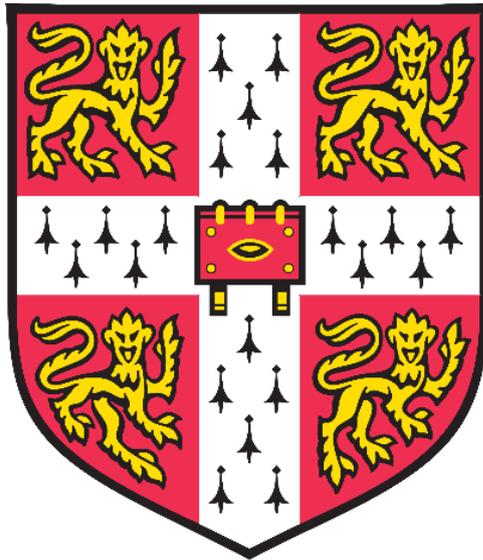


Optically Switched Quantum Key Distribution Network



Xinke Tang

**Churchill College
University of Cambridge**

**A dissertation submitted for the degree of
Doctor of Philosophy
September 2018**

Dedicated to my parents

Declaration

This thesis is the result of my own work and includes nothing that is the outcome of work done in collaboration except as specified in the text and declared in the acknowledgements.

It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my thesis has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text.

This thesis does not exceed the prescribed word limit for the Engineering Degree Committee.

Xinke Tang

September 2018

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisors, Professor Richard Penty, and my academic adviser, Professor Ian White, for their superb guidance and continued help throughout my PhD Study. Without their consistent support and encouragement, the work presented in this thesis could not have been done.

I wish to thank Dr. Adrian Wonfor for sharing with me his experiences with using the experimental equipment, his helpful discussions, and his consistent theoretical support. I would also like to thank Dr. Rupesh Kumar for teaching me the fundamental theories of CVQKD, his inspiring discussions, and his continued help with troubleshooting any experimental problems. The time he spent working with me on the optically switched CVQKD demonstration, as a part of Chapter 5, is very much appreciated.

I would like to acknowledge Shengjun Ren, Han Qin, Yupeng Gong, and many others of my colleagues in the group for the friendly and enjoyable environment during my PhD study.

I wish to thank the Cambridge Commonwealth, European and International Trust, and China Scholarship Council, as well as Pannett Fund from Churchill College for the financial support they provided for my PhD study.

I would like to thank my parents for their love, encouragement, and everything they have done for me. My PhD study would not have been possible without your love and support.

Abstract

Encrypted data transmission is becoming increasingly more important as information security is vital to modern communication networks. Quantum Key Distribution (QKD) is a promising method based on the quantum properties of light to generate and distribute unconditionally secure keys for use in classical data encryption. Significant progress has been achieved in the performance of QKD point-to-point transmission over a fibre link between two users. The transmission distance has exceeded several hundred kilometres of optical fibre in recent years, and the secure bit rate achievable has reached megabits per second, making QKD applicable for metro networks. To realize quantum encrypted data transmission over metro networks, quantum keys need to be regularly distributed and shared between multiple end users. Optical switching has been shown to be a promising technique for cost-effective QKD networking, enabling the dynamic reconfiguration of transmission paths with low insertion loss.

In this thesis, the performance of optically switched multi-user QKD systems are studied using a mathematical model in terms of transmission distance and secure key rates. The crosstalk and loss limitations are first investigated theoretically and then experimentally. The experiment and simulation both show that negligible system penalties are observed with crosstalk of -20 dB or below. A practical quantum-safe metro network solution is then reported, integrating optically-switched QKD systems with high speed reconfigurability to protect classical network traffic. Quantum signals are routed by rapid optical switches between any two endpoints or network nodes via reconfigurable connections. Proof-of-concept experiments with commercial QKD systems are conducted. Secure keys are continuously shared between virtualised Alice-Bob pairs over effective transmission distances of 30 km, 31.7 km, 33.1 km and 44.6 km. The quantum bit error rates (QBER) for the four paths are proportional to the channel losses with values between 2.6% and 4.1%. Optimising the reconciliation and clock distribution architecture is predicted to result in an estimated maximum system reconfiguration time of 20 s, far shorter than previously demonstrated.

In addition, Continuous Variable (CV) QKD has attracted much research interest in recent years, due to its compatibility with standard telecommunication techniques and relatively low cost in practical implementation. A wide band balanced homodyne detection system built from modified off-the-shelf components is experimentally demonstrated. Practical limits and benefits for high speed CVQKD key transmission are demonstrated based on an analysis of noise performance. The feasibility of an optically switched CV-QKD is also experimentally

demonstrated using two virtualised Alice-Bob pairs for the first time. This work represents significant advances towards the deployment of CVQKD in a practical quantum-safe metro network. A method of using the classical equalization technique for Inter-symbol-interference mitigation in CVQKD detection is also presented and investigated. This will encourage further research to explore the applications of classical communication tools in quantum communications.

List of Publications

X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, “Quantum-safe Metro Network with Low-Latency Reconfigurable Quantum Key Distribution”, *Journal of Lightwave Technology*, vol. 36, pp. 5230-5236, 2018

X. Tang, R. Kumar, D. Cunningham, A. Wonfor, R. V. Penty, I. H. White, “Inter-Symbol-Interference Reduction in Continuous Variable QKD using Equalization”, *IEEE Global Communications Conference*, Abu Dhabi, UAE, December 2018

X. Tang, A. Wonfor, R. Kumar, S. Ren, R. V. Penty and I. H. White, “Crosstalk Limitations on Reconfigurable QKD Networks”, 7th international conference on quantum cryptography (QCrypt), Cambridge, UK, September 2017

X. Tang, R. Asif, R. Kumar, A. Wonfor, S. Savory, I. H. White and R. V. Penty, “Practical Challenges in Classical Coherent Receivers for Detecting High Speed CV-QKD Signals”, 6th international conference on quantum cryptography (QCrypt), Washington DC, September 2016

X. Tang, R. Kumar, S. Ren, A. Wonfor, R. V. Penty and I. H. White, “Towards high speed Gaussian modulated CV-QKD”, in preparation.

R. Kumar, **X. Tang**, A. Wonfor, R. V. Penty and I. H. White, “Continuous variable quantum key distribution with multi-mode signals for noisy detectors”, accepted by *Journal of the Optical Society of America B*, 2019

S. Ren, R. Kumar, A. Wonfor, **X. Tang**, R. V. Penty and I. H. White, “Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise”, *Journal of the Optical Society of America B*, vol. 36, pp. B7-B15, 2019

A. Wonfor, H. Qin, R. Kumar, **X. Tang**, J. F. Dynes, A. J. Shields, R. V. Penty, I. H. White, “Field trial of a QKD and high-speed classical data hybrid metropolitan network”, *Broadband Access Communication Technologies XII*, 2018

S. Ren, R. Kumar, A. Wonfor, **X. Tang**, R. V. Penty and I. H. White, “Reference pulse attack on continuous variable quantum key distribution with local local oscillator”, 7th international conference on quantum cryptography (QCrypt), Cambridge, UK, September 2017

R. Kumar, **X. Tang**, R. Asif, A. Wonfor, R. V. Penty, S. Savory and I. H. White, “Continuous Variable Quantum Key Distribution with Displaced Coherent State”, 6th international conference on quantum cryptography (QCrypt), Washington DC, September 2016

Contents

Chapter 1 Introduction	1
1.1 Brief introduction to cryptography	1
1.2 Quantum Key Distribution	3
1.2.1 DV QKD protocols	3
1.2.2 CV QKD protocols	6
1.2.3 Post processing	7
1.3 Overview of QKD in fibre-optic communication: from single link to network.....	8
1.4 Motivation	10
1.5 Thesis organisation	11
1.6 Novel contributions	12
Chapter 2 Review of practical PTP QKD links	14
2.1 Introduction	14
2.2 Practical DV QKD links	14
2.2.1 Photon source and single photon detector	14
2.2.2 Practical implementation	17
2.2.3 Secret key analysis and modelling.....	21
2.3 Practical CV QKD links	27
2.3.1 Coherent detection	27
2.3.2 Practical implementations	29
2.3.3 Secret key analysis and modelling.....	32
2.4 State of the art QKD performance	38
2.5 Summary.....	39
Chapter 3 Optically switched QKD systems.....	41
3.1 Introduction	41
3.2 Review of multiuser QKD systems	42
3.2.1 Passive splitting scenario	42
3.2.2 Trusted repeating scenario	43
3.2.3 Optical path switching scenario	45
3.3 Optical switching techniques.....	46
3.4 Evaluation of optically switched QKD systems	54
3.5 Proof-of-concept experiments	61
3.6 Summary.....	64
Chapter 4 Reconfigurable QKD over Metro network.....	65

4.1 Introduction	65
4.2 Reconfigurable quantum-safe metro network	66
4.3 Proof-of-concept Experiment	73
4.4 Experimental results	76
4.5 Summary.....	80
Chapter 5 Towards Reconfigurable CVQKD network	81
5.1 Introduction	81
5.2 Noise analysis in high speed CVQKD	82
5.3 Experimental demonstration of a GHz CVQKD detector	92
5.4 Feasibility of optically Switched CVQKD systems	94
5.5 Equalization in CVQKD detection	101
5.5.1 Equalization Principle.....	101
5.5.2 CVQKD detection with Equalization	103
5.6 Summary.....	105
Chapter 6 Conclusion and Future work	106
6.1 Conclusion.....	106
6.1.1 Feasibility and limitation of optically switched QKD	107
6.1.2 Reconfigurable Quantum-safe metro network.....	107
6.1.3 Towards a reconfigurable CVQKD network	108
6.2 Future work	110
References	112

List of Figures

Figure 1.1 Illustration of a basic cryptographic solution	1
Figure 1.2 Bit encoding with two bases in BB84.....	4
Figure 1.3 Illustration of Gaussian modulated coherent states in GG02	7
Figure 1.4 Paradigms of a multi user QKD system based on (a) passive splitting; (b) PTP trusted repeating; (c) optical switching	10
Figure 2.1 Scheme for the single photon source based on a pulsed laser.	15
Figure 2.2 Photon distribution in optical pulses with mean photon number of a) 0.1, b) 0.2, c) 0.3, and d) 0.4.....	16
Figure 2.3 Typical implementation configuration of polarisation-based DVQKD [12, 76]....	18
Figure 2.4 Typical implementation configuration of phase-based DVQKD. a) double MZI configuration. b) plug-and-play configuration [1, 76, 78]	19
Figure 2.5 Schematic of the practical implementation of COW DVQKD [80].....	20
Figure 2.6 The calculated secure bit rate as a function of transmission distance for the standard BB84 QKD system using a Poisson or an ideal single photon source	24
Figure 2.7 The simulated secure bit rate as a function of transmission distance for the QKD links using BB84 and COW protocols	26
Figure 2.8 schematics of (a) the balanced homodyne and (b) the heterodyne detection [86]..	27
Figure 2.9 Practical implementation of GMCS CVQKD with TLO. [46, 89].....	30
Figure 2.10 Practical implementation of GMCS CVQKD with LLO. [91-93]	31
Figure 2.11 a) Illustration of the misalignment between Alice's and Bob's phase reference frames. b) corrected state based on the phase value of the reference state [92].....	32
Figure 2.12 The calculated secure key rates for TLO and LLO- based CVQKD with homodyne(hom)/heterodyne(het) detection	36
Figure 2.13 State-of-the-art performance of practically implemented QKD PTP links	38
Figure 3.1 Schematic of passive-splitting multi-user QKD systems based on a) downstream and b) upstream configurations [51]	43
Figure 3.2 Schematic of a typical trusted repeating multi-user QKD systems	44
Figure 3.3 Secure key sharing scheme with a trusted repeater in QKD links with three users	45
Figure 3.4 Schematic of a typical optically switched multi-user QKD system	45
Figure 3.5 Schematic of an interferometric switching element using a a) MZI or b) directional coupler [108, 117]	48

Figure 3.6 Scheme of a basic acousto-optic switching element [117]	49
Figure 3.7 Scheme of a basic liquid crystal switching element [117].....	49
Figure 3.8 Scheme of a basic SOA based switching element.	50
Figure 3.9 Schematic of a basic Opto-Mechanical switching element.	51
Figure 3.10 Schematics of (a) Tree (b) Crossbar (c) Clos and (d) Benes switch architectures [120].....	52
Figure 3.11 a) The simulated QBER as a function of transmission distance of the decoy state QKD with and without optical switch. b) The simulated secure bit rate as a function of transmission distance of decoy state QKD with and without optical switch	57
Figure 3.12 a) The simulated QBER and b) the simulated secure bit rate as a function of transmission distance of the decoy state QKD with different levels of additional losses.....	59
Figure 3.13 a) The simulated QBER and b) the simulated secure bit rate as a function of transmission distance of the decoy state QKD with different levels of additional crosstalk ...	60
Figure 3.14 Experimental setup	61
Figure 3.15 Detection of both polarisation using the same SPD	62
Figure 3.16 The measured (solid symbols) and calculated (dashed lines) QBER	63
Figure 4.1 Schematic of a metro network structure.	67
Figure 4.2 The proposed quantum safe metro network architecture.....	68
Figure 4.3 Schematics for the co-existence scheme of quantum and classical channels. Classical channel includes both conventional data transmission and post-processing signals for QKD systems [129]	71
Figure 4.4 Mechanism of exchange secure key between two distant QKD hops	72
Figure 4.5 a) Equivalent system schematic. b) Experimental setup. EDFA: Erbium-doped Fibre Amplifier. BERT: Bit Error Rate Test.....	74
Figure 4.6 (a) The real-time measurement of QBER with path reconfiguration for the quantum channel only (b) Corresponding average secure key rate measured for each path. ..	77
Figure 4.7 (a) The real-time measurement of QBER with path reconfiguration for the quantum channel multiplexed with the classical channel and routing signal (b) Corresponding average secure key rate measured at each path	78
Figure 5.1 (a) Estimation of the noise terms at different CVQKD repetition rates. (b) Estimation of the total electronic noise and total excess noise with changing repetition rate.	89
Figure 5.2 Secure key rate as a function of distance at clock rates of 1 MHz 100 MHz, 250 MHz and 1 GHz in a TLO CVQKD system	90

Figure 5.3 Secure key rate as a function of distance at clock rate of 1 MHz 100 MHz, 250 MHz and 1 GHz in a CVQKD system with an LLO scheme	91
Figure 5.4 Balanced Homodyne detector experimental setup.....	93
Figure 5.5 Output variance measurement as a function of LO power. The green line shows the region where the output variance is approximately linearly proportional to LO power. ...	94
Figure 5.6 (a) Equivalent schematic diagram of the optically switched system. (b) Experimental setup for the reconfigurable CVQKD systems	96
Figure 5.7 Illustration of the transmission pattern of signal packets.	97
Figure 5.8 Illustration of phase drift in pilot pulses	98
Figure 5.9 Experimental measurements on the phase drift within each signal packet	99
Figure 5.10 Continuous estimations on channel transmission with optical switching	100
Figure 5.11 Illustration of the method of FFE	102
Figure 5.12 Frequency response resulted from system and equalization, illustrating the electronic noise enhancement.	103
Figure 5.13 CVQKD detection system with equalization.....	104
Figure 5.14 Simulated (a) cross-correlation and (b) ξ_{ISI} of the detected quadrature values with and without the application of equalization.	105

List of Tables

Table 1.1 Illustration of a basic BB84 protocol	5
Table 3.1 Representative experimental demonstrations of optically switched QKD transmission.....	54
Table 5.1 Parameters and secure key estimations	99

List of Abbreviations

ADC: Analogue to digital converter

AES: Advanced Encryption Standard

AM: Amplitude modulator

APD: Avalanche Photodiode

ASE: Amplified spontaneous emission

ATT: Optical attenuator

BER: Bit error ratio

BERT: Bit error rate test

BHD: Balanced homodyne detection

BS: Beam splitter

CM: Classical monitor

CMRR: Common mode rejection ratio

COW: Coherent one-way

CV: Continuous variable

CW: Continuous-wave

DAC: Digital to analogue convertors

DES: Data Encryption Standard

DIO: Digital input/output

DL: Optical delay line

DR: Direct reconciliation

DV: Discrete variable

EC: Error correction

EDFA: Erbium-doped fibre amplifier

EO: Electro-optic

FFE: Feed forward equalization

FM: Faraday mirror

FPGA: Field-programmable gate array

GMCS: Gaussian modulated coherent state protocol

IP: Internet protocol

IPDR: Input power dynamic range

ISI: Inter-symbol interference

LC: Liquid crystal

LDPC: Low-density parity-check code

LLO: Local Local Oscillator

LO: Local oscillator

MEMS: Microelectromechanical system

MI: Monitoring interferometer

MSE: Mean square error

MZI: Mach-Zehnder interferometer

NBF: Narrow band filtering

OE: Opto-electronic

OS: Optical switch

OTP: One-time pad

PA: Privacy amplification

PBS: Polarisation beam splitter

PC: Polarisation controller

PM: Phase modulator

PNS: Photon number splitting

PON: Passive optical networking

PRBS: pseudorandom binary sequence

PS: Polarisation scrambler

PSRR: Power supply rejection ratio

PTP: point-to-point

QBER: Quantum bit error rate

QKD: Quantum key distribution

RIN: Relative intensity noise

RNG: Random number generator

RR: Reverse reconciliation

SDN: Software defined networking

SFP: Small form-factor pluggable

SNR: Signal-to-noise ratio

SNU: Shot noise unit

SOA: Semiconductor optical amplifier

SPD: Single photon detector

SSMF: Standard single mode fibre

TDM: Time-division multiplexing

TIA: Transimpedance amplifier

TLO: Transmitted Local Oscillator

WDM: Wavelength division multiplexing

Chapter 1 Introduction

1.1 Brief introduction to cryptography

Cryptography is a field of applications allowing the transfer of confidential communications in the presence of unauthorised parties called eavesdroppers [1]. A standard cryptographic system consists of a message space M , a ciphertext space C , a key space K and a pair of encryption/decryption algorithms E/D [2]. As shown in Figure 1.1, an ordinary message (also known as plaintext) $m \in M$ from the sender (conventionally named 'Alice') is encrypted with additional information referred to as the 'key' $k \in K$ based on an encryption algorithm E . The encrypted message (called the ciphertext or cryptogram) $c = E(m, k) \in C$ is sent to the receiver (conventionally named 'Bob') through an insecure channel. Bob conducts the reverse operation and employs a decryption algorithm together with the key to retrieve plaintext from the ciphertext he reviewed, ie. $m = D(c, k)$. During the transmission of secret information, there would be a potential unauthorised third party (commonly known as 'Eve') attempting to retrieve the transmitted ciphertext [1-3]. A secure cryptographic system should be able to protect the ciphertext from Eve's attacks, and the security must rely on keeping the changeable key secret rather than a undisclosed encryption/decryption algorithm [2, 4].

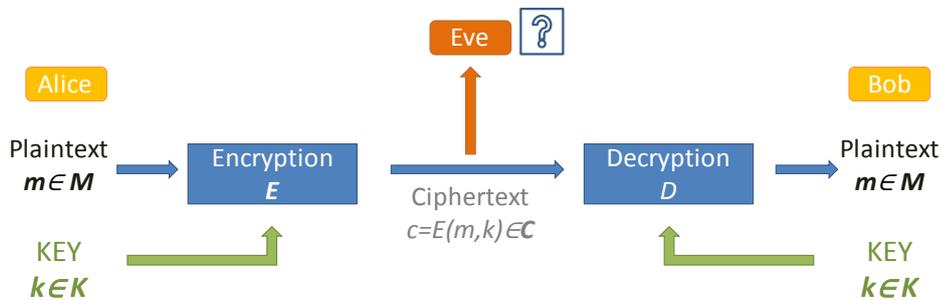


Figure 1.1 Illustration of a basic cryptographic solution

Cryptography has a long history of war with cryptanalysis, which is the study of eavesdropping [1, 5]. Research has been conducted to build more secure cryptographic systems, while techniques are also developed and improved to break them. The breakthrough happened in 1917, when the so-called 'one-time pad' (OTP) cryptosystem was introduced by Vernam [6]. OTP is a symmetrical cryptographic solution/protocol, as a randomly generated key must be securely shared between Alice and Bob in advance. The ciphertext c can be then produced by Alice by combining the key k and original plaintext m : $c = m \oplus k$, where \oplus is a bitwise exclusive

OR operation. As Bob has the same key, he can decrypt the ciphertext by the calculation: $c \oplus k = m \oplus k \oplus k = m$. This process requires the key to be the same length as the transmitted message [1, 2, 6]. In principle, OTP is proven to be unbreakable as long as the random keys are not reused [7]. However, the secure distribution of the non-reusable large-size key cannot be practically guaranteed over an insecure transmission channel. Although the algorithm is provably secure, the cryptographic system would collapse if Eve is able to reveal the key. The same problem also exists in the implementation of other symmetrical cryptographic systems, such as Advanced Encryption Standard (AES), and Data Encryption Standard (DES), even though they require fewer shared keys [1, 5].

Another class of classical cryptography is commonly called public-key or asymmetrical cryptographic systems, which aims to avoid this problem [1]. In public-key cryptography there is no need to securely distribute the key between Alice and Bob. Instead, Bob publicly announces a public key which is computed from a pre-prepared private key. Alice then encrypts her plaintext into ciphertext using the public key and sends it back to Bob, who is the only one able to decrypt this ciphertext with his private key. Any potential Eve in the middle would face enormous challenges, requiring complicated calculations to decode the message. Indeed, the security of public-key cryptographic systems is based on assumptions about the limits of Eve's computational capability, also commonly known as computational security [1, 8]. The most typical example is the Rivest, Shamir, and Adleman (RSA) algorithm [9]. Firstly, Bob randomly uses two different prime numbers p and q to generate a public key as a pair of integers (e, n) , where $n = pq$ and e satisfies $\gcd(e, \phi(n)) = 1$, and $\phi(n) = (p-1)(q-1)$. p and q are kept secure, but the public key can be shared with Alice via an insecure classical channel. The private key can then be obtained by Bob as $d \equiv 1 \pmod{\phi(n)}/e$. The information m encrypted by Alice as $C = M^e \pmod{n}$ can be decrypted by Bob using $M \equiv C^d \pmod{n}$. When Eve attempts to calculate the private key using the information, she faces a great challenge in factoring the number n [9]. For example, factoring a 232-decimal digit number took two years and employed hundreds of machines [2]. Therefore, the security relies on Eve's limited ability to factor large integers. Whilst this can currently be considered a reasonable assumption currently for very large integers, the future advent of sufficiently powerful quantum computers could easily break today's cryptographic systems [10, 11].

The field of cryptography is becoming more and more important as information security plays a vital role in modern communication networks. We should be severely concerned with the security of communication when we access our personal information online such as banking

data [12]. Although today's cryptographic systems are able to provide security under computational complexity assumptions, which is referred to as 'computational secure', a countermeasure needs to be prepared for more powerful Eves in the near future [1, 5].

1.2 Quantum Key Distribution

Quantum Key Distribution (QKD) is a promising solution for unconditional secure cryptography due to its ability to ensure secure key distribution via insecure channels by virtue of quantum mechanics. It was invented by Bennett and Brassard in 1984 [13]. Generally speaking, in a QKD system, Alice and Bob obtain the key from shared random bits encoded in the quantum states of particles, e.g. photons. Those encoded bits are commonly known as 'qubits' (quantum bits) [14]. The security of QKD is fundamental thanks to the Quantum Non-Cloning Theorem, which states that an unknown quantum state cannot be identically duplicated [15]. Any attempt at eavesdropping by Eve inevitably disturbs the transmitted quantum states, which could then be detected by Bob. As the distributed key is guaranteed to be secure, it can be used in symmetrical cryptographic algorithms such as OTP to achieve unconditionally secure cryptographic systems, in which the security does not rely on unproven mathematical assumptions [5]. QKD was first experimentally demonstrated in 1992 by distributing a key encoded in photons states between Alice and Bob [16], and it has been widely researched in the optical communications field over the last two decades. An increased number of protocols have also been developed.

In general, current protocols can be grouped into two main classes: Discrete Variable (DV) protocols and Continuous Variable (CV) protocols. In DV QKD, transmitted random bits are encoded in discrete phase or polarisation states of single photons, and single photon detection is used for measuring their quantum states. On the other hand, CV QKD employs the quadratures of the electromagnetic field to carry the bit information, and measurements are conducted based on coherent detection (e.g. Homodyne detection). This thesis does not cover the full range of QKD protocols. The representative DV and CV protocols used in the work of this thesis are introduced in this section.

1.2.1 DV QKD protocols

DV protocols are the original approach to QKD. The earliest and the best known QKD protocol is BB84 which was first conceived in 1984 by Bennett and Brassard [13]. The principle of

BB84 can be illustrated using Table 1.1. Alice encodes her random bit sequence in the polarisation of a train of single photons using two randomly chosen bases: the rectilinear (+) and diagonal (×) bases, as shown in Figure 1.2. As a result, each bit is encoded as a polarised single photon in one of four possible polarisation states: horizontal, vertical, -45° and $+45^\circ$ [17]. Alice and Bob agree that a photon polarised horizontally or at $+45^\circ$ represents bit value ‘0’, while photons polarised vertically and at -45° stand for bit value ‘1’. The polarised photons are then sent to Bob via a quantum channel. Bob conducts polarisation measurements using two polarisation analysers which correspond to the diagonal basis and rectilinear basis. He chooses one of analyzers/bases randomly to measure each photon from Alice. For each photon detection, there is a 50% possibility of getting an error when the basis chosen by Bob is different from Alice’s selection, as the ‘0’ and ‘1’ cannot be distinguished by the wrong base [17].

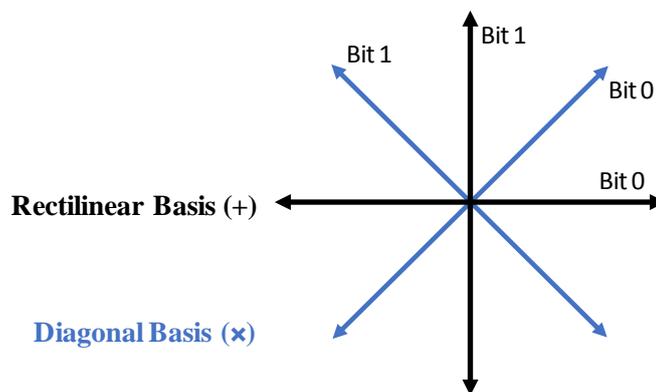


Figure 1.2 Bit encoding with two bases in BB84

After detecting all photons, Alice and Bob then communicate over an insecure public channel to let each other know the sequence of bases they used without sharing the bit values that were sent or received. To sift errors out, the bits detected when Alice and Bob used different bases are discarded, and the remaining bit sequence is called the ‘sifted key’ [1]. The sifting process is also illustrated in Table 1.1. The sifted keys recorded by Alice and Bob are ideally the same, but additional error will be caused by imperfections of practical devices or possibly by Eve’s intercept. The ratio of the number of different bits of the sifted key between Alice and Bob to the total length of sifted key is normally represented as the quantum bit error rate (QBER) [1, 18]. As the presence of eavesdropping will inevitably increase the number of error bits, Alice and Bob publicly share a fraction of the sifted key to evaluate the QBER, and hence the existence of Eve. If the QBER is higher than a predefined threshold, the corresponding key

fraction will not be used. The final secure key can be then obtained from the rest of the sifted key by classical post processing [14]. Despite encoding the bit information in the polarisation of photons, phase encoding has been shown as an alternative and more practical scheme for fibre communication, which will be discussed in detail in Chapter 2.

Table 1.1 Illustration of a basic BB84 protocol

Alice's random bits	Alice's basis	Sending polarisations	Bob's basis	Received bits	Public discussion	Sifted key
0	+		+	0	Same basis	0
0	×		+	1		
1	+		×	1		
0	+		+	0	Same basis	0
1	×		×	1	Same basis	1
1	+		×	1		
0	×		+	1		
1	×		×	1	Same basis	1

Ideally, a single photon source is required for preparing the sending states. However, regarding the practical generation of single photons, since the technology for true single photon generators is still under development [19, 20], DV-QKD systems generally employ highly attenuated pulsed lasers as photon sources, of which the average optical power is at sub single photon level. The problem with this method is that a small number of the emitting pulses have more than one photon, if even the average power is less than one photon per pulse.

This problem opens the possibility that Eve may perform what is called the photon number splitting (PNS) attack [21]. Eve can split and store one photon from these multi-photon pulses and transmit the rest to Bob. Therefore, she would be able to read some or all of the key after learning the base information from the public channel without introducing additional QBER. As a promising solution for defending from PNS attack, the idea of a ‘decoy state’ was first proposed by Hwang [22] in 2003 as a modification of the BB84 protocol. A similar idea was also later applied to other protocols. In this method, in addition to generating weak pulses (i.e. ‘signal’ or ‘key’ pulses) as in the standard BB84 protocol, Alice also prepares some additional ‘decoy’ pulses which have a different mean photon number per pulse, and hence a different possibility distribution. ‘Decoy’ pulses are randomly mixed in position with the original pulses and sent to Bob. Eve is not able to tell the difference between the signal pulses and the decoy

state pulses. Attempts at PNS can be then realized by investigating the QBER and yields of the decoy pulses [18, 23]. Following this work, a more efficient variation of the decoy state BB84 was developed as the so-called 'T12' protocol [24], in which two bases are selected with uneven possibilities depending on system characteristics.

A more practical way of implementing DVQKD, the coherent-one-way (COW) protocol has been conceived [25]. Instead of coding bit information on individual pulses, COW uses the coherence between the transmitting photon pulses. Alice encodes each random bit in a two-pulse sequence consisting of a vacuum and a single-photon-level pulse. To improve the security, decoy states, consisting of two successive laser pulses with the same energy levels, are randomly added to the sequence [26]. When transmitted to Bob, bit information can be then measured by determining the arrival time of the photons, and the existence of Eve is detected by monitoring the coherence between consecutive photon pulses [14]. The security of DVQKD systems has been rigorously proven [14, 23, 27-29]. A more detailed security analysis and practical QKD setup is given in Chapter 2.

1.2.2 CV QKD protocols

The CV QKD protocol is much recent, and was introduced in 1999 by Ralph [30]. It uses the amplitude and phase quadratures of a coherent laser to encode the bit information, therefore single photon detection is replaced by coherent detection consisting of classical photodiodes. As these sources and receivers are cost-effective and more compatible with standard telecommunication techniques, this has attracted a lot of research interest in recent years. Several protocols based on continuous variables have been proposed and demonstrated experimentally [31-35]. Among these, the Gaussian modulated coherent state protocol (GMCS or GG02) [31] has been widely investigated and mostly implemented. It has been thoroughly analyzed and proven to be secure against collective attacks [36] and general attacks [37]. In GMCS, Alice first prepares N pairs of random numbers $X_A = \{X_1, X_2 \dots X_N\}$ and $P_A = \{P_1, P_2 \dots P_N\}$. Both X_A and P_A follow a Gaussian distribution $\mathcal{N}(0, V_A)$, with a variance V_A and a mean of zero. This is the distribution that offers maximised information rate in a noisy channel [38]. She then prepares a sequence of coherent states $|\alpha\rangle = |X_A + iP_A\rangle$ and then sends it to Bob via a quantum channel. The preparation of Gaussian modulated coherent states can be visualised in Figure 1.3.

