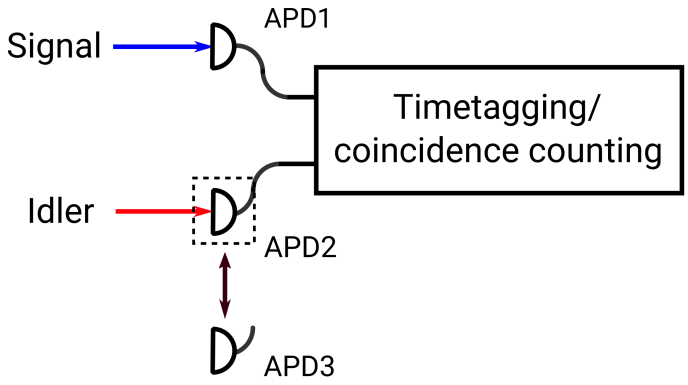

Figure 2.11: The setup used for comparing the detection efficiencies, as well as for estimating the timing jitters between two APDs. In an efficiency comparison measurement, the coincidence rate of a correlated photon source is measured twice between APD1 and APD2/APD3 respectively. The ratio of efficiencies between APD2 and APD3 is approximately the ratio between the detected coincidence rates. In a timing jitter measurement, the arrival times of the signal and idler photons are timestamped and cross-correlation between the two sets of timestamps is performed. The timing jitters of APDs can be inferred from pair-wise measurements between more than two detectors.

where $R_{1,2}$ and $R_{1,3}$ are the measured coincidence rates between APD1 and APD2/APD3, respectively. Given a detector with known detection efficiency, one can reliably infer the efficiency of other APDs by comparing them to this reference detector.

The InGaAs APDs used in this thesis include four commercial devices (ID220 infrared single-photon detector from IDQuantique), as well as four bare diodes (PGQ-022U1550TFT negative feedback diode from Princeton Lightwave) assembled with the passive-quenching circuit shown in Fig. 2.9. The detection efficiencies for the 4 commercial devices were measured to be about 12%, 10%, 8%, and 5%, respectively. On the other hand, the detection efficiencies of the other four APD diodes were set to about 10% by adjusting the reverse bias voltage.

Timing jitter

The precise timing of a photon's arrival is an essential task in many applications, including QKD. However, measuring the photon arrival time with an APD typically yields statistical variation larger than the fundamental timing uncertainty of the photon. This variation is known as the timing jitter and is caused by various physical effects in the detection process as well as electronic noise in the detection/timing

circuitry.

Measuring the timing jitter statistics of an APD directly can be difficult. One needs to first generate photons with precise timing, which can in principle be realized with an attenuated pulsed laser with a short duration (femtosecond level). Alternatively with a few assumptions, one can use the same setup shown in Fig. 2.11 to estimate the timing jitter of detectors provided more than two of them are available.

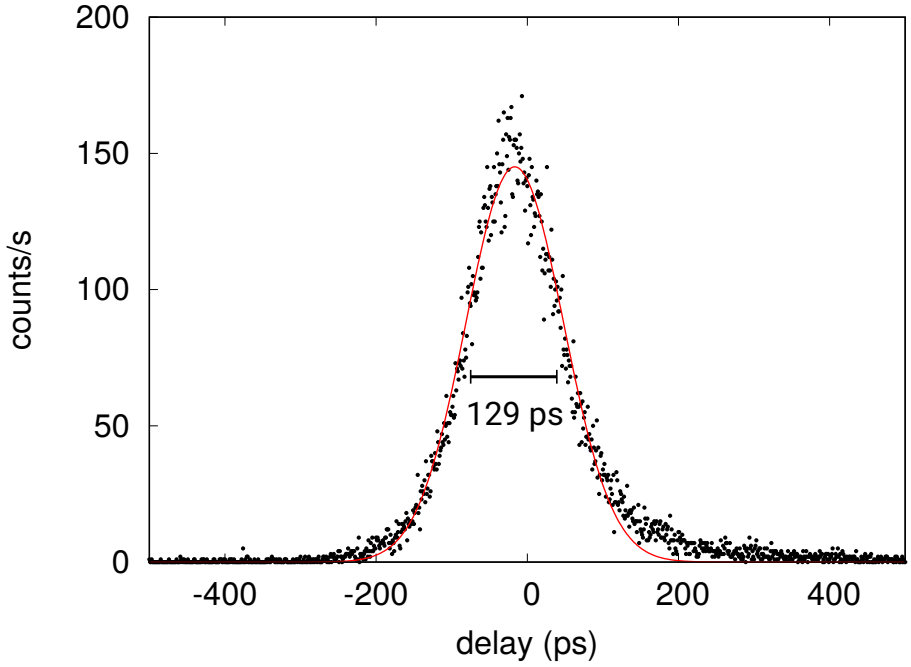

Figure 2.12: An exemplary cross-correlation histogram obtained by detecting signal and idler photons with two commercial InGaAs APDs (ID220 APD module from IDQuantique). The coincidence peak is fit to a Gaussian distribution with a standard deviation $\sigma = 64.5\,\text{ps}$. If one assumes an identical performance between the two detectors, then they each have a standard deviation in timing jitter of 45.6 ps.

Using a pair of APDs, one can timestamp the signal and idler photons and obtain a cross-correlation histogram. If we assume an APD's timing jitter to be a random variable with a Gaussian distribution, the resultant coincidence peak in the histogram is also a Gaussian distribution (as shown in Fig. 2.12) with a standard deviation

$$\sigma = \sqrt{\sigma_1^2 + \sigma_2^2},$$

where σ_1 and σ_2 are the standard deviations of timing jitter for APD1 and APD2. In an exemplary case where three APDs are available, three such measurements can be carried out in a pair-wise manner:

$$\sigma_{12} = \sqrt{\sigma_1^2 + \sigma_2^2}$$
$$\sigma_{23} = \sqrt{\sigma_2^2 + \sigma_3^2}$$
$$\sigma_{31} = \sqrt{\sigma_3^2 + \sigma_1^2}$$

With the measured standard deviations σ_{12}, σ_{23} and σ_{31}, one can solve for σ_1, σ_2 and σ_3 which indicate the standard deviations of timing jitter in the three APDs, respectively. For practical reasons, we usually refer to the timing jitter of a detector as twice the standard deviation. With this method, we observed a nominal timing jitter around 100 ps for the InGaAs APDs in this thesis.

Dead time and afterpulsing

As mentioned in Section 2.2.1, an APD needs a short period of time to deplete the free charge carriers and recover back its initial non-conducting state after an avalanche. This period is called the dead time of an APD and can range from a few tens of nanoseconds to even a few microseconds depending on the junction capacitance of the APD and its external biasing circuitry. After a photon is detected, an APD cannot detect any more photons until the dead time is over and the detector is fully recovered.

Another effect that also happens after a photon detection is afterpulsing, which refers to a spontaneous retriggering of the APD shortly after a detection event. Afterpulses are usually caused by charge carriers trapped in lattice defects in the P-N junction who are later released by thermal excitation, triggering another avalanche in the detector. The probability of afterpulsing depends on the material and structure of an APD and can vary from unit to unit, but is generally higher in InGaAs detectors than silicon devices. The time constant of afterpulsing (the average time that an afterpulse takes place after a detection event) for an InGaAs APD is on the order of hundreds of nanoseconds (black trace in Fig. 2.13) and is usually longer at a lower temperature.

The effect of afterpulsing can be suppressed by adopting an active-quenching circuit or by deliberately adding an extra detector dead time. As a trade-off, the

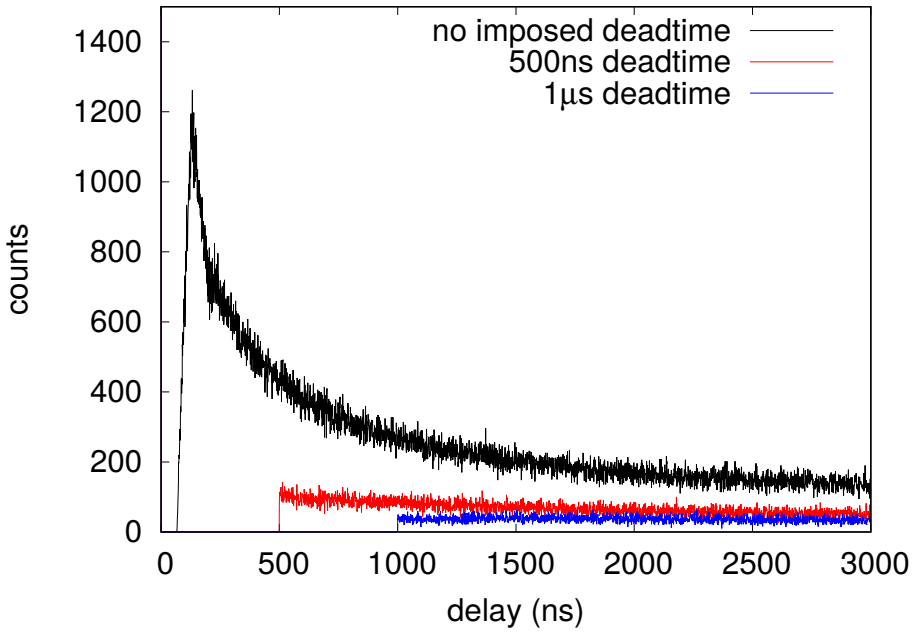

Figure 2.13: Autocorrelation histograms processed from photon timestamp traces, which reflect the distribution of timing intervals between subsequent detection events. The photons are generated from a strongly attenuated 1310 nm laser and are detected with a passively quenched APD diode (PGQ-022U1550TFT from Princeton Lightwave) using different dead time settings. With no extra dead time imposed (black trace), afterpulses are likely to occur within 1 μs following a detection event. The APD recorded a count rate of about 370 000 counts/s, and this rate is reduced to about 181 000 counts/s after imposing a 1 μs dead time to the detector (blue trace).

choice of dead time also limits the maximum number of detectable events per unit time. For the InGaAs APDs in our work, we typically set a dead time of 1 μs (blue trace in Fig. 2.13) with a maximum detectable photon rate of 10^6 counts/s which is higher than the typical measured count rate in our setup ($< 3 \times 10^5$ counts/s). As a result, this choice of deadtime effectively suppressed the number of afterpulsing events without imposing any significant detection loss to our system.

Chapter 3

Breakdown Flash from InGaAs Avalanche Photodiodes

The security of QKD protocols can be proven under models in which assumptions are made on the parameters of the physical channels and devices, such as loss, efficiency and dark count rate [22, 27]. However, there is a gap between the behavior of realistic devices and parameters in a model. The realistic behavior of devices sometimes lead to vulnerablities that can be exploited by an eavesdropper, which compromise the security of a QKD implementation. These vulnerablities, also referred to as side channels in some context, include mismatches in detector efficiencies [89–91], flaws in light source [92] and many more.

One of such side channels in QKD implementations comes from a property of realistic single photon avalanche photodiodes. Upon the detection of a photon, an APD emits fluorescence light after the avalanche breakdown process. This light emission is due to the recombination between free electrons and holes in the APD junction, which are previously excited to conduction band during the avalanche process. This fluorescence light was first observed in silicon based APDs [93–95] which shows a spectrum ranging from 700 nm to 1000 nm [96]. Similar fluorescence has been observed recently in InGaAs APDs [97–99] as well as InGaAs APD arrays [100, 101] which have wavelengths also within the telecommunication range ($\sim$1500 nm) [98].

It was pointed out in [96] that this fluorescence (typically referred to as 'breakdown flash', 'backflash' or 'electroluminescence') can reveal information about the photon detection process to an eavesdropper. As suggested in Fig. 3.1, an eavesdropper can monitor the optical channel for breakdown flash which leaks information

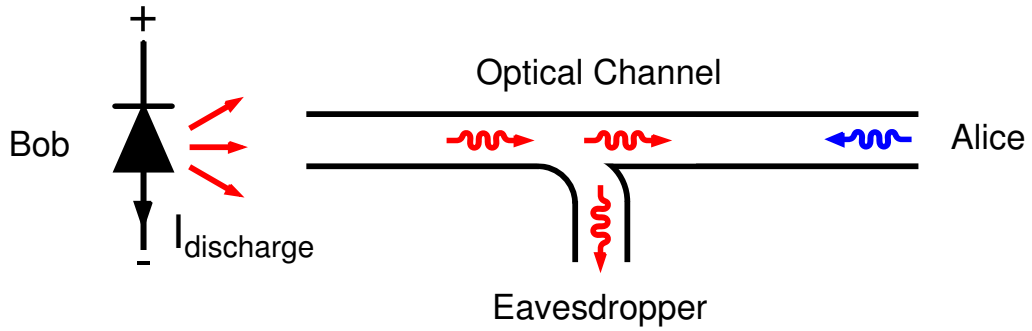

Figure 3.1: A single photon carrying information on phase or polarization is sent from Alice to Bob. The detection of the photon triggers breakdown flash which is partially coupled back into the fiber channel, giving Eve access to the timing and/or polarization information of the detected photon.

about the arrival times of QKD photons. Moreover, in polarization encoding QKD with passive basis-choice scheme, the leaked breakdown flash photons from different detectors can have different polarization states as they propagate through different ports of polarization beam splitters in the measurement setup [102]. In this case, an eavesdropper can determine which detector receives a photon at any given time simply by measuring the polarization of breakdown flash light leaked back to the optical channel.

As such, a strategy must be in place to reduce or eliminate this side channel. In this chapter, we investigate the breakdown flash from two commercial InGaAs single photon detector modules. We utilize a simple method to identify breakdown flashes from these devices which only involves a coincidence measurement between the two detectors. In doing so, we provide an estimation of the breakdown flash probability. We also characterize its spectral distribution over the entire telecom wavelengths and conclude that the breakdown flash can be effectively supressed by applying spectral filtering.

3.1 Identifying Breakdown Flash from InGaAs APDs

The emission of breakdown flash happens when an avalanche is triggered in an APD, which is accompanied by a detection event being registered. This detection

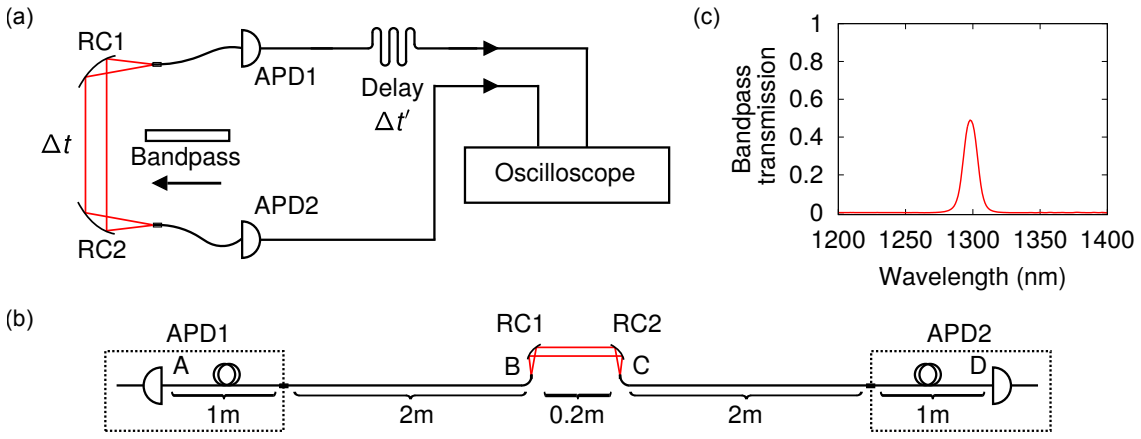

Figure 3.2: (a) Experimental setup for detecting the breakdown flash. The two APDs are optically coupled to each other by a pair of reflective collimators (RC1 and RC2). It takes $\Delta t \approx 32.5\,\text{ns}$ for a photon to travel the optical distance between APD1 and APD2. (b) Schematics of the lengths of fibre patchcords. The output signals from APDs are sent to an oscilloscope with an electrical delay $\Delta t' \approx 127\,\text{ns}$ applied to APD1. The oscilloscope triggers on signals received from APD2, and records the arrival times of signals from APD1. We record coincidence both events where APD1 emits a breakdown flash that is detected by APD2, and the other way round. An optical bandpass filter in a another measurement to suppress the number of breakdown flash events. The transmission profile of the bandpass filter is shown in (c).

event can be an actual impinging photon or a dark count in the detector. Either type of events can induce avalanche breakdown in an APD and therefore emits the same breakdown flash light [103]. While the amount of light emitted in a breakdown flash is not necessarily microscopic [93], previous studies suggest that the detectable emission intensity (factor in the coupling loss and detector efficiency) is on the single photon level [96, 98]. As such, an APD can both generate and detect a breakdown flash.