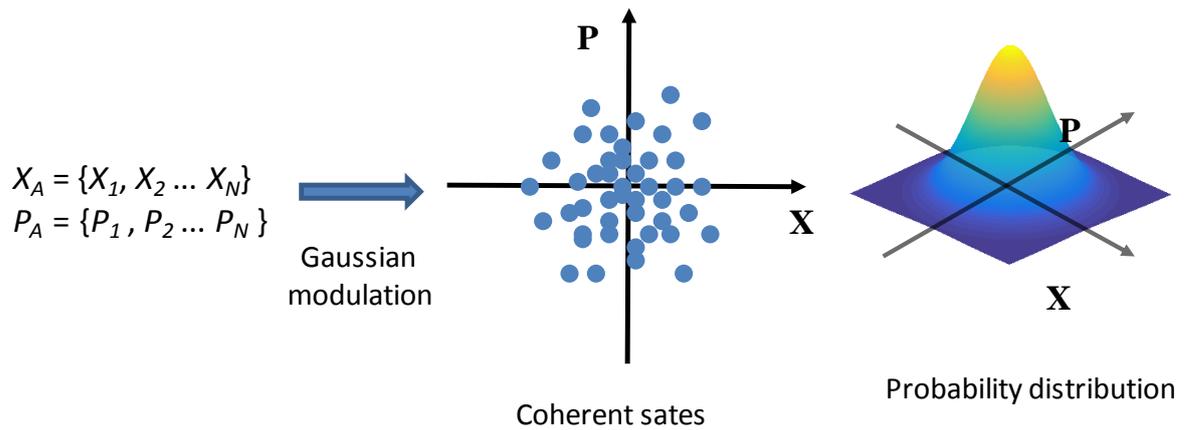


Figure 1.3 Illustration of Gaussian modulated coherent states in GG02

Bob randomly chooses to measure either quadrature X or P of the received states using coherent detection, from which he gets a corresponding sequence of numbers. Then he announces his choice of quadrature measurement to Alice publicly, so that she can do the sifting and store only the random numbers used in the modulation of correlated quadratures. Alice and Bob randomly sample and reveal a fraction of their strings of numbers and use it to estimate the channel transmittance and excess noise, and hence evaluate the amount of information mutually shared between Alice and Bob and the maximum information available to Eve [31, 39]. The evaluation is further explained in the secure key analysis in the next chapter. After this, the final secure key can be distilled from non-revealed numbers between Alice and Bob (i.e. the sifted key) by performing classical post processing (i.e. error correction and privacy amplification). The practical implementation and security analysis of a GMCS QKD system is given in Chapter 2.

1.2.3 Post processing

Despite the employed protocol, Alice and Bob would have a large number of sifted keys after quantum channel transmission. However, the key at this point has a certain QBER level, which is due to system imperfections and possible interception by Eve. Practically, all errors are regarded as the result of Eve's presence, as Alice and Bob would not be able to distinguish the causes of errors. Therefore, Alice and Bob have to involve post processing via a classical channel to correct the errors as well as reduce the information available to Eve. The final secret key is then decided after this procedure. Although post processing is a necessary step in QKD, its basic idea and technique is in common with classical communication and not exclusive to quantum physics.

The first step is called error correction (EC), which is also known as information reconciliation, making Alice's and Bob's bits identical. In general, Alice and Bob agree on a EC code first (e.g. a low-density parity check (LDPC) code [40]), and then EC can be practically conducted in either of two directions. In 'direct reconciliation' (DR), Bob corrects his bits based on the classical EC information sent from Alice. In 'reverse reconciliation' (RR), Alice corrects her bits based on the classical EC information sent from Bob [14, 41]. DR and RR affect the security key analysis of CV QKD systems, but make no difference to DV systems. At the end, EC results in a shortened but perfectly correlated key between Alice and Bob.

Since Alice and Bob conduct EC over an insecure classical channel, some part of the information can possibly be obtained by Eve. This needs to be solved by the second step of post processing following the EC process: privacy amplification (PA) [42]. PA is a method of eliminating the information leaked to Eve [14, 43]. In general, Alice and Bob publicly share a random hash function, and each of them applies it to the error corrected key. The resulting key will be compressed to a shorter length but still be identical between Alice and Bob, while Eve's knowledge of the key will be greatly minimised.

1.3 Overview of QKD in fibre-optic communication: from single link to network

From a practical point of view, since the first experimental demonstration of a QKD system in 1992 [16], both DV and CV QKD have been widely demonstrated over standard single mode fibre (SSMF), and significant progress has been achieved in the performance of point-to-point (PTP) links. For QKD systems with DV protocols, the maximum transmission distance between Alice and Bob has been extended to over hundreds of kilometres of optical fibre [29], and the secure bit rate achievable has reached megabits per second (Mbps) over 50 km [44]. On other hand, recent experimental demonstrations of CV QKD point-to-point GMCS CVQKD have shown key distribution using SSMF over increased transmission distances of 80 km [45] and 100 km [46], or with a secure bit rate in the range of Mbps [47]. Such achievements make QKD applicable in both metropolitan backbone and access telecommunication networks [26].

In order to realize QKD encrypted data transmission in a metro area and establish a quantum safe network, the first thing is to make sure that quantum keys can be properly distributed and shared between multiple users. Currently, multi-user QKD systems (or QKD networks) are

realized based on three main types of elements: passive splitters, trusted repeaters, and optical switches, all of which have advantages and disadvantages. These topologies are shown in Figure 1.4. A multi-user QKD (or QKD network) experiment was first demonstrated by Townsend et al. [48], using a passive optical splitter to realize point-to-multipoint quantum key transmission. Optical splitters were then implemented in passive QKD networks by many research groups [49-52]. Although QKD networks based on this technology have low network complexity and low cost, they all share two major weaknesses: the connections cannot be selected on demand, and the number of users is limited owing to the loss from passive splitters. The use of trusted repeaters has been shown to be a much simpler and scalable technique to establish QKD networks from fixed point-to-point links [53-55]. However, they are practically expensive and, similar to passive splitters, less reconfigurable. Optical switching has been shown to be an alternative technique for cost-effective QKD networking, enabling the dynamic reconfiguration of transmission paths with low insertion loss. The earliest optically-switched QKD system was demonstrated by Toliver et al. [56], in which a secure key was established between Alice and Bob through different types of optical switching elements, such as microelectromechanical (MEMS), Lithium Niobate (LiNbO₃), and optomechanical switches [56]. Optical switching has since been employed in multiuser QKD systems in lab and field environments [57-62]. These techniques cannot be used to extend the QKD transmission distance. Such a problem can be solved by adding trusted repeaters into switched QKD systems [63]. An optical switching technique can be predicted to be the most promising candidate in the practical realization of reconfigurable multiuser QKD with minimum infrastructure. Most efforts in the investigation of QKD networks have been made for DV QKD protocols, CVQKD networks based on simple point-to-point configuration have been not demonstrated until recently [26, 64].

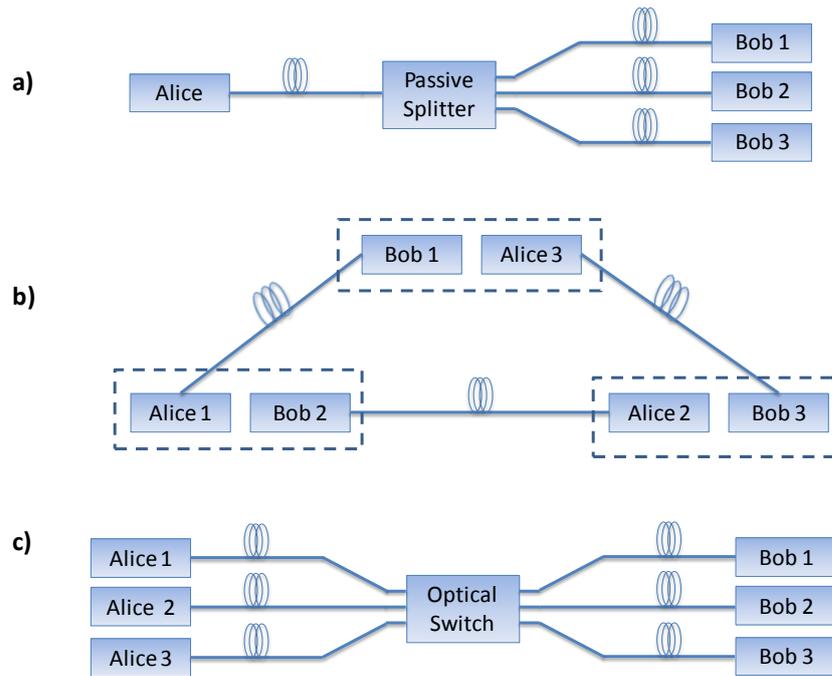


Figure 1.4 Paradigms of a multi user QKD system based on (a) passive splitting; (b) PTP trusted repeating; (c) optical switching

Another step towards a metro quantum safe network is the deployment of multiuser QKD systems in the existing metro network, thanks to the previous studies into the feasibility of the “co-existence scheme”, in which a quantum signal and classical signals are simultaneously transmitted through the same optical fibre using a wavelength division multiplexing (WDM) and narrow band filtering (NBF) technique [39, 61, 65-67]. Although some recent research suggests the possibility of practical integration of switched QKD in current metro networks [68, 69], there is still a lack of detail regarding the practical application of a switched multiuser QKD in a realistic metro network.

1.4 Motivation

This thesis focuses on the implementation of practical quantum encrypted (quantum-safe) communications in a metro network, integrating optically-switched QKD systems with high reconfigurability to protect classical network traffic. Although PTP QKD in fibre-optic communications has become a mature technology ready for practical use in cryptographic systems, there are still a number of challenges and loopholes in the practical application of QKD in existing metro telecommunication networks.

To establish cost-effectively multiuser QKD systems to provide secure reconfigurable network communications between multiple parties, optical switching techniques may be applied between QKD end-points, reducing the amount of deployed hardware. However, as the weak quantum signals are very sensitive to loss and noise, any optical switch used in routing quantum signals will more or less degrade the secure bit rate of each user. The loss and crosstalk limitations of optically switched QKD systems need to be investigated, not only to illustrate their feasibility but also to set criteria for the design or selection of switch components in QKD systems.

The deployment of optically switched QKD in today's network still needs further investigation. A practical solution needs to be drawn for effectively integrating reconfigurable QKD in the existing metro network to secure classical data traffic, in which the quantum channel and hence the secure key transmission can be switched between multiple network users. In addition, the system reconfiguration time would significantly limit the reconfigurability of the network and reduce the overall quantum key transmission speed. However, this is either not fully mentioned or for relatively long (in many minutes) in the demonstrated practical QKD systems and networks. The method for reducing reconfiguration time in the optically switched QKD metro network needs to be developed.

In addition, there has not been a demonstration of an optically switched CVQKD system so far. This may be owing to its relatively poor practical performance as the system speed of most CVQKD demonstrations is still 1 MHz. Therefore, the feasibility of higher speed CVQKD systems needs to be investigated, and hence enable their implementation in reconfigurable quantum-safe metro networks.

1.5 Thesis organisation

The organisation of this thesis is as follows:

Chapter 1 gives a general introduction of QKD and its role in cryptography. Some of the typical DV and CV protocols are explained. Research on moving QKD PTP links towards QKD networks is briefly overviewed. The motivation and contribution of this thesis are described.

Chapter 2 reviews the different approaches of practical PTP implementations using DV and CV QKD protocols. A detailed security key analysis is also provided. The different

performances of DV and CV QKD links in term of their secure key rate and transmission distance is modelled and discussed.

Chapter 3 first introduces optical switch techniques and reconfigurable networks. A security key analysis of switched QKD systems is carried out. The feasibility and limitations of a basic reconfigurable multi-user QKD system are studied. The performance of QBER of QKD paths (based on the BB84 protocol) through optical switches is predicted using the security key analysis, and a series of proof-of-principle experiments are carried out featuring additional emulated switch losses and crosstalk from an interferer.

Chapter 4 demonstrates an effective quantum-safe network solution which integrates reconfigurable QKD into a realistic metro network. The proposed network architecture and the operational principles of both dynamic key sharing and data encryption are described. A series of proof-of-concept experiments demonstrate the feasibility of a switched multi-node QKD system with reduced reconfiguration time within this architecture. Experimental results are shown and discussed.

Chapter 5 first discusses the feasibility of achieving high speed CV-QKD with a practical wideband balanced homodyne detection (BHD) system. The limitations and benefits of high clock rate CVQKD systems are illustrated by analysing the noise performance at different system speeds. With a GHz BHD, the feasibility of an optically switched CVQKD system is experimentally demonstrated. In addition, a method of using equalization in CVQKD detection to mitigate inter-symbol-interference is proposed and investigated.

Chapter 6 summarises the work undertaken in this project so far, and draws conclusions. Possible future work is also discussed.

1.6 Novel contributions

The main works that have been carried out during the author's PhD study are as follows:

- A mathematical model describing an optically switched QKD system was constructed, which is derived from the general secure key analysis for point to point links. In this model, the optical switch used in the system is featured as an additional channel loss and crosstalk, which inevitably degrades the QKD performance. Based on this model, the degradation in QBER and hence the secure key rate caused by optical switches in a reconfigurable QKD system was theoretically investigated. In addition, a series of proof-of-concept experiments

was conducted, which verified the mathematical model as well as studied the feasibility and limitations of an optically switched QKD system.

- A novel quantum-safe network solution was demonstrated, which cost-effectively integrates reconfigurable QKD into current metro networks. This solution also offers the potential for rapidly switching the quantum channel between multiple users and then immediately resuming secure key transmission between different Alices and Bobs. The feasibility of the proposed network scheme was experimentally demonstrated using commercially available QKD devices. In this experiment, one common Bob continuously shared secure keys with four virtualised Alices, via an opto-mechanical switch with four different path attenuations corresponding to transmission distances of 30 km, 31.7 km, 33.1 km and 44.6 km. The average QBER for the four paths were obtained as 2.6%, 3.2%, 3.6% and 4.1%, with secure key rates of around 1.8×10^3 , 1.6×10^3 , 1.3×10^3 , and 0.7×10^3 bits/s being obtained, respectively. A maximum reconfiguration time of 20s was predicted within this proposed network solution, far shorter than previously demonstrated.

- A theoretical analysis of repetition rate-dependent noise performance in CVQKD systems was conducted for the first time. The noise sources which behave proportionally to the system repetition rate were categorised and investigated. Based on this analysis, the noise behaviours and hence the feasibility of the high speed CVQKD system was evaluated. In addition, a GHz BHD, which was built using modified commercial components, was experimentally demonstrated in term of its feasibility in a CVQKD protocol.

- With this BHD, the feasibility of an optically switched high speed (250 MHz) GMCS CVQKD system was experimentally demonstrated. This part of the work was conducted in collaboration with Dr. Rupesh Kumar. The quantum signal transmission was routed between two virtualised Alice-Bob pairs. The secure key rates are predicted to be 1.0×10^5 bits/s and 1.2×10^6 bits/s for the two paths with total transmission losses of 4 dB and 7.5 dB.

- A method of using the classical equalization technique in CVQKD detection was proposed and implemented, for the first time, to mitigate the inter-symbol-interference that occurs in a BHD with limited bandwidth and hence enables detection on higher speed CVQKD data with a lower detector bandwidth.

Chapter 2 Review of practical PTP QKD links

2.1 Introduction

From a hardware point of view, a practical PTP QKD system consists of three basic components: a photon source, a channel and a detector. Lasers, after regarded as the most practical photon sources, have been widely employed in QKD links [14]. For single photon DVQKD generation, the output of a laser is highly attenuated, and coherent optical pulses generated from a weakly modulated laser are used in CVQKD links. There are two main types of physical channel for optical quantum keys: free space and optical fibre. Taking account of the existing global fibre network and the maturity and performance of advanced optical fibre communication systems and devices [70], this thesis mainly focuses on single-mode fibre (SMF)-based QKD links and systems. In this review, the detection technique is also discussed in detail, as this is another major difference between practical DV and CV QKD links. For the DV protocol, photon counting techniques must be used to detect the key information encoded in single photons. On the other hand, CVQKD employs coherent detection to distil the key from quadrature values of the coherent laser pulses.

In practical implementation, optical fibre-based quantum key transmission has been carried out based on different schemes. The focus of this section therefore is to review the main experimental configurations for the point-to-point distribution of quantum keys using DV and CV protocols. The corresponding secret key analysis under the presence of Eve is also introduced, this being an important measure used in evaluating the practical performance of a QKD link.

2.2 Practical DV QKD links

2.2.1 Photon source and single photon detector

In DV QKD, qubits are carried by single photon pulses which are commonly generated by a highly attenuated laser. Specifically, as shown in Figure 2.1, optical pulses generated from a directly modulated laser (or a laser followed by an amplitude modulator) are attenuated to an average power of less than one photon per pulse.

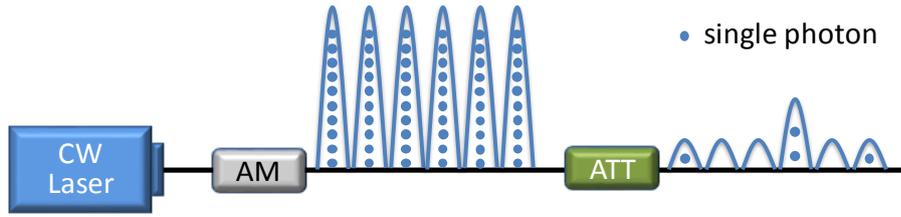


Figure 2.1 Scheme for the single photon source based on a pulsed laser. AM: amplitude modulator; ATT: Optical attenuator

The number of photons in each emitting laser pulse follows a Poisson distribution, which can be expressed in **Eq. (2.1)** [14, 71]:

$$p(k, \mu) = e^{-\mu} \frac{\mu^k}{k!} \quad (2.1)$$

where μ is the mean number of photons per pulse and k is the actual number of photons in a pulse. In Figure 2.2, the photon distributions according to **Eq. (2.1)** are visualised for a mean photon number μ of 0.1, 0.2, 0.3, and 0.4, respectively. As shown, there is a lower probability of having multiple photons present in a single pulse when using a lower value of μ . Therefore, the issue of Eve's PNS attacks on multi-photon pulses can be mitigated in a QKD link by further reducing the intensity of the signal pulses. However, having a lower value of μ also gives a limited possibility of single photon pulses. This will decrease the yield of raw keys as well as the maximum transmission distance due to the inevitable loss in the channel. As discussed in Section 1.2.1, this problem can be efficiently solved in practice by the use of decoy states, which are added into the optical pulse train by randomly modulating the power of some of the emitted pulses.

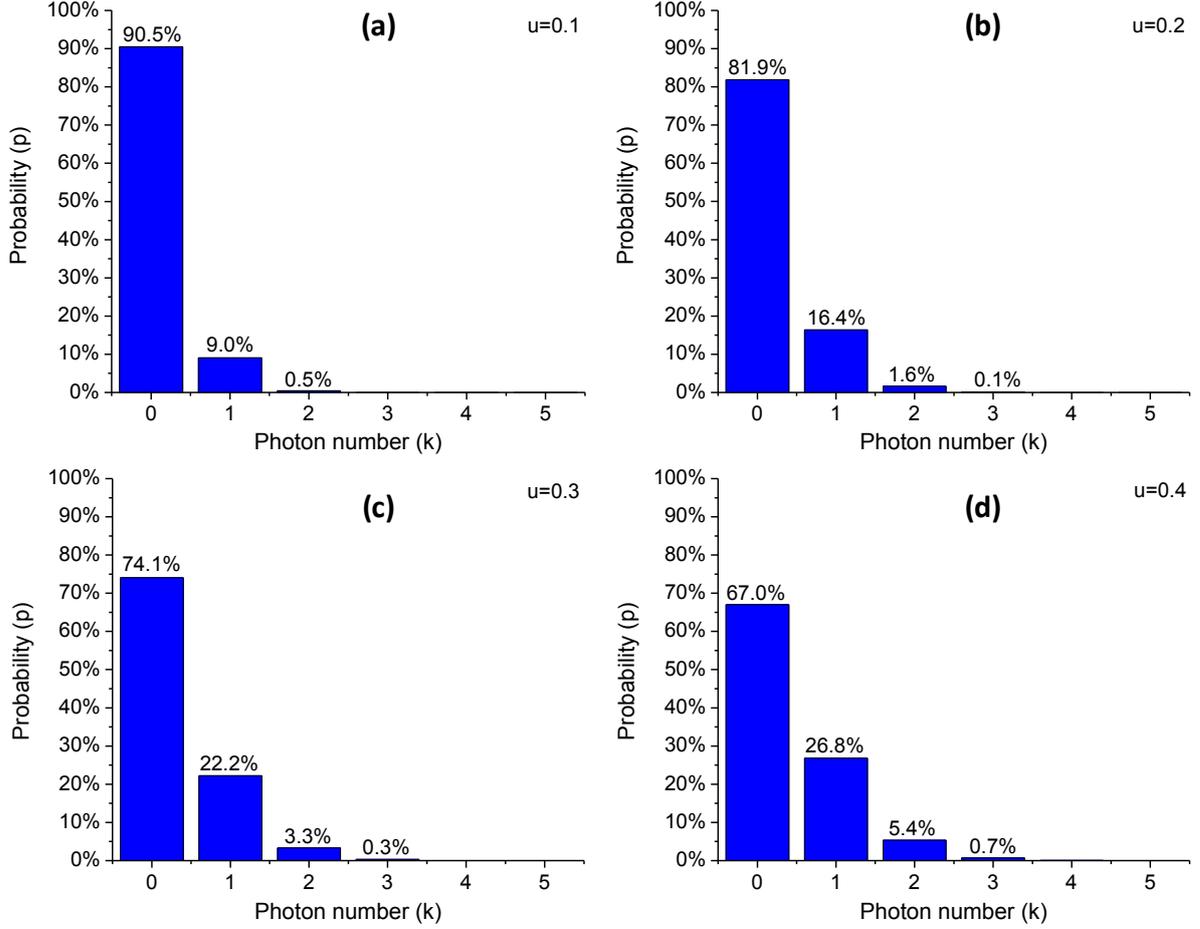


Figure 2.2 Photon distribution in optical pulses with mean photon number of a) 0.1, b) 0.2, c) 0.3, and d) 0.4

At the receiver end, Bob uses single photon detectors (SPDs) to detect the single photons sent from Alice. The most often used SPDs in DVQKD systems uses InGaAs/InP Avalanche Photodiodes (APDs), which are able to detect photons with wavelengths from about 950 to 1650 nm [14]. APD-based SPDs normally work in Geiger mode, in which a reverse bias voltage higher than the breakdown voltage is applied on a APD so that a significant avalanche effect can be triggered by an electron hole pair created by a single incident photon. To avoid the damage to the APD by the huge current, a quenching circuit is necessary to reset the APD operation repeatedly by pulling down the bias voltage to below the breakdown voltage. Gated-mode quenching is commonly used in DVQKD detections, in which the applied bias DC voltage is set to be slightly lower than the breakdown voltage so that the APD does not detect single photons. At the arrival time of each photon pulse from Alice, Bob increases the bias voltage above the breakdown voltage of the APD for a short time window so that the avalanche effect is then triggered periodically [5]. The maximum repetition rate of a gated Geiger mode

InGaAs/InP APD is typically limited to tens of MHz, although GHz rates have been demonstrated by using techniques such as self-differencing circuits [72] and the sine wave gating method [18, 19, 73].

In general, the main parameters used to characterise SPDs in DVQKD links are [1, 5, 18]:

- Quantum detection efficiency: the probability of a detection event when a photon is incident. This efficiency is desired to be as high as possible.
- Background noise counts: including Dark counts and Afterpulses. A Darkcount is the background noise generated in the SPD without an incoming photon being present. This current is caused by carriers created by a thermal or tunnelling process. Afterpulses cause wrong photon counts induced by previous photon detections. This is fundamentally due to trapped carriers, created by previous avalanches [1]. Background noise counts are unwanted detection events, which lead to an increased QBER [18].
- Dead time: the recovery time for an APD to be reset after a detection. During this period, the APD is unable to detect photons. Dead time limits the detection rate. However, the carriers trapped in defect states reduce in number exponentially with time [74]. Therefore, the dead time needs to be optimised with regards to the trade-off between minimal afterpulses and a maximised count rate [75].

2.2.2 Practical implementation

As discussed in Section 1.2.1, in the original BB84 QKD proposal, the qubits are encoded in the polarisation of single photons. A typical QKD schematic based on a polarisation encoding scheme is shown in Figure 2.3 [12, 76]. For Alice, four laser sources are used to generate photon pulses polarised in four states (i.e. horizontal, vertical, -45° , $+45^\circ$). The optical paths are combined using optical couplers onto a single fibre, and each of the lasers is triggered correspondingly to generate different polarisation states. Alternatively, state selection can be implemented by optical switching with the lasers kept on all the time. The modulated photon pulses are then attenuated to the single photon level by an optical attenuator before being sent to Bob via optical fibre. At this stage, decoy states can be added by giving some of the pulses lower average power. At Bob, a polarisation controller is normally used to compensate for polarisation rotation in the optical fibre. The photon pulses are then split or switched to two different paths for detections in rectangular and diagonal bases, and each base corresponds to two SPDs to represent '1' and '0', respectively [12, 76].

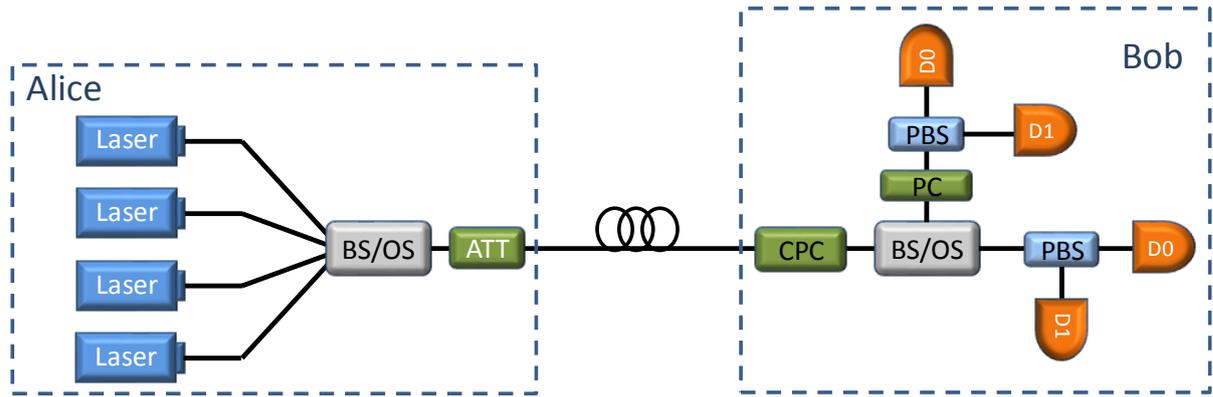


Figure 2.3 Typical implementation configuration of polarisation-based DVQKD. BS: beam splitter, OS: optical switch, ATT: optical variable attenuator, CPC: compensating polarisation controller, PBS: polarisation beam splitter, PC: polarisation controller (45° rotation), D1 and D0: SPDs [12, 76]

Alternatively, BB84 based DVQKD can be also used in phase encoding schemes. The idea of encoding qubits into the phases of single photons was proposed in 1992 [77]. The practical implementation is based on phase modulation/demodulation using a Mach-Zehnder interferometer (MZI). The two most common configurations are the double MZI implementation and the so-called “plug-and-play” implementation. In a double MZI configuration, Alice and Bob each have an MZI installed, as shown in Figure 2.4(a) [76, 78]. Optical pulses from a laser are sent through an MZI, and Alice applies a phase shift ϕ_A to one arm using a phase modulator (PM) and an optical delay in the other arm. The power of the two consecutive pulses is then attenuated to the desired level and sent to Bob via the optical fibre link. Bob uses another MZI. A phase shift ϕ_B is applied to one of the paths, and the same delay line is used for the other path. For each pulse generated from the laser, three peaks will be detected at different times. The first peak and the third peak correspond to travel of the photons through the PMs and delay lines of the MZIs, respectively. The centre peak is due to the photons that successively travel through the PM in Alice and the delay line in Bob, or successively travel through the delay line in Alice and the PM in Bob [1]. Therefore, the key can be distilled from the central peak due to the interference between phase modulations applied by Alice and Bob. Specifically, Alice controls the phase modulator and encodes bits 0 and 1 in the phase shifts ϕ_A of 0 and π (first basis) or $1/2\pi$ and $3/2\pi$ (second basis). To detect the bit values, Bob applies a phase shift of 0 to the arrival photons for the first basis and a phase shift of $1/2\pi$ for the second basis [18, 76, 78].

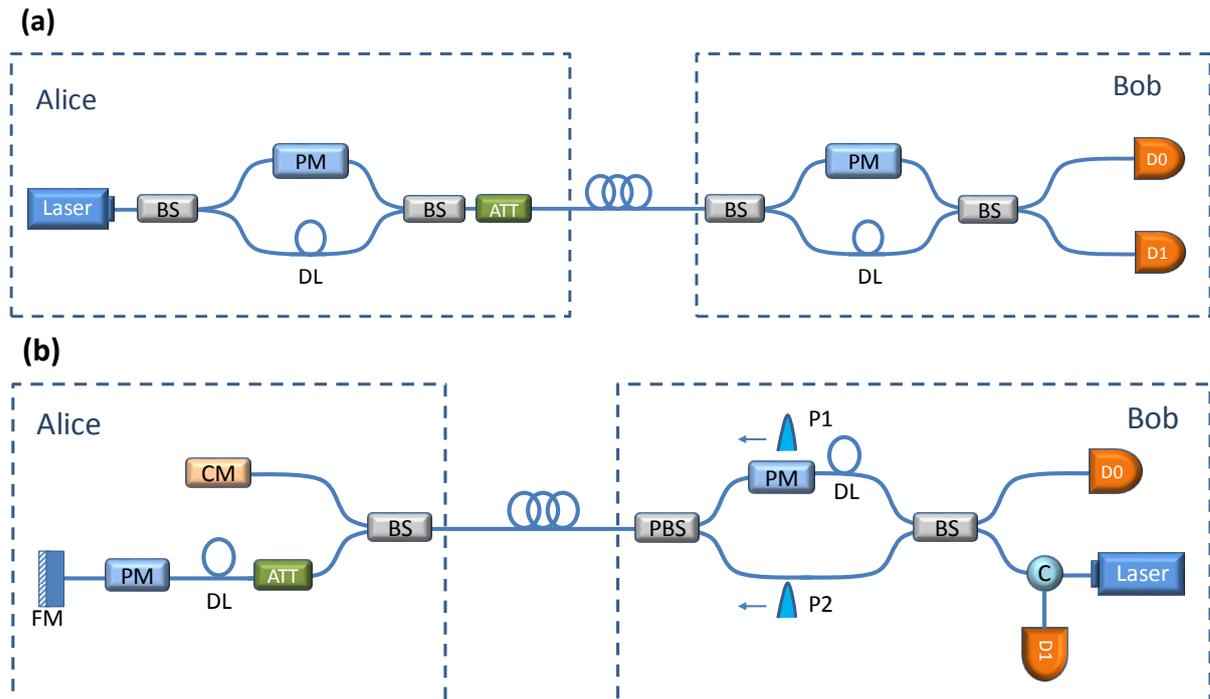


Figure 2.4 Typical implementation configuration of phase-based DVQKD. a) double MZI configuration. b) plug-and-play configuration. PM: phase modulator, DL: optical delay line, CM: classical monitor, C: circulator, FM: Faraday mirror [1, 76, 78]

Phase encoding QKD can be also implemented in a “plug-and-play” configuration [79], in which both the laser source and detector are put in the same physical location. As shown in Figure 2.4(b) [1], each laser pulse is split into two half pulses, P1 and P2, which travel through the upper and lower arms of the MZI, respectively. As P1 takes a longer optical path than P2, P1 experiences a short delay with respect to P2 at the output of Bob. Since P1 and P2 are combined in the polarisation beam splitter (PBS), their polarisations are orthogonal to each other. The PM at Bob remains inactive at this stage. The pulses are then sent to Alice via an optical fibre and split by a BS. The BS normally has an uneven coupling ratio (e.g. a coupling ratio of 90/10) with the purpose of passing a large fraction of photons to a classical monitor, which is used as a synchronizing signal. The rest of the photons successively travel through an attenuator, delay line and a phase modulator, and are reflected by an Faraday mirror (FM) which returns light with a 90° rotation of polarisation. Alice only applies phase modulation to P2 to encode her random bit value on it. Due to the presence of the FM, P1 and P2 are reflected back and their polarisations are orthogonally shifted. An attenuator is again used to reduce the photon number to the desired level. The delay line is used to avoid Rayleigh backscattering in the reflected quantum signal from Alice due to the strong pulse received from Bob. When the pulses travel back to Bob and arrive at the PBS, P1 now is routed to the lower path and P2 to

the upper path as their polarisations are orthogonal to the original orientations. In order to decode the bit value, Bob applies his phase modulation to P2 as his basis selection. P1 and P2 are then combined and interfered at BS, and the bit values can be detected by the corresponding SPD [1].

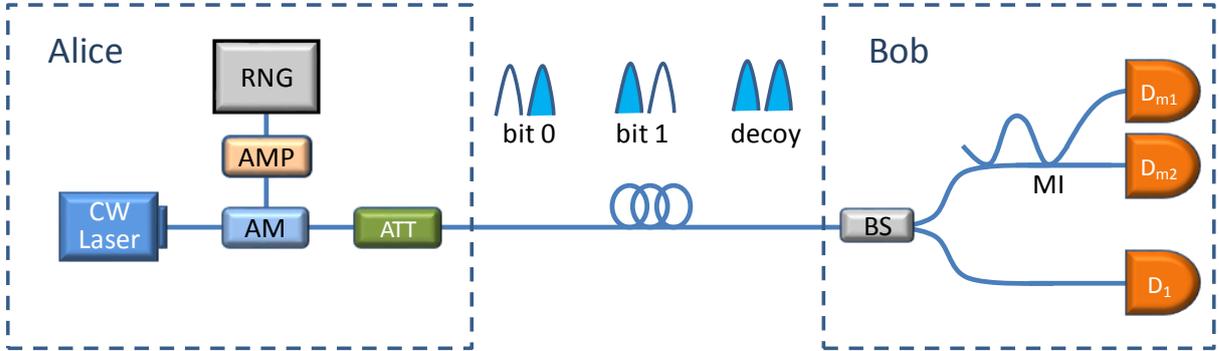


Figure 2.5 Schematic of the practical implementation of COW DVQKD. RNG: random number generator, AMP: electrical amplifier, AM: amplitude modulator, MI: monitoring interferometer [80]

Last but not least, DVQKD can also be implemented using the COW protocol with a simpler practical setup [25, 80], this being currently used in the commercialized QKD system of *id Quantique*. The conceptual schematic of its implementation is illustrated in Figure 2.5 [80]. Alice modulates a continuous wave laser using an amplified random number generator, resulting in coherent laser pulses with desired time shifts. The pulses are then attenuated to the single photon level for secure transmission. This approach can be regarded as a time encoding scheme. Each bit value is encoded into a two-pulse sample with an empty pulse and a full pulse. For example, bit 1 is carried by an empty pulse followed by a non-empty pulse, while bit 0 is encoded in the other way around. In addition, decoy states are randomly added into the pulse train as two successive full pulses to increase the security. At Bob's site, the received pulses are split into a signal path and a monitoring path by an asymmetric BS with a splitting ratio of $t_B:(1-t_B)$, where t_B is close to 1. Bit values are detected as the arrival time of the photons at D_1 following the signal path. The detection of decoy states at D_1 is random and is discarded after Alice announces their time slots at the end of transmission. The coherence between any two adjacent pulses is checked by D_{m1} and D_{m2} , together with an asymmetrical interferometer to monitor eavesdropping. This is practical thanks to the coherence of the laser, as any two successive non-empty pulses (i.e. either two pulses within a decoy state or a bit sequence of 1-0) would interfere at the interferometer and will always trigger the same monitoring detector D_{m1} . Detection in D_{m2} indicates possible attacks by Eve. After transmitting all the bits, Alice

and Bob can estimate the extent of information accessed by Eve by evaluating the visibility of the interferometer for two successive non-empty pulses. The visibility is defined as [25]:

$$V = \frac{p(D_{m1}) - p(D_{m2})}{p(D_{m1}) + p(D_{m2})} \quad (2.2)$$

where $p(D)$ is the probability of a detection event at the corresponding detector. The lower the value of V , the more information can be accessed by Eve [25, 53, 80].

2.2.3 Secret key analysis and modelling

The performance of any practical QKD system is evaluated in terms of the QBER and the secure key rate varying with transmission distance. In general, the lower bound of the secure fraction of transmitted information is given as the common information between Alice and Bob minus the minimum Eve's information from either Alice or Bob [14]:

$$r = I(A:B) - \min(I_{EA}, I_{EB}) \quad (2.3)$$

In a standard BB84 QKD system and assuming a truly single photon source, $I(A:B) = 1 - H_2(QBER)$ and $\min(I_{EA}, I_{EB}) = f_{ec}H_2(QBER)$ [81]. $H_2(x)$ is the binary Shannon entropy function: $H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$. f_{ec} corresponds to the efficiency of error correction. Therefore, the secure key rate in the unit of bits per pulse can be expressed as [14, 82]:

$$S = qQ\{1 - H_2(E) - f_{ec}H_2(E)\} \quad (2.4)$$

where q is the basis reconciliation factor which depends on the protocol implementation, $q = 0.5$ for the standard BB84 protocol because the probability Alice and Bob have compatible bases is 50%. Q is the gain of the signal pulse, which indicates the probability of transmission of the qubits, and E stands for the QBER.

In a practical BB84 QKD link, highly attenuated laser pulses are used instead of truly single photon sources. The secure key is only distilled from single photon pulses. Thus, **Eq. (2.4)** is modified to be [23, 83]:

$$S = q\{Q_1[1 - H_2(e_1)] - Q_\mu f_{ec}H_2(E_\mu)\} \quad (2.5)$$

where Q_1 and e_1 are the gain and error rate for the single photon states, while Q_μ and E_μ are the total gain and QBER, respectively. The Q and E are explained in detail as follows. Firstly, the gain of n -photon pulses Q_n is defined as:

$$Q_n = Y_n p(n, \mu) = Y_n \frac{\mu^n}{n!} e^{-\mu} \quad (2.6)$$

where $p(n, \mu)$ is the Poisson distribution given in **Eq. (2.1)**. The first term Y_n is defined as the probability of a detection event on Bob's side given that Alice sends out an n -photon pulse [83], which is a function of the background noise counts Y_0 (e.g. dark counts) and the transmittance of the n -photon state η_n :

$$Y_n = Y_0 + \eta_n - Y_0 \eta_n \cong Y_0 + \eta_n \quad (2.7)$$

$$\eta_n = 1 - (1 - \eta)^n \quad (2.8)$$

where η is the transmittance of the whole link, taking into account losses inside Bob and the transmission of the fibre link t . Thus, the total gain of photons Q_μ can be expressed as the sum of all the possibilities [83]:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu} \quad (2.9)$$

Then, let us investigate the photon number dependent QBER generated in the link. The error rate of the n -photon pulse e_n is defined as [83]:

$$e_n = \frac{e_0 Y_0 + e_d \eta_n}{Y_n} \quad (2.10)$$

where e_0 is the error rate from a vacuum pulse, which is 50% assuming that the output due to the background is random, and e_d denotes the probability of wrong detection (i.e. a photon is detected by the non-corresponding detector). Then the total QBER is then expressed as [83]:

$$E_\mu = \frac{\sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} e^{-\mu}}{Q_\mu} = \frac{e_0 Y_0}{Q_\mu} + \frac{e_d (1 - e^{-\eta\mu})}{Q_\mu} \quad (2.11)$$

The first term in the above equation is the contribution from the dark count and other background noise, which increases with distance. The second term can be considered to be independent of the distance, as the background noise rate is relatively small (of the order of 10^{-6}). It is normally used to evaluate a QKD optical setup [1].

In a BB84 link without decoy states, Eve can block out single photon pulses and make the channel transparent to multi-photon pulses. Therefore, to estimate the worst-case secure key rate, the following two conditions must be assumed.

1. All multi-photon pulses are detected by Bob and all losses are from the pulses containing only one photon. Thus, the lower bound for the gain of single photon pulses Q_1 can be estimated as [84]:

$$Q_1 = Q_\mu - \sum_{n=2}^{\infty} \frac{\mu^n}{n!} e^{-\mu} \quad (2.12)$$

The second term of the above equation stands for the probability of sending multi-photon pulses from Alice. When a truly single photon source is assumed, this term is equal to zero.

2. All the error (i.e. QBER) is assumed to be caused by single photon pulses, while multi-photon pulses do not cause any error. Thus, the upper bound for error rate from the single photon states e_1 is given by [84]:

$$e_1 = \frac{E_\mu Q_\mu}{Q_1} \quad (2.13)$$

Now, the performance in terms of key generation of the standard BB84 DVQKD can be evaluated by substituting Q and E in to **Eq. (2.5)**. For practical cases using Poisson sources, the performance of QKD links depends largely on the mean photon number. When a higher value of μ is set, secure key generation is limited to a very short distance. This is due to the higher probability of having more than one photon in a transmitting pulse. On the other hand, when μ is very small, the QKD link has a lower gain of single photon pulses Q_1 and hence worse performance. Therefore, the mean photon number of sending pulses μ needs to be optimised for maximum secure key generation, by making a trade-off between having a lower probability of multiphoton pulses from a practical laser source and getting a higher value for Q_1 .

Figure 2.6 shows the secure key rates as a function of transmission distance, calculated for an example BB84 QKD link with an ideal truly single photon source and a practical Poisson source (a highly attenuated laser) with different levels of μ (the mean photon number). The system parameters used in the calculations are shown in the caption of Figure 2.6, which is from one of the state-of-the-art experimental demonstrations of a QKD link [85].

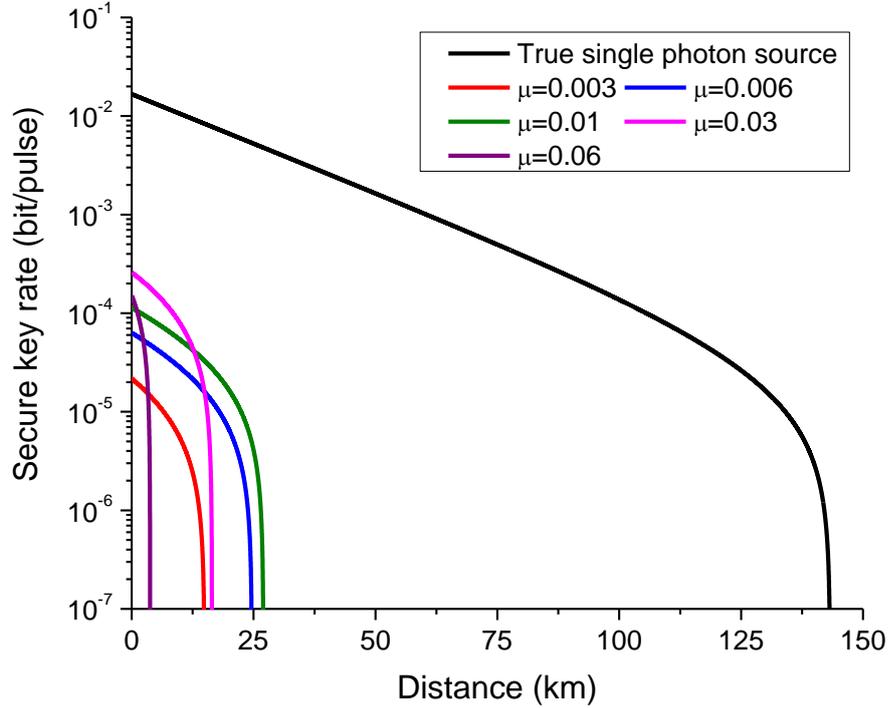


Figure 2.6 The calculated secure bit rate as a function of transmission distance for the standard BB84 QKD system using a Poisson or an ideal single photon source. (The error correction efficiency f_{ec} is assumed to be 1.1, the system error e_a is fixed at 2.3%, the background noise is assumed to be 6.8×10^{-6} , the channel loss coefficient is set as 0.2 dB km^{-1} , and Bob's detection efficiency is fixed at 5% [85])

It can be seen from Figure 2.6, that all curves dramatically drop at a maximum transmission distance beyond which Eve is able to access more information than that shared between Alice and Bob. With a Poisson source, the maximum secure key transmission distance is first increased as μ increases, due to the increased gain of the photons according to **Eq. (2.9)**. However, when μ is further increased, the probability of having multiple photons in a single pulse rises, increasing the possibility of PNS attacks. Therefore, the secure key can be only shared within a short range. Overall, compared to the case with an ideal single photon source, the performance of a practical Poissonian source is much worse due to the presence of multiphoton pulses.

Fortunately, the security of BB84 can be enhanced by adding decoy states. In the simplest decoy protocol, a set of decoy pulses also from a highly attenuated laser source but with mean photon number v ($v < \mu$) are randomly interleaved into the signal pulse trains. The values of

μ and v are decided by Alice, which normally needs to be optimised to maximise the secure key rate [83]. Using a similar approach to that for Q_μ and E_μ for the signal pulses, the gain Q_v and QBER E_v for decoy states are given by [83]:

$$Q_v = \sum_{n=0}^{\infty} Y_n \frac{v^n}{n!} e^{-v} \quad (2.14)$$

$$E_v = \frac{\sum_{n=0}^{\infty} e_n Y_n \frac{v^n}{n!} e^{-v}}{Q_v} \quad (2.15)$$

Due to the presence of decoy states, the lower bound of single photon gain Q_1 becomes [71, 83]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v - v^2} \left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - E_\mu Q_\mu e^\mu \frac{\mu^2 - v^2}{\frac{1}{2}\mu^2} \right) \quad (2.16)$$

By assuming that all errors are in single photon states, the upper bound of the error rate for states e_1^U is written as [71, 83]:

$$e_1^U = \frac{E_\mu Q_\mu}{Q_1^L} \quad (2.17)$$

Substituting the updated Q_1 and e_1 to **Eq. (2.5)**, the improved secure key rate can be obtained. Normally, in an advanced decoy-state BB84 protocol, two sets of decoy states with different intensities v_1 and v_2 are generated by Alice along with the signal pulses. In this case, the lower bound for the gain of single photon states Q_1 and the upper bound for the QBER for single e_1 photon states can be estimated as [85]:

$$Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu v_1 - \mu v_2 - v_1^2 + v_2^2} \left(Q_{v_1} e^{v_1} - Q_{v_2} e^{v_2} - \frac{v_1^2 - v_2^2}{\mu^2} (Q_\mu e^\mu - Y_0^L) \right) \quad (2.18)$$

$$e_1^U = \frac{E_\mu Q_\mu e^\mu - \frac{1}{2} Y_0^L}{Q_1^L e^\mu} \quad (2.19)$$

Similarly, secure key rates at different transmission distances can be then evaluated by substituting the updated Q_1 and e_1 to **Eq. (2.5)**.

In a DVQKD link using the COW protocol, the secure key rate equation is also derived from **Eq. (2.3)** as follows [80]:

$$S = qfQ\{1 - H_2(E) - I_E\} \quad (2.20)$$

where, Q and E can be calculated using **Eq. (2.9)** and **Eq. (2.11)**. Unlike the BB84 protocol, in which the quantum signal is generated and gathered pulse by pulse, Eve's information I_E in the COW is derived differently [25, 80]:

$$I_E = \mu(1 - t) + (1 - V) \frac{1 + e^{-\mu t}}{2e^{-\mu t}} \quad (2.21)$$

where, V is the visibility of the monitoring interferometer given in **Eq. (2.2)**.

In Figure 2.7, we estimate the secure key rate as a function of transmission distance for a BB84 QKD link with and without decoy states as well as using the COW protocol. The system parameters are kept as the same as in Figure 2.6 [85].

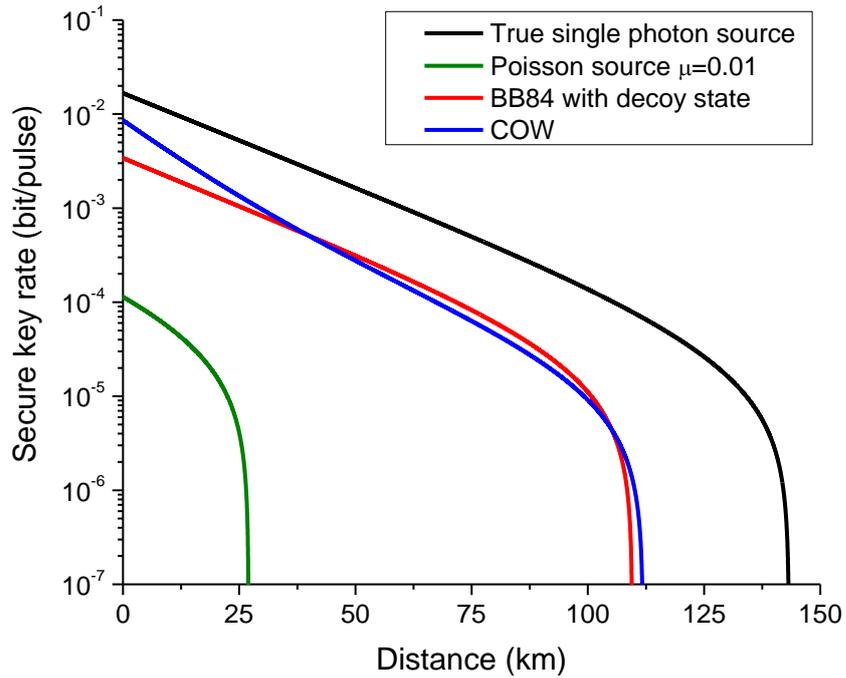


Figure 2.7 The simulated secure bit rate as a function of transmission distance for the QKD links using BB84 and COW protocols. (For decoy state BB84, the mean photon numbers for signal and decoy states from [85] are $\mu = 0.55$ $v_1 = 0.1$ and $v_2 = 7.6 \times 10^{-4}$, respectively. The calculation for COW protocol uses typical value of $\mu = 0.5$ and $V = 0.9$ [25])

The plot clearly shows that introducing decoy states to the BB84 protocol not only extends the maximum key transmission distance but also significantly improves the secure bit rate. With

decoy states, the maximum transmission distance of a BB84 QKD link is extended from less than 27 km to 109 km in this example simulation. The calculated secure key rates are also greatly improved by the addition of decoy states. In addition, a QKD link using the COW protocol under the same systemic parameters offers a similar performance using the security analysis approach given in [80].

2.3 Practical CV QKD links

2.3.1 Coherent detection

The most distinctive difference between the practical implementations of DVQKD and CVQKD is the detection techniques employed. Unlike the single-photon transmission in DVQKD, CVQKD is based on modulating and measuring the quadrature values of electromagnetic fields. Therefore, the detection of qubits is conducted using coherent detection: a balanced homodyne detector (BHD) (or balanced heterodyne detector which is composed of two BHDs) rather than SPDs. The schemes can be illustrated in Figure 2.8.

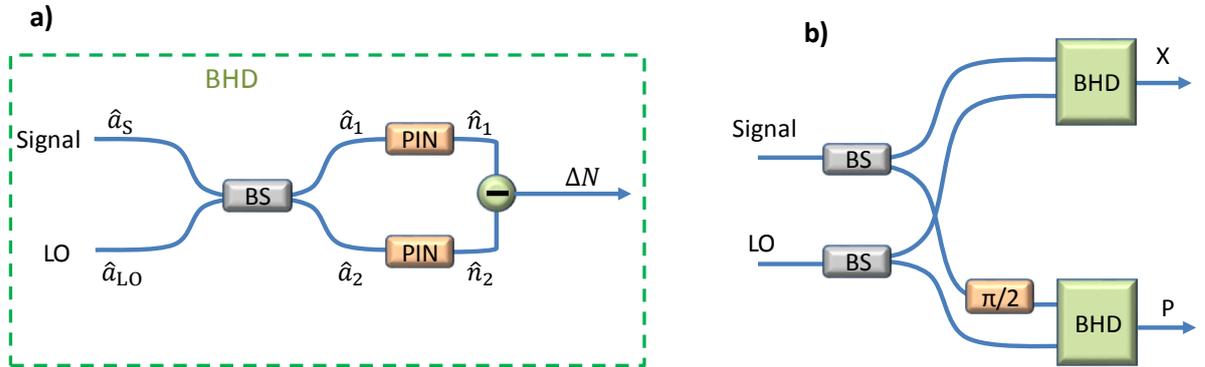


Figure 2.8 schematics of (a) the balanced homodyne and (b) the heterodyne detection [86]

As introduced before, in GMCS CVQKD, Alice modulates quadratures x and p of each coherent laser pulse and sends them to Bob. When the optical signal pulse train arrives at Bob's BHD, it is superimposed on strong synchronous reference light known as local oscillator (LO), at a balanced beam splitter. LO is also normally pulsed in real implementations, as it is practically generated from the same source as the signal and time-multiplexed with signal pulses during the transmission, as shown in the next Section. By expressing the signal quantum states and LO using annihilation operators \hat{a}_S and \hat{a}_{LO} , the outputs from the beam splitter are given by [3, 86]:

$$\hat{a}_{1,2} = \frac{1}{\sqrt{2}}(\hat{a}_S \pm \hat{a}_{LO}) \quad (2.22)$$

They are then detected by PIN diodes, and the photocurrents can be represented by photon number operators $\hat{n}_1 = \hat{a}_1^\dagger \hat{a}_1$ and $\hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2$, where \hat{a}^\dagger (creation operator) represents the adjoint of the operator \hat{a} . The output of the BHD is finally obtained by subtracting these two photocurrents [3, 86]:

$$\Delta N = \hat{n}_2 - \hat{n}_1 = \hat{a}_S^\dagger \hat{a}_{LO} + \hat{a}_{LO}^\dagger \hat{a}_S = |L|(\hat{a}_S^\dagger e^{i\theta} + \hat{a}_S e^{-i\theta}) \quad (2.23)$$

where $|L|$ and θ are the amplitude and relative phase of the LO. Since the signal states can be decomposed into quadrature components as:

$$\hat{a}_S = \frac{1}{\sqrt{2}}(\hat{a}_X + j\hat{a}_P) \quad \text{and} \quad \hat{a}_S^\dagger = \frac{1}{\sqrt{2}}(\hat{a}_X - j\hat{a}_P) \quad (2.24)$$

ΔN can be expressed using quadrature operators \hat{a}_X and \hat{a}_P [87]:

$$\Delta N = \sqrt{2}|L|\{\hat{a}_X \cos(\theta) + \hat{a}_P \sin(\theta)\} \quad (2.25)$$

The term inside the bracket indicates the phase-dependent quadrature quantities of the detected signal states. Therefore, the value of the signal quadratures x or p which are projected onto the field of the LO can be determined by Bob by modulating the relative phase θ of the LO to 0 or $\pi/2$. For the case of heterodyne detection, as shown in Figure 2.8(b), the signal is split into two BHDs and Bob can simultaneously measure both quadratures x and p by applying a phase shift of $\pi/2$ to the signal path of only one BHD.

In a practical GMCS CVQKD link, after Bob records the correlated quadrature values of the incoming states $|\alpha\rangle = |X_A + iP_A\rangle$ sent from Alice, two parameters need to be estimated which are used for later secure key distillation: the overall channel transmission T , and the excess noise ξ (due to device imperfections or the action of an eavesdropper). Parameter estimation can be done through the following equations [39]:

$$\text{Var}(X_A) = \text{Var}(P_A) = V_A \quad (2.26)$$

$$\langle X_A X_B \rangle = \langle P_A P_B \rangle = \sqrt{\eta_B T} V_A \quad (2.27)$$

$$\text{Var}(X_B) = \text{Var}(P_B) = \eta_B T V_A + N_0 + \eta_B T \xi + N_{ele} \quad (2.28)$$

$$\text{Var}(X_{B0}) = \text{Var}(P_{B0}) = N_0 + N_{ele} \quad (2.29)$$

where η_B is the overall transmission efficiency of Bob, N_0 is the shot noise variance (vacuum noise) which is obtained by presenting the LO alone to BHD, and N_{ele} is the electronic noise of the BHD. When the parameters T and ξ are determined, Alice and Bob can bound Eve's information and extract the final secure key, as explained in Section 2.3.3.

In contrast to the APDs employed in DVQKD, the BHD detects the qubits using PIN diodes with higher detection efficiency, which offer the promising potential of enabling much higher raw key rates in CVQKD. In addition, the BHD used in a CVQKD link is compatible with standard telecommunication techniques, which offers better practicability and feasibility in integrating with today's communication networks. However, the common disadvantage of BHDs is the noisy measurement of quadratures. The loss experienced by the quantum signal in the fibre and additional noise added during the transmission cause a decrease in the signal-to-noise ratio (SNR) which limits the transmission distance of secure keys [14].

2.3.2 Practical implementations

As introduced earlier, in a GMCS CVQKD link, Bob performs coherent detection to measure the quadratures of coherent states together with a reference LO, hence obtaining the quantum signal. From a practical point of view, the coherent states are prepared by Alice in the form of modulated weak pulses from a coherent laser, while the LO can be generated either from the same laser by Alice or an independent laser used by Bob. Depending on the location of LO generation, the link can be implemented using either the Transmitted Local Oscillator (TLO) or Local Local Oscillator (LLO) schemes [88].

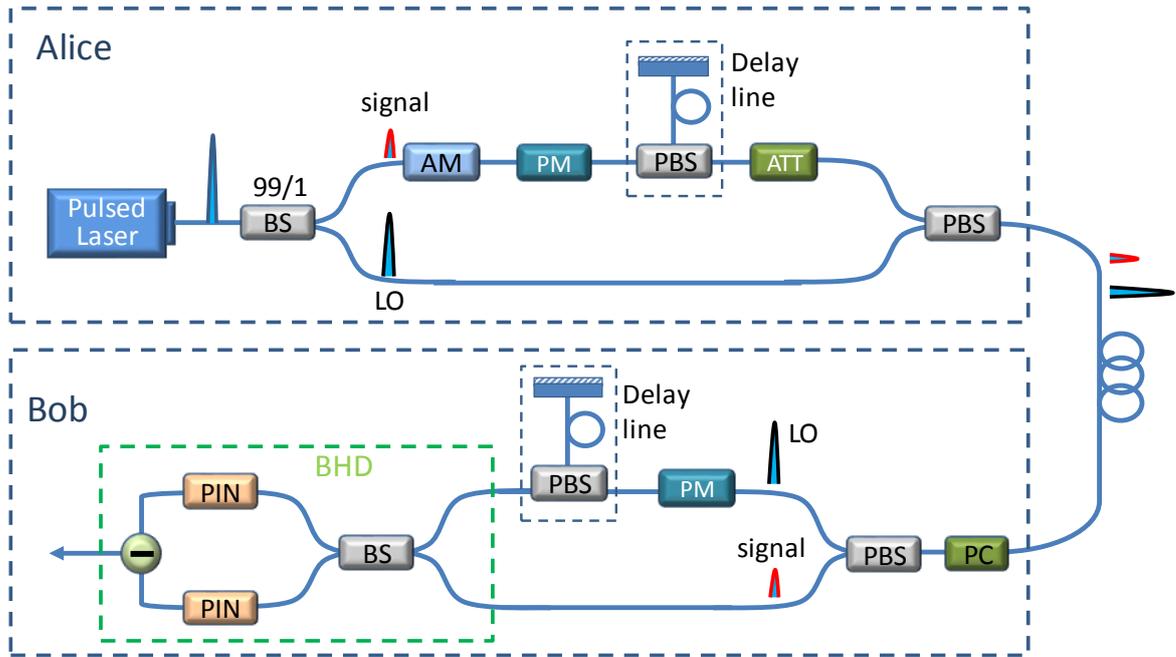


Figure 2.9 Practical implementation of GMCS CVQKD with TLO [46, 89]

Most implementations of GMCS CVQKD are based on the TLO approach with a BHD, as detailed in Figure 2.9 [45, 46, 89, 90]. In Alice, coherent optical pulses are generated from a pulsed laser and split into a weak quantum signal and a bright LO by an asymmetric BS (normally with a high splitting ratio of 99/1). In the signal path, the amplitude and phase of the pulses are modulated so that the two quadratures x and p follow a Gaussian distribution, using an intensity modulator and a phase modulator, respectively. A delay line is used to set the delay between the signal path and the LO path, which is normally implemented by an FM and a length of fibre. The power of the signal pulses is then controlled by an optical attenuator so that the quadratures have the desired variance. The LO and signal are multiplexed at a PBS in both polarisation and time and sent to Bob through the same fibre channel, so that crosstalk from the LO to the weak signal is greatly reduced. In addition, during propagation, the quantum signal and LO experience the same phase drift. Therefore, a stable phase difference between them can be maintained. This is the major advantage of a TLO scheme. On Bob's side, a polarisation controller is first used to compensate for the change of polarisation in the fibre link. The signal and LO are then polarisation-demultiplexed by a PBS into two optical paths which are connected to a BHD. In order to match the arrival time of signal pulses at the input of the homodyne detector, the same length of delay line is applied to the LO path. From the output of the BHD, Bob can obtain the value of either the x or p quadrature by randomly applying a $\pi/2$ or 0 phase shift to the LO pulses with the help of a PM [46, 89]. The GMCS CVQKD with TLO can be also implemented using heterodyne detection, in which case Bob is able to measure

both the quadratures of each signal pulse without a phase modulator. However, the additional BS introduces a 3dB loss to the signal which in turn reduces the key rate.