The detectors under investigation are two InGaAs APD based single-photon counting modules (ID220, ID Quantique, with fibre input), labelled APD1 and APD2. We use the setup shown in Fig. 3.2 (a) where each detector acts as both source and detector. In order to observe the breakdown flash events, the fibre-coupled detectors APD1 and APD2 are optically coupled through free space by a pair of reflective collimators (RC1 and RC2) with an overall transmission of 89% (including

fibre losses). The reflective collimators are placed about 20 cm apart with each one connected to a detector through 3 meters of optical fiber.

The output from the two detectors are connected to two channels of an oscilloscope (Lecroy Waverunner 640 Zi) which serves as a time tagging device in this measurement. Once the oscilloscope receives a signal from APD2 as a trigger ($t = 0\,\text{ns}$), it waits for any signals comes from APD1 within the next 250 ns and timestamp these signals with respect to the trigger with a timing resolution of 100 ps. A variable electrical delay is applied to APD1 to offset the signal arrival times such that only positive time differences for all interesting events are recorded by the oscilloscope.

The experimental setup is kept in the dark such that the breakdown flash is only caused by dark breakdown events in the APDs. Under this condition, we observe single detector event rates of $(1.00 \pm 0.016) \times 10^4\,\text{s}^{-1}$ for APD1, and $(0.533 \pm 0.019) \times 10^4\,\text{s}^{-1}$ for APD2 which corresponds to the dark count rates of the two detectors.

When there is a breakdown event in APD2 at $t = 0\,\text{ns}$, the oscilloscope is triggered. Such an event in APD2 causes a breakdown flash and emits photons that arrive at APD1 after a traveling time $\Delta t \approx 32.5\,\text{ns}$ (about 6 m of fiber length). These photons are detected and generate a signal from APD1 which is delayed by $\Delta t' \approx 127\,\text{ns}$ due to the electrical delay. This signal is timestamped by the oscilloscope at $t = \Delta t + \Delta t'$, which indicates a breakdown flash emitted from APD2 and detected by APD1.

Alternatively, a breakdown event in APD1 at $t = -\Delta t$ will cause a breakdown flash that reaches APD2 at $t = 0$ and triggers the oscilloscope. The corresponding breakdown signal from APD1 reaches the oscilloscope and is recorded at $t = \Delta t' - \Delta t$. In contrary to the previous case, this indicates a breakdown flash from APD1 detected by APD2.

With this setup, we accumulate events for 12 hours and obtained a histogram of the event timings which is shown in Fig. 3.3 (a). Two dominant peaks are identified with peak 1 located at $t_1 = \Delta t' - \Delta t \approx 95\,\text{ns}$ and peak 2 located at $t_2 = \Delta t' + \Delta t \approx 159\,\text{ns}$. With different nodes in this setup labelled in Fig. 3.2 (b), these peaks correspond to breakdown flash events between the two APDs along paths A-B-C-D and D-C-B-A, respectively. Each peak has a full width at half maximum (FWHM) of about 700 ps. The separation between the two peaks is

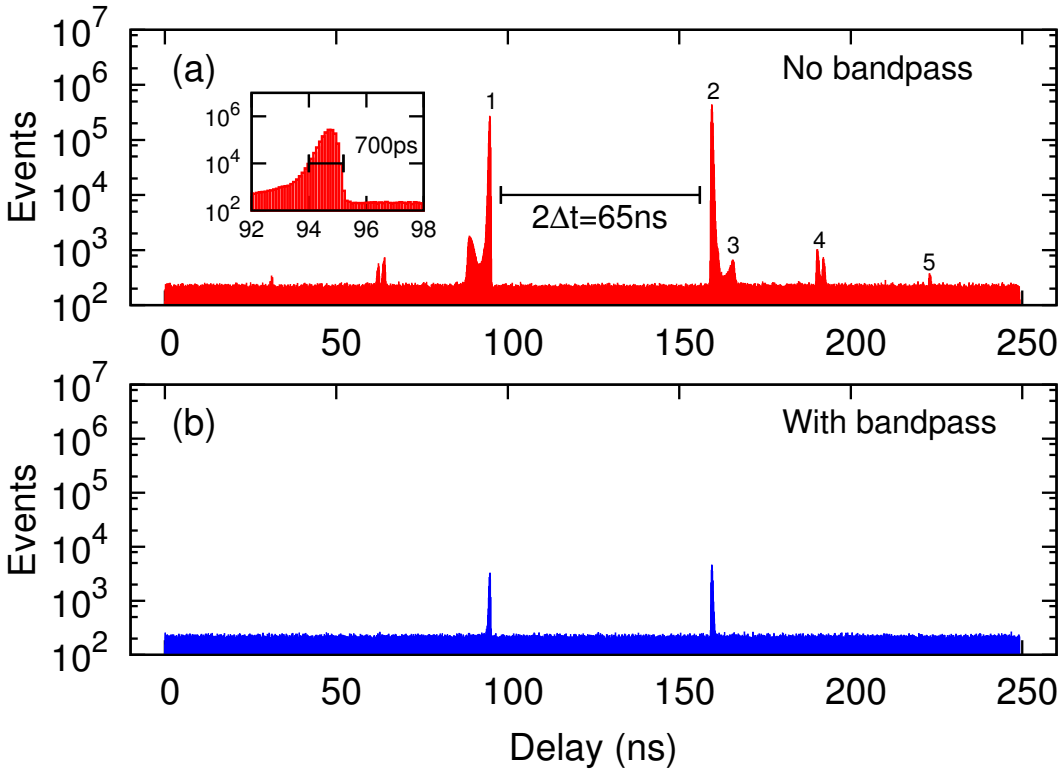

Figure 3.3: (a) Histogram of signal arrival times from APD1 recorded by an oscilloscope. Peak 1 corresponds to APD1 emitting a breakdown flash that detected by APD2 (path A-B-C-D), peak 2 to the reverse direction (path D-C-B-A). Peak 3 is suspected to be due to the afterpulsing of APD1. Peaks 4 and 5 are due to the back reflection of breakdown flash light at fibre joints (paths A-B-C-D-C/B-D and D-C-B-A-B/C-A). (b) Same measurement, but with a bandpass filter in the optical path. The number of breakdown flash events is suppressed by a factor of over 100. An integration time of 12 hours is used for both measurements.

$t_2 - t_1 = 2\Delta t \approx 65\,\text{ns}$, which is about twice the optical transit time from A to D.

Peak 3 ($t \approx 166\,\text{ns}$) and its counter part ($t \approx 88\,\text{ns}$) are suspected to be breakdown flashes triggered by afterpulsing counts in the APDs [97]. Peak 4 ($t \approx 190\,\text{ns}$) actually consists of two small peaks seperated 1.8 ns apart. They are possibly due to photon back reflections at the reflective collimators from a secondary breakdown flash in APD1 (triggered by flash photons from APD2), i.e., follow a path D-C-B-A-B/C-A. The timing difference between peak 4 and peak 2 is about 31 ns, which corresponds to a fibre length of about 6 meters (from point A to B/C then back to A, Fig. 3.2(b)). Peak 5 ($t \approx 223\,\text{ns}$) is suspected to be a tertiary breakdown from APD2 (triggered

by photons from the secondary flash in APD1), as it is approximately 64 ns away from peak 2 and the timing difference matches a fibre length of about 12 meters (from point A to D then back to A, Fig. 3.2(b)).

This measurement was repeated with a bandpass filter (transmission profile shown in Fig. 3.2(c)) inserted between RC1 and RC2. The passing band of the filter is centered at 1300 nm with a FWHM of 10 nm. The events timing histogram obtained from this measurement is shown in Fig. 3.3 (b). At the same positions, the main peaks are suppressed by a factor of about 100, while the other small peaks are no longer observable. This indicates that spectral filtering could be used as a countermeasure to effectively reduce the breakdown flash.

While an oscilloscope can identify breakdown flash events with excellent timing resolution, the recorded timing histogram (Fig. 3.3) in the previous measurement does not allow us to directly determine the absolute detection rates of breakdown flash photons. This is because the timing acquisition of an oscilloscope is constantly interrupted by data processing which takes an unpredictable amount of time. Therefore we replaced the oscilloscope with a hardware coincidence stage to obtain an estimation of the absolute probability of detecting a breakdown flash event. (Fig. 3.4(a)).

The physical setup remains mostly the same as the previous measurement, except that the electrical delay after APD1 is adjusted to be the same value as the photon propagation time Δt. Under this configuration, an initial breakdown signal from APD1, and the breakdown flash signal from APD2 arrive at the coincidence stage at approximately the same time. A coincidence event is identified when the two signals arrive within a time window of 500 ps, which indicates a breakdown flash emitted from APD1 detected by APD2. The number of coincidences is continuously recorded by a hardware counter thus avoiding the dead time of the oscilloscope in the data processing. Similarly, the number of breakdown flash events from APD2 is measured in the same manner, except that the same electrical delay is applied after APD2.

For each configuration, we continuously record the number of coincidences for 12 hours. We detect a rate of $44.4 \pm 2.2\,\mathrm{s}^{-1}$ from APD1 to APD2, and $22.2 \pm 1.6\,\mathrm{s}^{-1}$ from APD2 to APD1. These coincidence rates are normalized by the count rate of the emitting APDs, which then yields a probability of $0.44\% \pm 0.02\%$ for APD2 detecting

a breakdown flash from APD1, and a probability of $0.42\% \pm 0.03\%$ in the reverse direction. As a noise baseline, the rate of accidental coincidences is also measured by blocking the optical path between the APDs, yielding a rate of $0.032 \pm 0.057\,\mathrm{s}^{-1}$, with dark count rates of $(9.55 \pm 0.18) \times 10^3\,\mathrm{s}^{-1}$ and $(5.46 \pm 0.20) \times 10^3\,\mathrm{s}^{-1}$ for APD1 and APD2, respectively.

When the bandpass filter shown in Fig. 3.2 (c) is applied, these probabilities are reduced to $0.0049\% \pm 0.0023\%$ and $0.0057\% \pm 0.0033\%$, which corresponds to detection rates less than $0.5\,\mathrm{s}^{-1}$. Therefore, applying spectral filtering can effectively suppress the rate of breakdown flash by two orders of magnitude.

3.2 Spectral Distribution of Breakdown Flash

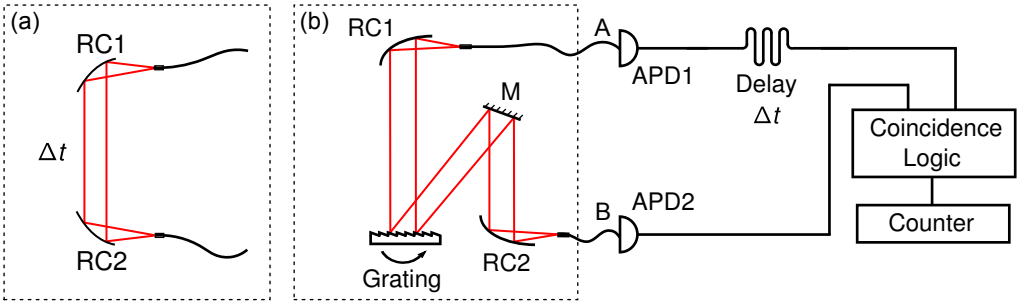

Figure 3.4: (a) Setup for a coincidence measurement to determine the rate of detecting breakdown flashes from APD1. An electrical delay is applied to APD1 such that the dark count signal from APD1 and the breakdown flash signal from APD2 arrive at the coincidence stage at the same time. A counter is used to log the number of events per second. The setup can also measure the breakdown flash rates from APD2 with the electrical delay connected to APD2. (b) Setup for measuring the spectral distribution of the breakdown flashes. The working principle is the same as the one in (a), except that the reflective collimators are replaced by a grating monochromator to select different transmission wavelength.

In the previous section, we saw that a large suppression in breakdown flash probability can be achieved even with a relatively wide-band filter (10 nm FWHM). This suggests that the spectral distribution of breakdown flash photons could be covering a much wider wavelength range than the bandwidth of the filter. However, spectral information available from a single bandpass experiment is somewhat limited to draw such a conclusion.

We therefore analyze the spectral distribution of the breakdown flash with a setup shown in Fig. 3.4(b). A monochromator consisting of a reflective grating (600 lines/mm, blazed at 1.25 μm) and a pair of reflective collimators (RC1 and RC2) is inserted in the optical path between the two APDs. The grating acts as a tunable filter that changes the central transmission wavelength by adjusting its rotation angle. To estimate the spectral resolution of the monochromator, we measure the instrument response to a 1310 nm single mode diode laser, and find a full width at half maximum (FWHM) of 3.3 nm. For the first-order diffraction of the same 1310 nm light, we observe an overall transmission of 51% from point A to B in Fig. 3.4(b).

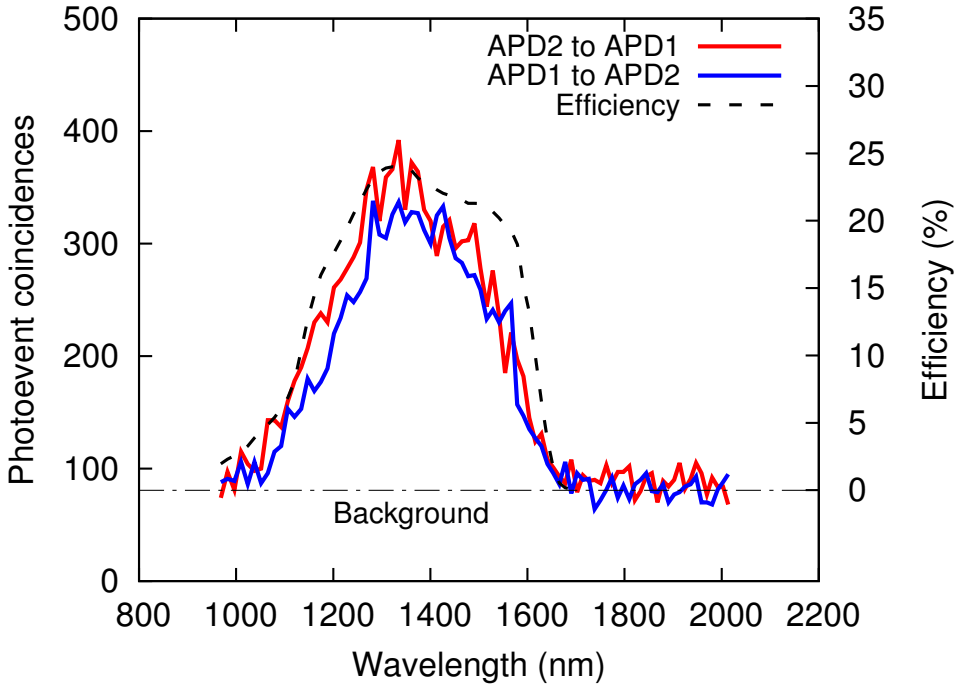

Figure 3.5: Spectral distribution of the InGaAs APD breakdown flash. The integration time for each data point is 30 minutes. We record cases where APD1 emits a breakdown flash that is detected by APD2 and vice versa. The two spectra range from 1000 nm to 1600 nm and peak at about 1300 nm. The dashed line indicates the background due to accidental coincidences.

We sampled 84 wavelengths ranging from 1000 nm to 2000 nm with a grating angle incrementation of 0.28 °. The same coincidence measurement used in Fig. 3.4 (a) is performed here, but with an integration time of 30 minutes. The results are shown in

Fig. 3.5. The detected coincidence events span a wide range from 1000 nm to 1600 nm, with a maximum at about 1300 nm. We note that these results are not corrected for the transmission efficiency of the monochromator, nor the wavelength-dependent detection efficiencies of the APDs. However, the observed spectra (Fig. 3.5, left axis) follow closely the wavelength-dependent quantum efficiency of the APDs [104] (right axis). As a result, we are not able to detect spectral components outside this 1000 nm-1650 nm band bounded by APD efficiency. The close match of spectral sensitivity and observed spectrum suggests that the spectral distribution of the breakdown flash photons could be relatively flat over the whole region we are able to observe, and could even extend beyond that sensitivity range. A more comprehensive measurement of the actual spectrum would require more wide-band photodetectors. The recent progress with superconducting nanowire detectors [74] would make these devices a good choice for such a measurement.

Concusion

Similar to their silicon counterparts [96], commercial InGaAs single-photon detectors do exhibit breakdown flash. We characterized the breakdown flashes from two such devices by measuring the coincidences between the breakdown flash photons and the dark count events that triggered them. We measured the detection probability of breakdown flash events which is about 0.4% with these devices. Given that these APDs have a nominal detection efficiency of about 10%, the breakdown flash could contain at least 0.04 photons emerging from the fiber connector of the devices. This non-negligible amount of photons may result in an amount of information leakage that cannot be overlooked in practical QKD implementations.