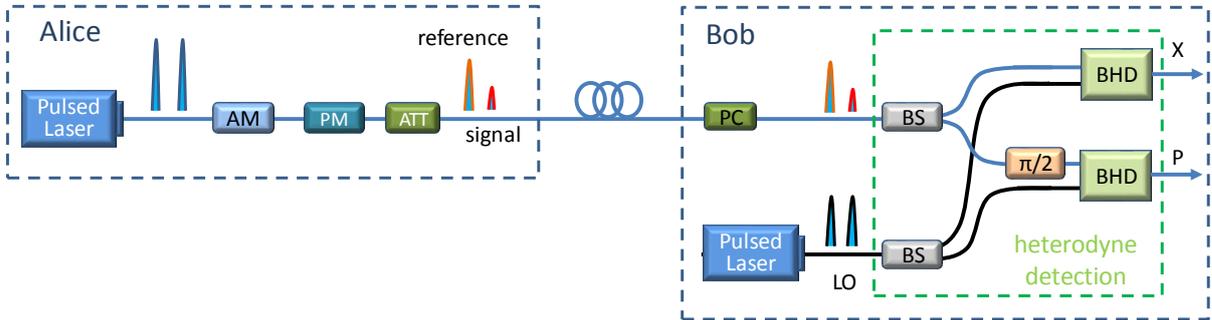


Figure 2.10 Practical implementation of GMCS CVQKD with LLO. [91-93]

A typical implementation of a GMCS CVQKD system based on the LLO scheme has been reported in [91-93] which avoids the need for multiplexing the LO and signal as well as the transmission of the LO from Alice to Bob. A schematic of the setup is shown in Figure 2.10. Similar to the signal path in a TLO design, coherent states in the form of Gaussian modulated optical pulses are prepared by Alice and sent to Bob via fibre link. Another set of pulses with a fixed phase and amplitudes, which are known as the “phase reference”, are generated by Alice in different time bins and transmitted along with the signal. The amplitude of phase reference pulses is set to be much higher than the signal. Bob uses the two BHDs (i.e. heterodyne detection) to measure both quadratures of the signal and phase reference pulses. The phase information from the measured reference pulses is then used to correct the phase change of the signal during transmission. Specifically, as the LO is generated by a second free-running laser which is locally located with Bob, the quadrature measurements have a reference frame which is misaligned from the frame used by Alice by a phase difference θ_d , as shown in Figure 2.11 [92]. By publicly announcing the phase information (or quadrature values) of the reference pulses, the estimated phase angle θ_d is applied to rotate and remap Alice’s or Bob’s state quadrature values.

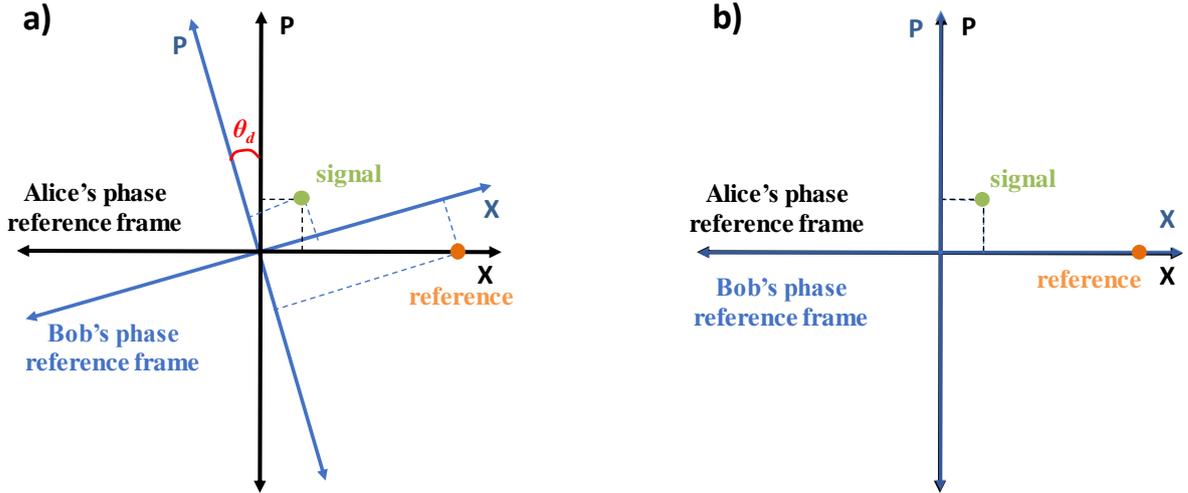


Figure 2.11 a) Illustration of the misalignment between Alice's and Bob's phase reference frames. The same signal states would give Alice and Bob different quadratures. b) corrected state based on the phase value of the reference state [92]

From the perspective of practical implementation, both TLO and LLO designs have their advantages and disadvantages. In a TLO design, the main benefit is that a constant phase difference between the signal and LO is promised during the transmission. This is because the LO and signal are generated from the same source and propagate through the same fibre channel, where they experience equivalent phase noise. However, for a given LO laser located at Alice, the power of the received LO pulses is reduced over longer transmission distances, and it is not able to meet the requirement for coherent detection by Bob [88]. There is also a practical challenge to providing significant power output from Alice's laser.

On the other hand, although LLO-based CVQKD also has those problems, the main challenge is to practically keep a stable relative phase between the signal and LO [88]. Practically, the rotated signal states using reference pulses are still not truly corrected due to the effect of linewidth of the two individual lasers, which causes unstable drift between the reference frames of Alice and Bob. This inevitably introduces extra phase noise during the key transmission of the LLO based CVQKD link, which will be further discussed in the secret key analysis in the next section.

2.3.3 Secret key analysis and modelling

As in the case of DVQKD, the performance of CVQKD links is evaluated using the secure key rate as a function of transmission distance. The calculation of secure keys in this thesis is based

on the commonly used approach given in [94] and [95], with reverse reconciliation [96]. In the following, the same formulas can be applied to both TLO and LLO based CVQKD, except that the LLO scheme introduces additional excess noise contributed by phase drifting, as shown later in this section. First of all, the formula for the final secure key information between Alice and Bob is given by [14]:

$$r = \beta I_{AB} - \chi_{BE} \quad (2.30)$$

where I_{AB} is the mutual information shared between Alice and Bob, β is the reconciliation efficiency, and χ_{BE} is the maximum information accessible to Eve limited by the Holevo bound [97]. Using Shannon's equation, I_{AB} can be derived as [94]:

$$I_{AB} = \frac{1}{2} \kappa \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \quad (2.31)$$

where $\kappa = 1$ in the case of homodyne detection and $\kappa = 2$ in case of heterodyne detection. V is defined as $V = V_A + 1$, where V_A is Alice's modulation variance. χ_{tot} is the total noise added during the transmission, and is normally referred to as the channel input (i.e. at Alice). It includes both the noise added in the channel χ_{line} (contributed from both channel loss and excess noise) and the homodyne/heterodyne detection noise χ_h , and can be expressed using **Eq. (2.32)–(2.34)**. All the parameters here are implicitly expressed in the shot noise unit (SNU) N_0 , which is the vacuum noise fluctuation.

$$\chi_{line} = \frac{1}{T} - 1 + \xi \quad (2.32)$$

$$\chi_{hom} = \frac{[(1-\eta_B)+V_{ele}]}{\eta_B} \text{ or } \chi_{het} = \frac{[1+(1-\eta_B)+2V_{ele}]}{\eta_B} \quad (2.33)$$

$$\chi_{tot} = \chi_{line} + \frac{\chi_h}{T} \quad (2.34)$$

where η_B is the overall transmission efficiency of Bob, V_{ele} is the variance in output due to the detector's electronic noise, and T and ξ are the aforementioned transmission and excess noise featured by the channel, which can be experimentally estimated from Bob's measurement using **Eq. (2.26)–(2.29)**. Theoretically, ξ is assumed to have originated from eavesdropping. But, in practice, ξ can be contributed to by a range of experimental imperfections, such as relative intensity noise (RIN) noise, modulation noise, quantisation noise and phase noise. A full range of noise sources can be found in [98]. Here, the phase noise estimation is discussed which is the only term that differs in the secure key calculation in LLO and TLO based implementations.

Firstly, the relative phase φ_s between signal and LO can be written as:

$$\varphi_s = \theta_{sLLO} - \theta_{sSource} \quad (2.35)$$

In general, the phase noise V_{phase} is the variance of the difference between the estimated and actual relative phase φ_s , which can be expressed as [88]:

$$V_{phase} = V_{linewidth} + V_{channel} + V_{est} \quad (2.36)$$

The first term $V_{linewidth}$ corresponds to the variance due to the relative phase drift between two free running lasers in the LLO scheme, which can be estimated using their spectral linewidths $\Delta\nu_A$ and $\Delta\nu_B$ [88]:

$$V_{linewidth} = 2\pi \frac{\Delta\nu_A + \Delta\nu_B}{f_{rep}} \quad (2.37)$$

This represents the major contribution to phase noise in LLO implementations, because it is impractical to have an extremely low linewidth laser. Increasing the repetition rate would also pose other practical challenges related to the noise performance, which will be also discussed in Chapter 5.

The second term $V_{channel}$ is due to the relative phase φ_s changes during propagation in the optical fibre. In an LLO scheme, as the transmitting reference pulses used for phase correction follow exactly the same optical paths as the signal pulses, this effect will not contribute to the phase noise $V_{channel} = 0$ [88]. In a TLO scheme, the signal pulses and LO pulses propagate through different optical paths inside Alice and Bob, as shown in Figure 2.9. Practically, this effect can be mitigated by periodically sending pilot pulses along with the signal pulses, and similar phase estimation to that in an LLO can be applied.

The third term V_{est} indicates the estimation efficiency, which is the variance of the difference between the phase of the sending reference pulse and the estimated phase of reference pulse on reception in the LLO scheme. Similarly, this noise term applies to the pilot pulses in the TLO scheme. This term is inversely proportional to the amplitude of the reference/pilot pulse as [92]:

$$V_{error} = var(\hat{\varphi}_{R/P} - \varphi_{R/P}) = \frac{(\chi_{tot} + 1)}{E_{R/P}^2} \quad (2.38)$$

Therefore, the difference between the phase noise estimation of LLO and TLO schemes can be seen as:

$$V_{phase_TLO} = V_{channel} + V_{est} \quad (2.39)$$

$$V_{phase_LLO} = V_{linewidth} + V_{est} \quad (2.40)$$

The corresponding contribution to excess noise is given by [91]:

$$\xi_{phase} = 2V_A(1 - e^{-V_{phase}/2}) \approx V_A \times V_{phase} \quad (2.41)$$

Practically, as the term $V_{linewidth}$ normally dominates other contributions in the phase noise estimation, the phase noise ξ_{phase} in the LLO scheme. Hence the total excess noise ξ , is higher than that of TLO scheme [88].

Next, let us evaluate the maximum bound of Eve's information regarding Bob's key, which is bounded as [91, 95]:

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right) \quad (2.42)$$

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$:

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})} \quad (2.43)$$

with:

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{line})^2 \quad (2.44)$$

$$B = [T(V\chi_{line} + 1)]^2 \quad (2.45)$$

The second term of χ_{BE} , $\lambda_{3,4}$ is given by:

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})} \text{ and } \lambda_5 = 1 \quad (2.46)$$

where C and D are expressed differently for homodyne detection and heterodyne detection. For the case of a single BHD:

$$C_{hom} = \frac{A\chi_{hom} + V\sqrt{B} + T(V + \chi_{line})}{T(V + \chi_{tot})} \quad (2.47)$$

$$D_{hom} = \sqrt{B} \frac{V + \sqrt{B}\chi_{hom}}{T(V + \chi_{tot})} \quad (2.48)$$

For the case of heterodyne detection:

$$C_{het} = \frac{[A\chi_{het}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T(V + \chi_{line})) + 2T(V^2 - 1)]}{(T(V + \chi_{tot}))^2} \quad (2.49)$$

$$D_{het} = \left(\frac{V + \sqrt{B}\chi_{het}}{T(V + \chi_{tot})}\right)^2 \quad (2.50)$$

As a comparison, the secure key rate at different transmission distances is estimated and plotted in Figure 2.12 for an example GMCS CVQKD link with the different implementation methods introduced in Section 2.3.2. The phase noise in the LLO scheme is estimated by assuming that the linewidth of the lasers is 50 kHz and that there is a state of art system clock rate of 50 MHz [47].

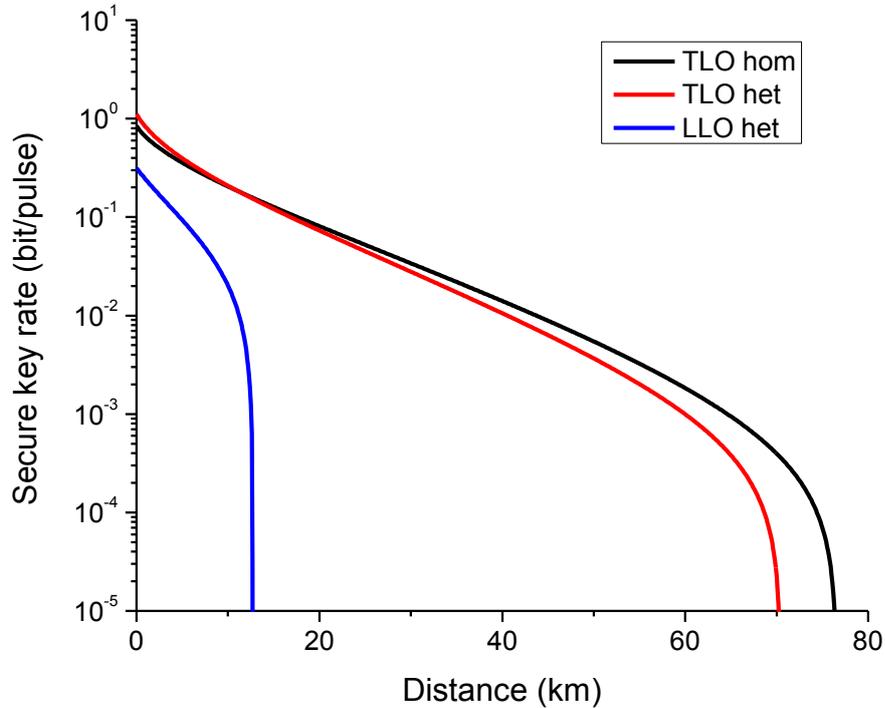


Figure 2.12 The calculated secure key rates for TLO and LLO- based CVQKD with homodyne(hom)/heterodyne(het) detection (electronic noise V_{ele} is fixed at 0.01, excess noise without phase noise contribution is assumed to be 0.03, the overall transmission efficiency of Bob η_B is set to 0.5, and V_A is assumed to be 10. All the systematic parameters are expressed in SNU)

Figure 2.12 shows that the CVQKD links with TLO have better performance compared with LLO. This is because the phase noise is enhanced due to the phase drift between Alice's and

Bob's lasers, which in turn increases the total excess noise. Therefore, Eve has more freedom to manipulate the transmitting keys, and hence reduces the secure key information shared between Alice and Bob. In addition, the use of heterodyne detection offers higher secure key rate over a shorter distance, because the measurements taken of both quadratures of the received states doubles the mutual information shared between Alice and Bob. However, the information accessible to Eve increases faster with distance for the case of heterodyne detection, and starts to dominate. As a result, both secure key rates over long-distance transmission and maximum transmission distance for heterodyne detection are surpassed by a single BHD. For a LLO based CVQKD link, only heterodyne detection can be employed, as the phase of each reference pulse needs to be determined from the simultaneous measurement of the two quadratures.

2.4 State of the art QKD performance

The previously demonstrated experimental implementation of state-of-art fibre-based PTP QKD links with the different protocols and configurations discussed in this chapter are summarised and plotted in Figure 2.13. For a fair comparison, the secure key rate is plotted as a function of channel loss instead of distance, as the optical fibre loss (in dB/km) varies in these demonstrations.

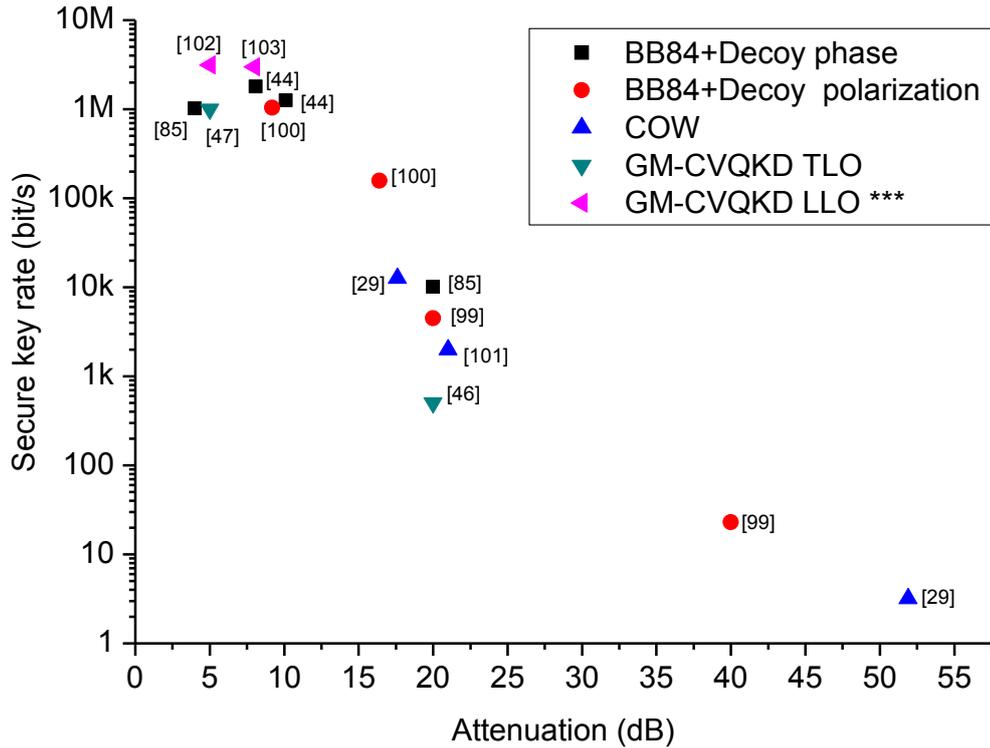


Figure 2.13 State-of-the-art performance of practically implemented QKD PTP links, using the BB84+decoy protocol with phase encoding scheme [44, 85] and polarisation encoding scheme [99, 100], COW protocol [29, 101], and GMCS CVQKD with TLO scheme [46, 47] and LLO scheme [102, 103]. (***) The secure key results for GMCS CVQKD with LLO scheme are not experimentally measured but predicted from estimated system parameters.)

A Mbit/s secure key rate for DVQKD was first reported by A. R. Dixon et al. with a phase encoded QKD link using the BB84 protocol with decoy states at a 20 km transmission distance (with a channel loss of about 4 dB) [85]. In addition, 10.1 kbit/s was achieved in their experiment when the transmission distance is increased to 100 km, which is still being able to mark the state-of-the-art performance of a fibre-based PTP QKD link. Later, L. C. Comandar et al. improved the secure key rate to 1.26 Mbit/s at 50 km (with 10.1 dB loss) with an enhanced InGaAs avalanche photodiode integrated with the self-differencing circuit [44]. Polarisation

encoded DVQKD links using the BB84 protocol with decoy states have also been demonstrated with Mbit/s secure key rate with 9.2 dB transmission loss [100] and about 40 dB transmission loss with a secure key rate of 23 bit/s [99]. The implementation of DVQKD using the COW protocol by B. Korzh et al. achieved the longest QKD transmission distance of 307 km (with 51.9 dB loss) with a secure key rate of 3.18 bit/s [29].

The state-of-the-art practical demonstrations of GMCS CVQKD is based on the TLO scheme in terms of secure key rate (1 Mbit/s at 5 dB transmission loss) [47] and maximum transmission distance/loss (20 dB loss with ~ 0.5 kbit/s secure key rate) [46] were both reported by D. Huang et al.. The GMCS CVQKD with LLO is a much younger design and has been recently proposed and investigated [91]. Although there has not yet been a practical system demonstrated that can generate final secure keys using the LLO scheme, the latest experiments have demonstrated the feasibility of a Mbit/s secure key rate at a transmission loss of less than 10 dB [102, 103].

2.5 Summary

This Chapter reviews the common approaches of fibre-based QKD point-to-point implementations with both DV and CV protocols. For DVQKD links, the practical photon source and single photon detection technologies are discussed. The practically used highly attenuated laser (i.e. Poisson source) for single photon generation poses a security issue for PNS attack, which can be efficiently solved by the simple use of decoy states. APD based SPD are widely used in DVQKD links, of which the main characteristics are introduced. The two most common implementation configurations, polarisation and phase encoding schemes, are reviewed in detail for practical fibre-based QKD links. The most commonly used secret key analysis for DVQKD links is provided, based on which the problem of using a practical Poisson source and the improved performance offered by decoy states are illustrated in terms of secure key rate simulations. State-of-the-art experiments have achieved a Mbit/s secure key rate within a range of 50 km [44], and over hundreds of kilometres of optical fibre with a 3.18 bit/s secure key rate [29].

In CVQKD, instead of using single photon technologies, key information is carried by the quadrature values of electromagnetic fields. The coherent detection used for quadrature measurement in CVQKD links uses a BHD or heterodyne detector (composed of two conjugated BHDs). The LO required for coherent detection can be practically implemented

based on either TLO or LLO design, depending on whether the LO laser is sent from Alice or locally located with Bob's. With widely used secret key analysis, the secure key rate is simulated for CVQKD links in both TLO and LLO configurations. From a practical point of view, a GMCS CVQKD link demonstration with the TLO design has achieved a 1 Mbit/s secure key rate over 25 km of optical fibre [47]. In addition, the maximum transmission distance has been extended to 100 km [46]. A complete LLO-based CVQKD system is still under development, but the feasibility of a Mbit/s secure key rate at a transmission loss less than 10 dB has been demonstrated [102, 103].

The QKD links introduced and investigated so far only operate point-to-point connections between two users. With the final goal of applying QKD in the today's networks, secure keys need to be distributed between multiple users instead of a single pair of Alice and Bob [26]. Different QKD networking structures have been proposed and studied over the last decade, which will be introduced in the next chapter. Among those approaches, optical switching has been shown to be a promising technology for the realization of reconfigurable multi-user QKD networks.

Chapter 3 Optically switched QKD systems

3.1 Introduction

The QKD links introduced and studied in the previous chapters operate in the configuration of a point-to-point connection between two parties. Several techniques such as passive splitting, trusted repeating, and optical switching have been investigated for the purpose of extending the scope of key distribution to multiple users and to provide secure communications over existing telecommunication networks. This section begins with a detailed review of these three topologies, and the pros and cons of each are illustrated. Among them, optical switching has been shown to be a promising method for the cost-effective realization of multi-user QKD systems.

Following this review of past work, different optical switching techniques are studied, and the important parameters for the evaluation of optical switch performance are introduced. Although the practical application of optical switching with large data capacity using conventional telecommunications is still under development due to the limited scalability and switching time of optical switches, optically switched quantum key distribution would be feasible. As weak quantum signals are very sensitive to loss and noise [68], the insertion loss and crosstalk introduced by an optical switch affects the quantum key transmission between each pair of users.

In this chapter, the feasibility and issues of using optical switching in QKD are comprehensively analysed and discussed. Specifically, a mathematical model describing an optically switched QKD system is constructed by modifying the conventional secure key analysis to include additional crosstalk and loss. Based on this, the performance of optically switched QKD systems can be theoretically evaluated in terms of QBER and secure key rate. The impact of switch crosstalk and loss on QKD transmission is practically investigated via a series of proof-of-concept experiments, amply demonstrating the feasibility of optically switched QKD system. The experimental results are also verified by the mathematical model.

This chapter focuses on the introduction of optical switches and the examination of their effect on a reconfigurable QKD system. Given that all current demonstrations on multiuser systems use DVQKD devices, the protocol used here is the basic BB84 DVQKD protocol.

3.2 Review of multiuser QKD systems

3.2.1 Passive splitting scenario

Multiuser QKD systems using passive beam splitters (BS) have been implemented by many research groups [49-52] since the first demonstration by Townsend et al. [48]. Representative example setups are illustrated in Figure 3.1 [51]. An optical connection between a single terminal and multiple terminals is implemented by the use of a $1 \times N$ passive splitter. The key distribution can be conducted in either an upstream or a downstream configuration. In conventional cases, implementation normally employs a downstream configuration. The sending quantum signal from Alice is routed to a different path and forwarded to different Bobs. Such a scenario enables simultaneous secure key distribution from one user to multiple users. However, this configuration suffers from three practical problems: firstly, each Bob needs to have at least one single photon detector installed, which leads to higher cost. Secondly, the bandwidth of each detector is not sufficiently used, as most of the time each detector is not activated. Thirdly, the splitter cannot deterministically direct the photon to each Bob, as the photon at each time slot will be randomly routed to one of the N paths of the splitter [49, 51]. A further multi-user QKD system is based on an upstream configuration, in which the splitter works as a combiner, and the quantum signal from multiple Alices are combined into a single link connected to a common Bob [51]. Time-division multiplexing (TDM) techniques are employed, in which the quantum signals for different destinations are allocated to specific time slots and the detector in Bob detects only one photon from each Alice at each time slot. In this configuration, only one detector is required, which significantly reduces the overall cost of the system.

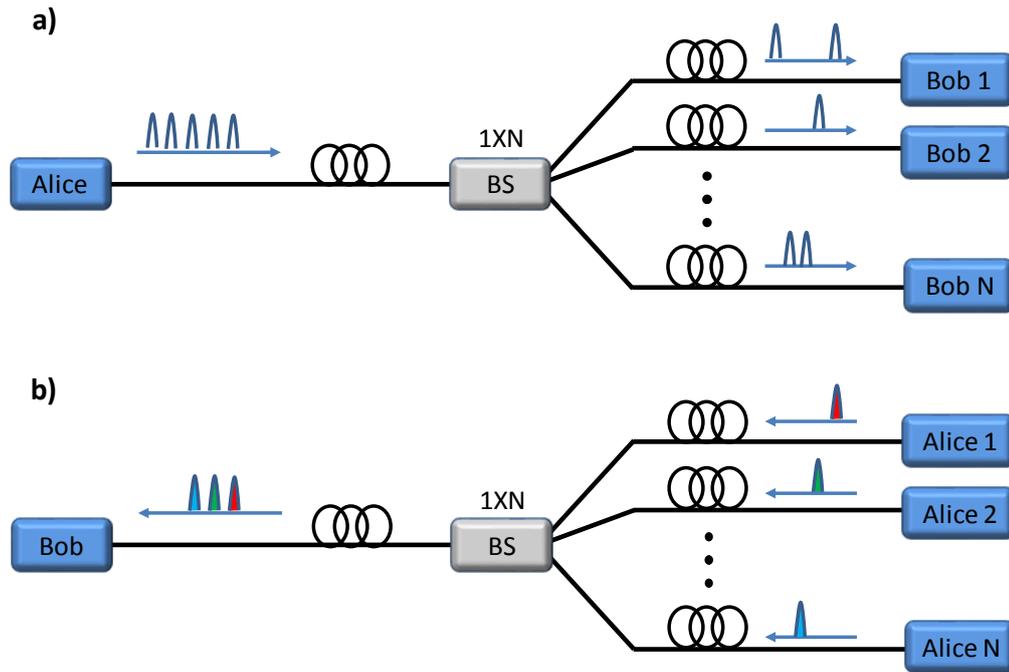


Figure 3.1 Schematic of passive-splitting multi-user QKD systems based on a) downstream and b) upstream configurations [51]

Although multiuser QKD systems based on this type of upstream passive splitting have benefits of low network complexity and low cost, the weaknesses are obvious. The main challenge is the reduced scalability due to the increasing transmission loss when involving more end users [104]. For example, a three-node key distribution requires a 1×2 passive optical splitter which gives 3 dB of additional loss in the transmission. However, a 17-node system would experience a 12 dB loss from the passive optical splitter. As discussed previously, the secure key rate dramatically decreases with increasing transmission distances due to increasing fibre loss. A 12 dB additional loss can be predicted to reduce the maximum transmission distance by 60 km, assuming an attenuation coefficient of 0.2 dB/km at 1550 nm. In addition, the connections within this networking scenario cannot be dynamically selected on demand.

3.2.2 Trusted repeating scenario

The use of trusted repeating is another method for implementing multiuser QKD systems with less network complexity and respectable scalability. A typical structure is composed of a group of fixed PTP QKD links, as shown in Figure 3.2. Each user is located at a secure place and equipped with a classical memory gathering the key from others. Every two adjacent QKD users are connected by a unique link with a pair of Alice and Bobs, and the secure key can be

then distributed between them. For users that are not directly connected (e.g. User 2 and User 3), the key can be retransmitted via one intermediate user or a few intermediate users (i.e. User 1 or User 4).

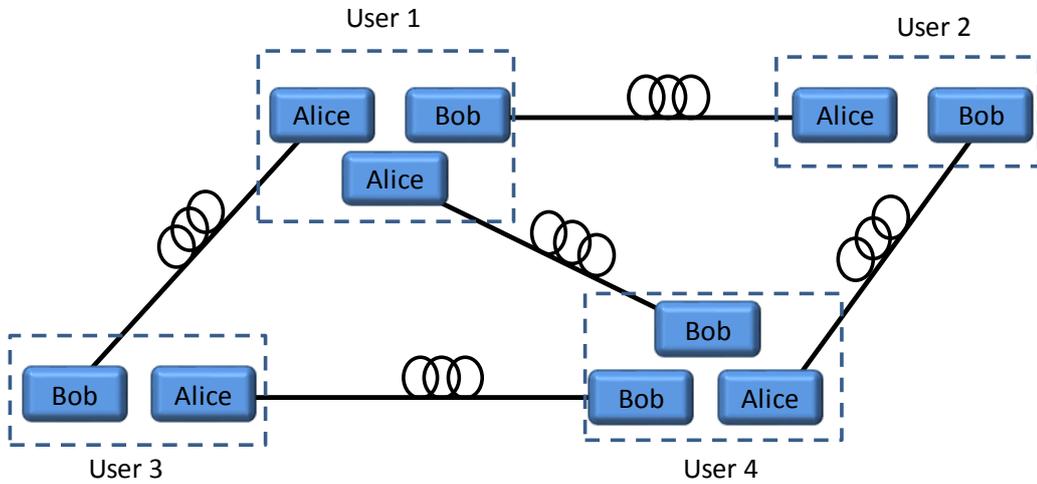


Figure 3.2 Schematic of a typical trusted repeating multi-user QKD systems

Specifically, the intermediate user acts as a trusted ‘repeater’, which respectively shares the individual keys with the users on each transmitting or receiving side. As shown in Figure 3.3, the two keys are combined using the OTP method, guaranteeing the security [59, 105]. The resulting final key is sent to the receiving end user, which can be converted back to a private key shared with the source user. Therefore, this type of multiuser system can be easily extended over longer distances or scaled to large areas as a chain of QKD links by such a ‘hop-by-hop’ mechanism [106]. Representative multiuser QKD systems based on this topology have been demonstrated in [53, 54]. Theoretically, the transmission distance of this type of system can be extended as far as desired, if all the intermediate nodes are guaranteed to be secure and trusted. The other benefit is that each link can employ different types of QKD systems. For example, in the QKD system established by SECOQC [53], different protocols, including COW BB84 GMCS, etc. are employed for different links.

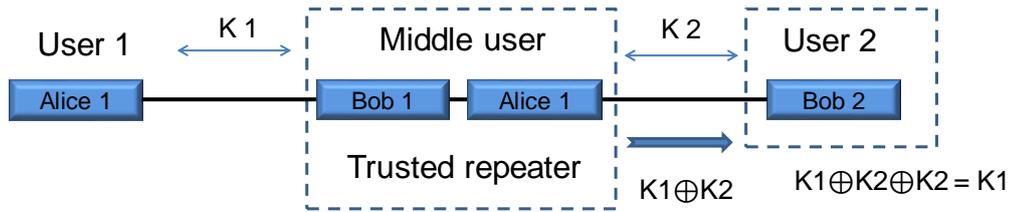


Figure 3.3 Secure key sharing scheme with a trusted repeater in QKD links with three users. K_1 and K_2 are the two individual keys shared between the middle trusted repeater and adjacent users

However, in the practical implementation, the privacy of the intermediate users or repeaters must be guaranteed [63], otherwise the security of the whole network will be broken. In addition, although this topology in principle has the best scalability as it does not introduce additional topology's inherent attenuation, a large-scale multiuser QKD network solely based on this scenario is not practical due to the significant cost, as each user needs to be equipped with at least one pair of QKD devices.

3.2.3 Optical path switching scenario

A third type of multi-user QKD is based on the optical path switching scenario, in which transparent end-to-end connections are created and dynamically configured using transparent optical switches. The basic schematic is shown in Figure 3.4.

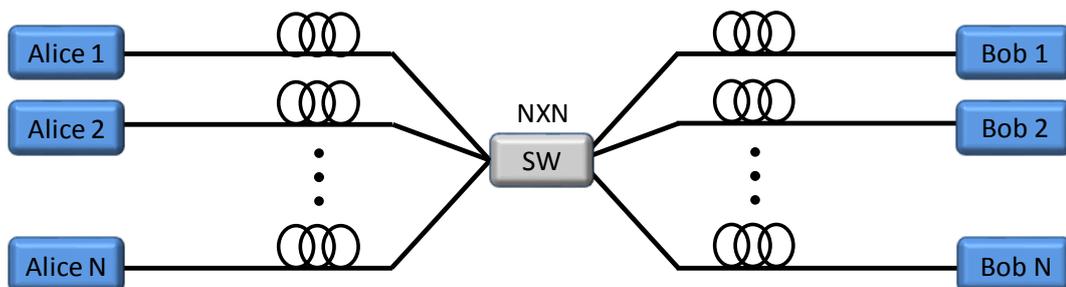


Figure 3.4 Schematic of a typical optically switched multi-user QKD system

The optical switch connects optical paths (i.e. fibres) to different Alices and Bobs. The routing of the paths is normally electronically controlled on demand to perform dynamic interconnections between multiusers. The secure key can be shared between any pair of Alice and Bob. The earliest optically switched multiuser QKD system was demonstrated by Toliver et al. [56], in which a secure key was established between Alice and Bob through different types of optical switch elements, such as MEMS, lithium niobate (LiNbO_3), and

optomechanical switches. Honjo et al. reported a QKD experiment through an 8x8 matrix switch which employs the thermo-optic effect in silica glass [57]. Tajima et al. developed an optically switched QKD system in which a single Bob was used as a central node and shared keys with two remote Alices [58]. Optical switching has since been employed in many QKD network field trials (e.g. the DARPA QKD network [59], the three-node QKD network by NIST [107], as well as the reconfigurable QKD network in US [61]) [26].

Optical switching has lower transmission loss and provides a more flexible path reconfiguration compared with the passive splitting scenario. It allows for the selective connection of any pair of Alice and Bobs connected to the switch. In addition, Multi-user QKD systems based on this topology can be realized with end-to-end optical channels, without trusting any node in the middle. The quantum signal will not be interrupted or regenerated by any middle point during the transmission. The corresponding cost of building a multi user system is also effectively reduced, since fewer QKD devices are involved in the switching architecture. Although the common concern is that the optical switching scenario cannot be used to extend the QKD transmission distance, this problem can be solved in conjunction with a small number of trusted nodes [26, 63].

3.3 Optical switching techniques

Optical switching technologies were initially studied for conventional telecommunication networks. In today's networks, data is mainly transmitted in the optical domain but is switched by electronic switches, alongside which two processes are used: opto-electronic (OE) and electro-optic (EO) conversion. Although such 'OEO' electronic switching is a reliable and widely employed technique in current commercial systems, it has a limited capacity due to its electronic components which poses a problem for future communications system with higher data rates. Therefore, optical switching techniques have drawn much research interest, due to the absence of signal conversion and hence the capacity limitations on electronic components. In addition, the switches also have the benefit of lower energy consumption. The major parameters used to evaluate an optical switch are listed below [108] :

- Switching time: the time spent for setting up new connections within the optical switches. Different switching times may be required depending on applications.
- Insertion loss: the end-to-end transmission loss in the optical path added by the switch, including both coupling loss and internal loss. Although the value is desired to be as low

as possible, this loss is normally compensated for by optical amplifiers in conventional communication systems.

- Crosstalk: the fraction of the signal intensity in the desired switched path contributed by the other source ports rather than the corresponding input. This parameter indicates the noise due to the leakage from other source signals.
- Extinction ratio: the ratio between the power at the signal output port in the ON and OFF states.
- Input power dynamic range (IPDR): The input operating power range with the desired minimum bit error ratio (BER) performance. This value indicates the noise introduced by the switch itself, and the maximum power limitations due to the distortion.
- Scalability: the practical number of input/output ports to which a given switch technology can be scaled. This is normally restricted by increased insertion loss, crosstalk and signal dynamic range in a large-scale switch design.

There are various optical switching technologies, mainly using one or more of electro-optical, thermo-optical, acousto-optical, liquid crystal, semiconductor optical amplifier (SOA), and opto-mechanical technologies [109]. The optical switches are basically categorized based on the corresponding fundamental physical effects used for triggering the switches. In this section these optical switching technologies will be briefly introduced and compared, and their use in QKD will be discussed. In a typical electro-optical switch element, the switching of the state relies on the electro-optic effect, in which the refractive index of an optical medium can be altered by an external electric field. It is normally implemented in an interferometric structure, either MZI [110] [111] or a directional coupler [112], as shown in Figure 3.5. In both configurations, the electric-optic material, such as Lithium niobate (LiNbO_3), is used as a phase shifter. The applied voltage induces a change in the refractive index and hence a phase shift in the corresponding optical path. Thus, the interference between signals in the two arms would be either constructive or destructive (or in-between), and if in either full constructive or destructive state, the signal is output to one of the two ports [109]. Electro-optic switches have relatively low power consumption and a high switching speed with nanosecond timescale, but normally suffer from high insertion loss and crosstalk.

Similarly, a thermo-optical switch is also realized based on the interferometric configurations in Figure 3.5. Instead of relying on the electric-optic effect, the phase change and hence the switching function is realized by the change of refractive index via temperature variations [109]. Commonly used materials include silica [113], silicon [114], polymer [115], and LiNbO_3 [116].

This type of optical switch has moderate loss and crosstalk level, but a lower switching speed of the order of milliseconds. In addition, the high-power consumption of the heating process limits the scalability to a large switch size [108].

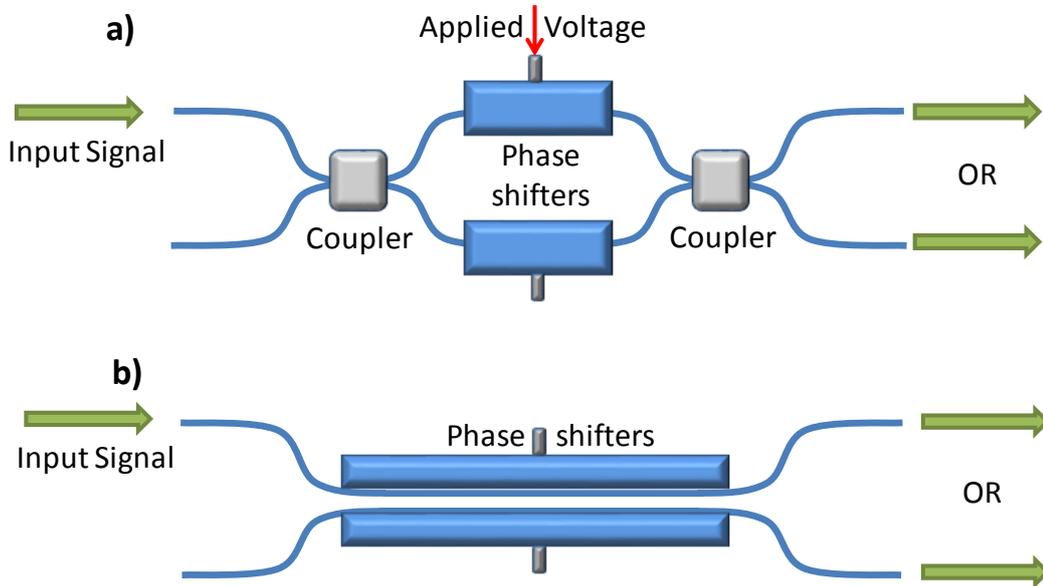


Figure 3.5 Schematic of an interferometric switching element using a) MZI or b) directional coupler [108, 117]

In an acousto-optic switch, as the name suggests, the switching function is conducted based on the acousto-optic effect. When acoustic waves propagate along the surface of an acoustic material, the consequent mechanical strains induce changes in the refractive index. Such changes lead to a diffraction grating in the material, which alters the polarisation state of the optical signal propagating through it [109]. The structure of a basic switching element is shown in Figure 3.6 [117]. The 2x2 polarisation beam splitter splits the incoming optical signal into two paths with horizontal and vertical components, respectively. The acousto-optic material is normally LiNbO_3 [118]. Without an applied acoustic wave, the split orthogonal optical signal recombines at another 2x2 polarisation beam splitter and is output from one of the ports. When an acoustic wave is applied in the same direction as the signal, the polarisation is rotated. Thus, the output signal can be routed from one port to another. Although an acousto-optic switch normally has a faster switching speed of around a microsecond timescale, the scalability of such a technique is restricted by its relatively high loss and crosstalk [108].

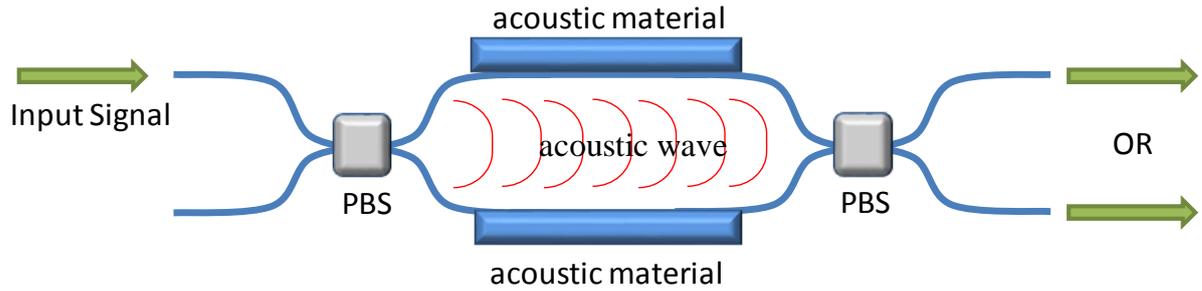


Figure 3.6 Scheme of a basic acousto-optic switching element [117]

Liquid crystal (LC) switches use the change of polarisation of an incoming signal related to the orientation of molecules within LC cells. The principle of a basic switching element is shown in Figure 3.7. The input signal is polarised and travels through an LC cell, which works as a voltage controlled polarisation rotator. Application of an electric field causes a change in orientation of the LC cell and hence induces a rotation of polarisation in the passing signals. Then the signal is routed at the polarisation combiner and output from one of the output ports. This type of switch has moderate loss and crosstalk, and has a switching time in the range of microseconds and milliseconds [109, 117].

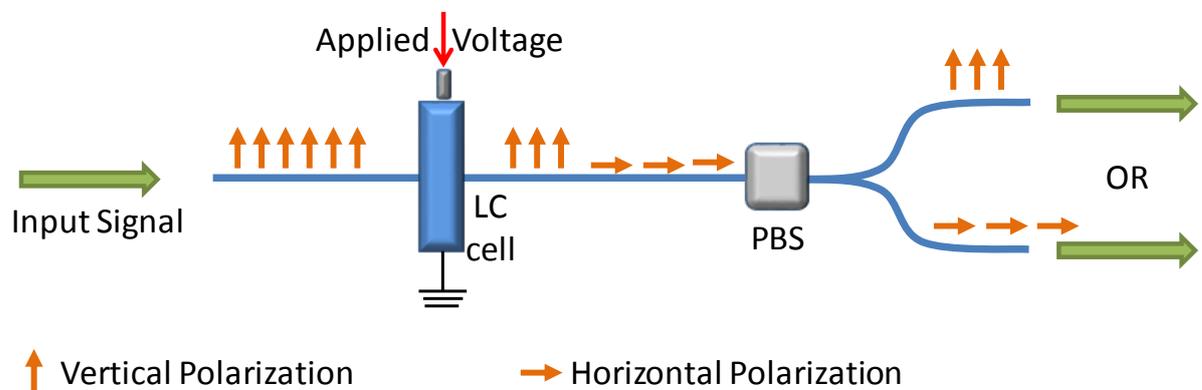


Figure 3.7 Scheme of a basic liquid crystal switching element [117]

SOA-based optical switches use SOAs as gating elements. For an optical signal travelling through an SOA element, a biased SOA element produces desirable optical gain, while an inactive SOA introduces a significant amount of loss. The switching principle of a basic 1x2 SOA-based optical switch is illustrated in Figure 3.8. The input signal is split into two paths by a beam splitter, and the SOA in each path is used as a gating element. The signal in the desired path is amplified by a biased SOA element, while the signal in the other path is ‘blocked’ by turning off the electrical bias current to the corresponding SOA element [108, 109].

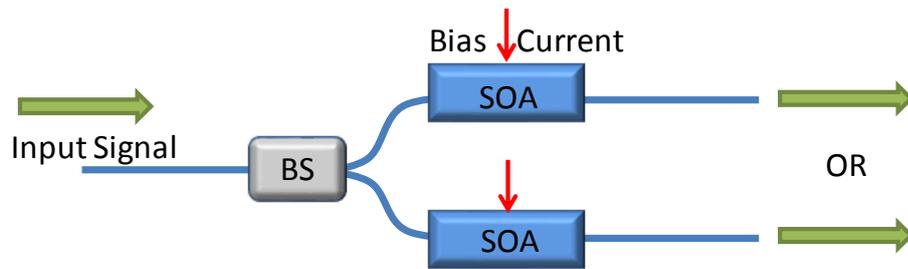


Figure 3.8 Scheme of a basic SOA based switching element

SOA based switches have many advantages, such as a fast switching time of nanosecond timescales, low insertion loss, and high extinction ratio. However, the scalability of SOA based switches is limited by the amplified spontaneous emission (ASE) noise [119]. The ASE also makes this type of switch not applicable to QKD, as the weak quantum signal is very sensitive to noise. Their high power consumption due to the injected bias current to SOA elements is another disadvantage.

Opto-mechanical switches were the first commercialized optical switching technology, and are still the most practically used in conventional communications. Generally speaking, the idea is based on physically moving free-space optical elements, including mirrors, prisms, and shutters [117]. Two examples of an opto-mechanical switching element based on the motion of a mirror are illustrated in Figure 3.9, in which the switching function is performed by rotating or moving the mirror between inputs and outputs, respectively. For building large scale optical switches, MEMS technology is usually employed in the fabrication of smaller and integrated switching elements. Opto-mechanical switches have been attractive for practical purposes as they have low insertion loss and low crosstalk level as well as low cost. The response time ranges from microseconds to milliseconds, making them not suitable for fast switching applications [108].

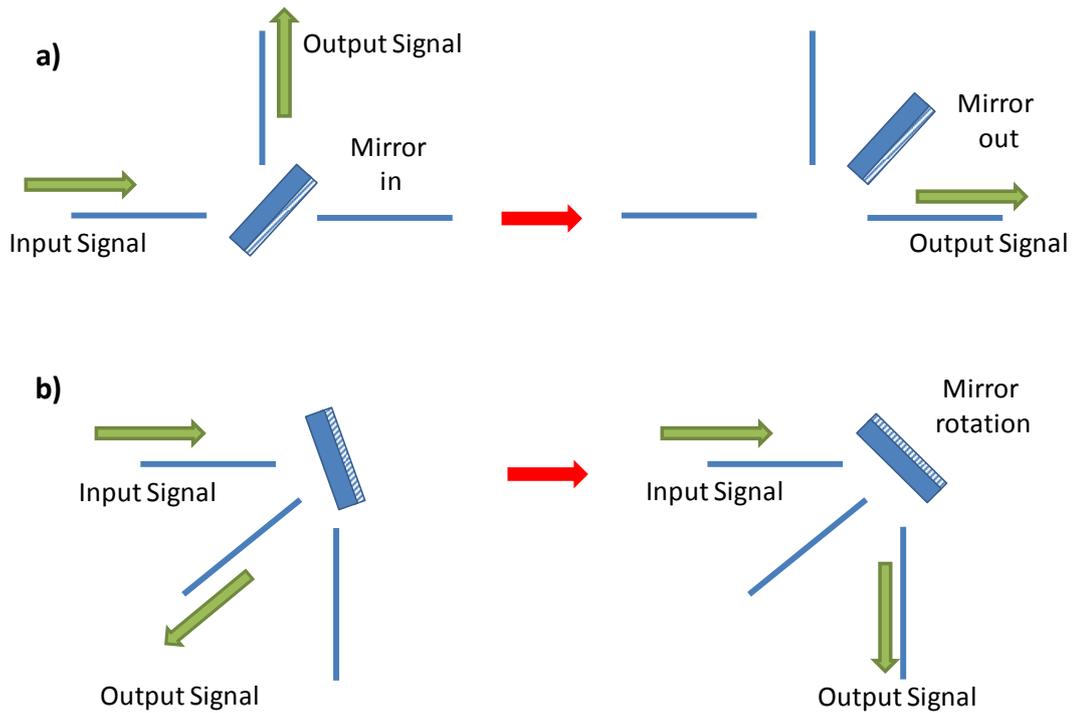


Figure 3.9 Schematic of a basic Opto-Mechanical switching element.

Regardless of different switching technologies, large scale $N \times N$ optical switches are practically realized by cascading the basic 1×2 or 2×2 switching elements as building blocks [117]. Therefore, this section also introduces the typical switch architectures that enable large-scale optical switch designs: Tree, Benes, Crossbar and Clos [120]. A tree architecture is illustrated in Figure 3.10(a). It consists of a number of splitters/combiners at the input/output. The splitters and combiners can be either passive couplers or active switching elements [120, 121]. The major disadvantage of this architecture is that the number of splitters/combiners increases with the size of the switch, which in turn results in a significant path loss in the large-scale design. Crossbar architecture, as indicated in Figure 3.10(b), is a square matrix with rows as inputs and columns as outputs, or vice-versa. N^2 basic switching elements are required for an $N \times N$ crossbar switch. Hence, in a large-scale switch design, a huge number of switching elements are required. The other problem of this architecture is that the insertion loss and propagation time can be different for different paths. This would introduce imbalanced performance between paths [108]. In Clos architecture, a large-scale switch is integrated from smaller switch blocks. As shown in Figure 3.10(c), an $N \times N$ Clos architecture has three stages. Let $r \times n = N$, the first stage has r switches of size $n \times m$, the middle stage has m switches of size $r \times r$, and the last stage has r $m \times n$ switches [120]. Benes architecture can be seen as a special form of Clos architecture. As shown in Figure 3.10(d), each of the first stage and the third stage have $N/2$

2x2 switches, and the middle stage consists of two $r \times r$ Benes switches. Compared to other architectures, the Benes architecture requires a minimum number of switching elements as well as offering the lowest insertion loss [120].

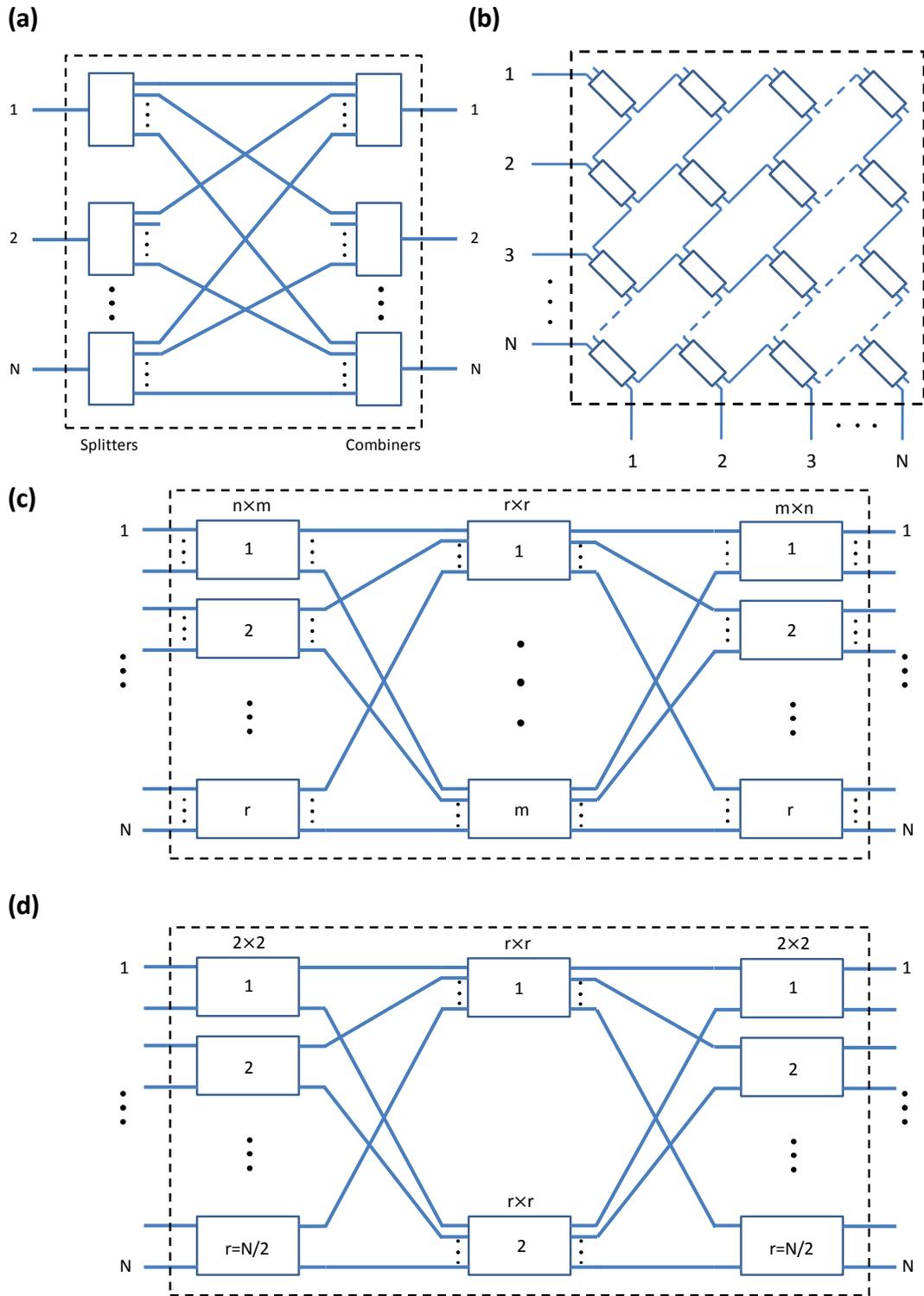


Figure 3.10 Schematics of (a) Tree (b) Crossbar (c) Clos and (d) Benes switch architectures [120]

Although optical switches have become the focus of much research with their maturing fabrication techniques, their practical use in current classical communication systems is still challenged by their limited scalability and switching time to handle today's large data capacity. However, optical switching technologies show great potential for use in QKD systems. In switched QKD systems, the use of optical-electrical-optical (OEO) switches is not practical, as each port of the switch must perform the optical to electrical conversion, which involves key detection and hence a significant number of QKD devices. To use optical switching techniques, the weak quantum signals are very sensitive to loss and noise [68]. Any optical switch used in routing quantum signals will more or less degrade the secure bit rate of each user. Thus, optical switches used in QKD systems need to be carefully designed to introduce minimal loss and crosstalk. SOA based switches cannot be used in this case, as they intrinsically introduce ASE noise which severely impairs the weak quantum signals. The following sections in this Chapter focus on the investigation of QKD performance in terms of the secure key rate under additional loss and crosstalk.

Table 3.1 summarizes representative experimental demonstrations of QKD transmission via optical switches. In reference [56], the quantum signal is transmitted through 10km of fibre followed by a switch element between one Alice and one Bob. The loss of the MEMs switch is not particularly mentioned, but the total path losses at the four switch outputs range from between 5.5 and 5.9 dB.

Crosstalk is not explicitly mentioned in most of those experiments. This is because no spontaneous QKD signal from two or more Alice-Bob pairs has been tested through the switches in previous experimental demonstrations, which have focused on point- to-point or point-to-multi-point transmissions through optical switches. However, the crosstalk effect should not be overlooked as it introduces additional noise photons to the desired path and hence degrades the QKD performance. This is considered and discussed in the theoretical model and experimental demonstration presented in the flowing sections of this chapter.

Table 3.1 Representative experimental demonstrations of optically switched QKD transmission (Crosstalk is not explicitly mentioned in most of those experiments)

Reference	Switch technique	Switch size	Loss	Crosstalk	No. of users in experiment
Toliver [56]	MEMS	4x4	N/A	N/A	Two
Toliver [56]	LiNbO ₃	2x2	5.4 dB	N/A	Two
Honjo [57]	Thermal-optical	8x8	5.7 dB	-42.4 dB	Three
Chapuran [61]	MEMS	4x4	2.1dB	N/A	Two
Chen [63]	Opto-mechanical	8 ports	0.9-1.2dB	N/A	Five
Ma [122]	MEMS	2x4	1.5-1.8dB	N/A	Four

3.4 Evaluation of optically switched QKD systems

The commonly used mathematical model of a back-to-back QKD transmission has been introduced in Chapter 2, showing how the QBER and secure key rate can be estimated for a point-to-point link with an Alice and Bob. Here, the back-to-back model is modified for the purpose of evaluating switched QKD systems as shown in Figure 3.4. The optical switch in the middle can be characterised as introducing additional noise and loss that occurs in the key transmission path.

When the QKD signal is transmitted through an optical switch, a fraction of the signal power is lost due to both coupling loss and internal switch loss. Therefore, the transmittance of the each QKD link through optical switch becomes:

$$\eta = \eta_B 10^{-\frac{\alpha l + L_s}{10}} \quad (3.1)$$

where L_s is the total loss due to the optical switch (in dB). η_B is the transmittance of Bob's setup. α and l are the attenuation coefficient (in dB/km) and the length (in km) of the fibre link, respectively.

In addition, because of crosstalk effects within the optical switches, QKD signals transmitted along other paths through the switch add in a noise part c_n to the yield Y_n of an n -photon state (defined in **Eq. (2.7)**) of the desired transmission path, because of the switch crosstalk:

$$Y_n = Y_0 + \eta_n + c_n \quad (3.2)$$

where c_n is sourced from other QKD inputs to the optical switch, which can be defined in the same way as η_n in **Eq. (2.8)**:

$$c_n = 1 - (1 - c)^n \quad (3.3)$$

$$c = \eta 10^{-\frac{CT}{10}} \quad (3.4)$$

where CT is the value of switch crosstalk in dB.

Therefore, the overall gain in signal states and decoy states through the desired transmission path can be described as:

$$Q_\mu = \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu} + 1 - e^{-c\mu} \quad (3.5)$$

$$Q_\nu = \sum_{n=0}^{\infty} Y_n \frac{\nu^n}{n!} e^{-\nu} = Y_0 + 1 - e^{-\eta\nu} + 1 - e^{-c\nu} \quad (3.6)$$

and the overall QBER in signal states is rewritten as:

$$E_\mu = \frac{\sum_{n=0}^{\infty} e_i Y_n \frac{\mu^n}{n!} e^{-\mu}}{Q_\mu} = \frac{e_0 Y_0 + e_d (1 - e^{-\eta\mu}) + e_0 (1 - e^{-c\mu})}{Q_\mu} \quad (3.7)$$

The lower bound for the gain of single photon states Q_1^L and the upper bound for the QBER for single e_1^U photon states can be then obtained using **Eq. (2.16)** and **Eq. (2.17)** for the desired transmission path. Substituting Q_1^L and e_1^U into the secure key rate equations, we can calculate the secure bit rate of the QKD transmission through an optical switch with loss L_s and crosstalk value CT . Based on our mathematical model, the performance of an optically switched QKD system can be theoretically evaluated.

In order to show the performance degradation induced by an optical switch and hence study the feasibility of an optically switched QKD system, the mathematical model has been used to simulate an example QKD transmission system using a decoy-state BB84 protocol and a practical 8x8 Benes MZI electro-optical switch [123]. The QKD system parameters are the same as those used in the calculations in Chapter 2 from [85], which are listed in the caption

of Figure 3.11. The optical switch has an insertion loss of 6.52 dB and a crosstalk level of -19.57 dB [123]. With the back-to-back performance as a reference, the estimated QBER and corresponding secure key rate is plotted in Figure 3.11 as a function of transmission distance. The extra loss and crosstalk introduced in this 8x8 MZI optical switch inevitably degrades the performance of the QKD system. The minimum QBER at zero distance rises from 2.3% to 2.9%. At a moderate 50km transmission distance, eg.in a metropolitan area, the QBER is increased from 2.5% to 3.8%. In this case, the maximum secure key transmission distance drops from about 109 km to 72 km with such a switch and the maximum secure key rate at 50 km is significantly degraded from 3.1×10^{-4} to 3.7×10^{-5} bit/pulse.