In some sense, this should not come as a surprise, as light emission for electron-hole recombinations in direct bandgap semiconductors like InGaAs is more likely to happen compared to indirect bandgap semiconductors like Silicon. However, a direct comparison with photon numbers due to the breakdown flash between the two APD types is not directly obvious: the overall number of photons in a breakdown flash is likely to be proportional to the number of free charge carriers released in a breakdown, which is significantly smaller in InGaAs APDs compared to Silicon APDs due to the lower excess voltage above breakdown. The optical coupling of the

detectors is also different between the devices used in this measurement (multi-mode fibers coupled to the diodes) and ones used in earlier experiments [96] (free-space coupled), which makes it difficult to make a fair comparison between the reported rates.

The spectral distribution of breakdown flash from these InGaAs APDs appears to be relatively wide. Thus, a spectral filter in front of an APD is an effective countermeasure to prevent potential information leakage in a quantum key distribution scenario. With the measurements shown in this chapter, the observed breakdown flash probability can be used to provide an upper bound for estimating the number of photons being leaked back to the optical channel due to breakdown flash.

Chapter 4

Distributing Correlated Photon Pairs across Telecom Fiber

Utilizing fibers to distribute entangled photon pairs to different parties in QKD is a tempting alternative to photon distribution over free space. Within a small metropolitan area, optical links can be established through existing telecommunication fiber networks to connect strategic locations at a low cost. The optical links can be easily switched between different pairs of users by rerouting the fibers, and even enable multi-user QKD services [105] or QKD/conventional-data coexistence [106] through wavelength division multiplexing.

Despite all the merits, challenges remain when it comes to the transmission of photon pairs across long optical fibers. Apart from the higher transmission loss ($\sim 0.34\,\mathrm{dB/km}$ at $1310\,\mathrm{nm}$), dispersion effects in fiber can have various effects on the timing and polarization states of the entangled photon pairs. In this chapter, we will focus on the fiber chromatic dispersion, which affects the timing correlations of an entangled photon pair.

4.1 Effect of chromatic dispersion on photon pair distribution

Chromatic dispersion refers to the phenomenon by which different spectral components of light travel at different velocities in a medium. This difference in velocity causes a spread in the group delay of an optical pulse, which results in a broadening in the time domain. In a telecommunication fiber with length L, the spread in duration ΔT of an optical pulse with bandwidth $\Delta\omega$ is approximately:

$$\Delta T = L|\beta_\lambda|\Delta\omega, \tag{4.1}$$

where the coefficient $|\beta_\lambda|$ is the group velocity dispersion parameter at wavelength λ [57]. In fiber optics communication where optical bandwidth is typicall expressed as difference in wavelengths $\Delta\lambda$, Eq. 4.1 can also be written as:

$$\begin{aligned}\Delta T &= -\frac{2\pi c}{\lambda^2} L|\beta_\lambda|\Delta\lambda \\ &= L|D_\lambda|\Delta\lambda, \end{aligned} \tag{4.2}$$

where c is the speed of light in vacuum. In this expression, an equivalent dispersion parameter D_λ is adopted taking units of ps/(nm·km). This dispersion parameter depends on the material property of the medium as well as the waveguide structure in the case of fiber transmission. For SMF28 fibers, the dispersion parameter is about 18 ps/(nm·km) at 1550 nm, which is the typical wavelength for fiber optics communication [54].

The dispersion parameter D_λ in Eq. 4.2 (or β_λ in Eq. 4.1) can take both positive and negative values at different wavelengths. A positive dispersion parameter means that shorter wavelength components of a pulse travel faster than longer ones, and vice versa for a negative dispersion. In standard SMF28 fibers, both positive and negative dispersion is available due to a competition between the material property of silica and the fiber waveguide structure [107]. As a balance between the two contributions, a zero-dispersion wavelength can be found typically between 1304 nm and 1324 nm, with a slope of dispersion as low as 0.092 ps/(nm$^2\cdot$ km) [54].

Similar to pulse broadening, chromatic dispersion increases the timing uncertainty of a photon as it propagates through a fiber. This effect can be easily observed when measuring the timing correlations between a pair of photons generated from SPDC process. As shown in Fig. 4.1 (a), time-correlated photon pairs are generated via type-0 SPDC and are routed to two single photon detectors through two fibers. The arrival times of photons at detectors 1 and 2 are registered by two time-tagging units as $\{t_i\}$ and $\{t_j\}$ respectively. These timestamps are processed into sets of delays (d_1 and d_2) such that:

$$d_1(t) = \sum_i \delta(t - t_i); \quad d_2(t) = \sum_j \delta(t - t_j).$$

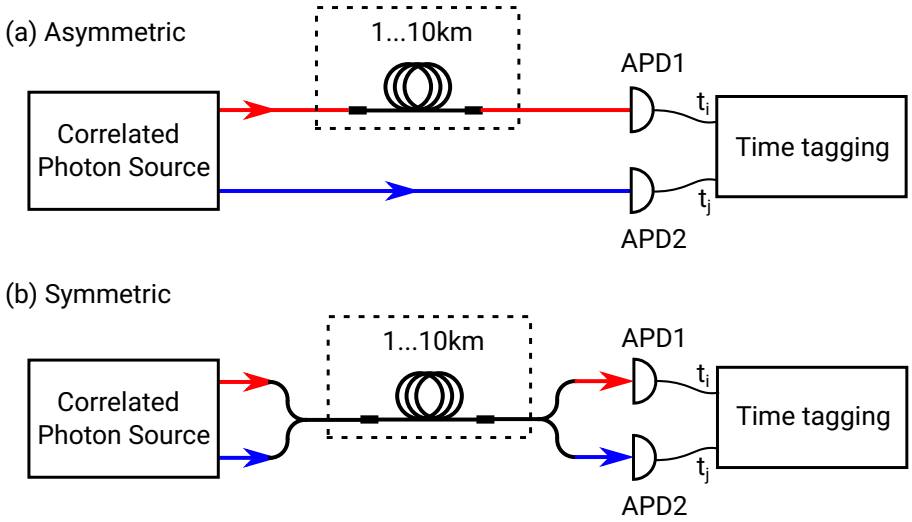

Figure 4.1: Experimental setup for measuring the timing correlations of photon pairs propagating over long fibers. In the asymmetric configuration (a), one of the photons is transmitted through a long fiber while the other photon is detected locally. In the symmetric case (b), both photons are sent through the same long fiber and are only separated after fiber transmission. Both measurements are repeated with different fiber lengths ranging from 1 km to 10 km.

The cross-correlation between the two sets of delays can be computed as $c(\tau)$:

$$c(\tau) = \int d_1(t) d_2(t+\tau) dt.$$

The cross-correlation between pairs of SPDC photons will exhibit a peak at $\tau = t_0$, where t_0 corresponds to the difference in time of flight between the two fibers. Locating this peak allows us to identify photons from the same pair, which is an important step in entanglement-based QKD [108]. Broadening of this coincidence peak lowers the ratio between true coincidences and accidental events which eventually increases the number of errors in QKD. As a result, minimizing the width of this coincidence peak is an important consideration in entanglement-based QKD [109].

With the setup shown in Fig. 4.1 (a), a different amount of dispersion is introduced by increasing the length of fiber from 1 km to 10 km, using multiple 1 km-long fiber spools. The resulting cross-correlation histograms are shown in Fig. 4.2, which exhibits an obvious increase in the width of coincidence peaks in longer fibers. The FWHM of the coincidence peak is approximately a linear function of fiber length with a slop of about 167 ps/km (Fig. 4.6).

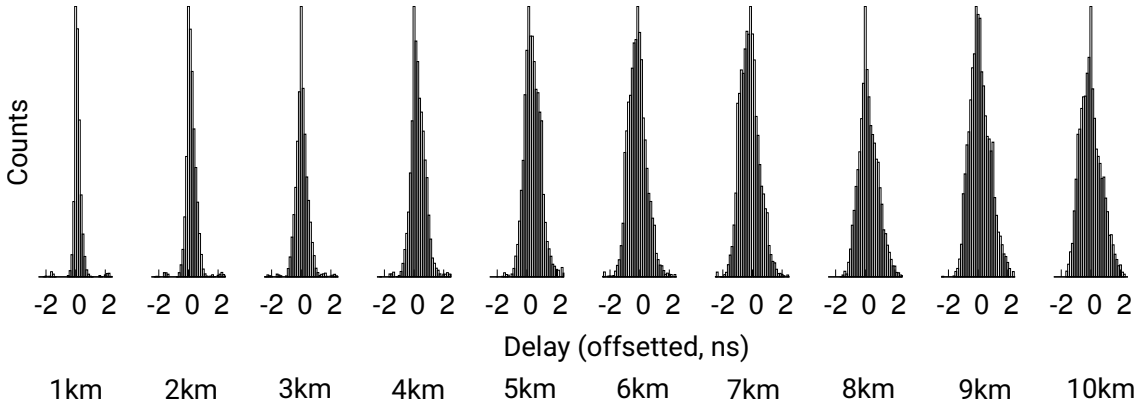

Figure 4.2: Timing correlation of photon pairs with only one of the photons propagates through a long fiber with lengths varying from 1 km to 10 km. The delay in the time of flight in fiber is offset to zero and the count rates in different measurements are normalized to the same height for easier comparison of the coincidence width.

With our SPDC source operating around 1316 nm which is close to the zero-disperison wavelength, the degradation of timing correlation is still manageable with this amount of increase in the width of the coincidence peak. The effect can be significant for SPDC photons generated at wavelengths with significant dispersion (e.g. at 1550 nm with dispersion parameter of 18 ps/(nm·km)). In such cases, narrow-band spectral filtering is required for fiber transmission of photon pairs at the cost of reducing the throughput of the entire system [110].

4.2 Nonlocal dispersion compensation at telecom O-band

If two optical pulses are initially coincident and propagate through fibers with dispersion, both pulses will experience broadening regardless of the sign of dispersion. A cross-correlation measurement on the arrival times of the two pulses using single photon detectors (assuming the pulses are attenuated to single photon level intensity) will yield a width of coincidence peak larger than the duration of any of the broadened pulses. This result is intuitive as the time discrepancies of two independent pulses can only add up in a cross-correlation measurement.

However, this is not necessarily the case for the propagation of a pair of SPDC

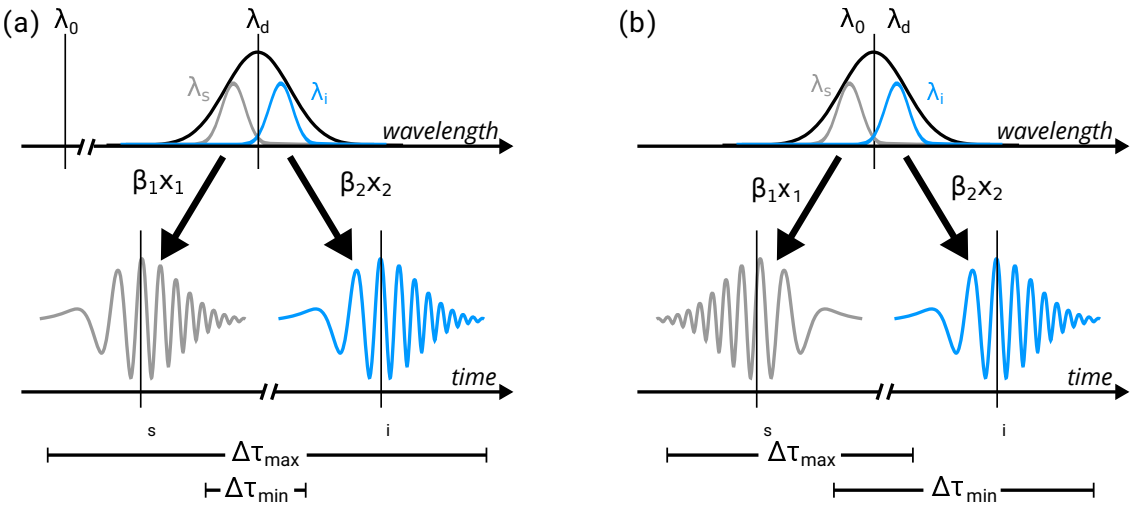

Figure 4.3: Mechanism of nonlocal dispersion compensation. (a) Both signal and idler photons are generated far away from the zero-dispersion wavelength λ_0 of the fiber. The two photons are dispersed by $\beta_1 x_1$ and $\beta_2 x_2$, respectively, where the dispersion coefficients β_1 and β_2 are both positive. In the time domain, both photons are chirped with shorter wavelength components taking a lead in time. As the signal and idler photons are anticorrelated in wavelength, the difference between the minimum and maximum possible delays $\Delta\tau_{min}$ and $\Delta\tau_{max}$ is large which denotes an increased discrepancy in the timing correlation. (b) When the degenerate wavelength λ_d of photons coincide with the zero-dispersion wavelength of fiber λ_0, the signals and idlers undergo opposite dispersion. In this case, the anticorrelation in wavelength minimizes $\Delta\tau_{max} - \Delta\tau_{min}$, which yields a smaller discrepancy in timing correlation.

photons. It was shown by Franson in 1992 that the chromatic dispersion experienced by one photon can be canceled out by the dispersion experienced by the other photon in a way that the two photons remain coincident [111]. This cancellation is nonlocal as it can happen between two spatially separated photons. As a result of this cancellation, the timing correlation between the two photons which is represented by the width of the coincidence peak can be well preserved as if there were no dispersion at all. In his work, he derived the width of the coincidence peak σ in the presence of dispersion:

$$\sigma^2 = 2\sigma_0^2 + \frac{(\beta_1 x_1 + \beta_2 x_2)^2}{2\sigma_0^2}, \tag{4.3}$$

where σ_0 is the coherence time of the photons (assuming the two photons have identical bandwidth) and x_1, x_2 are the propagation distances. The dispersion coefficients β_1 and β_2 can have opposite signs, which corresponds to a partial

compensation in the total dispersion amount. Perfect cancellation of dispersion is achieved when $\beta_1 x_1 + \beta_2 x_2 = 0$ [111].

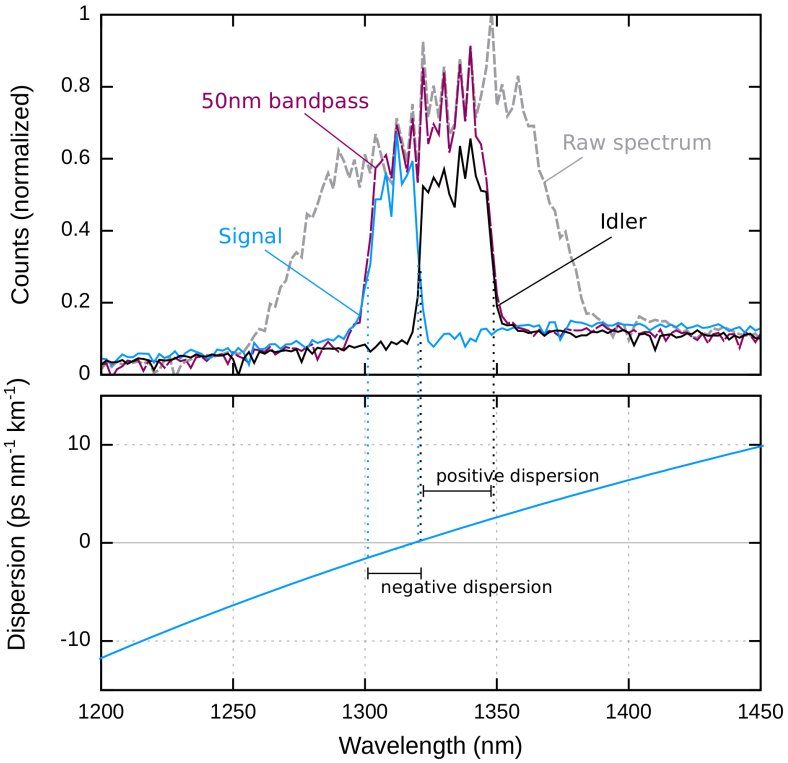

Figure 4.4: Spectrum of the correlated photons used to investigate effects of chromatic dispersion in fiber. Photon pairs are generated from the SPDC source described in Chapter 2 of the thesis, which is centered around 1316 nm and limited by a 50 nm bandpass filter. The bottom diagram shows the dispersion value of the standard SMF-28e fiber from Corning [54], with a particular zero-dispersion wavelength at 1316 nm. The signal and idler photons propagating in this fiber experience negative and positive chromatic dispersion, respectively.

The effect of nonlocal dispersion cancellation can be understood by considering the energy (wavelength) anticorrelation of a photon pair generated from SPDC in the presence of dispersion. Due to the conservation of energy, the longer wavelength (lower energy) components of a photon are temporally correlated with the shorter wavelength (higher energy) components of its sister photon. When propagating in a fiber with positive dispersion, shorter wavelength components of a photon travel faster while the longer wavelength components lag behind, which eventually leads to a chirp in the photon.