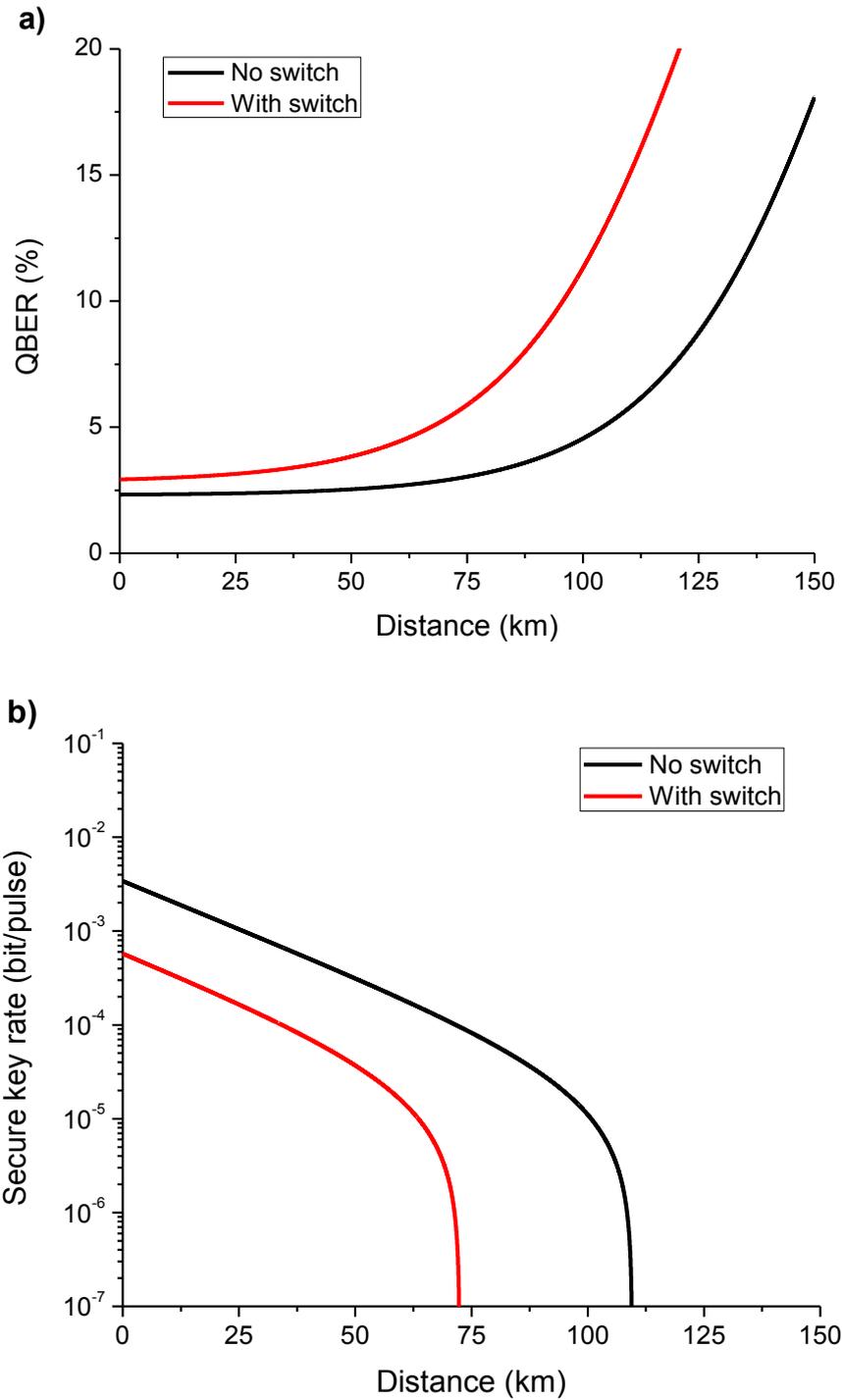


Figure 3.11 a) The simulated QBER as a function of transmission distance of the decoy state QKD with and without optical switch. b) The simulated secure bit rate as a function of transmission distance of decoy state QKD with and without optical switch. (The optimised mean photon numbers for signal and decoy states are $\mu = 0.55$, $v_1 = 0.1$ and $v_2 = 7.6 \times 10^{-4}$, The error correction efficiency f_{ec} is assumed to be 1.1, the system error e_d is fixed at 2.3%, the background noise is assumed to be 6.8×10^{-6} , the channel loss coefficient is set as 0.2 dB/km, and Bob's detection efficiency is fixed at 5% [85])

Applying the mathematical model to more general cases, the optically switched QKD system performance degradation has also been investigated for different levels of additional losses and crosstalk due to an optical switch. The simulated results are presented in Figure 3.12 and Figure 3.13, respectively. Figure 3.12(a) shows that the QBER increases with additional losses as more quantum signals vanish during transmission. At a transmission distance of 50 km, the QBER doubles when a 12 dB loss is added into the channel. On the other hand, the maximum transmission distance decreases from 104.2 km to 89.2 km, 74.2 km, 59.2 km, and 44.2 km with an optical switch with loss of 3 dB, 6 dB, 9 dB, and 12 dB, respectively, if a level of QBER of 5% needs to be guaranteed. The corresponding secure key rates are plotted in Figure 3.12(b). Firstly, the key transmission distance is significantly reduced by the additional losses. If an optical switch introduces a 3 dB loss to the QKD transmission path, the maximum transmission distance is shortened by 15 km assuming an attenuation coefficient of 0.2 dB/km at 1550 nm in SSMF. The transmission distance would be further reduced to about 79.5 km, 64.5 km, or 49.5 km with 6 dB, 9 dB, or 12 dB additional loss introduced by an optical switch. Then, at a fibre distance of 50 km, secure key rate drops from 3.1×10^{-4} to 1.4×10^{-4} , 6.1×10^{-5} , 1.9×10^{-5} and *Null* bit/pulse with an optical switch with an insertion loss of 3 dB, 6 dB, 9 dB and 12 dB, respectively. Given that an optical amplifier cannot be used during the quantum signal transmission, the optical switch need to be selected to introduce as little insertion loss as possible to realize a scalable QKD network.

The QBER and secure key rates have also been simulated with different levels of crosstalk. Figure 3.13(a) shows that values of crosstalk less than -25 dB would not introduce significant errors into the received quantum signal. For a crosstalk level worse than -25 dB, the QBER raises sharply at a short transmission distance. At 50 km, the QBER rises from 2.5% to 4.0% and 6.8% with a crosstalk level of -15 dB and -10 dB, respectively. Over a longer distance, as both the signal from the desired port and the interference from other source ports of the optical switch are both significantly reduced by the high channel loss, the crosstalk effect therefore has less dominance on the QBER. This is the reason why the QBER curves for different crosstalk levels converge with increasing transmission distance. The secure key rate has been calculated in Figure 3.13(b). No secure key can be guaranteed with a crosstalk level of -10 dB in our simulated case, while crosstalk levels better than -20 dB would not significantly affect the secure key rates.

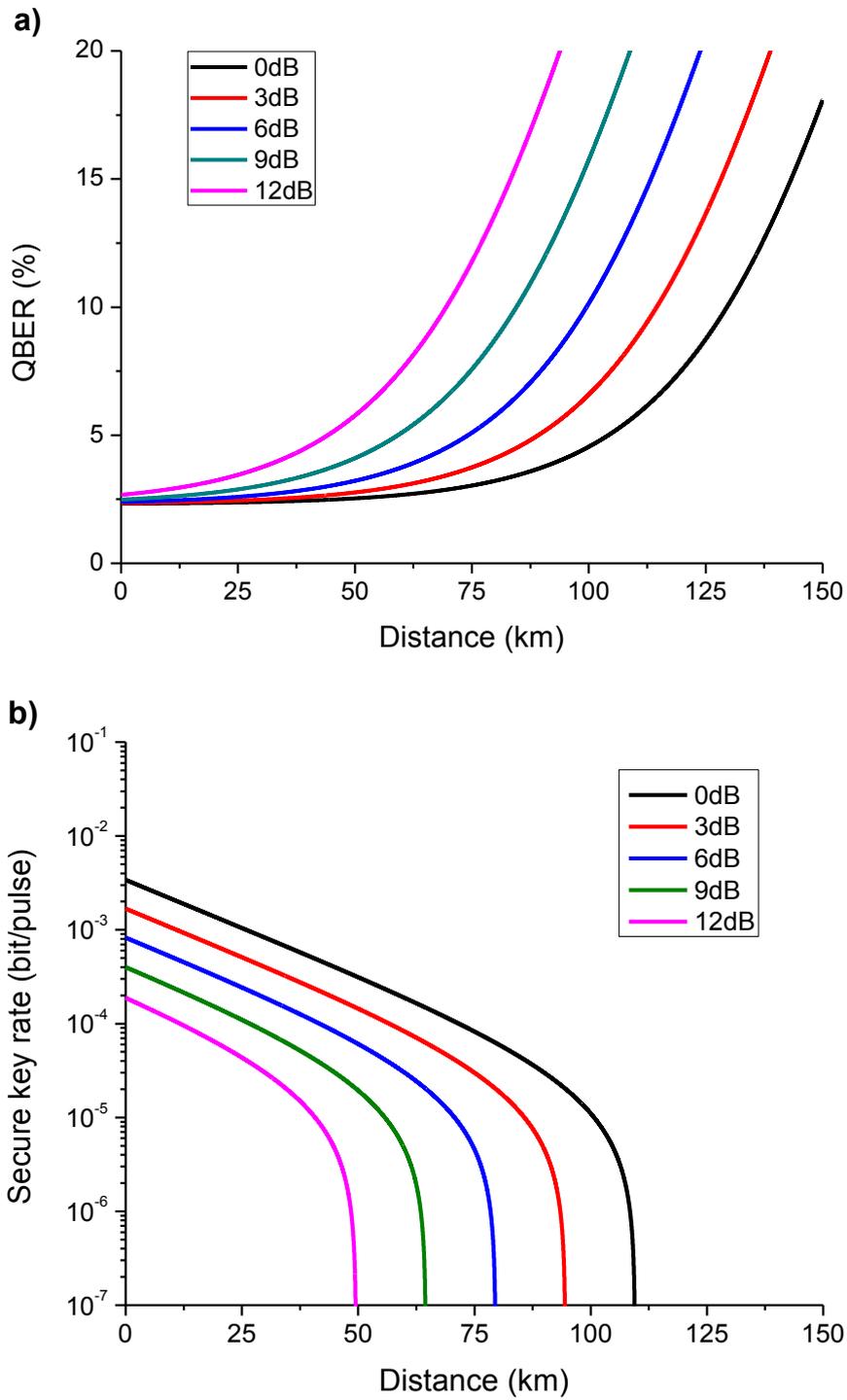


Figure 3.12 a) The simulated QBER and b) the simulated secure bit rate as a function of transmission distance of the decoy state QKD with different levels of additional losses.

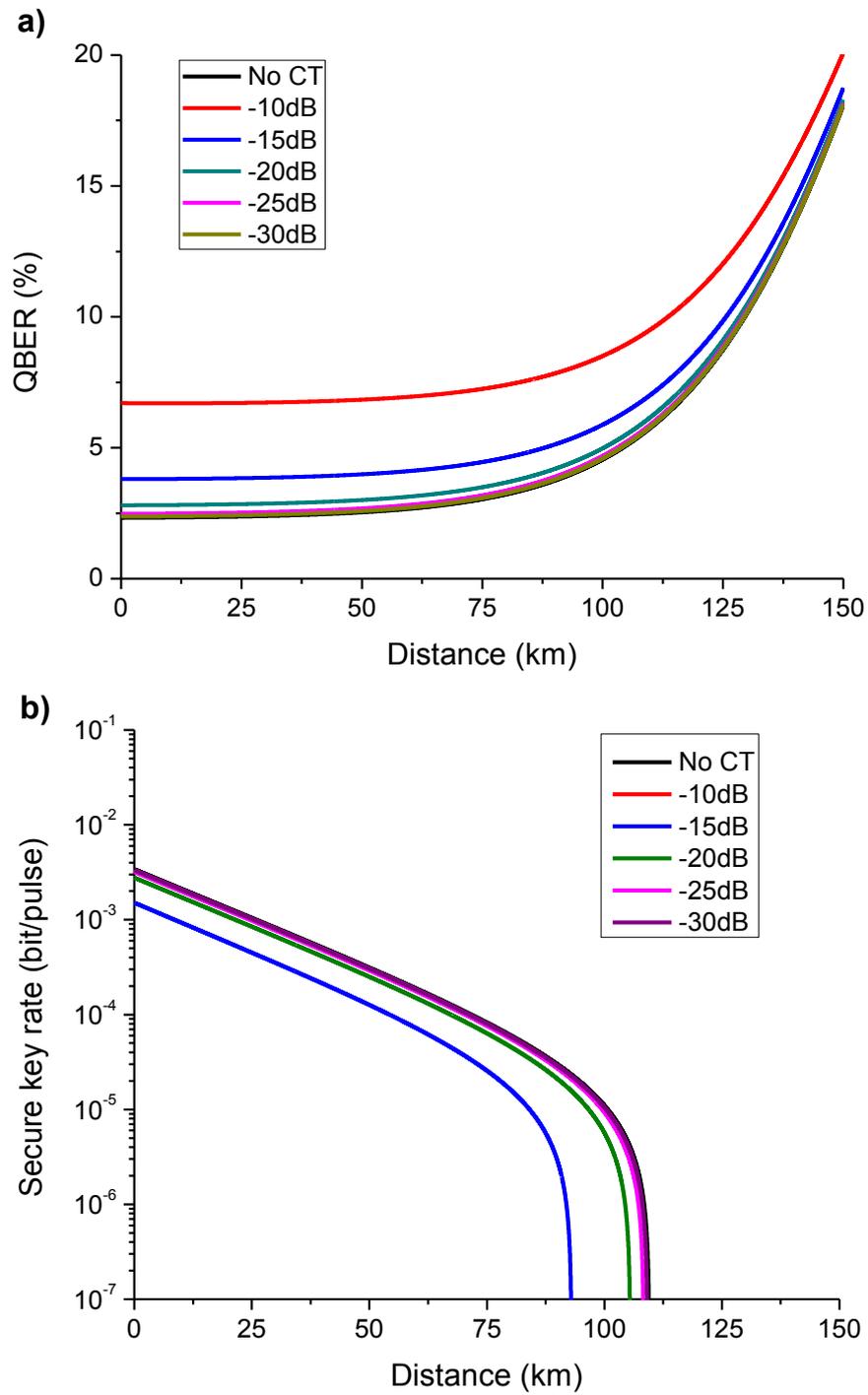


Figure 3.13 a) The simulated QBER and b) the simulated secure bit rate as a function of transmission distance of the decoy state QKD with different levels of additional crosstalk.

3.5 Proof-of-concept experiments

In order to study practically the feasibility of a basic optically switched multi-user QKD system, the performance in term of the QBER of QKD paths through optical switches was investigated by a series of proof-of-concept experiments featuring additional emulated switch losses and crosstalk from an interferer. The detailed experimental setup of a polarisation encoding QKD system based on the BB84 protocol is shown in Figure 3.14.

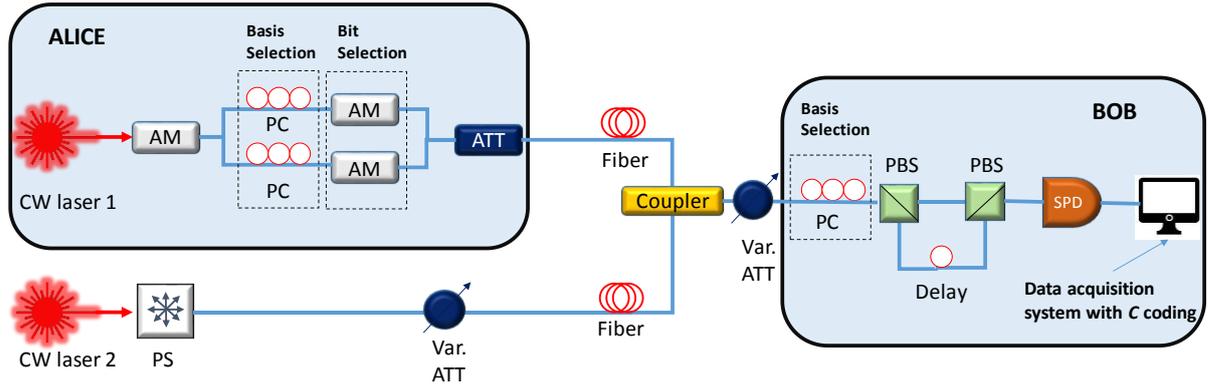


Figure 3.14 Experimental setup. AM: amplitude modulator; PS: polarisation scrambler; PC: polarisation controller; ATT: attenuator; PBS: polarisation beam splitter; SPD: single photon detector

The sender (Alice) generated an optical pulse train from a 1547.72 nm wavelength continuous wave laser (laser 1) modulated by an amplitude modulator, which is driven by a 2 MHz electrical signal from an arbitrary wave generator. The pulse duration is fixed at 2 ns. The optical pulses are then split into two equal loss paths at an optical coupler. The polarisation controllers in the two paths are used to encode the photon pulses in one of the four polarisation states within two pairs of polarisation bases (i.e. horizontal and vertical using a rectilinear basis, and 45° and 135° using a diagonal basis). Horizontal (or 45°) and vertical (or 135°) polarised photons represent the logic bit values '0' and '1' respectively. Two amplitude modulators operating as on/off gating components are used to select which logical bit is transmitted. An optical attenuator is used at the output of Alice and the signal is attenuated to an average level of 0.4 photons per pulse.

In order to investigate the effect of crosstalk within an optical switch, crosstalk photons from another quantum path are emulated as randomly polarised photons from an additional highly attenuated laser source (laser 2), which has the same wavelength of 1547.72 nm. Specifically, the polarisation of crosstalk photons from laser 2 are randomised by a commercial polarisation

scrambler (PS), and the different level of crosstalk are tuned by an optical variable attenuator. Then, the resulting crosstalk photons are coupled into the desired quantum transmission path via an optical coupler. Another variable attenuator is used at the output of the coupler to emulate different levels of channel loss for the signal with crosstalk photons.

In Bob's setup, a polarisation controller performed the basis selection. In this experiment we chose arbitrarily to examine the horizontal and vertical basis. Owing to resource constraints, only one time-gated SPD is involved in the experiment. Therefore, the two orthogonal polarisations of the incoming signal from Alice are resolved using two polarising beam splitters and 50 m of fibre. This enabled the horizontal polarisation to be delayed by 250 ns with respect to the vertical polarisation, allowing both polarisations to be detected using one SPD operating at a clock rate of 4 MHz, as illustrated in Figure 3.15. Thus, both correct and error detections can be measured at different time slots. For example, if the received pulse is initially vertically polarised in Alice (ie. encoded as bit '1'), the detection of SPD of the first pulse corresponds to the correct detection of bit '1', and the detection of the second pulse is the error count which is due to the background noise including dark counts and crosstalk photons. A digital data acquisition system, consisting of a software controlled digital input/output card installed in a computer, is used to record the output from the SPD and calculate QBER from the measurements. The overall setup of Bob has a total loss of about 1.5 dB, which come from the polarisation controllers, polarising beam splitters and the connectors.

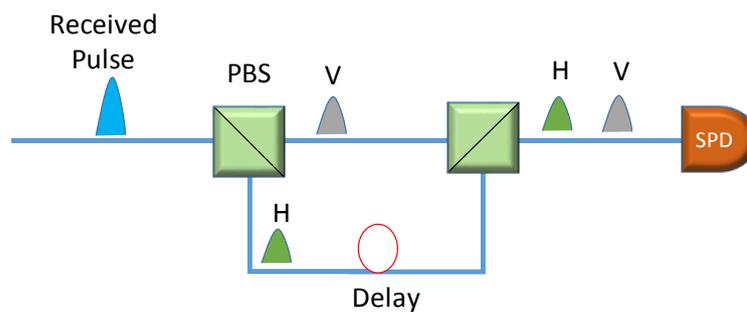


Figure 3.15 Detection of both polarisation using the same SPD

QBER can be experimentally measured by comparing both 0 s (horizontally polarised) and 1 s (vertically polarised) bits between those Alice sent and those Bob received under the condition that they are using the same basis. The bits are discarded when the bases of Alice and Bob are different during the sifting processing. The experimental results for different levels of crosstalk and loss are plotted in Figure 3.16 together with calculated results using our mathematical

model introduced in Section 3.4. It can be seen that the estimated QBER (dashed lines) and the experimental results (solid symbols) are in excellent agreement. The error bar indicates the observed error in the measurement from the SPD. The minimum measured QBER at 0 dB loss and without crosstalk is about 2%, and is caused by finite modulation extinction and misalignment of the system. This QBER increases to 2.4%, 3.5%, 4.8%, 7.4% and 10.6% for an additional 2 dB, 4 dB, 6 dB, 8 dB, and 10 dB channel loss, respectively. Channel loss arises from both the fibre link and the optical switch. The addition of an optical switch would shorten the maximum transmission distance for a required QBER level. It can be predicted that the use of a 2 dB loss optical switch in the channel would reduce the maximum transmission distance by 10 km (assuming an attenuation coefficient of 0.2 dB/km at 1550 nm).

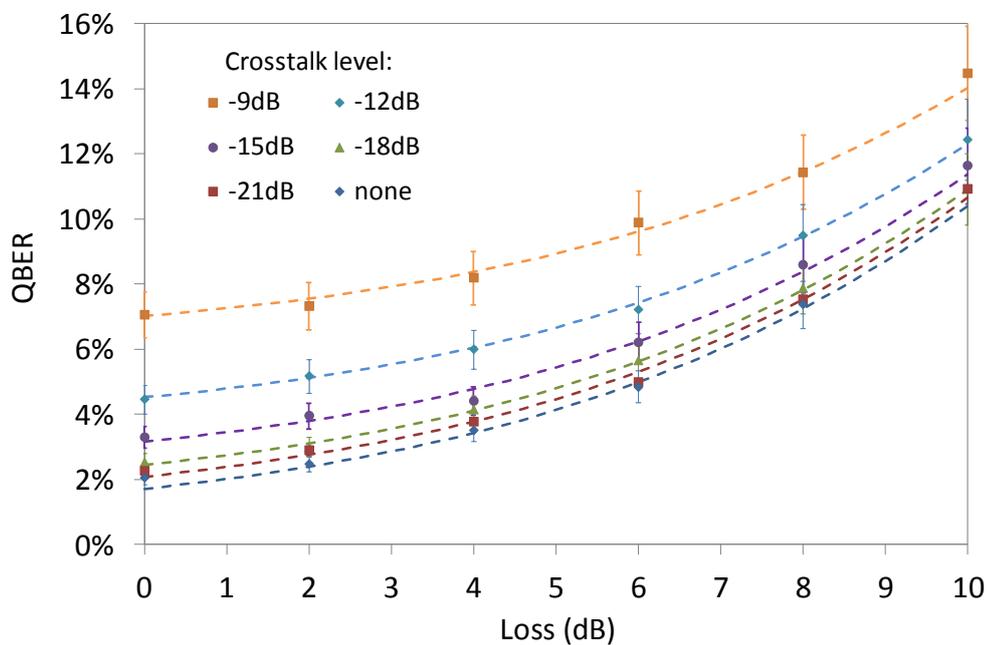


Figure 3.16 The measured (solid symbols) and calculated (dashed lines) QBER

With regard to the crosstalk effect, a crosstalk level of -9 dB, -12 dB, -15 dB and -18 dB introduces 4.7%, 2.5%, 0.9%, and 0.6% extra QBER respectively at a channel loss of 4 dB. (The 4 dB channel loss can correspond to a 10km transmission if the optical switch has a 2 dB loss). As the channel loss increases the received signal becomes dominated by detector noise, which has a greater impact than that of crosstalk on the QBER. Thus, the crosstalk does not have a large effect on the QBER at higher channel losses. The values of crosstalk better than -21 dB do not introduce a significant additional penalty to the QBER performance of the QKD system at any transmission distance, as very few crosstalk photons are leaked from the other source signals into the desired signal path. This is also predicted by our mathematical model.

3.6 Summary

In this chapter, three scenarios of establishing multi user QKD systems have been reviewed. These are based on passive splitting, trusted repeating and optical switching. In the system with passive splitters, the loss increases with the number of users, which limits the scalability. Trusted repeating requires a pair of QKD devices in each of the middle points. Although the transmission distance can be easily extended by cascading more repeating nodes, the accompanying significant cost makes this scenario impractical. Optical switching is the most promising technique in the realization of reconfigurable systems. It offers lower transmission loss and higher flexibility compared with the multi user systems based on a passive splitting scenario. On the other hand, unlike trusted repeating multi user systems, the use of optical switches provides end-to-end key distribution without the need for intermediate trusted nodes. It can be used cost-effectively to share secure keys between multiple parties.

A range of main switching techniques have been introduced and reviewed, and the corresponding pros and cons of each one discussed in terms of the important evaluation parameters. When using optical switches in a QKD system, the accompanying loss and crosstalk level unavoidably affect the transmission of quantum signals. The feasibility and issues of optically switched QKD systems have been theoretically studied via a mathematical model derived from the general secure key analysis for point to point links, featuring an optical switch as having an additional channel loss and crosstalk. Based on this model, the changes in QBER and hence secure key rates caused by a practical optical switch have been simulated for a typical QKD system. This has been then applied to the general cases with different levels of loss and crosstalk that an optical switching element would introduce. The simulation shows that loss should be carefully minimised and crosstalk kept below about -20 dB when designing or selecting optical switch elements for a reconfigurable QKD system.

Following that, with a series proof-of-concept experiments, the mathematical model has been verified experimentally and the feasibility of the optically switched multi-user QKD system has been experimentally studied. The performance in term of QBER has been investigated at different levels of losses and crosstalk with a basic QKD setup. As predicted by the mathematical model, the experimental result shows that -21 dB of crosstalk introduces a negligible penalty, but a -9 dB crosstalk level adds 5% QBER. The increasing channel loss introduced by both the optical fibre channel and optical switch significantly affect the QKD performance.

Chapter 4 Reconfigurable QKD over Metro network

4.1 Introduction

As discussed in the previous chapters, a QKD system can achieve secure key transmission over hundreds of kilometres of optical fibre link [29], making QKD applicable for encryption in metropolitan area networks. As DVQKD has been commercialized by a few companies, the technique has reached a mature level, being considered for practical deployment. In addition, optical switching has been shown to be a promising method for achieving QKD between multiple end users within a flexible network structure. As mentioned previously, optical switches are used not only in lab demonstrations [56, 57, 60] but also in a few QKD network field trials [59, 61-63]. However, the smooth and cost-effective integration of reconfigurable QKD into the current practical metro network still needs further investigation.

In addition, most previous lab demonstrations of optically switched QKD systems have focused only on the system function and performance in terms of QBER and secure key rate at each path. The overall system reconfiguration time has not attracted much research attention to date, and is either not described in detail or for relatively long (many minutes) in most practical network demonstrations in terms of practical transmission loss/distance. For example, in the field trial of a practical optically switched QKD system by T.E.Chapuran et al. [61], the QKD transmission was switched between a distance of 25 km and 10 km. The system reconfiguration times for the two paths were 19 minutes and 7 minutes, respectively. In the most recent demonstration, an optically switched QKD was applied to a software defined networking (SDN) controlled optical network [62]. The overall system reconfiguration time was greater than 21 minutes when switching from back-to-back to a 25 km distance. However, for the practical integration of QKD in metro networks, this reconfiguration time would significantly limit the reconfigurability of the network and reduce the overall quantum key transmission speed between users.

This chapter describes a novel quantum-safe network solution which smoothly integrates a reconfigurable QKD with a reduced system reconfiguration time to protect the data traffic in a realistic metro network. This solution shows the potential for fast switching quantum channels between multiple users and resuming secure key transmission immediately between different

Alices and Bobs. The proposed network architecture and operational principle of dynamic key sharing are described. A coexistence scheme is employed for the transmission of the classical channel and quantum channel, which are placed in different wavelength bands in the same fibre infrastructure. Efficient quantum encryption topologies between different end-users are also presented. Optimisation of the reconciliation and clock distribution architecture is predicted to result in a reduced system/network reconfiguration time.

Next, by a series of proof-of-concept experiments, the feasibility of a switched multi-node QKD system within the proposed network architecture has been demonstrated. The experimental setup includes a centralised Bob that exchanges quantum keys with multiple virtualised Alices in either TDM or handshake modes. Classical data and control signals in the C-band coexist in the same fibre as quantum signals which has a wavelength of 1310 nm. As in the current system, the reconfiguration time is not limited by the switch itself, opto-mechanical switches with millisecond switching times are employed, which have low loss and negligible crosstalk. The work presented in this chapter was submitted and accepted by Journal of Lightwave Technology in 2018 [26].

4.2 Reconfigurable quantum-safe metro network

A conventional metropolitan-scale network architecture may be considered in two parts: the access network and the metro network, as shown in Figure 4.1. The metro network interconnects a number of metro nodes to span different physical metro areas and provides high capacity paths between them. At the periphery of the metro network, edge routers with relatively lower traffic capacity transfer data between the metro network and local access networks. An optical access network normally uses passive optical networking (PON). The data packet transferred within the network includes the header, which gives information of the source and destination address in addition to the transmitted information. Both edge and metro routers are able to retrieve the Internet Protocol (IP) address from the header of the data packets from end users at the inputs and route them to their desired destinations at the outputs, using the electrical domain. Therefore, OE conversion is performed at the inputs of each router, and EO conversion is performed at the outputs of the routers. By comparison, edge routers receive (send) customer data packets from (to) the metro network while metro routers forward the data packets between other metro/edge routers within the metro network [124].