When both photons experience positive dispersion as shown in Fig. 4.3 (a), the maximum delay $\Delta\tau_{max}$ corresponds to the case where a signal photon is detected on the trailing edge (longer wavelength) of the wavepacket while an idler photon is detected on the leading edge (shorter wavelength). In contrast, the minimum delay $\Delta\tau_{min}$ is the time difference between the leading edge of the signal photon and the trailing edge of the idler photon. In this case, where both photons are positively dispersed, $\Delta\tau_{max} - \Delta\tau_{min}$ is large which implies an increased timing discrepancy between the detection of two photons.

Dispersion cancellation happens when the two photons encounter dispersion with opposite signs as shown in Fig. 4.3 (b), which corresponds to the case where β_1 and β_2 in Eq. 4.3 takes different signs. Under this condition, the chirp imparted on one of the photons is reversed compared to its sister photon. The difference between the maximum and minimum delay between the photon detection times $\Delta\tau_{max} - \Delta\tau_{min}$ is smaller compared to the previous case and therefore leads to a smaller timing discrepancy.

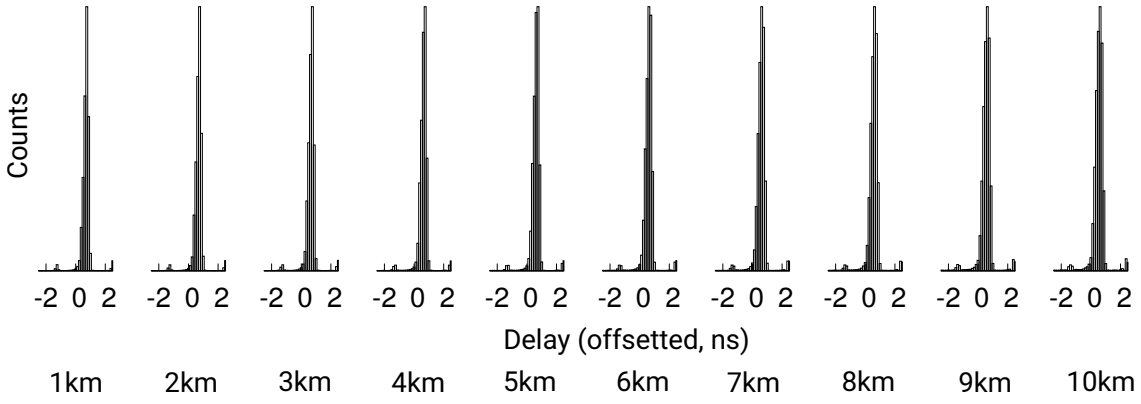

Figure 4.5: Timing correlation of photon pairs with both photons propagating through the same fiber with varying lengths. The timing correlation is much better preserved over these distances as compared to the previous case (Fig. 4.2)

.

We experimentally demonstrate the effect of dispersion cancellation using a setup shown in Fig. 4.1 (b). The degenerate wavelength of the correlated photon pair source is at 1316 nm which is close to the zero-dispersion wavelength in standard telecommunication fibers. The source emits photons with a 50 nm bandwidth which spans over both sides of this wavelength (Fig. 4.4). In this measurement, both signal

and idler photons are coupled into the same fiber with lengths varying from 1 km to 10 km. The photons are separated after fiber propagation with a wavelength division demultiplexer edged at 1316 nm, and are detected and time-tagged respectively.

With the dispersion experienced by signal and idler photons canceling each other, the timing correlation of photon pairs is better preserved over increasing fiber length (Fig. 4.5). The widening of coincidence peaks over distance is reduced to about 18 ps/km in this symmetric configuration as shown in Fig. 4.6.

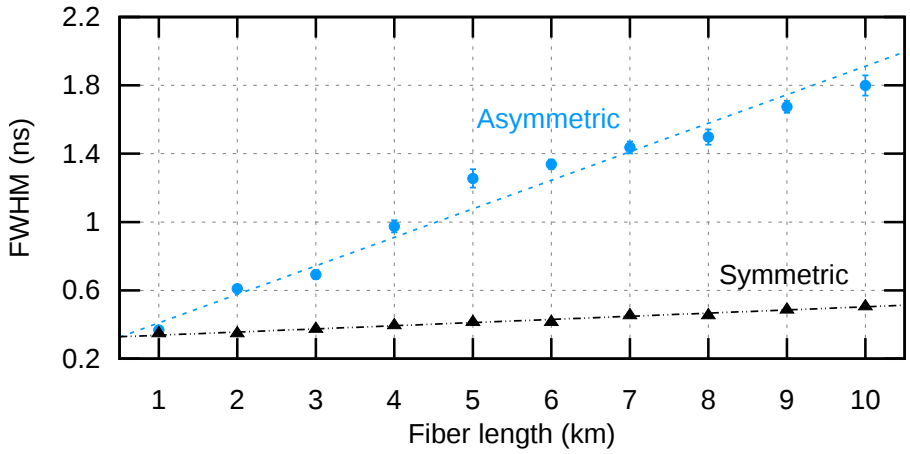

Figure 4.6: Cross-correlation peak width (FWHM) for photon pairs after propagating through various lengths of SMF28 fiber. In the asymmetric case where one photon is detected locally with a negligible amount of chromatic dispersion while the other photon travels through different fiber lengths, the FWHM increases with lengths with a slope of 167 ps/km. In the symmetric case where both photons propagate through the same fiber length, this slope is reduced to 18 ps/km.

We also observe the effect of dispersion cancellation as we transmit photons through two individual deployed telecommunication fibers each with a span of about 10 km. We conduct similar measurements with only one photon propagating over fiber, as well as with both photons transmitted through two fibers separately. The obtained histograms are shown in Fig. 4.7 (a) and (b). We observe a coincidence peak FWHM of 1.93 ns with only one photon being transmitted and an FWHM of 0.26 ns when both photons are transmitted.

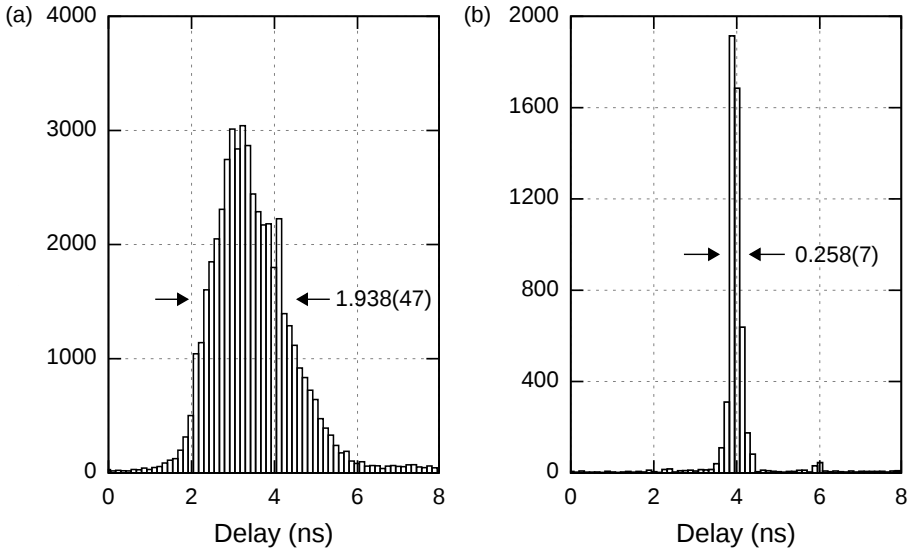

Figure 4.7: Timing correlation of photon pairs propagating in deployed telecommunication fibers.

Concusion

The measurements shown in Fig. 4.6 and 4.7 demonstrate that correlated photon pairs with appropriately engineered spectral properties can exhibit nonlocal dispersion cancellation which results in better-preserved photon timing correlation over long distances. This capability makes it possible to use entangled photon sources with a broad spectrum without being susceptible to significant broadening in timing coincidence due to chromatic dispersion. For photon pairs at the telecom O-band, the degree of dispersion cancellation can be adjusted by tuning the spectral properties of the photons, therefore eliminating the usage of extra dispersion-compensating fibers.

Chapter 5

Entanglement-Based Quantum Key Distribution with Active Polarization Compensation

In chapter 4 we discussed the issue of fiber chromatic dispersion and how it causes degradation of timing correlation between a pair of SPDC photons. This effect on the timing of photons can be alleviated by operating QKD at the telecom O-band which is close to the zero-dispersion wavelength of standard fibers.

Apart from the timing effect, a long fiber can also affect the polarization states of propagating photons due to its routing geometry as well as the presence of fiber birefringence. These polarization effects include depolarization and random rotations of the polarization states of propagating photons. These polarization effects can cause an increased error rate in QKD operation, and eventually prevents keys from being generated. This leads to a limited usage of optical fibers as the transmission channels for polarization-entangled QKD.

In this chapter, we investigated these polarization effects in a deployed fiber link and propose a scheme to actively compensate for polarization state rotation. This compensation is an essential step to enable the operation of polarization-encoded QKD over fiber. With this compensation scheme, we implement a full QKD setup over a deployed fiber and demonstrated a stable generation of encryption keys.

5.1 Polarization effects in a deployed fiber

The cross-section of a real fiber does not have perfect circular symmetry. The shape of a fiber core can deviate slightly from a circle due to imperfections in manufacturing or external stress. As a result, a short segment of fiber typically

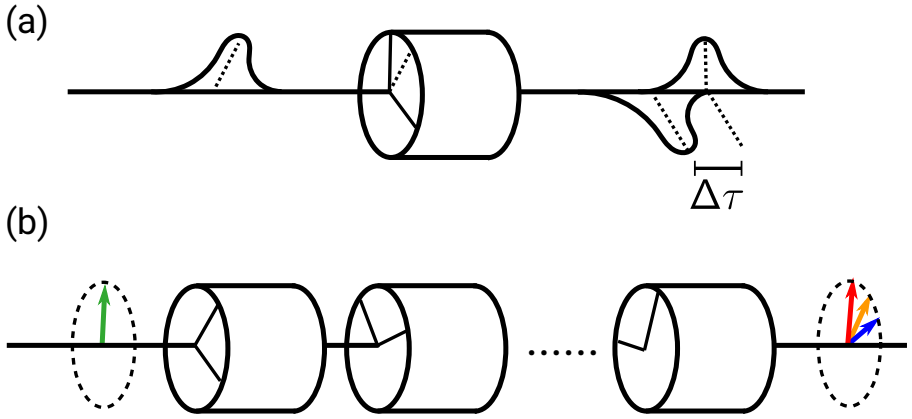

Figure 5.1: (a) A short segment of fiber possesses a small amount of birefringence. When an optical pulse is not polarized along the fast/slow axis of the fiber segment, its two orthogonal polarization components will experience a difference in group delay $\Delta\tau$. (b) A longer fiber is modeled as a series of short fiber segments concatenated together, with each segment having an unknown amount of birefringence and being oriented randomly. When broadband light propagates across such a long fiber, the polarization of different spectral components of light undergoes different transformations which leads to depolarization.

possesses a small amount of birefringence, which gives rise to two different group velocities for propagating optical pulses polarized along the fast or slow axis. If an optical pulse is polarized along neither axis, its two orthogonal polarization components will experience different amount of group delay which eventually leads to pulse broadening as shown in Fig. 5.1 (a) [112]. This effect is somewhat similar to chromatic dispersion in which pulse broadening is caused by the wavelength-dependent phase velocity, and is therefore called Polarization Mode Dispersion (PMD).

A longer fiber can be considered as a concatenation of a series of short fiber segments, with each segment having a random amount of birefringence oriented in arbitrary directions as shown in Fig. 5.1 (b). As a consequence, the accumulated difference in group delay $\Delta\tau$ (also sometimes referred to as the total link PMD) follows a random walk, and is proportional to the square root of fiber length L [113]:

$$\Delta\tau = D_{pmd}\sqrt{L} \tag{5.1}$$

where the coefficient D_{pmd} is called the PMD parameter of the fiber and is typically expressed in units of ps/$\sqrt{\text{km}}$. The PMD parameters for telecommunication fibers

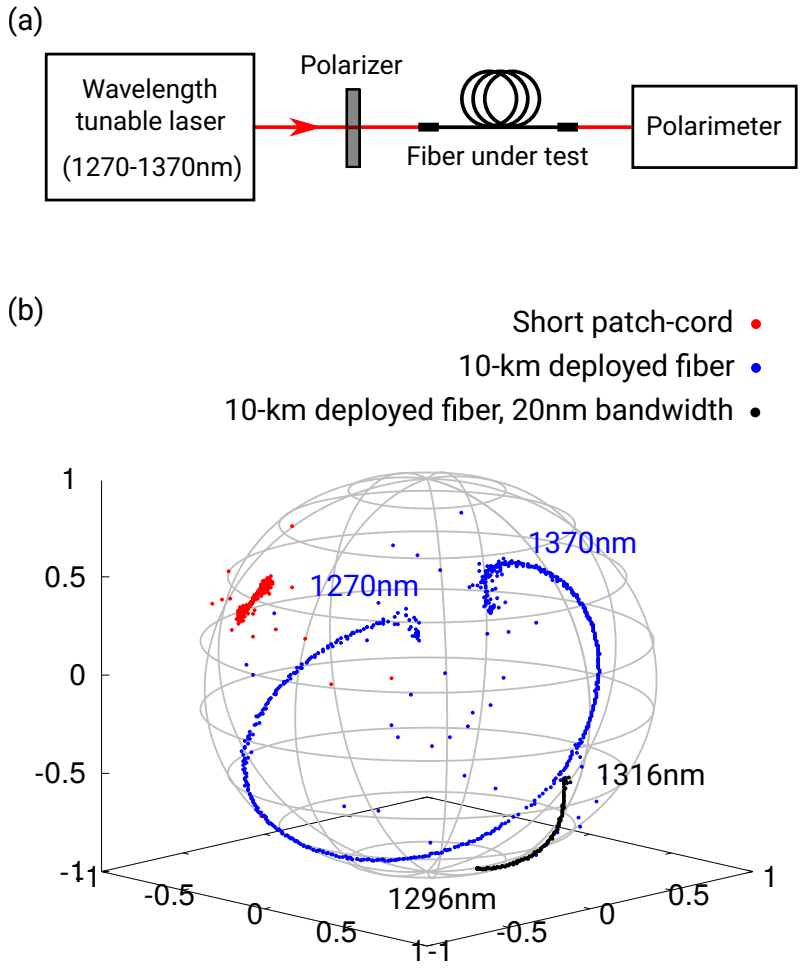

Figure 5.2: (a) Experimental setup for characterizing the effect of fiber depolarization due to PMD. Laser light with tunable wavelength (1270 nm to 1370 nm) propagates through a linear polarizer and is coupled into the fiber under test. At different wavelengths, the polarization of the transmitted light is measured with a polarimeter at the end of the fiber. (b) The measured polarization states with different input wavelengths follow trajectories on the surface of the Poincaré sphere. The measurement was first conducted over a short fiber patch-cord with a negligible amount of PMD (red trace), then over a deployed 10 km fiber with different wavelength ranges (blue and black).

in modern days can be as low as $0.04\,\mathrm{ps}/\sqrt{\mathrm{km}}$ [54], while older fibers may exhibit higher values on the order of $1\,\mathrm{ps}/\sqrt{\mathrm{km}}$ [114]. Even with a moderately long fiber (e.g. $\sim$100 km), PMD causes a difference in group delay on the order of a few picoseconds and is negligible compared to the contribution from chromatic dispersion. As a result, PMD has a limited influence on the timing correlation of entangled photon pairs as long as the chromatic dispersion is not fully compensated.

Depolarization due to PMD

However, PMD can have a significant effect on the polarization state of photons, especially when they are generated from a SPDC process and have a large spectral bandwidth. If the coherence time of these photons τ_c is shorter than the differential group delay $\Delta\tau$ caused by PMD, the two orthogonal polarization components of the photons will no longer overlap coherently and the photons become depolarized. This depolarization effect can also be viewed as the consequence of a change in the output polarization with wavelength [115]. When propagating across a fiber, different spectral components of a photon, despite having the same initial polarization, are transformed into different polarization states at the fiber output due to the presence of PMD.

A common method to characterize this depolarization effect is illustrated in Fig. 5.2 (a) [116]. Light from a wavelength-tunable laser is prepared with a fixed polarization using a linear polarizer. This light propagates across the fiber under test and incident on a polarimeter. At each wavelength within the range of the tunable laser (1270 nm to 1370 nm), the laser light is approximately monochromatic and the polarization at the fiber output is recorded as a point on the surface of the Poincaré sphere.

For a short fiber patch-cord with a negligible amount of PMD, the output polarization stays mostly constant over the entire 100 nm wavelength range as shown by the red trace in Fig. 5.2 (b). The wavelength dependence of output polarization becomes significant when the short patch-cord is replaced with a 10 km deployed fiber, which corresponds to the blue trace in the same figure. With the laser wavelength tuned over 100 nm, the output polarization states cover a large span over the surface of the Poincaré sphere surface. The situation can be improved by narrowing down the wavelength range to 1296-1316 nm as shown by the black trace in Fig. 5.2 (b). This wavelength range corresponds to the 20 nm bandwidth of the signal photons from our SPDC source. With this narrower bandwidth, the output polarization states are more localized and the depolarization effect becomes less severe.

In each measurement, the Degree of Polarization (DOP) can be estimated by taking a vector average of the ensemble of points on the Poincaré sphere, wherein the DOP is the magnitude of the resulting averaged state vector. With a 100 nm

bandwidth, the DOP of light propagating across the short patch-cord (red trace) is about 0.99, which suggests that light is hardly depolarized across the short fiber [1]. With the same optical bandwidth, the DOP drops to about 0.31 across the 10 km deployed fiber (blue trace) and is brought back to about 0.95 when the bandwidth is limited to 20 nm (black trace).

From this measurement, we deduce that the 10 km deployed fiber can be used to transmit photons with 20 nm bandwidth without causing too much depolarization to their states. This deduction is double confirmed with a separate measurement on the total link PMD, which is conducted with a commercial device (FTB-5500B PMD analyzer from EXFO). This measurement yields a total link PMD of about 0.1 ps, which is smaller than the coherence time of the down-converted photons from out SPDC source (~ 0.28 ps for 20 nm bandwidth at 1310 nm). From these measurement results, we conclude that this 10 km deployed fiber exhibits only a small amount of depolarization and therefore can be utilized as the transmission channel for polarization-entangled QKD.

Polarization rotation in an optical fiber

If a photon propagates across a fiber whose link PMD is smaller than its coherence time, then the photon's orthogonal polarization components are still overlapped coherently at the fiber output. The resulting difference in group delay only causes a change in the photon's polarization similar to the effect of a series of randomly oriented waveplates. This effect, combined with the fiber routing geometry, leads to an overall rotation of polarization state when represented as a point on the Poincaré sphere.

This rotation of polarization state is typically time-dependent due to the fact that fiber birefringence can be sensitive to changes in environmental parameters such as temperature and stress. Depending on different types of fiber deployment (i.e. aerial/underground), the rate of change in this polarization rotation can vary significantly [117]. For the same 10 km deployed fiber mentioned in the previous section, we also characterized its stability by sending in light with a fixed polarization across the fiber and monitoring the change in polarization with a polarimeter [118].

[1] Light with DOP=1 suggests that its fully polarized, whereas light with DOP=0 means it is completely depolarized.

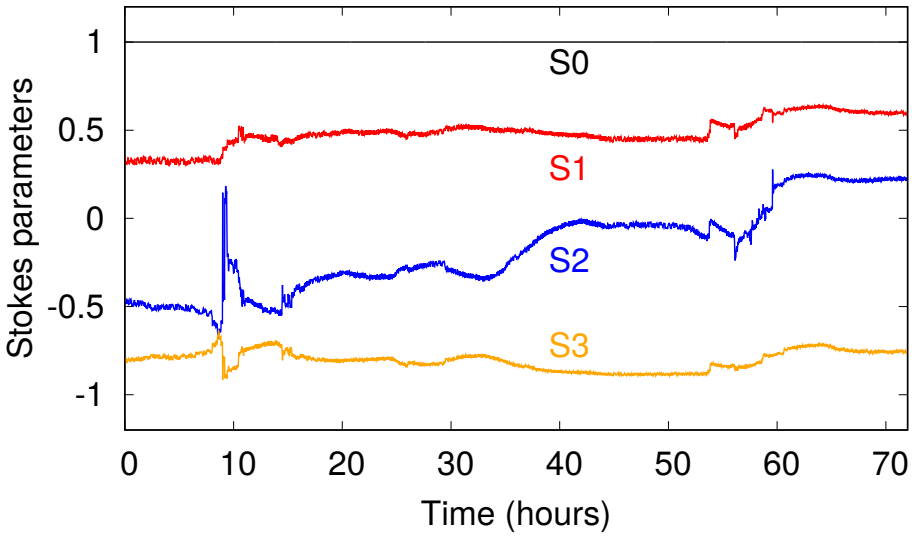

Figure 5.3: Stokes parameters of polarisation state at the fiber output logged over 3 days showing drifts on a time scale of days. The measurement setup is the same as the one shown in Fig. 5.2 (a) with the laser wavelength kept constant at 1310 nm. The measured polarization drifts slowly for the majority of time with sudden jumps occuring occasionally.

The Stokes parameters of the output polarization state is recorded for 3 days and are displayed in Fig. 5.3. The measurement shows a slow drift in polarization for the majority of the time with sudden jumps happening occasionally. For this particular fiber, changes in the output polarization state take place on a time scale of hours.

5.2 Compensating for polarization rotation across fiber

In polarization-encoding QKD, the fiber-induced state rotation causes an increased quantum bit error rate (QBER) and eventually prevents keys from being generated. As a result, this random polarization rotation needs to be actively monitored and compensated. Compensation is usually achieved by placing a polarization controller in the fiber link which is controlled with a feedback loop. The polarization controller implements a unitary transformation which is set to invert the polarization rotation induced by the fiber. The resulting transformation of the entire fiber link is neutralized to identity such that the polarization states of photons transmitted through the fiber remain unchanged.

Typically, the particular setting of a controller that neutralizes the fiber can be found by measuring the polarization of two reference light signals sent across the same fiber. In such schemes, a pair of reference signals are prepared with two non-orthogonal polarization states. Polarization of the transmitted reference signals is constantly monitored while the polarization controller is adjusted accordingly to reach a configuration where it restores the states of both reference signals at the output of the fiber. The reference signals can co-exist with the QKD photons in the same fiber through either time-division or wavelength-division multiplexing [117, 119, 120]. This type of compensation scheme can operate at a high bandwidth at the cost of increased hardware complexity and is suitable for QKD systems with rapidly oscillating environmental noise present in the transmission channel [117].

A different compensation scheme was proposed more recently that does not require any reference light signals [121, 122]. In this scheme, one utilizes the number of erroneous bits in the revealed portion of the sifted keys during the error correction process, which has to be monitored in a QKD protocol anyways to assess potential information leakage to an eavesdropper. This error rate, which is an estimation of the system's QBER, is used as an error signal for the polarization controller. This compensation simplifies the physical setup at the cost of a relatively low bandwidth of the feedback loop [122].

In this work, we adopt a similar polarization compensation technique and implement it in an entanglement-based QKD system. Our scheme uses a set of liquid crystal variable retarders as a polarization controller and is optimized in a feedback loop using the estimated QBER as the error signal. We show that for entanglement-based QKD, this technique exploits the rotational invariance of the distributed entangled state and only requires one of the two fiber links to be compensated. With minimal hardware overhead, this compensation setup is implemented in a QKD system over a deployed telecom fiber link and achieves optimal compensation in under 20 minutes.

Controlling polarization with liquid crystal variable retarders

As shown previously in Fig. 5.3, our 10 km deployed fiber exhibits good polarization stability. The polarization state of the transmitted photons slowly drifts on a time scale of hours. To compensate for this drift, a polarization controller

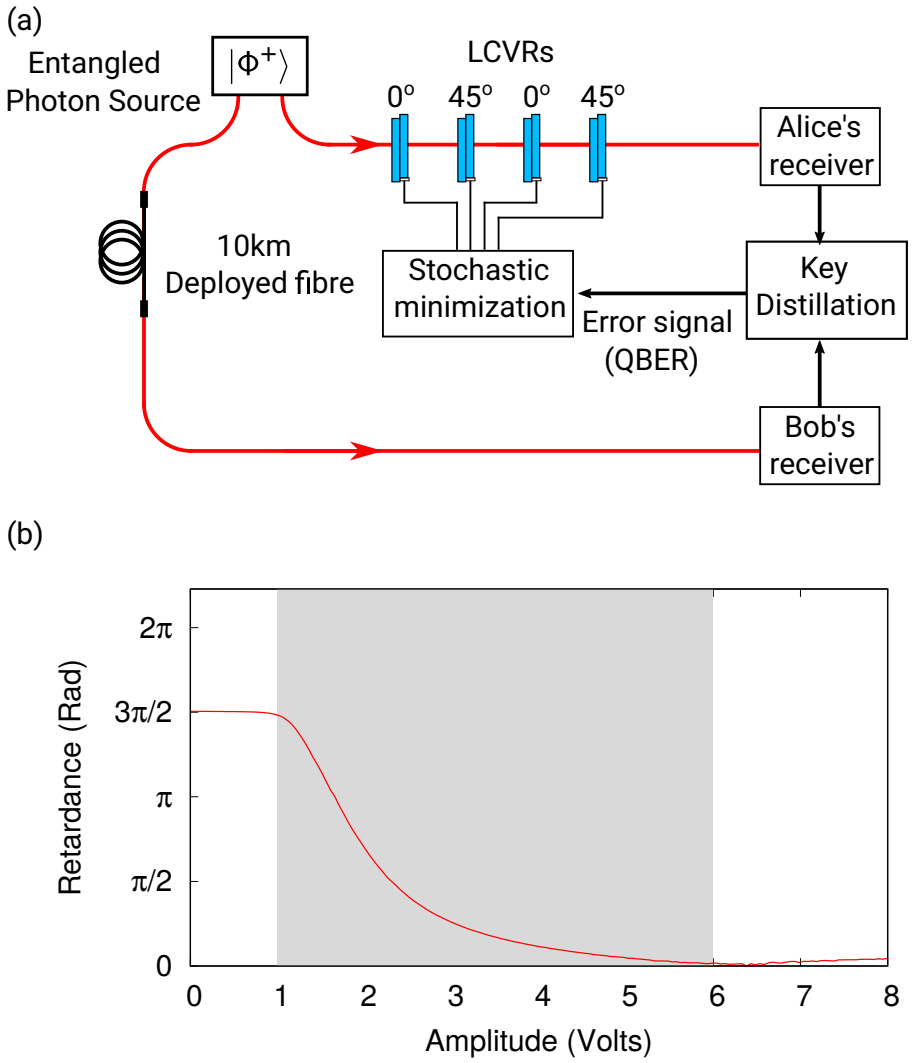

Figure 5.4: (a) A simplified diagram of a polarization-entangled QKD setup with a polarization compensation scheme implemented. The polarization compensation setup consists of 4 liquid crystal variable retarders (LCVRs) placed before Alice's receiver, which serve as a polarization controller. The LCVR voltages are controlled with a feedback loop which seeks to minimize its error signal, which is the QBER of the system. (b) LCVR retardance versus applied voltage amplitudes of 2 kHz square wave at 1310 nm. The LCVRs in this setup are driven with voltage amplitudes between 1 and 6 Volts, which corresponds to a retardance range slightly lower than 2π radians.

based on Liquid Crystal Variable Retarders (LCVRs) is adequate. The reaction time of the LCVRs was measured to be about 5 ms, which is sufficiently fast to compensate for the polarzation drifts we encounter. Moreover, the LCVRs include no macroscopically moving parts and offer high transparency at telecom wavelengths (>95%).

A simplified diagram highlighting the polarization compensation setup in a QKD system is shown in Fig. 5.4 (a). A set of four LCVRs are placed before Alice's receiver to serve as the polarization controller. The LCVRs are driven with 2 kHz square waves with voltage amplitudes varying between 1 and 6 Volts. As shown in Fig. 5.4 (b), each LCVR can provide a voltage-controlled retardance from 0 to about $\frac{3}{2}\pi$ radians at 1310 nm. The LCVRs' optical axes are oriented at 0°, 45°, 0°, and 45° to allow for sufficiently independent polarization transformations.

An arbitrary polarization transfer can be completely described by a rotation direction and angle in the Poincaré sphere, and thus 3 degrees of freedom should be sufficient to encode any transformation required by the polarization controller. However in this setup, we chose to use four retarders to ensure continuous evolution of the control parameters within their limited range, and that a gimbal lock situation is avoided [2]. In this way, any continuously varying unitary transformation between any arbitrary pair of input and output states can be implemented.

Polarization compensation for entangled state

While QKD implementations based on "prepare-and-measure" protocols only require a single fiber connecting the sender and receiver, an implementation based on entangled photon pairs needs two fibers to distribute photons to both receivers. In this case, both fibers will alter the polarization state of propagating photons and therefore intuitively requires two sets of polarization controllers applied to both fiber links, respectively.

However, in our setup shown in Fig. 5.4 (a), only one such polarization controller is applied to the fiber connecting the entangled photon source to Alice's receiver while the other fiber is left un-compensated. For polarization-entangled QKD, we

[2] A gimbal lock situation corresponds to the case where the polarization of incident light is aligned with the optical axis of the first variable retarder, thus effectively eliminating one degree of freedom in the polarization controller.

show that it is in fact sufficient to only apply polarization compensation to one of the fibers as the polarization states of both photons are correlated.

To see this, let us first consider a source that generates photon pairs in a state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. This Bell singlet state is known to be rotationally invariant, meaning that if both photons undergo the same unitary transformation $\hat{T}$ (i.e. a polarization rotation), the overall entangled state remains unchanged:

$$(\hat{T} \otimes \hat{T})|\psi^-\rangle = |\psi^-\rangle$$

For two photons A and B that undergo different fiber-induced polarization rotations $\hat{R}_A$ and $\hat{R}_B$, the resulting two-photon state is $(\hat{R}_A \otimes \hat{R}_B)|\psi^-\rangle$. In order to perform polarization compensation, a polarization controller acting on photon A can be set to a particular transformation $\hat{T}_A$ such that $\hat{T}_A\hat{R}_A = \hat{R}_B$. The resulting state:

$$(\hat{T}_A\hat{R}_A \otimes \hat{R}_B)|\psi^-\rangle = (\hat{R}_B \otimes \hat{R}_B)|\psi^-\rangle = |\psi^-\rangle \tag{5.2}$$

is again the singlet state $|\psi^-\rangle$ due to its rotational invariance. Thus, for QKD using a polarization-entangled $|\psi^-\rangle$ state, a single polarization compensation operation on one side is sufficient to remove the effect of fiber-induced rotations $\hat{R}_A$ and $\hat{R}_B$ on both transmission channels.

This result can be easily extended to other Bell states such as $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ in our entangled photon source. The state $|\Phi^+\rangle$ can be transformed into $|\psi^-\rangle$ by applying a unitary transformation $\hat{\sigma}_A$ to photon A alone:

$$|\psi^-\rangle = (\hat{\sigma}_A \otimes \hat{I}_B)|\Phi^+\rangle$$

with $\hat{\sigma}_A = |H\rangle\langle V| - |V\rangle\langle H|$ and $\hat{I}_B$ being an identity transformation on photon B. Similar to Eq. 5.2, compensation can be achieved by setting a single polarization controller transformation $\hat{T}_A$ such that $\hat{T}_A\hat{R}_A = \hat{\sigma}_A^{-1}\hat{R}_B\hat{\sigma}_A$. The overall change of polarization state becomes:

$$\begin{aligned}
(\hat{T}_A\hat{R}_A \otimes \hat{R}_B)|\Phi^+\rangle &= (\hat{\sigma}_A^{-1}\hat{R}_B\hat{\sigma}_A \otimes \hat{R}_B)|\Phi^+\rangle \\
&= (\hat{\sigma}_A^{-1}\hat{R}_B \otimes \hat{R}_B)|\psi^-\rangle \\
&= (\hat{\sigma}_A^{-1} \otimes \hat{I}_B)|\psi^-\rangle \\
&= |\Phi^+\rangle
\end{aligned}$$

and is therefore compensated with polarization controller applied to only one fiber.