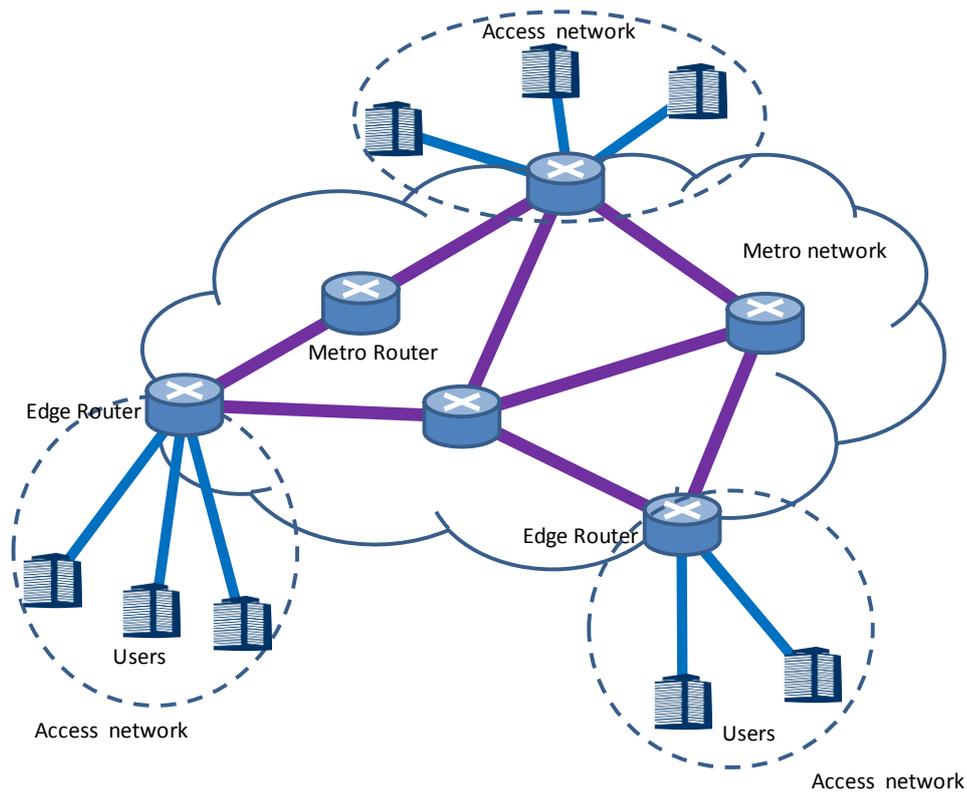


Figure 4.1 Schematic of a metro network structure.

The system proposed in this chapter integrates QKD into the existing metro network as shown in Figure 4.2. Within the metro network, a QKD system is installed (including an Alice-Bob pair and a QKD server PC) at the physical location of each metro router within a metro node (e.g. Metro Node A in Figure 4.2). OEO conversion of the classical signal is conducted at the ports of each router. The Alice and Bob sub-systems are connected via an optical switch, which enables the reconfiguration of quantum signal routes between different nodes. In order to maximise the transmission distance as well as the secure key rate, the optical switch must have minimum loss and crosstalk. Pairs of Alice and Bob are all electronically connected and controlled by a QKD server PC via an Ethernet switch. Through a switch, the QKD server also stores and provides the quantum keys to external encryption devices (e.g. line cards), and communicates with its relevant Alice-Bob pairs. The line cards, installed at each port of a metro router, are then used for the point-to-point encryption which will be explained in detail later. Separately, each end user in an access network has a QKD device. To reduce the overall cost of the practical implementation, the device belonging to each end user would be an Alice rather than a Bob, as the detection system is usually much expensive than the transmitter in a QKD link.

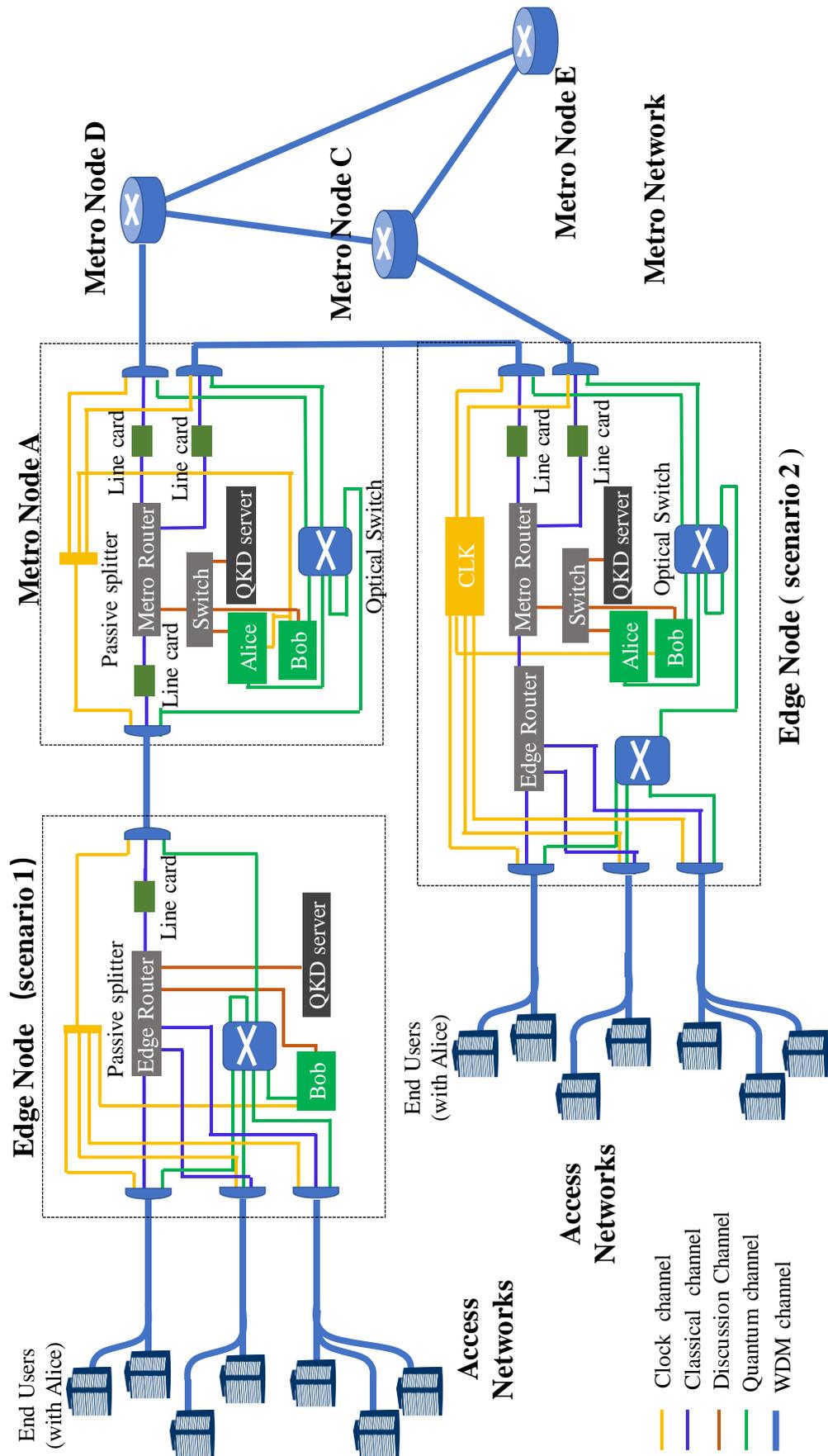


Figure 4.2 The proposed quantum safe metro network architecture

Between the metro node and the end users in the access network, there are two options for integrating QKD depending on the distance between the edge router and its adjacent metro router. Firstly, as illustrated in the edge node scenario 1 in Figure 4.2, if an edge router is located physically far away from its metro router, an edge router is integrated with a QKD Bob device. A low loss optical switch is also employed within such an edge node to switch the Bob device to different Alices in the access or metro nodes. Secondly, if the edge router is at the same physical location as a metro router, the edge node includes both an edge router and a metro router. This node structure is shown as the edge node (scenario 2) in Figure 4.2, which is a combination of the edge node (scenario 1) and metro node A. Thus, this approach removes the need for a line card between the edge router and metro router and the need for an extra Bob device. Similarly, Alice can send quantum signals to different metro nodes, while Bob can detect quantum signals from different end users, or metro nodes, via reconfigurable optical switches.

As has been discussed, it is important to study and enhance the reconfigurability of the QKD network which depends greatly on the system reconfiguration time, being the time required to produce secure key material when setting up a new connection. Three components normally contribute to the overall system reconfiguration time: the speed of the optical switch itself, the time taken for initialization of the system, and the final key regeneration time [60].

The first component corresponds to the time taken for a new connection to be physically set up. This depends on the intrinsic switching time of the optical switch. As discussed in Chapter 3, different optical switching techniques offer different switching times. Normally, optical switches with shorter switching times (in the nanosecond range) have a relatively higher loss and crosstalk (as in the case of electro-optic switches), while those with slower speeds (in the millisecond range) have lower insertion loss and crosstalk levels (as in the case of opto-mechanical switches) [125]. This time is relatively short compared to the other two contributions and does not represent the major limit on the reconfigurability of the QKD network. Therefore, an opto-mechanical switch can be used in this proposed network.

The second component contributing to the system reconfiguration time is the initialization time for a newly connected Alice-Bob pair. This mainly depends on the time needed for the alignment of timing information between Alice and Bob, as well as for optimising the system parameters. Conventionally, the initialization must be performed every time the optical route is switched for a new Alice-Bob pair. This contribution to current practical/commercialized

QKD systems can be many minutes and normally dominates the system reconfiguration time. In this proposed network, this can be reduced by the broadcast of the clock signal to all endpoints from a single source, and the timing and frame information being stored after the first connection and later recalled for subsequent connections. The clock signal can be produced by a master clock, which can use duplicated optical sources for failover protection. This optical clock signal can be distributed with Erbium-Doped Fibre Amplifier (EDFAs) placed as necessary to provide split and transmission loss compensation for the clock signal.

The third component is the time taken to collect enough raw key material (normally a few Mbits) to perform the post processing, including error correction and privacy amplification, and hence to begin secure key generation for a new connection between a pair of Alice and Bob [60, 126]. This time is therefore dependent on the raw data transmission rate and error rate which are a function of the channel loss and the presence of interference. A longer transmission distance or higher channel loss will result in a longer delay due to this contribution. This time delay can be reduced by optimisation of the protocol implementation.

While secure keys are being established between users in a quantum channel, traditional communication encrypted by the keys and the clock broadcasting are meanwhile conducted over a classical channel. The post-processing is also carried out using the classical channel. Conventionally, since the signal level in the classical channel is much higher (more than 70 dB higher) than that of the quantum signal, the two channels are physically isolated in separate fibres to avoid impairments to the key transmission by leakage from the classical to the quantum channel [127]. However, the installation of additional fibres when integrating QKD into the existing network would lead to a high cost. Fortunately, later studies have focused on the so called ‘co-existence scheme’ [128-132], using Wavelength Division Multiplexing (WDM) technology, as shown in Figure 4.3 [129]. In this scheme, the quantum channel is multiplexed with the classical channel using different wavelengths on Alice’s side and transmitted over the same fibre, where it is demultiplexed at Bob with the classical data being filtered out by the de-multiplexer. Such an idea eliminates the need for additional fibre infrastructure [133] and enables the cost-effective integration of optically switched QKD into classical networks.

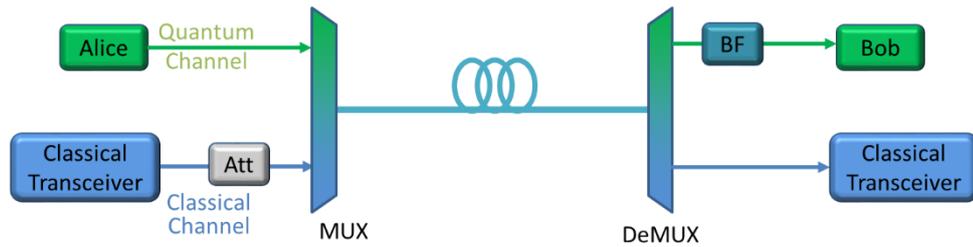


Figure 4.3 Schematics for the co-existence scheme of quantum and classical channels. Classical channel includes both conventional data transmission and post-processing signals for QKD systems. BF: bandpass filter. Att: attenuator. Mux/Demux: multiplexer/demultiplexer [129]

One important problem with this scheme arises from photon leakage of the classical channel into the quantum channel, which introduces additional noise to the key transmission. This can be mainly caused by insufficient isolation between the wavelength channels in the mux/demux as well as the effect of Raman scattering during transmission. Raman scattering is a phenomenon in which photons are inelastically scattered through excitation by photon–phonon interactions [128, 134]. The scattered photons have different energies and hence different wavelengths from the incident photons. A bandpass filter (BF) can be used at the input of Bob to further reduce the passband and then mitigate the photon leakage from the classical channel. The launch power of the classical channel can also be reduced to a limit that corresponds to the photodetector’s sensitivity [129], as shown in Figure 4.3. Practically, the C-band (in the wavelength range of 1530–1565 nm) is widely used nowadays for classical communication, taking advantage of the lower optical fibre attenuation coefficient (0.2 dB/km in a standard single mode fibre) [69]. In addition, the C-band is approximately the wavelength range within which an EDFA is widely deployed. To mitigate the effect of the noise caused from Raman scattering, the weak quantum signal of the integrated QKD needs to be allocated spectrally away from the classical channel. Therefore, the O-band (around 1310 nm) is often used as the quantum channel, though this has a higher fibre attenuation of 0.3 dB/km in a standard single mode fibre [61, 66, 135].

Based on this coexistence scheme, the quantum, classical and clock signals are all wavelength-multiplexed together and transmitted using the same optical fibre from node to node/endpoint. To suppress the effect of noise photons leaking between the classical channel and the quantum channel, the classical signal and the clock signal are allocated in the C-band, while the QKD

signals are placed in the O-band. Each Bob has a narrow BF at the input to further mitigate this effect.

To encrypt the data within such a network, the secure keys must first be properly generated and distributed. The arrangement of the quantum channel is therefore shown as green lines in Figure 4.3. The routing of the quantum signals is transparently reconfigurable due to optical switching, and quantum keys can be dynamically established between any two QKD end points (Alice/Bob) within the maximum achievable transmission distance of the QKD system. As discussed in the previous chapter, the secure key rate of a point to point QKD link dramatically decreases with increasing transmission distance, which corresponds to increasing channel loss. Although state of the art QKD links have enabled secure key transmission over hundreds of kilometres [29], the insertion loss and the crosstalk of the optical switch in use needs to be minimised to guarantee a transmission distance with a secure key rate suitable for a metropolitan area. The system degradations due to both loss and crosstalk induced by the optical switch must be considered in the system design. An optical switch must be carefully selected and designed, as discussed in Chapter 3.

In addition, to further extend the transmission distance, trusted repeating techniques can be combined with optically switched QKD networks [63]. By deploying this kind of hybrid network, the reconfigurability offered by optical switching complements the network scalability offered by trusted repeating. Therefore, QKD connections can be reconfigured between different users and cost effectively extended to longer distances. Thus, in the proposed network structure, when exchanging keys between two physically distant QKD Alice-Bob pairs, the node can also operate as a trusted node (repeater). In this case, the mechanism of key sharing is shown in Figure 4.4. Endpoint 1 and Endpoint 2/Node 2 first establish secure keys K_1 and K_2 with the middle trusted node (Node 1), respectively. Then Alice and Bob are optically switched in Node 1. As the trusted node knows both K_1 and K_2 , it will then send $K_1 \oplus K_2$ to Endpoint 2/Node 2 using the classical channel. Endpoint 2/Node 2 thus knows K_1 by applying $K_1 \oplus K_2 \oplus K_2 = K_1$ (where \oplus is an exclusive OR operation).

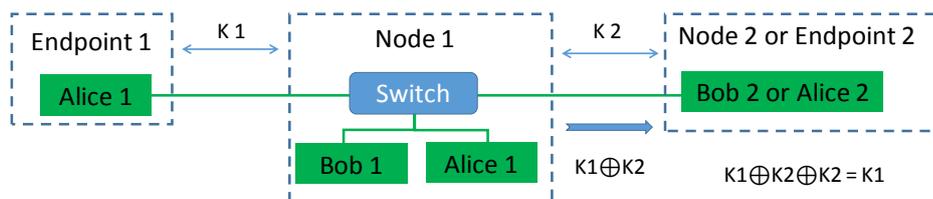


Figure 4.4 Mechanism of exchange secure key between two distant QKD hops

The encryption is based on two different topologies in two corresponding steps: “point-to-point” (PTP) encryption between adjacent nodes (Layer 1 encryption) and “end-to-end” (ETE) encryption between distant end users (Layer 3 encryption). First, ETE encryption uses quantum secure keys shared between source and destination end users. At this step, only the payload (data section) of the data packets are encrypted and the header is left unencrypted, as the router in the edge node needs to be concerned with the destination address when transferring the encrypted data. Secondly, the Layer 1 data encryption between network routers uses PTP encryption realized by the line cards. Specifically, line cards encrypt/decrypt the full length of the passing data packets (both header and data section), which are payload-encrypted data packets in the first step, using the quantum secure keys shared between network nodes.

4.3 Proof-of-concept Experiment

The feasibility of the dynamic reconfiguration of QKD routing and secure key establishment between multiple metro nodes in the proposed network structure has been studied experimentally. The commercial Clavis 3 *ID Quantique* (IDQ) QKD system [136] is employed in the experiments, which is based on a COW protocol [25]. Before the introduction of the experimental setup, the QKD platform is briefly illustrated as follows [137].

In Alice, a train of optical pulses is generated by a continuous-wave laser with a wavelength of 1310 nm modulated by an intensity modulator at 1.25 GHz. The bit values are encoded into the pulse train based on the COW protocol, which has been introduced in Chapter 2. Decoy states are randomly added into the pulse train to enhance the security. The optical pulses are then highly attenuated to the desired intensity level by a variable optical attenuator. This level is normally optimised for different transmission distances/losses. The pulses are then sent from Alice to Bob over the quantum channel.

In Bob, using an asymmetric optical coupler, most of the intensity is split out and used to record the arrival time of each pulse by an SPD, while the rest of the intensity is sent to the interferometer and another SPD to check the phase relation between consecutive pulses and hence decode the bit information. The SPD operates in free running mode. To reduce afterpulsing and hence the background noise, increased deadtime is applied to the detectors [138].

In each Alice or Bob device, postprocessing and key distillation are conducted using a field-programmable gate array (FPGA) module, which is controlled by software installed in a QKD

PC via an Ethernet cable. The software also performs automatic initialization, including frame and time-slot alignments for the connected Alice-Bob pair before the transmission of the quantum signal. After the exchange of raw keys, error correction is conducted based on a LDPC algorithm. Privacy amplification is conducted using Wegman-Carter strongly universal hashing to reduce the information available to a potential eavesdropper. The user interface continuously updates the QBER and the secure key rate. In addition, the QKD PC stores quantum secure keys from Alice and Bob and sends them to the encryption device [137].

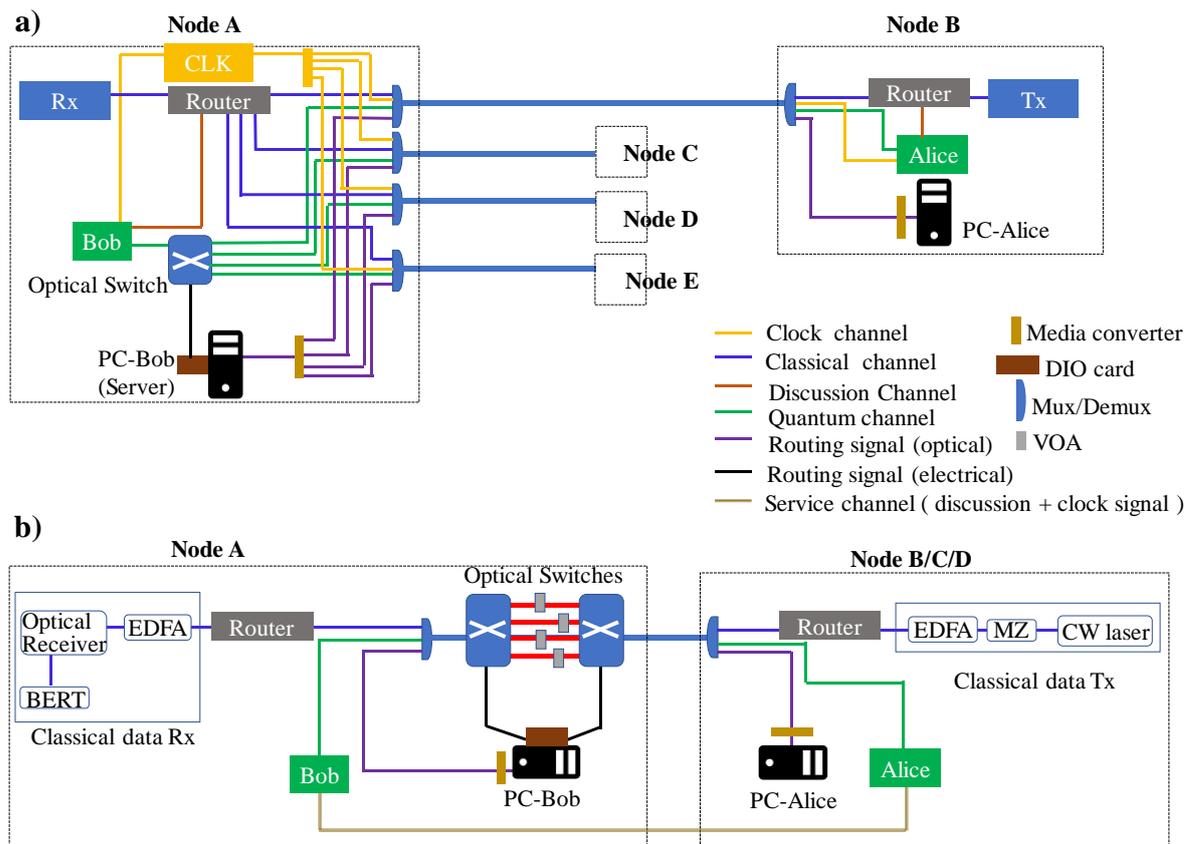


Figure 4.5 a) Equivalent system schematic. b) Experimental setup. EDFA: Erbium-doped Fibre Amplifier. BERT: Bit Error Rate Test

Figure 4.5 shows the proof-of-concept experimental setup as well as the equivalent system schematic. Bob at Node A dynamically shares keys with the Alices in four different nodes via an optical switch. Given that the speed of the optical switch itself does not currently dominate the system reconfiguration time of the optically switched QKD system, an opto-mechanical switch with a switching time of a few milliseconds can be used in this proposed network architecture. In the current setup, 1x4 port opto-mechanical switches (Lightwave, 1x4 / 4x1 latching optical switch module) are employed. Each switch has approximately 1 dB insertion

loss and a crosstalk level of -80 dB. Therefore, the effect of crosstalk can be negligible. Owing to the limited number of IDQ boxes available, the current setup employs only one pair of IDQ Alice and IDQ Bob. Two 1x4 optical switches combine to establish four paths to the same Bob, as shown in Figure 4.5(b). Different transmission lengths are mimicked by adding different optical attenuations. Four paths with losses of 11.6 dB, 11.1 dB, 10.5 dB, and 15.6dB are used in the switching experiments.

In addition to the quantum channel, a service channel, which consists of an optical fibre pair is also connected back-to-back between Alice and Bob units using small form-factor pluggable (SFP) transceivers [137]. The service channel, which is shown in Figure 4.5(b) as dark yellow lines, was originally designed by the supplier to provide both the clock signal and reconciliation function between an Alice and Bob pair. This design is convenient for a point-to-point QKD transmission, and the service channel is designed not to be disturbed. Any reconnection of the service channel stops the system software measurement on the QKD server. Although the clock signal currently cannot be separated out or regenerated without modifying the units in use, private communications with IDQ have indicated that it would be possible to split the two functions of clock transmission and the reconciliation channel into two separate channels [138]. The separated clock is then distributed to all recipients, as shown in the proposed network structure, avoiding any loss or jitter of the clock during the switching function. However, this would not introduce any change in system performance from the presented experimental setup.

The classical data transmission is multiplexed with the quantum channel based on the co-existing schemes. The classical data transmitter (Tx) uses a continuous wave laser operating at a wavelength of 1556 nm and modulated by a Mach-Zehnder modulator (MZM) driven by a $2^{31}-1$ PRBS 10 Gb/s signal. An Erbium-doped Fibre Amplifier (EDFA) is used to amplify the signal. A 0.4 nm filter is added after the EDFA to suppress the amplified spontaneous emission noise, which is not shown in the schematic. After transmission along the same fibre as the quantum signal to Bob, the classical data is demultiplexed and amplified by another EDFA to compensate for the channel loss. A 0.4 nm filter is used again for noise reduction. Then the classical data is detected by a conventional photodetector and measured by a bit error rate tester (BERT).

The discussion channel between the PC in Bob of Node A and each PC in Alice of Nodes B/C/D provides the routing signals for controlling the optical switch. This was originally an electrical signal from the PC but is converted into the optical domain using media converters

(an ethernet switch with SFP ports) at a wavelength of 1531 nm, which is also multiplexed into the quantum channel and classical data channel using WDM couplers and transmitted to Node A. The routing signal from Alice is split out and read by the PC (PC-Bob) via a media converter, and a high-speed Digital Input/Output (DIO) Card (ADLINK, PCIe-7360) in PC-Bob electronically controls the optical switch and routes the quantum signals onto the required path. Quantum signals from the Alice in the desired Node pass through the switch and are read by Bob. A 1310 nm wavelength filter (about 80 dB extinction) is used at the receiver end of the quantum channel to avoid an increase in QBER due to the classical channel crosstalk.

Owing to resource constraints, the multi-user system was virtualised by server-client threads by designing a network program based on C# coding. As previously mentioned, two 1x4 optical switches are combined to establish four paths to the same Bob. The software enables sending switching commands as routing signals from PC-Alice to PC-Bob based on two regimes: periodic mode or request mode. Before the start of key transmission, the connection between PC-Bob and PC-Alice is established by knowing each other's IP address. Then, PC-Bob waits for commands from Alice. If 'periodic mode' is agreed between Alice and Bob, PC-Bob controls the optical switch via the DIO card and changes the path after every time period without a command from PC-Alice. The time period can be defined by users, based on the secure key rate and the required number of keys for encryption in the corresponding path. PC-Bob will stop changing switch states as long as it receives a 'termination' command from Alice. On the other hand, if "request mode" is chosen, each virtual Alice client sends remote 'request' commands to PC-Bob upon the need of key transmission. At PC-Bob, the requests are queued by receiving time. The first request is processed and controls the switch state to set up the corresponding connection for a user-defined period, while subsequent requests are placed on hold. Thus, all the requests are processed in order, and each switching period is defined as the time needed for the collection of sufficient number of keys for each path.

4.4 Experimental results

Figure 4.6(a) shows the real-time measurement of QBER for each path without coexistence with the classical channel and routing signal in the same fibre. The switch is controlled under the periodic mode with 5-minute measurements for each path. The different colours indicate the different paths from Node A to virtual Node B, C, D, E, respectively, using 'A-B' 'A-C' 'A-D' 'A-E' for short. As previously mentioned, the transmission losses of those paths are 11.6 dB, 11.1 dB, 10.5 dB, and 15.6dB, respectively, (corresponding to a fibre length of

33.1 km 31.7 km, 30 km and 44.6 km, assuming an attenuation coefficient of 0.35 dB/km at 1310 nm). QBER measurements are continuously conducted without any interruption when changing the path. The average QBER is approximately 2.6% for the path A-D with the minimum transmission loss. As expected, the path with a higher channel loss has a higher QBER due to the dissipation of quantum signal during the transmission. The average QBER increased to around 3.2%, 3.6%, and 4.1% for the paths A-C, A-B, and A-E, respectively.

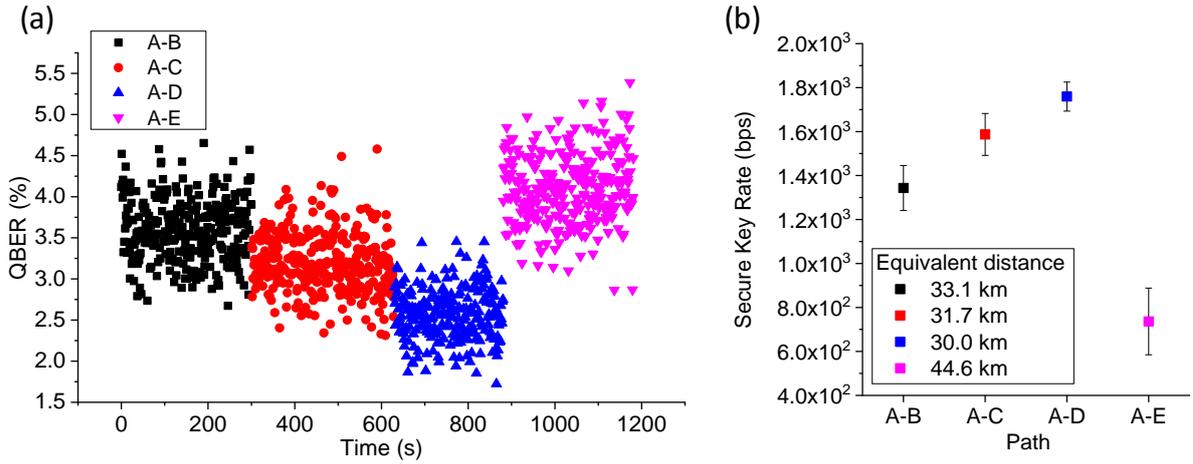


Figure 4.6 (a) The real-time measurement of QBER with path reconfiguration for the quantum channel only (without the classical signal and routing signal being co-existed in the same fibre). The legend indicates the switch states, e.g. A-B stands for the connection from Node A to Node B. (b) Corresponding average secure key rate measured for each path. The error bars indicate the standard deviations in the measurements for each path.

Secure keys are continuously generated between four virtualised Alice-Bob pairs and stored in the QKD PC for the purpose of encrypting classical communication. The secure key rate measurements are also updated in the software. The average secure key rate at each path is plotted in Figure 4.6(b) with standard deviation error bars for the 5-minute measurements. The legend shows the corresponding equivalent transmission distance. A maximum Secure key rate of round 1.8×10^3 bits/s is obtained for the path A-D with the minimum channel loss of 10.5 dB, equivalent to a transmission distance of 30 km. As the QBER increases over a longer transmission distance, the corresponding secure key rate falls to round 1.6×10^3 bits/s, 1.3×10^3 bits/s and 736.3 bits/s for the equivalent transmission distances of 31.7 km (path A-C) 33.1 km (path A-B) and 44.6 km (path A-E), respectively.