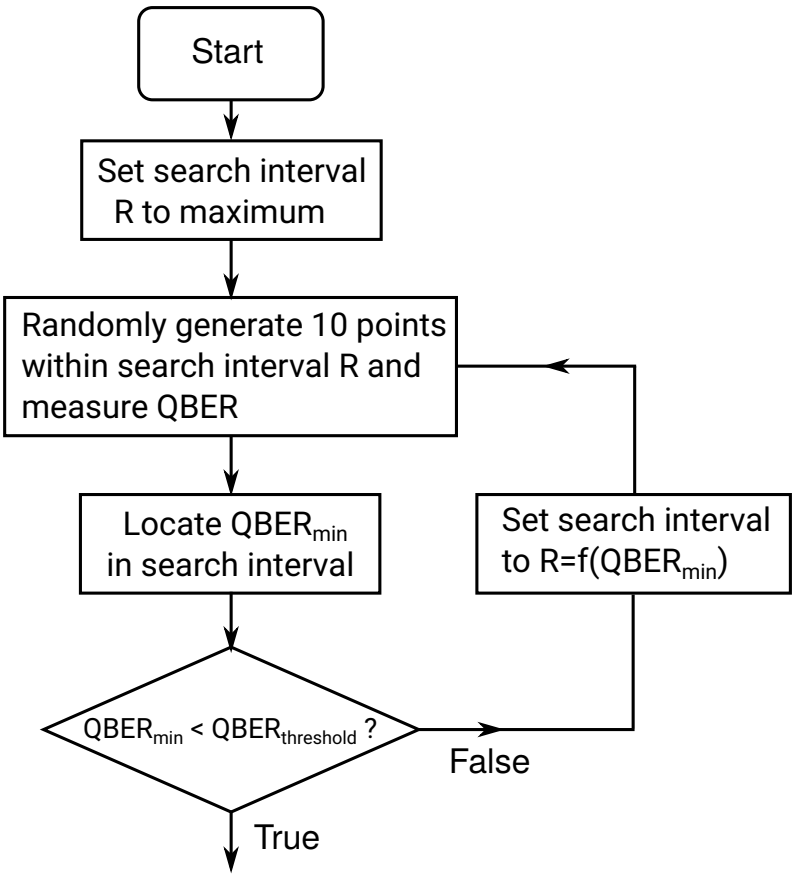

Figure 5.5: Flow chart of the stochastic search algorithm.

QBER minimization with stochastic method

In the polarization compensation setup shown in Fig. 5.4 (a), the LCVRs are utilized as the actuator in a control loop in which the measured system QBER is used as an error signal. This control loop for polarization compensation can be considered as an optimization problem that aims to find the minimum of the estimated QBER of the QKD system. The system QBER is considered as a function of four variables, $\mathrm{QBER} = f(V_1, V_2, V_3, V_4)$, namely the control voltages $V_{1...4}$ of the LCVRs. While this problem can be solved using any efficient optimization algorithms in principle, such as the gradient-descend method, we adopted a different approach in this work due to practical considerations.

Firstly, it is impractical to obtain an accurate expression of the estimated QBER as a function of the control voltages as the voltage response curve of an LCVR varies from unit to unit. Secondly, the estimated QBER cannot be measured with very

high accuracy due to the limitation of finite sample sizes. These limitations make it difficult to compute the gradients of $f(V_1, V_2, V_3, V_4)$ from measurements, and a gradient-descend algorithm cannot be efficiently implemented. Instead, we use a stochastic search algorithm which is depicted in Fig. 5.5.

The algorithm conducts a random search within a finite 4-dimensional parameter space (V_1, V_2, V_3, V_4). Each control voltage takes a value between 1 V and 6 V which corresponds to retardation from 0 to about $\frac{3}{2}\pi$ at 1310 nm. The search algorithm randomly samples a set of points in the entire parameter space and measures the QBER for each point. Among each set, the point with the smallest QBER will be chosen as the center of the next iteration of parameter search, which will be conducted with the same number of points within a parameter hypercube of smaller size R. This size R decreases with decreasing minimal QBER obtained in each iteration. As the algorithm proceeds, the center point of the search will gradually approach the minimum in the entire space.

During QKD operation, the two receivers registered a coincidence rate of $670\,\mathrm{s}^{-1}$ between Alice and Bob, which yields a sifted key rate of about $340\,\mathrm{s}^{-1}$ after basis reconciliation. To reduce Poissonian noise, the system QBER is evaluated from sifted keys accumulated over every 2 seconds. In an exemplary QKD operation, a typical starting condition before polarization compensation leads to a QBER of $58 \pm 2.6\%$, where the uncertainty is inferred from the Poissonian counting statistics. With this initial QBER, the stochastic search begins its first iteration with a set of 10 points.

The reduction of the search range R within the parameter space in each iteration is accomplished with an ad-hoc chosen function $R = A \times (\mathrm{QBER}_{\mathrm{min}} - \mathrm{QBER}_{\mathrm{threshold}})^B$, where $\mathrm{QBER}_{\mathrm{min}}$ is the minimal QBER in any given iteration. The coefficients A and B set the rate at which the search algorithm converges to the global minimum, while the offset $\mathrm{QBER}_{\mathrm{threshold}}$ sets a lower bound of the QBER value determined by other elements than the optical fiber in the QKD system. The last choice assures that the parameter space is still probed in a reasonable neighborhood of the global QBER minimum. Continuously operation of this algorithm allows the polarization controller to follow the drift of this minimum location in the parameter space over time in a control-loop-like fashion. We found that in our system, a choice of $A = 6.5\,\mathrm{Volts}$, $B = 2$, and $\mathrm{QBER}_{\mathrm{threshold}} = 4\%$ worked well.

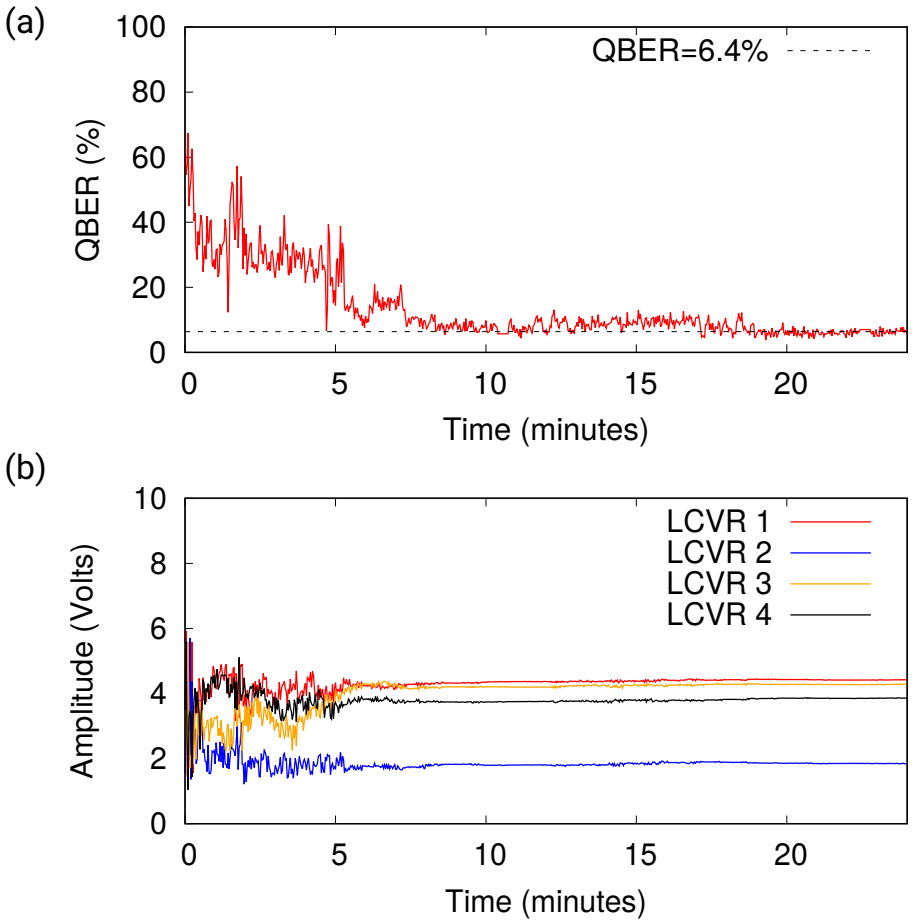

Figure 5.6: (a) System QBER recorded during the stochastic search. The QKD operation starts with an initial QBER of about 58% which signals a severe basis mismatch. This value is reduced to about 7% after 30 iterations of search which takes about 10 minutes. The compensation scheme eventually lowers the QBER to about 6.4% and the system remains stable for over five hours afterwards. (b) Applied voltage amplitudes for the LCVRs during stochastic search. The control voltages converge to stable values as the QBER approaches its minimum.

Fig. 5.6 (a) shows the performance of our polarisation compensation technique in an exemplary single run. The stochastic search algorithm reduces the system QBER from an initial value of $58 \pm 2.6\%$ to about $7 \pm 0.7\%$ after about 10 minutes (about 30 iterations of search). We then observed a small increase of QBER by about 3% around the 15 minutes mark, possibly due to a small disturbance experienced by the fiber. Despite that, the algorithm eventually lowers the QBER down to $6.4 \pm 0.7\%$. The corresponding control voltages of the LCVRs during the search process are shown in Fig. 5.6 (b). They converge to stable values as the QBER approaches its

minimum given by other system constraints.

5.3 Stable polarization entanglement-based QKD over deployed fiber

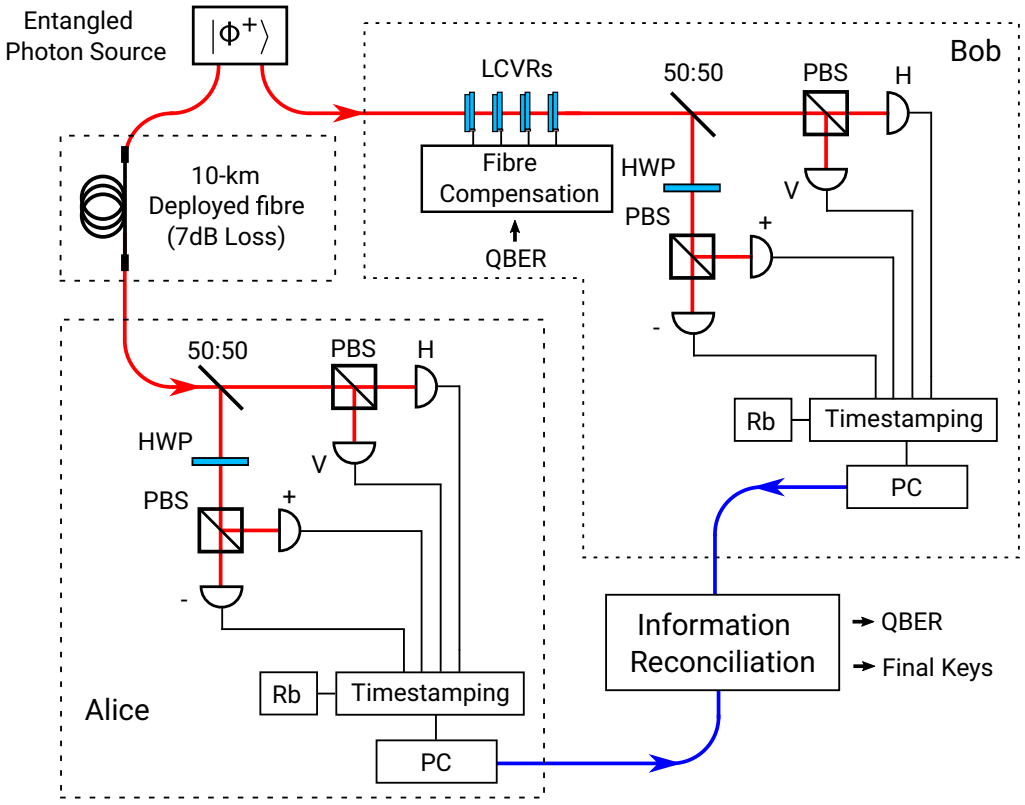

Figure 5.7: QKD setup over 10 km deployed fiber link. The fiber loops back to the lab to simplify the experimental procedure. The Alice and Bob nodes are run on independent clocks. Alice's analyzer is connected to the entanglement source via the 10 km deployed fiber while Bob's setup is locally connected using a short patch cord. The two hosting PCs are connected to the same local area network in order to exchange timestamp data for coincidence identification.

With a working polarization compensation scheme, we are now able to demonstrate a stable operation of polarization-entangled QKD over a deployed fiber. The full setup of the QKD system is shown in Fig. 5.7. A polarization-entangled photon source generates pairs of signal and idler photons in a $|\Phi^+\rangle$ state. With a pump power of 2.4 mW, we observed a local pair rate of 4300 s^{-1}. The entangled photon pairs are distributed to two nodes, Alice and Bob, with a polarization analyzer

placed on each side. The signal photons are transmitted through a 10 km telecom fiber that connects the source to Alice's analyzer while Bob's setup is connected locally via a short patchcord carrying the idler photons.

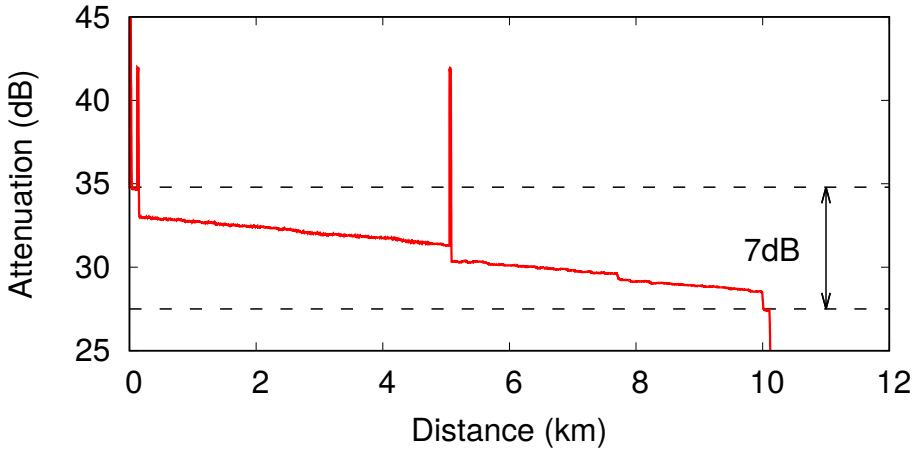

Figure 5.8: Optical time-domain reflectometer trace of the deployed fiber, identifying a high reflection loss point about 5 km away from both endpoints. Two more points with high reflection/absorption loss are also identified about 100 meters from the endpoints, which is due to a patching cable between the deployed fiber and the laboratory setup.

The 10 km telecom fiber is deployed underground by Singapore Telecommunications Limited in a loop configuration with both ends located at Center for Quantum Technologies, National University of Singapore. Measurement using an optical time-domain reflectometer (OTDR) shows a total fiber length of 10.4 km with about -7 dB channel loss (Fig. 5.8). The optical absorption of the fiber contributes only about -4 dB to the total channel loss, with another -3 dB loss due to reflections at patching points and losses at splicing points.

Upon receiving the photons, Alice and Bob follow the BBM92 protocol by measuring polarization in one of the two bases: H/V and D/A [24]. The random detection basis choice is made by a non-polarizing beam splitter in each setup which transmits and reflects photons with equal probability [123]. Four Indium Gallium Arsenide Avalanche Photodiodes (InGaAs APDs) are used in each analyzer setup for single photon detection. The APDs diodes are cooled down to below -40 °C and are operated in freerunning mode with a nominal detection efficiency of around 10% and an average dark count rate of about 12000 s^{-1}. On each side, detected photons are

time-tagged to a resolution of 125 ps with a 4-channel timestamping device locked to a rubidium frequency standard [108].

The recorded timestamps of arriving photons are continuously exchanged through a network connection between two hosting lab computers. To enable coincidence identification, the clocks on both sides are synchronized in advance by exploiting the intrinsic timing correlations of the SPDC photons [124]. Uncertainty in the coincidence time difference is about 1.9 ns (FWHM) due to fiber chromatic dispersion, detector timing jitter, and other noise in the system [2]. For coincidence identification, a coincidence window of 0.5 ns was chosen to optimize the coincidence/accidental ratio without losing too many coincidence events.

Raw key data are generated after coincidence identification and key sifting following a typical BBM92 protocol. Error correction is then performed in real time on each block of raw key data accumulated over 25 seconds utilizing a modified CASCADE/BICONF algorithm [108, 125, 126]. An estimated QBER is also obtained during error correction and is used to determine the amount of secure key bits to be extracted from the raw key bits. Privacy amplification is then performed on both sides for obtaining the final secure keys [127].

We estimate a total system loss of -33 dB in our entire QKD system, with -7 dB contributed by the total channel loss of the deployed fiber, -6 dB from the optical coupling loss in the polarisation compensation and analyzer setup, and another -20 dB solely due to the detection efficiency of the InGaAs APDs on both sides. Therefore, detector efficiency is the dominant contribution to the overall system loss in our setup.

With the 10 km deployed fiber connected and the source pump power kept at 2.4 mW, the rate of detected single photons is about $40\,000\,\mathrm{s}^{-1}$ on Alice's analyzer, and $242\,000\,\mathrm{s}^{-1}$ at Bob's side, respectively. We observe a coincidence rate of $670\,\mathrm{s}^{-1}$ and an accidental coincidence rate of $19\,\mathrm{s}^{-1}$. After an initial fiber compensation, the QKD setup operated continuously over 5.7 hours until one of the detectors ceased operation due to a temperature overrun. The average sifted key rate after basis reconciliation is $340\,\mathrm{s}^{-1}$ with an average estimated QBER of 6.3%. About 1.4% of the error bits are contributed by the accidental coincidences and only 0.4% are due to state preparation from the entanglement source. The remaining 4.5% in QBER is caused by imperfections in polarization optics and fiber compensation, as well as

possible depolarization in the fiber link [48]. The final key rate after error correction and privacy amplification is about 109 bits/second (Fig. 5.9).

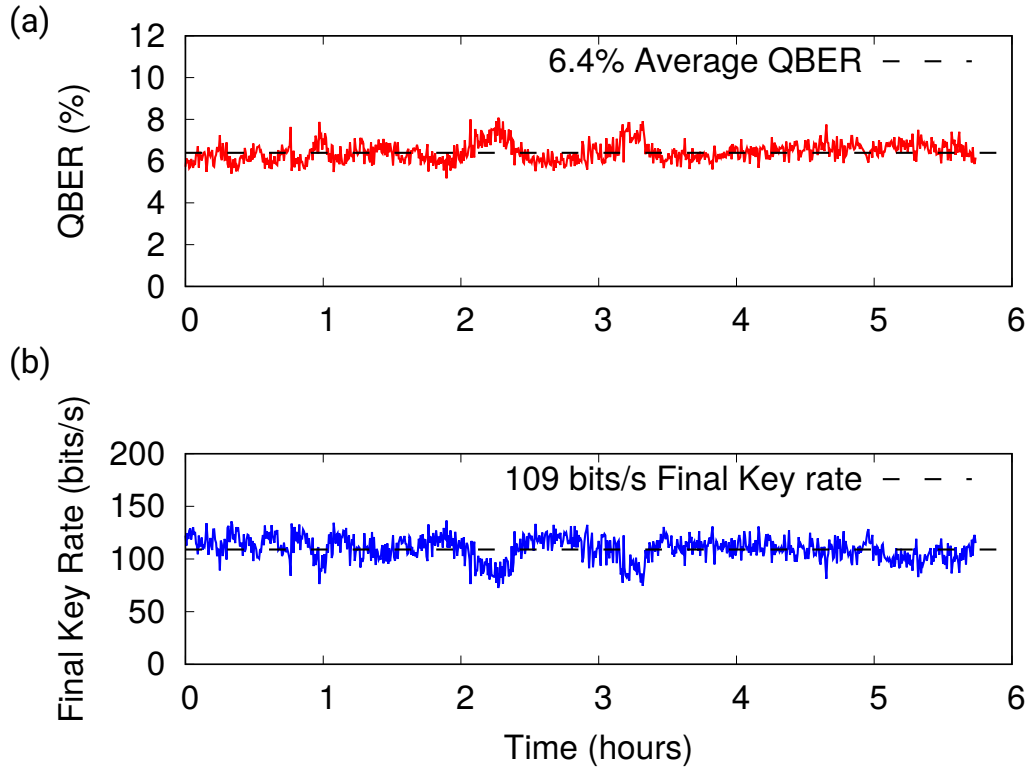

Figure 5.9: QBER (a) and finaly key rate (b) logged over 5.7 hours of continuous operation. Error correction and privacy amplification are performed over blocks of raw key bits integrated over 25 seconds. Data collection stopped after 5.7 hours due to a detector failure.

This final key rate is comparable to other reported entanglement-based implementations at telecom C-band [128, 129] or at wavelengths detectable by Silicon APDs [130]. Secure transfer of messages with this key rate is practical using one-time pad encryption for low bandwidth communications such as command & control of industrial systems. Alternatively, the key can be utilized in fast encryption schemes using e.g. AES-256, with a much more frequent re-keying compared to conventional methods [131].

The final key rate in our demonstration is mainly limited by the low detection efficiencies (∼10%) and high dark count rates ($\sim 10^4\,\mathrm{s}^{-1}$) of the InGaAs APDs in our setup. A significant increase in key rate is expected when replacing them with superconducting nanowire detectors (∼80% detection efficiency) [33], which would

yield a final key rate on the order of kbits/s over the same fiber distance. Increasing the operating distance of our QKD setup can be made possible by not only lowering the system loss, but also narrowing down the spectral width of the down-converted photons, which was shown in reference [128, 129].

Chapter 6

Conclusion

This thesis presented several studies on the implementation of polarization-entangled QKD over telecommunication fibers. Such a QKD implementation can make use of the existing telecommunication fiber network and provide secure key generation for users within a metropolitan area.

In order to utilize a deployed fiber as the optical transmission channel for QKD, we need to generate and detect polarization-entangled photon pairs around 1310 nm which is at the O-band of standard telecommunication fibers. In chapter 2, I presented our entangled photon pair source based on spontaneous parametric downconversion which generates pairs of signal and idler photons centered about 1316 nm. Our source is capable of generating photon pairs with polarization-entangled state $|\Phi^+\rangle$ at a rate as high as 57000 pairs/s/mW. The same chapter also contains a brief overview of avalanche photodiodes based on Indium Gallium Arsenide (InGaAs), which are utilized in this work to detect single photons at telecommunication wavelengths.

Chapter 3 reported an investigation of a vulnerability in InGaAs single photon detectors known as the breakdown flash, which refers to a phenomenon whereby a detector emits photons upon detection of a single photon. We measured the rate of breakdown flash with a pair of commercial InGaAs detectors acting as both emission and detection units and found it contained at least 0.04 photons per flash event. We also found the spectral distribution of the breakdown flash photons to be wideband (1000 nm to 1600 nm), which allows for efficient suppression via simple spectral filtering.

The distribution of photon pairs across telecommunication fibers without degrading their timing correlation and altering their polarization states has been a major challenge for fiber-based QKD. In chapter 4, we address the effect on the

timing correlation of photon pairs, which is mainly due to chromatic dispersion in a long fiber. Fiber chromatic dispersion broadens the temporal profile of a photon which leads to an increased timing discrepancy. This makes it difficult to identify whether two sister photons are generated from the same pair and eventually reduce the number of coincidence events in a QKD system. This degradation in timing correlation is mitigated by operating QKD at telecom O-band, which is near the fiber's zero-dispersion wavelength around 1310 nm. For entangled photon pairs generated from our source, the signal photons propagate across 10 km of deployed fiber and remain coincident with idler photons with a timing discrepancy of about 1.9 ns. We also show that this effect can be even alleviated through nonlocal dispersion cancellation, in which the signal and idler photons undergo an equal amount of chromatic dispersion with opposite signs.

Apart from degrading a photon pair's timing correlation, a telecommunication fiber can also alter its polarization states. In chapter 5 we discussed the effect of fiber polarization mode dispersion, which rotates the polarization state of propagating photons randomly and can even cause depolarization for photons with large bandwidth. While the effect of depolarization was avoided by limiting the bandwidth of photons pairs to about 20 nm, the random state rotation caused by the fiber requires active compensation. We investigated the rate of such polarization rotation over a deployed 10 km fiber, and then set up a full QKD system utilizing this fiber as the optical channel. Within the QKD setup, a set of liquid crystal variable retarders are implemented as a polarization controller. This controller serves as the actuator in a feedback loop that seeks to compensate the polarization rotation by minimizing the quantum bit error rate of the QKD system.

With an active polarization compensation scheme, we eventually demonstrated stable QKD operation over a deployed fiber in which the BBM92 protocol is adapted. The QKD operation begins with an initial quantum bit error rate of about 58%, which descends to about 6.4% after 20 minutes of active polarization compensation. With the error rate minimized, the QKD operation remains stable for about 5.7 hours during which an average key generation rate of 109 bits/s is achieved.

Outlook

The results reported in this thesis form a proof-of-concept demonstration of integrating polarization-entangled QKD into an existing telecommunication fiber. While the reported final key rate of 109 bits/s can support one-time pad encryptions for low bandwidth communications such as industrial command & control, this key rate can be improved substantially.

Some of the limiting factors of the current QKD setup include the low efficiency and high dark count rate of the detectors, and the large bandwidth of entangled photons. The InGaAs detectors in our experiment have a nominal detection efficiency of about 10%, which contributes about 20 dB to the total system loss alone. Significant improvement can be achieved if the InGaAs detectors are replaced with superconducting nanowire detectors that can offer a detection efficiency of about 80% and a negligible dark count rate. Such an improvement in efficiency can increase the detected coincidence rate by a factor of 64. Meanwhile, the low dark count rates of nanowire detectors also lead to a lower quantum bit error rate. This makes it possible to increase the key generation rate into the kbits/s range or even higher.

The bandwidth of the entangled photon pairs is another factor potentially limiting the range of QKD implementation. As shown in chapter 4 and 5, photons with larger bandwidths are prone to dispersion effects in the fiber. While the effect of chromatic dispersion can be mitigated by carefully exploiting non-local dispersion cancellation at the telecom O-band, the depolarization effect caused by polarization mode dispersion is statistical in nature and cannot be compensated. As a result, a photon's coherence time needs to be longer than the differential group delay caused by polarization mode dispersion to avoid strong depolarization. Although this requirement has been greatly relaxed in present days due to the advancement in fiber technology [54, 114], having a narrow band entangled photon source with high spectral brightness is still preferred in general.

Implementing QKD over a single telecommunication fiber is a prelude to a potential quantum network, in which entangled photons are directed to different pairs of users through fiber network switching. The entangled photons can be consumed for QKD services provided to multiple users simultaneously via wavelength/time division multiplexing [132], or even utilized to mediate entanglement between atomic/ionic

systems at distant nodes. For our choice of operating QKD at the telecom O-band, it is also possible in principle to have QKD photons co-exist with the classical communication traffic at the telecom C-band, which further reduces the overhead cost of setting up a QKD network.

Bibliography

[1] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer. "Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes". In: *Opt. Express* 25.24 (Nov. 2017), pp. 30388–30394.

[2] J. A. Grieve, Y. Shi, H. S. Poh, C. Kurtsiefer, and A. Ling. "Characterizing nonlocal dispersion compensation in deployed telecommunications fiber". In: *Applied Physics Letters* 114.13 (2019), p. 131106.

[3] Y. Shi, H. S. Poh, A. Ling, and C. Kurtsiefer. "Fibre polarisation state compensation in entanglement-based quantum key distribution". In: *Opt. Express* 29.23 (Nov. 2021), pp. 37075–37080.

[4] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling. "Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber". In: *Applied Physics Letters* 117.12 (2020), p. 124002.

[5] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[6] G. S. Vernam. "Cipher printing telegraph systems: For secret wire and radio telegraphic communications". In: *Journal of the A.I.E.E.* 45.2 (1926), pp. 109–115.

[7] W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[8] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782.

[9] "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms". National Institute of Standards and Technology. 2013.

[10] S. Vaudenay. “Responses to NIST’s proposal”. In: *Communicationsof the ACM* 35 (July 1992), pp. 50–52.

[11] P. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134.

[12] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984*. 1984, pp. 175–179.

[13] S. Wiesner. “Conjugate Coding”. In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. ISSN: 0163-5700.

[14] P. W. Shor and J. Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. In: *Phys. Rev. Lett.* 85 (2 July 2000), pp. 441–444.

[15] D. Mayers. “Unconditional Security in Quantum Cryptography”. In: *J. ACM* 48.3 (May 2001), pp. 351–406. ISSN: 0004-5411.

[16] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (Oct. 1982), pp. 802–803. ISSN: 1476-4687.

[17] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”. In: *Phys. Rev. Lett.* 92 (5 Feb. 2004), p. 057901.

[18] H.-K. Lo, X. Ma, and K. Chen. “Decoy State Quantum Key Distribution”. In: *Phys. Rev. Lett.* 94 (23 June 2005), p. 230504.

[19] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. “Generalized Privacy Amplification”. In: *IEEE Transactions on Information Theory* 41.6 (Nov. 1995). Preliminary version: [**BBCM94**].

[20] D. Mayers. “Quantum Key Distribution and String Oblivious Transfer in Noisy Channels”. In: *Advances in Cryptology — CRYPTO ’96*. Ed. by N. Koblitz. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 343–357. ISBN: 978-3-540-68697-2.

[21] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". In: *Phys. Rev. Lett.* 77 (13 Sept. 1996), pp. 2818–2821.

[22] H.-K. Lo and H. F. Chau. "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* 283.5410 (1999), pp. 2050–2056.

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

[24] C. H. Bennett, G. Brassard, and N. D. Mermin. "Quantum cryptography without Bell's theorem". In: *Phys. Rev. Lett.* 68 (5 Feb. 1992), pp. 557–559.

[25] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin. "Experimental Quantum Cryptography". In: *J. Cryptology* 5 (1992), pp. 3–28.

[26] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. "Limitations on Practical Quantum Cryptography". In: *Phys. Rev. Lett.* 85 (6 Aug. 2000), pp. 1330–1333.

[27] N. Lütkenhaus. "Security against individual attacks for realistic quantum key distribution". In: *Phys. Rev. A* 61 (5 Apr. 2000), p. 052304.

[28] A. J. Shields. "Semiconductor quantum light sources". In: *Nature Photonics* 1.4 (Apr. 2007), pp. 215–223. ISSN: 1749-4893.

[29] D. C. Burnham and D. L. Weinberg. "Observation of Simultaneity in Parametric Production of Optical Photon Pairs". In: *Phys. Rev. Lett.* 25 (2 July 1970), pp. 84–87.

[30] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experimental quantum cryptography". In: *Journal of Cryptology* 5.1 (Jan. 1992), pp. 3–28. ISSN: 1432-1378.

[31] R. J. McIntyre. "Theory of Microplasma Instability in Silicon". In: *Journal of Applied Physics* 32.6 (1961), pp. 983–995.

[32] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa. "Evolution and prospects for single-photon avalanche diodes and quenching circuits". In: *Journal of Modern Optics* 51.9-10 (2004), pp. 1267–1288.

[33] V. B. Verma, B. Korzh, F. Bussieres, R. D. Horansky, A. E. Lita, F. Marsili, M. D. Shaw, H. Zbinden, R. P. Mirin, and S. W. Nam. "High-efficiency WSi superconducting nanowire single-photon detectors operating at 2.5K". In: *Applied Physics Letters* 105.12 (2014), p. 122601.

[34] B. Cabrera, R. M. Clarke, P. Colling, A. J. Miller, S. Nam, and R. W. Romani. "Detection of single infrared, optical, and ultraviolet photons using superconducting transition edge sensors". In: *Applied Physics Letters* 73.6 (1998), pp. 735–737.

[35] J. Breguet, A. Muller, and N. Gisin. "Quantum Cryptography with Polarized Photons in Optical Fibres". In: *Journal of Modern Optics* 41.12 (1994), pp. 2405–2412.

[36] J. Franson and H. Ilves. "Quantum Cryptography Using Polarization Feedback". In: *Journal of Modern Optics* 41.12 (1994), pp. 2391–2396.

[37] A. Muller, H. Zbinden, and N. Gisin. "Underwater quantum coding". In: *Nature* 378.6556 (Nov. 1995), pp. 449–449. ISSN: 1476-4687.

[38] J. G. Rarity, P. M. Gorman, and P. R. Tapster. "Secure key exchange over 1.9 km free-space range using quantum cryptography". In: *Electronics Letters* 37 (8 2001), p. 512.

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

[40] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. "A step towards global key distribution". In: *Nature* 419 (6906 2002), p. 450.

[41] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km". In: *Phys. Rev. Lett.* 98 (1 Jan. 2007), p. 010504.

[42] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (2017), pp. 43–47. ISSN: 1476-4687.

[43] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication". In: *Phys. Rev. Lett.* 82 (12 Mar. 1999), pp. 2594–2597.

[44] T. C. Ralph. "Continuous variable quantum cryptography". In: *Phys. Rev. A* 61 (1 Dec. 1999), p. 010303.

[45] M. Hillery. "Quantum cryptography with squeezed states". In: *Phys. Rev. A* 61 (2 Jan. 2000), p. 022309.

[46] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication". In: *New Journal of Physics* 15.2 (Feb. 2013), p. 023006.

[47] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du šek, N. Lütkenhaus, and M. Peev. "The security of practical quantum key distribution". In: *Rev. Mod. Phys.* 81 (3 Sept. 2009), pp. 1301–1350.

[48] N. Gisin, J. Von der Weid, and J. Pellaux. "Polarization mode dispersion of short and long single-mode fibers". In: *Journal of Lightwave Technology* 9.7 (1991), pp. 821–827.

[49] M. Brodsky, E. C. George, C. Antonelli, and M. Shtaif. "Loss of polarization entanglement in a fiber-optic system with polarization mode dispersion in one optical path". In: *Opt. Lett.* 36.1 (Jan. 2011), pp. 43–45.

[50] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experimental Quantum Cryptography". In: *J. Cryptol.* 5.1 (Jan. 1992), pp. 3–28. ISSN: 0933–2790.

[51] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. "Ground to satellite secure key exchange using quantum cryptography". In: *New Journal of Physics* 4 (Oct. 2002), pp. 82–82.

[52] D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin. "CubeSat quantum communications mission". In: *EPJ Quantum Technology* 4.1 (Apr. 2017), p. 6. ISSN: 2196-0763.

[53] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. "Satellite-based entanglement distribution over 1200 kilometers". In: *Science* 356.6343 (2017), pp. 1140–1144.

[54] "Corning SMF-28e Optical Fiber Produt Information". Corning Inc. 2005.

[55] "G.Sup39 : Optical system design and engineering considerations". International Telecommunication Union. 2016.

[56] E. Desurvire and J. Simpson. "Amplification of spontaneous emission in erbium-doped single-mode fibers". In: *Journal of Lightwave Technology* 7.5 (1989), pp. 835–845.

[57] "Optical Fiber Transmission". In: *Fiber Optic Communications*. John Wiley Sons, Ltd, 2014. Chap. 2, pp. 35–92. ISBN: 9781118684207.

[58] J. F. Clauser. "Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect". In: *Phys. Rev. D* 9 (4 Feb. 1974), pp. 853–860.

[59] R. Ghosh and L. Mandel. "Observation of nonclassical effects in the interference of two photons". In: *Phys. Rev. Lett.* 59 (17 Oct. 1987), pp. 1903–1905.

[60] D. Magde and H. Mahr. "Study in Ammonium Dihydrogen Phosphate of Spontaneous Parametric Interaction Tunable from 4400 to 16 000 Å". In: *Phys. Rev. Lett.* 18 (21 May 1967), pp. 905–907.

[61] C. K. Hong, Z. Y. Ou, and L. Mandel. "Measurement of subpicosecond time intervals between two photons by interference". In: *Phys. Rev. Lett.* 59 (18 Nov. 1987), pp. 2044–2046.

[62] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. "New High-Intensity Source of Polarization-Entangled Photon Pairs". In: *Phys. Rev. Lett.* 75 (24 Dec. 1995), pp. 4337–4341.

[63] Y. Shen. "The Principles of Nonlinear Optics". Wiley classics library. Wiley, 2003. ISBN: 9780471430803.

[64] P. A. Franken and J. F. Ward. "Optical Harmonics and Nonlinear Phenomena". In: *Rev. Mod. Phys.* 35 (1 Jan. 1963), pp. 23–39.

[65] R. S. Bennink. "Optimal collinear Gaussian beams for spontaneous parametric down-conversion". In: *Phys. Rev. A* 81 (5 May 2010), p. 053805.

[66] P. B. Dixon, D. Rosenberg, V. Stelmakh, M. E. Grein, R. S. Bennink, E. A. Dauler, A. J. Kerman, R. J. Molnar, and F. N. C. Wong. "Heralding efficiency and correlated-mode coupling of near-IR fiber-coupled photon pairs". In: *Phys. Rev. A* 90 (4 Oct. 2014), p. 043804.

[67] A. Lohrmann, C. Perumangatt, A. Villar, and A. Ling. "Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer". In: *Applied Physics Letters* 116.2 (2020), p. 021101.

[68] M. Fiorentino and R. G. Beausoleil. "Compact sources of polarization-entangled photons". In: *Opt. Express* 16.24 (Nov. 2008), pp. 20149–20156.

[69] H. Iams and B. Salzberg. "The Secondary Emission Phototube". In: *Proceedings of the Institute of Radio Engineers* 23.1 (1935), pp. 55–64.

[70] V. Zworykin, G. Morton, and L. Malter. "The Secondary Emission Multiplier-A New Electronic Device". In: *Proceedings of the Institute of Radio Engineers* 24.3 (1936), pp. 351–375.

[71] L. Kubetsky. "Multiple Amplifier". In: *Proceedings of the Institute of Radio Engineers* 25.4 (1937), pp. 421–433.

[72] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. "Invited Review Article: Single-photon sources and detectors". In: *Review of Scientific Instruments* 82.7 (2011), p. 071101.

[73] S. V. Polyakov. "Chapter 3 - Photomultiplier Tubes". In: *Single-Photon Generation and Detection*. Ed. by A. Migdall, S. V. Polyakov, J. Fan, and J. C. Bienfang. Vol. 45. Experimental Methods in the Physical Sciences. Academic Press, 2013, pp. 69–82.

[74] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski. "Picosecond superconducting single-photon optical detector". In: *Applied Physics Letters* 79.6 (2001), pp. 705–707.

[75] B. Korzh, Q.-Y. Zhao, J. P. Allmaras, S. Frasca, T. M. Autry, E. A. Bersin, A. D. Beyer, R. M. Briggs, B. Bumble, M. Colangelo, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, D. Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, S. W. Nam, A. G. Kozorezov, M. D. Shaw, and K. K. Berggren. "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector". In: *Nature Photonics* 14.4 (Apr. 2020), pp. 250–255. ISSN: 1749-4893.

[76] A. E. Lita, A. J. Miller, and S. W. Nam. "Counting near-infrared single-photons with 95% efficiency". In: *Opt. Express* 16.5 (Mar. 2008), pp. 3032–3040.

[77] "Si APD Technical note". Hamammatsu. 2021.

[78] R. Hadfield. "Single-photon detectors for optical quantum information applications". In: *Nature Photonics* 3.12 (Dec. 2009), pp. 696–705. ISSN: 1749-4885.

[79] K. Nishida, K. Taguchi, and Y. Matsumoto. "InGaAsP heterostructure avalanche photodiodes with high avalanche gain". In: *Applied Physics Letters* 35.3 (1979), pp. 251–253.

[80] A. Lacaita, F. Zappa, S. Cova, and P. Lovati. “Single-photon detection beyond 1 μm: performance of commercially available InGaAs/InP detectors”. In: *Appl. Opt.* 35.16 (June 1996), pp. 2986–2996.

[81] M. A. Itzler, r. Ben-Michael, C. .-. Hsu, K. Slomkowski, A. Tosi, S. Cova, F. Zappa, and R. Ispasoiu. “Single photon avalanche diodes (SPADs) for 1.5m photon counting applications”. In: *Journal of Modern Optics* 54.2-3 (2007), pp. 283–304.

[82] M. A. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova. “Advances in InGaAsP-based avalanche diode single photon detectors”. In: *Journal of Modern Optics* 58.3-4 (2011), pp. 174–200.

[83] K. E. Jensen, P. I. Hopman, E. K. Duerr, E. A. Dauler, J. P. Donnelly, S. H. Groves, L. J. Mahoney, K. A. McIntosh, K. M. Molvar, A. Napoleone, D. C. Oakley, S. Verghese, C. J. Vineis, and R. D. Younger. “Afterpulsing in Geiger-mode avalanche photodiodes for 1.06m wavelength”. In: *Applied Physics Letters* 88.13 (2006), p. 133503.

[84] G. Vincent, A. Chantre, and D. Bois. “Electric field effect on the thermal emission of traps in semiconductor junctions”. In: *Journal of Applied Physics* 50.8 (1979), pp. 5484–5487.

[85] S. Cova, M. Ghioni, M. A. Itzler, J. C. Bienfang, and A. Restelli. “Chapter 4 - Semiconductor-Based Detectors”. In: *Single-Photon Generation and Detection*. Ed. by A. Migdall, S. V. Polyakov, J. Fan, and J. C. Bienfang. Vol. 45. Experimental Methods in the Physical Sciences. Academic Press, 2013, pp. 83–146.

[86] F. Zappa, P. Lovati, and A. Lacaita. “Temperature dependence of electron and hole ionization coefficients in InP”. In: *Proceedings of 8th International Conference on Indium Phosphide and Related Materials*. 1996, pp. 628–631.

[87] J. Donnelly, E. Duerr, K. Mcintosh, E. Dauler, D. Oakley, S. Groves, C. Vineis, L. Mahoney, K. Molvar, P. Hopman, K. Jensen, G. Smith, S. Verghese, and D. Shaver. “Design Considerations for 1.06-<tex>*mu*</tex>m InGaAsP–InP Geiger-Mode Avalanche Photodiodes”. In: *IEEE Journal of Quantum Electronics* 42.8 (2006), pp. 797–809.

[88] X. Jiang, M. A. Itzler, R. Ben-Michael, and K. Slomkowski. "InGaAsP–InP Avalanche Photodiodes for Single Photon Detection". In: *IEEE Journal of Selected Topics in Quantum Electronics* 13.4 (2007), pp. 895–905.

[89] A. Lamas-Linares and C. Kurtsiefer. "Breaking a quantum key distribution system through a timing side channel". In: *Opt. Express* 15.15 (July 2007), pp. 9388–9393.

[90] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. "Time-Shift Attack in Practical Quantum Cryptosystems". In: *Quantum Info. Comput.* 7.1 (Jan. 2007), pp. 73–82. ISSN: 1533-7146.

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

[92] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo. "Experimental quantum key distribution with source flaws". In: *Phys. Rev. A* 92 (3 Sept. 2015), p. 032305.

[93] A. G. Chynoweth and K. G. McKay. "Photon Emission from Avalanche Breakdown in Silicon". In: *Phys. Rev.* 102 (2 Apr. 1956), pp. 369–376.

[94] J. Bude, N. Sano, and A. Yoshii. "Hot-carrier luminescence in Si". In: *Phys. Rev. B* 45 (11 Mar. 1992), pp. 5848–5856.

[95] A. L. Lacaita, F. Zappa, S. Bigliardi, and M. Manfredi. "On the Bremsstrahlung Origin of Hot-Carrier-Induced Photons in Silicon Devices". In: 40 (Apr. 1993), pp. 577–582.

[96] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?" In: *Journal of Modern Optics* 48.13 (Nov. 2001), pp. 2039–2047. ISSN: 1362-3044.

[97] L. Marini, R. Camphausen, C. Xiong, B. Eggleton, and S. Palomba. "Breakdown Flash at Telecom Wavelengths in Direct Bandgap Single-Photon Avalanche Photodiodes". In: *Photonics and Fiber Technology 2016 (ACOFT, BGPP, NP)* (2016).

[98] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese. "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution". In: *Light: Science & Applications* 6.6 (Dec. 2016), e16261.

[99] F. Acerbi, A. Tosi, and F. Zappa. "Avalanche Current Waveform Estimated From Electroluminescence in InGaAs/InP SPADs". In: *IEEE Photonics Technology Letters* 25.18 (Sept. 2013), pp. 1778–1780. ISSN: 1041-1135.

[100] I. Rech, A. Ingargiola, R. Spinelli, I. Labanca, S. Marangoni, M. Ghioni, and S. Cova. "Optical crosstalk in single photon avalanche diode arrays: a new complete model". In: *Opt. Express* 16.12 (June 2008), pp. 8381–8394.

[101] R. D. Younger, K. A. McIntosh, J. W. Chludzinski, D. C. Oakley, L. J. Mahoney, J. E. Funk, J. P. Donnelly, and S. Verghese. "Crosstalk analysis of integrated Geiger-mode avalanche photodiode focal plane arrays". In: *Proc.SPIE* 7320 (2009), pp. 7320 - 7320 –12.

[102] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov. "Eavesdropping and countermeasures for backflash side channel in quantum cryptography". In: *Opt. Express* 26.16 (Aug. 2018), pp. 21020–21032.

[103] W. Shockley and W. T. Read. "Statistics of the Recombinations of Holes and Electrons". In: *Phys. Rev.* 87 (5 Sept. 1952), pp. 835–842.

[104] "Data sheet for ID220 Infrared Single-Photon Detector". ID Quantique.

[105] P. D. Townsend. "Quantum cryptography on multiuser optical fibre networks". In: *Nature* 385.6611 (Jan. 1997), pp. 47–49. ISSN: 1476-4687.

[106] P. D. Townsend. "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing". In: *Electron. Lett.* 33.3 (Jan. 1997), pp. 188–190.

[107] L. G. Cohen and C. Lin. "Pulse delay measurements in the zero material dispersion wavelength region for optical fibers". In: *Appl. Opt.* 16.12 (Dec. 1977), pp. 3136–3139.

[108] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. "Free-space quantum key distribution with entangled photons". In: *Applied Physics Letters* 89.10 (2006), p. 101122.

[109] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan. "Practical challenges in quantum key distribution". In: *npj Quantum Information* 2.1 (Nov. 2016), p. 16025. ISSN: 2056-6387.

[110] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden. "Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods". In: *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics* 30.1 (July 2004), pp. 143–148. ISSN: 1434-6079.

[111] J. D. Franson. "Nonlocal cancellation of dispersion". In: *Phys. Rev. A* 45 (5 Mar. 1992), pp. 3126–3132.

[112] M. Karlsson. "Polarization mode dispersion induced pulse broadening in optical fibers". en. In: *Opt Lett* 23.9 (1998), pp. 688–690.

[113] R. Noe. "Essentials of modern optical fiber communication, second edition". Jan. 2016, pp. 1–337. ISBN: 978-3-662-49621-3.

[114] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. "Quantum cryptography". In: *Rev. Mod. Phys.* 74 (1 Mar. 2002), pp. 145–195.

[115] J. P. Gordon and H. Kogelnik. "PMD fundamentals: Polarization mode dispersion in optical fibers". In: *Proceedings of the National Academy of Sciences* 97.9 (2000), pp. 4541–4550. ISSN: 0027-8424.

[116] B. Heffner. "Automated measurement of polarization mode dispersion using Jones matrix eigenanalysis". In: *IEEE Photonics Technology Letters* 4.9 (1992), pp. 1066–1069.

[117] D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu, and J.-H. Liu. "Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback". In: *Opt. Express* 26.18 (Sept. 2018), pp. 22793–22800.

[118] A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer. "An optimal photon counting polarimeter". In: *Journal of Modern Optics* 53.10 (2006), pp. 1523–1528.

[119] G. B. Xavier, G. V. de Faria, G. P. Temporao, and J. P. von der Weid. “Full polarization control for fiber optical quantum communication systems using polarization encoding”. In: *Opt. Express* 16.3 (Feb. 2008), pp. 1867–1873.

[120] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng. “Stable quantum key distribution with active polarization control based on time-division multiplexing”. In: *New Journal of Physics* 11.6 (June 2009), p. 065004.

[121] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han. “Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits”. In: *Opt. Lett.* 42.6 (Mar. 2017), pp. 1023–1026.

[122] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi. “Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder”. In: *Optica* 7.4 (Apr. 2020), pp. 284–290.

[123] J. Rarity, P. Owens, and P. Tapster. “Quantum Random-number Generation and Key Sharing”. In: *Journal of Modern Optics* 41.12 (1994), pp. 2435–2444.

[124] C. Ho, A. Lamas-Linares, and C. Kurtsiefer. “Clock synchronization by remote detection of correlated photon pairs”. In: *New Journal of Physics* 11.4 (Apr. 2009), p. 045011.

[125] G. Brassard and L. Salvail. “Secret-key reconciliation by public discussion”. In: *Advances in Cryptology—EUROCRYPT ’93*. Ed. by T. Helleseth. Vol. 765. New York: Springer Verlag, 1994, p. 410.

[126] T. Sugimoto and K. Yamazaki. “A Study on Secret Key Reconciliation Protocol "Cascade"”. In: *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* E83-A (10 2000), p. 1987.

[127] C. H. Bennett, G. Brassard, and J.-M. Robert. “Privacy Amplification by Public Discussion”. In: *SIAM Journal on Computing* 17.2 (1988), pp. 210–229.

[128] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin. “Entanglement distribution over a 96-km-long submarine optical

fiber". In: *Proceedings of the National Academy of Sciences* 116.14 (2019), pp. 6684–6688.

[129] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, B. Liu, T. Scheidl, S. M. Dobrovolskiy, R. v. d. Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, A. Zeilinger, A. Xuereb, and R. Ursin. "Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre". In: *npj Quantum Information* 6.1 (Jan. 2020), p. 5. ISSN: 2056-6387.

[130] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. "Practical quantum key distribution with polarization entangled photons". In: *Opt. Express* 12.16 (Aug. 2004), pp. 3865–3871.

[131] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields. "Cambridge quantum network". In: *npj Quantum Information* 5.1 (Nov. 2019), p. 101. ISSN: 2056-6387.

[132] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin. "A trusted-node-free eight-user metropolitan quantum communication network". In: *Science Advances* 6.36 (2020), eaba0959.

Publications during PhD Study

[1] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer. "Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes". In: *Opt. Express* 25.24 (Nov. 2017), pp. 30388–30394.

[2] J. A. Grieve, Y. Shi, H. S. Poh, C. Kurtsiefer, and A. Ling. "Characterizing nonlocal dispersion compensation in deployed telecommunications fiber". In: *Applied Physics Letters* 114.13 (2019), p. 131106.

[3] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling. "Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber". In: *Applied Physics Letters* 117.12 (2020), p. 124002.

[4] Y. Shi, H. S. Poh, A. Ling, and C. Kurtsiefer. "Fibre polarisation state compensation in entanglement-based quantum key distribution". In: *Opt. Express* 29.23 (Nov. 2021), pp. 37075–37080.