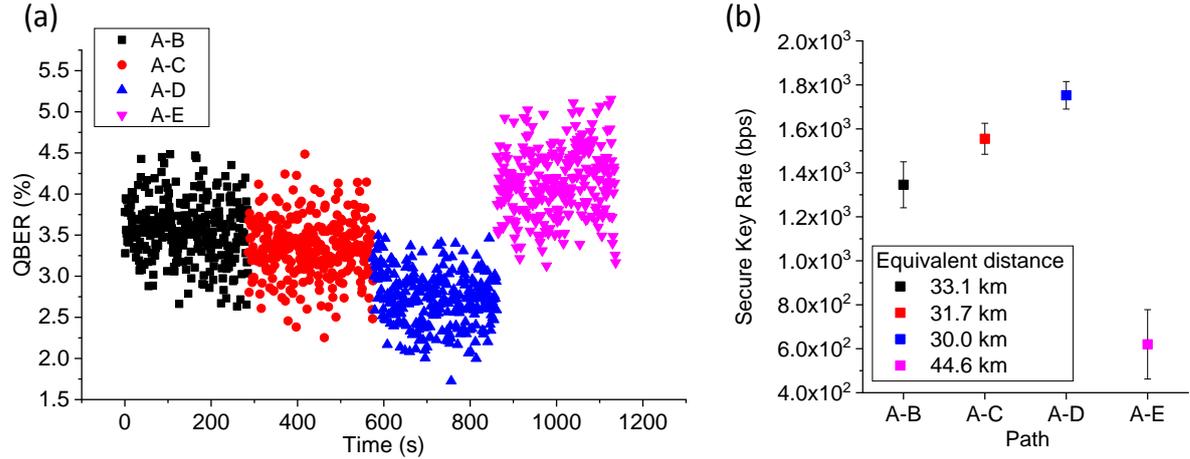


Figure 4.7 (a) The real-time measurement of QBER with path reconfiguration for the quantum channel multiplexed with the classical channel and routing signal. The legend indicates the switch states, e.g. A-B stands for the connection between Node A and Node B. (b) Corresponding average secure key rate measured at each path. The error bars indicate the standard deviations in the measurements for each path.

The classical data and routing signals are then added to the transmission via WDM couplers and the measurements are then repeated for each path. The launch power is fixed to -10 dBm, to minimise the noise due to the leakage to the QKD channel. The measurements are plotted in Figure 4.7. The average QBERs were obtained as 3.6% 3.3% 2.7% and 4.1% for the Paths A-B, A-C, A-D, and A-E, respectively. The similarities between Figure 4.6 and Figure 4.7 indicate that the classical signal and routing signal in the experiment do not affect the quantum channel due to the additional 1310 nm filter at Bob (after demultiplexing) which has more than 80 dB extinction against the 1550 nm band. The effective Q factor of the received classical data was calculated to be 21.4 dB, both with and without QKD transmission, which indicates that the classical data transmission is error-free and unaffected by QKD transmission.

To investigate the system reconfiguration time, the switching time is first measured. The delay between sending the electrical routing signal from the DIO card and the arrival of photons at the detector indicates that the switching time is less than 3 ms. In the normal operation of the IDQ QKD system used in the experiment, the start-up takes an extended time, as the system automatically conducts the alignment of timing information as well as determining appropriate parameters for the connected Alice- Bob pair. This may take about 20 minutes. As mentioned in the previous section, this corresponds to the initialization time contribution to the system reconfiguration time. However, it can be seen from the measurements in Figure 4.6 and

Figure 4.7 that the quantum signal transmission carries on without the need to restart and initialize the system *ab initio* each time the experiment switching between different virtual Alices. In a practical implementation with physically-distinct Alice elements, it is feasible to broadcast the clock signal from a single source, and to save the timing and frame information (as well as other system parameters) and reload from/to the QKD PC them for each Alice and Bob pair as soon as the link is switched to connect them [138]. It will then greatly reduce the reconfiguration time to recommence key generation from where it left off last time, rather than the minutes required at the moment for an automatic start. In the proof-of-concept experiment, the clock is ‘distributed’ within the service channel between an Alice-Bob pair, which will not make much difference in the reconfiguration time of the network proposed in Section 4.2.

In addition, it is observed that secure key exchange is achieved by no more than 20 seconds after completion of the automatic startup and configuration routines under conditions of moderate channel loss (15 dB). As discussed, this time is the final key regeneration time spent on accumulating the initial raw key for post processing before beginning the secure key exchange for a new connection between a pair of Alice and Bob. This time is clearly dependent on the raw key rate and QBER which are a function of the channel loss and the presence of interference. This then becomes the main contribution to the system reconfiguration time in our experiment without the need for reinitialization for different connections. Hence, it is justified to use this time in the prediction of the reconfiguration time of the architecture proposed in this chapter, rather than the many minutes required at the moment for an automatic start.

Thus, the proposed modification of the provided QKD enables the use of multiple physical Alice and Bob elements while still allowing much reduced system reconfiguration time, which is unlikely to be greater than 20 seconds, using the current implementations of the QKD equipment in use. This reduced system reconfiguration time, which is much shorter than that of currently demonstrated optically switched QKD systems or networks, would significantly improve network reconfigurability and increase the overall secure key rate of QKD between multiple users. It should be possible to further reduce this time by specifically optimizing the protocol and postprocessing for switched QKD systems. This is beyond the scope of this thesis and could be addressed in future work.

4.5 Summary

This chapter has demonstrated a novel method for integrating a reconfigurable QKD system into a realistic metro network. The network structure is designed for both classical and quantum transmission in a metropolitan area. Secure keys are continuously shared between nodes and end-users. The system reconfiguration time of the optically switched QKD is greatly reduced by broadcasting a master clock to all QKD users, and recalling the initially saved timing information as well as other system parameters for different connections. Efficient encryption solutions are presented based on both PTP and ETE topologies. Via a series of proof-of-concept experiments, the feasibility of the proposed network scheme has been demonstrated.

In the experiment, Bob continuously shared keys with four virtual Alices at different locations via remotely controlled optical switches. The QBER and secure key rate were investigated for four different channel attenuations corresponding to transmission distances of 30 km, 31.7 km, 33.1 km and 44.6 km. The classical data transmission negligibly affected the quantum transmission. As mentioned previously, in the physical setup, only one QKD Alice and Bob pair was involved, and the multiple Alices were realized by the software and an additional optical switch. The use of the clock distribution architecture was predicted to enable key reestablishment with much reduced reconfiguration time upon switching between different Alice and Bob pairs, with a maximum delay of approximately 20 seconds.

Chapter 5 Towards Reconfigurable CVQKD network

5.1 Introduction

CVQKD systems are promising alternatives to DVQKD systems, in which the secure key is encoded in continuous values of amplitude and phase – referred to as quadratures – of light [139, 140] and decoded with balanced BHDs. As introduced in Chapter 2, the reference pulses for the detection – used as a LO – are either transmitted or generated locally, and are referred as TLO and LLO schemes [88], respectively. CVQKD has attracted much research interest in recent years, due to its ability to perform in highly noisy environments, its compatibility with standard telecommunication techniques, and relatively low cost. Since the first CVQKD scheme was proposed [30], different CV protocols have been invented [31-35]. Among these, the most implemented and studied protocol is called the Gaussian-modulated coherent state protocol (GMCS), which was introduced by F. Grosshans and P. Grangier in 2002 [31]. This is therefore also known as the GG02 protocol. Its security has been comprehensively analysed theoretically and proven against collective attacks [36] as well as against general attacks [37]. Practically, point to point CVQKD key distribution has been shown over longer transmission distances of 80 km [45] and 100 km [46], and network field deployment [64].

In Chapter 4, an effective solution for integrating reconfigurable QKD in the existing metro network based on the practical DVQKD system was proposed. Although CVQKD has not been commercialized yet and, to the best of our knowledge, reconfigurable multiuser CVQKD systems or networks have not been demonstrated so far, it is important to study the feasibility of optically switched CVQKD systems, even before they reach the maturity level of practical use in metro networks. As CVQKD is a relatively young technique compared to DVQKD, its performance in terms of secure key rate has not been practically comparable to a DVQKD system and the use of it in practice is still under investigation. CVQKD suffers from lower raw data rates compared to recent demonstrations of GHz clock rate DVQKD systems [44, 137]. Most practical GMCS CVQKD systems work at a repetition rate of 1 MHz or below. To our knowledge, the state of the art secure key rate of a complete GMCS CVQKD system is around 1 Mbps at 25 km with a 50 MHz repetition rate using a 1 GHz BHD [47]. Although the speed of postprocessing after detection is one limiting factor [141], this is not a significant issue as it

can be mitigated by high-performance hardware. It has been pointed out that the computational complexity can be significantly reduced by modern GPUs which are able to efficiently process huge amounts of data in parallel [45, 142]. The fundamental speed limitation of the CVQKD is the noise performance.

In this chapter, therefore, we first consider the feasibility of a high speed GMCS CVQKD system in order to meet the demand of increasing QKD-enabled encrypted classical data traffic in metro networks. In particular, we conduct a noise analysis at a high clock rate, showing the rate-dependence of the different noise sources. Different noise contributions have previously been studied in [98], however, the influence of the system clock rate has not yet been taken into account. Then, with a practical GHz bandwidth BHD, which is built around modified commercially available components, the feasibility of an optically switched high speed (250 MHz) GMCS CVQKD system is experimentally investigated. This part of the work was conducted in collaboration with Dr. Rupesh Kumar.

In addition, we also propose the use of an equalizer for GMCS CVQKD detection to mitigate possible overlapping distortion and hence be able to use lower bandwidth BHD at higher rates. The reduction in noise due to the distortion in CVQKD detection is investigated via an analytical model. This work presented in Section 5.5 was submitted and accepted by IEEE Global Communications Conference 2018 [143].

5.2 Noise analysis in high speed CVQKD

As discussed in Chapter 2, in GMCS CVQKD, Alice prepares coherent states $|\alpha\rangle = |X_A + iP_A\rangle$, where X_A and P_A are quadrature values drawn from a set of normally distributed random variables, $\mathcal{N}(0, V_A)$, with a variance V_A and a mean of zero, and sends them to Bob through the quantum channel. At Bob, a BHD is used to randomly measure the X or P quadrature values of each state. The quantum channel is characterised by the transmittance T and excess noise ζ . Under the Gaussian linear model with additive Gaussian noise, parameter estimation can be conducted via **Eq. (2.26)–(2.29)** in Chapter 2. By estimating the parameter T and the noise variances ζ , Alice and Bob can bound Eve's information and extract the final secure key using **Eq. (2.30)**. In order to evaluate the performance of high bit rate CV-QKD systems, it is essential to study the behaviour of these noise terms at higher detection speeds. Theoretically, the excess noise ζ is assumed to have originated from eavesdropping. But, in practice, ζ can be contributed

by a range of experimental parameters. In the following, we investigate and categorize the noise contributions which behave proportionally to the system repetition rate.

Shot noise variance

The shot noise variance, N_0 , is the fundamental vacuum noise fluctuation associated with the coherent states. The Heisenberg uncertainty of quadratures is related to this noise variance as $\Delta x \Delta p \geq N_0$ [46]. As introduced in Chapter 2, all the parameters of a CV-QKD system are expressed in terms of shot noise units (SNU). Therefore, this requires careful and precise calibration of N_0 . In practice, N_0 is measured with respect to the LO power at Bob by blocking the signal port of the homodyne detector. To meet the Gaussian linearity model for the protocol, the BHD is set within the linear regime with sufficient LO power – typically by 10^6 to 10^9 photons per LO pulse. This will also reduce the electronic noise variance in the systems and hence the detection is said to be shot noise limited.

As the repetition rate increases, the LO pulse duration will decrease, assuming a fixed duty cycle. The requirement for maintaining the linear relationship between the output and input of the detector requires a corresponding increase in the peak power of the LO pulse. In practice, this cannot happen indefinitely with an increasing repetition rate, which is limited by the maximum power available from the LO laser as well as the optical power handling capability of the photodiodes in the BHD in both the TLO and LLO schemes. Additionally, at longer transmission distances, optical loss in the channel imposes a further requirement for increased peak power of LO pulses with TLO CV-QKD. This power constraint is not present in LLO based CV-QKD schemes as the local oscillator power is not affected by channel attenuation, since it is locally generated at Bob.

Imbalance in BHD

Like the transmitted signal distribution, the measured quadratures at Bob also follow a Gaussian distribution, $N(0, V_B)$ with a variance V_B (**Eq. (2.28)**) and a mean of zero. The zero mean of the distribution is set by balancing the homodyne detector.

Practically, the BHD output drifts from its balancing condition over time, and hence the measured mean value of each quadrature is not maintained constant during the key transmission. This can be due to multiple reasons such as temperature fluctuations, drift in data acquisition sampling or its clock, variation in the characteristics of the detector electronics, etc. Within the total data sampling interval, here 10^8 samples, this fluctuation in the mean value of the

distribution is manifested in the signal variance estimation, V_B , and adds extra noise, ξ_{bd} , in the CV-QKD system. This can be also explained in the following equations:

Firstly, any imbalance in the BHD results in a finite common mode rejection ratio (CMRR = g/g_c) at the output, which is given by [98]:

$$\begin{aligned} U &= \frac{hf}{\tau} \rho \left(g\Delta N + \frac{g_c}{2} (N_{sig} + N) \right) \\ &= \frac{hf}{\tau} \rho g \left(\Delta N + \frac{1}{2CMRR} (N_{sig} + N_{LO}) \right) \end{aligned} \quad (5.1)$$

where h is Planck's constant, f represents the optical frequency of the laser, N_{sig} and N_{LO} are the photon numbers per pulse in the signal and LO respectively, ΔN is the difference in photon numbers from each photodiode in the BHD, which is given in **Eq. (2.23)**, τ is the pulse duration of the laser pulse, and g and g_c are the differential gain and common mode gain of the amplifier at the output of BHD, respectively.

In **Eq. (5.1)**, the first term corresponds to the quadrature measurements, while the second term corresponds to the voltage output due to imbalance of the balanced detector. Clearly, a constant imbalance would cause a constant shift in the mean value but would not influence the variance in the measurement.

However, if the balancing condition drifts with time, then this contributes to the excess noise, ξ_{bd} , which in turn undermines the system performance. This can be then described in SNU as:

$$\xi_{bd} = \frac{\langle \sigma(t)^2 \rangle \Delta t^2}{G\eta_B} \times \frac{(N_{LO} + N_{sig})^2}{N_{LO}} \approx \frac{\langle \sigma(t)^2 \rangle \Delta t^2}{G\eta_B} \times N_{LO} \quad (5.2)$$

where η_B is Bob's transmission efficiency, G is the channel efficiency, σ is the time-varying imbalance factor between two different arms of homodyne detection, which is related to the CMRR as $\sigma = \frac{1}{2CMRR}$ [141], and Δt is the period of measurement.

A typical CVQKD experiment as demonstrated in [39] shows that the excess noise due to relative drift in the homodyne output can be negligible for Δt of 100 ms but increases to an observable level of $10^{-3}N_0$ over a period longer than a few hundred seconds. To mitigate this effect, shot noise measurement, parameter estimation and key transmission sessions should in principle be conducted repeatedly for different time slots. However, measurements within each session need to be conducted over 10^8 sampling points to reduce the statistical fluctuations [39].

For a system with a 1 MHz repetition rate, only 10^5 sampling points can be obtained with a session of 100 ms, while measurements can be more precisely conducted with 10^8 sampling points for a system with a repetition rate of 1GHz. Therefore, the use of high bit rate CVQKD can better mitigate excess noise due to drift in homodyne balancing and hence improve the system performance.

Phase drift noise

The phase noise in a GMCS CVQKD system, as explained in Chapter 2, contributes to the excess noise as $\xi_{phase} \approx V_A \times V_{phase}$ [88, 91]. V_{phase} , the variance of the difference between the estimated and actual phase of the signal relative to LO, is evaluated differently for TLO and LLO schemes.

In a TLO CV-QKD system, the signal and LO pulses propagate through different optical paths inside Alice and Bob. Thermal fluctuations in the path generate a drift in relative phase between the signal and the LO. Experimentally, phase noise corresponding to this drift is mitigated by periodically sending pilot pulses from Alice to Bob. Bob carries out the relative phase estimation of the pilot pulses with respect to the phase of LO. During the reverse reconciliation procedure, Alice compensates for the phase drift by phase correcting her transmitted quadrature values. The remaining phase noise after phase correction was given in **Eq. (2.39)**.

In this equation, the term, V_{error} corresponds to the phase measurement accuracy, which is the variance of the difference between the estimated and exact phase values of the pilot pulses. This is inversely proportional to the amplitude of the pulse and is considered to be independent of the repetition rate [88]. However, inspired by the work in [90], the term $V_{channel}$ can be expressed as:

$$V_{channel} = \Delta\theta_{ch}^2(\Delta t) \quad (5.3)$$

Given that θ_{ch} is the time dependent phase difference between the pilot and signal pulse (relative to the LO) when travelling through the transmission channel, $\Delta\theta_{ch}$ is the relative phase drift of θ_{ch} in one measurement frame Δt , which can be reasonably assumed to be constant under normal condition [90]. At high repetition rates the phase noise decreases as the relative phase drift experienced by the pulses within the phase sampling period (ie. measurement frame) approaches zero. Thus, the excess noise due to this noise increases with the time frame Δt , and is inversely proportional to the repetition rate.

In a LLO CV-QKD system, the signal and the LO are generated from two independent free-running lasers. A phase reference pulse is also generated and sent by Alice with each signal pulse. Signal and reference pulses are transmitted through the same optical path. Therefore, the signal and reference pulses experience the same phase change during their propagation ($V_{channel} = 0$). However, the finite spectral linewidths of the two interfering laser pulses creates a phase estimation uncertainty in the reference pulse. The difference between the estimated phase value of the reference pulse from the exact phase values contributes to the phase noise. The total phase noise in this case is given in **Eq. (2.40)**.

The $V_{linewidth}$ term in the equation is the relative phase drift between two free running lasers with spectral linewidths $\Delta\nu_A$ and $\Delta\nu_B$, and can be written as a function of the repetition rate f_{rep} [88]:

$$V_{linewidth} = 2\pi \frac{\Delta\nu_A + \Delta\nu_B}{f_{rep}} \quad (5.4)$$

This noise limits the achievable transmission distance of an LLO scheme to a few tens of km [91]. With a higher repetition rate, the drift $V_{linewidth}$ becomes smaller and hence the excess noise can be reduced. In turn, the system performance improves in terms of the secure key rate and transmission distance. From a practical point of view, narrow linewidth lasers are normally selected to minimise the phase noise. However, the use of high linewidth lasers are possible in systems with higher repetition rates.

In addition to the conventional LLO-based CVQKD, an LLO-delay line design has been recently proposed [88]. This scheme uses delay line interferometers to eliminate $V_{linewidth}$ by the simultaneous emission of signal and reference pulses. However, V_{phase} is then affected by the noise variance, $V_{channel}$, as in TLO-based CVQKD.

Quantisation noise

In practice, excess noise is introduced by imperfect modulation on Alice's part during the preparation of coherent states based on the Gaussian modulation. This happens in the digital to analogue convertors (DAC) used for amplitude and phase modulation in the translation from discrete bits into voltage levels. The quantisation noise at Alice affects the state preparation and that contributes to an excess noise term \mathcal{E}_q as [98]:

$$\xi_{q,Alice} \leq V_A \left(\pi\alpha \frac{\sqrt{V_q}}{V_\pi} + \frac{1}{2} \pi^2 \alpha^2 \frac{V_q}{V_\pi^2} \right)^2 \quad (5.5)$$

where, α is the gain factor of the amplifier, and V_π is the voltage required to achieve a phase rotation of π . Quantisation noise is also introduced at Bob from the analogue to digital converter (ADC) at the output of the BHD and transimpedance amplifiers (TIA), which is used to convert the measured output voltage to the measured quadrature at Bob. This also contributes to the excess noise as described in [98]:

$$\xi_{q.Bob} = \frac{\tau V_q}{hf g^2 \rho^2 P_{LO} \eta_B G} \quad (5.6)$$

where ρ is the responsivity of the PIN diodes. Similarly, V_q is the voltage noise variance of ADC due to the limited resolution, and P_{LO} and τ are the peak optical power and pulse duration of LO, respectively.

V_q in both of the above equations stands for the output voltage variance from the converter which is applied to the modulators. It is affected by the resolution of the digital to analogue conversion [144]:

$$V_q = \frac{LSB^2}{12} = \frac{V_{FS}^2}{12 \times 2^{2N}} \quad (5.7)$$

where LSB stands for the least significant bit, V_{FS} represents the full-scale voltage range, and N is the resolution of the converter in bits. V_q in both Alice and Bob will typically have system speed dependency which comes from the trade-off between the effective number of bits available and the sampling rate of the conversion. In Ref. [144], it was shown that approximately one bit of resolution is lost for every doubling of the sampling rate. As shown in [144], a 1 MHz ADC offers a typical resolution of 16 bits while a 250 MHz ADC has a typical resolution of 8 bits.

Electronic noise

The electronic noise, N_{ele} , at the BHD is mainly a result of the thermal noise associated with the TIA circuit. To detect quantum signals, a homodyne detector must be sensitive enough to distinguish shot noise from electronic noise. Electronic noise N_{ele} is therefore measured with respect to the shot noise variance and practically expressed in the SNU, which can be expressed as [98]:

$$N_{ele} = \frac{NEP_{ele}^2 B \tau \eta_B}{\rho^2 hf P_{LO}} \quad (5.8)$$

where NEP_{ele} is the electrical noise equivalent power in A/\sqrt{Hz} , referred to the power at the input of the TIA. B is the bandwidth of the detector. As can be seen, electronic noise (in SNU) increases with bandwidth. Lower bandwidth, 10 MHz, detectors are reported to have electronic noise 25 dB below the shot noise value, equivalent to 0.003 SNU, measured with a local oscillator power of 10^8 photons per pulse [39]. The GHz bandwidth detector reported in [46] exhibits electronic noise of 0.25 SNU, for local oscillator pulses with a mean photon number of 10^7 photons/pulse. In addition, the electronic noise is proportional to NEP which depends on the circuit components but has been shown to generally increase with the repetition rate for a given electrical bandwidth [145].

Please note that the noise analysis in this section assumes that the BHD possesses a high enough bandwidth which does not limit the repetition rate of the signal pulses. However, there may be an extra noise term: driving a homodyne detector near to its bandwidth limit would cause consecutive detected electrical pulses to overlap and thus contribute to additional excess noise. This noise contribution will be discussed separately with a proposed efficient solution in Section 5.5.

Based on the analysis of above noise sources, the noise variance Z contributions becomes:

$$Z = N_0 + \eta T (\xi_0 + \xi_{bd} + \xi_{phase} + \xi_{q,Alice} + \xi_{q,Bob}) + N_{ele} \quad (5.9)$$

where ξ_0 is the system excess noise, which stands for the frequency independent excess noise contribution. Each of the above noise components is plotted at different CVQKD repetition rates, as shown in Figure 5.1. The example parameters used in the calculation are shown in the figure caption. Although some of the parameters may vary with the experimental conditions, the estimation shows the practical trend of rate-dependent noise performance. The increase of quantisation noise in the plot is shown as ‘steps’. This is because the calculation uses the approximation stated in [144], that one bit of resolution is lost for every doubling of the sampling rate. The number of bits is assumed to be an integer. It can be seen that the phase noise and the noise due to imbalance drifting decrease with increasing repetition rate and can be considered negligible in a high speed CVQKD systems. On the other hand, the electronic noise and quantitation noise increase with the repetition rate, and become the limiting factor for high speed CVQKD implementations. Fortunately, by carefully selecting commercially available high bandwidth photodiodes with low electronic noise, it is possible to construct a shot noise limited GHz bandwidth homodyne detector. Later, we will evaluate the performance

of our GHz homodyne detector built from modified commercially available components and study the feasibility of a high speed CVQKD system with the estimated excess noises.

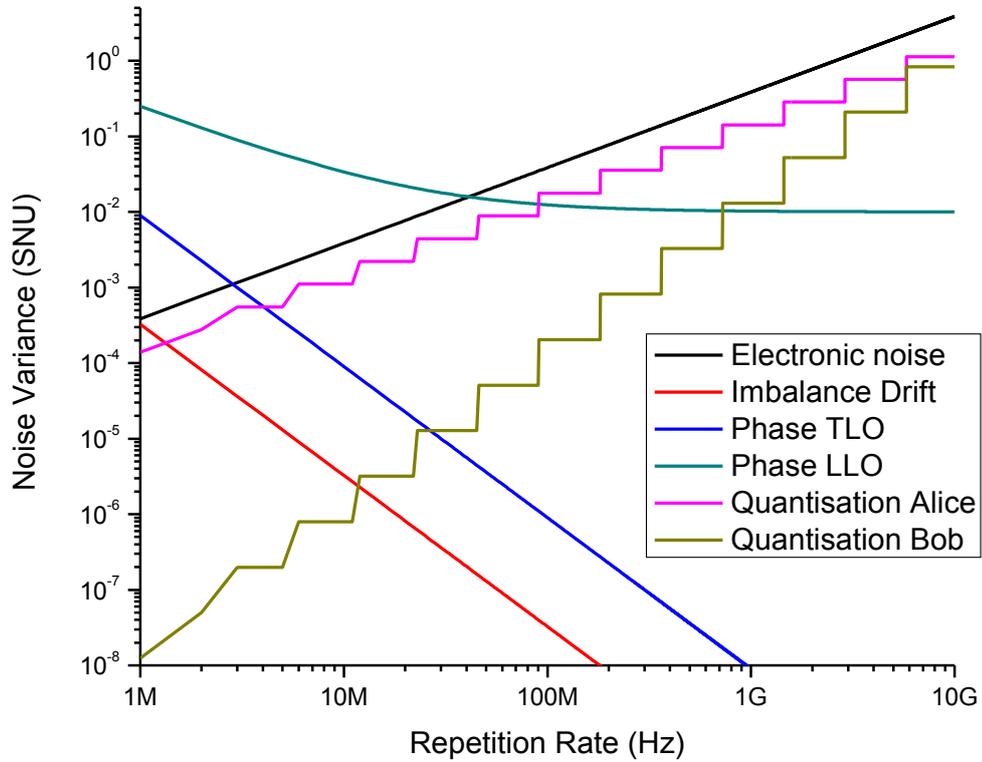


Figure 5.1 (a) Estimation of the noise terms at different CVQKD repetition rates. (b) Estimation of the total electronic noise and total excess noise with changing repetition rate. In the estimations, N_{LO} is fixed at 10^7 (with a P_{LO} of 3 mW and a t_d of 0.5 ns). η_B is set as 60%, and $V_A=10$. The time interval Δt of both shot noise drifting and phase noise drifting is set as the time corresponding to the 10^8 sampling point at different repetition rates. The linewidth of the lasers are assumed to be the state of the art value of 1.9 kHz [93]. V_π and V_{FS} are assumed to be 5 V and 1 V, respectively. The gain factors α and g are fixed at 5 V/V and 50 k A/V, respectively. N is 16 bits at a 1 MHz repetition rate and decreases to 8 bits at 250 MHz. The bandwidth of detector B is assumed to be four times higher than the repetition rate.

In order to show the effect of these noise changes on the CVQKD performance, the corresponding secure key rates are estimated at different repetition rates from 100 MHz to 1 GHz for both cases with TLO and LLO (Figure 5.2). The case for the typical repetition rate of 1MHz is also plotted as a reference for comparison. Here, excess noise and electronic noise at different clock rates are substituted in Eq. (5.9), and secure key rates are estimated using Eq. (2.30). Other excess noise contributions which do not change with speed are assumed to

be 0.02 SNU. The modulation variance is 10 SNU and reconciliation efficiency is assumed to be 95%.

Practically, the use of the quantum channel can be divided in three sessions. Firstly, Bob randomly blocks one session of receiving states for shot noise variance measurements. Then, two sessions are used for parameter estimation and key distillation. For security reasons, these three sessions are conducted randomly in time. Therefore, in the following calculation, two thirds of the raw key are assumed to be used for parameter estimation and shot noise measurements, while only one third of transmitted pulses are used for the key generation.

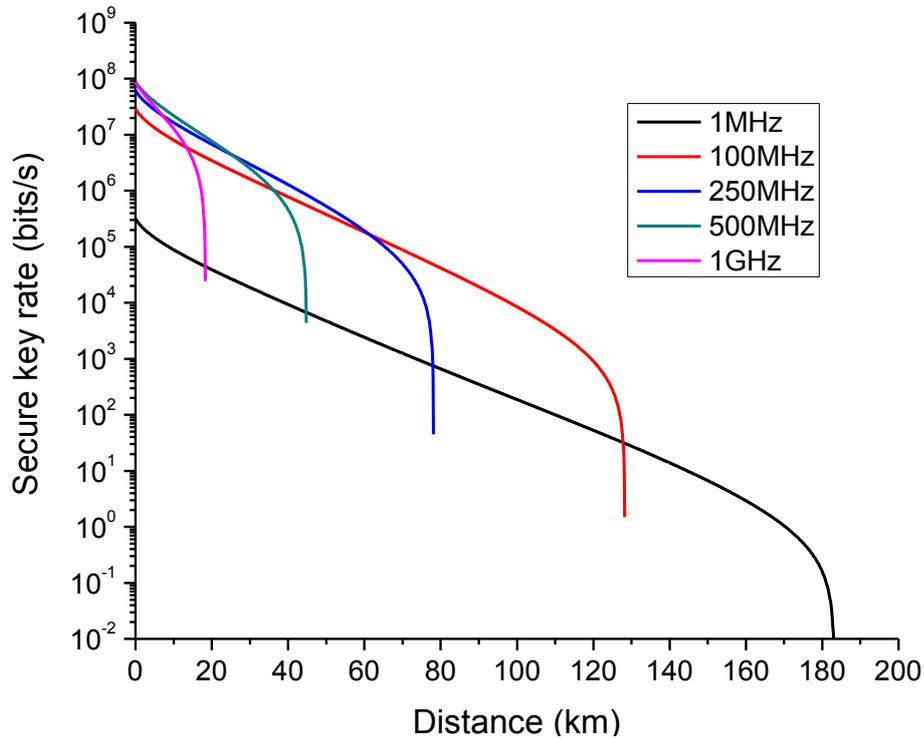


Figure 5.2 Secure key rate as a function of distance at clock rates of 1 MHz, 100 MHz, 250 MHz and 1 GHz in a TLO CVQKD system

Firstly, for a TLO CVQKD system, the excess noise can be estimated as 0.009 SNU, 0.018 SNU, 0.036 SNU, 0.074 SNU and 0.155 SNU for repetition rates of 1 MHz to 100 MHz, 250 MHz, 500MHz and 1 GHz, respectively, based on the above analysis. The secure bits in each pulse and the maximum transmission distance are reduced with increasing clock rate due to the reinforcement of excess noise and electronic noise. The maximum transmission distance decreases from 183 km to 128 km, 78 km, 45km and 18km when the repetition rate increases from 1 MHz to 100 MHz, 250 MHz, 500MHz and 1 GHz, respectively. However, as the repetition rate (ie. pulse rate) goes up, a higher secure key rate in bits/second can be achieved

over relative shorter transmission distances. The secure key rate per second with a 1 GHz repetition rate is highest with a distance below 10 km. At a transmission distance of 30 km, the secure key rates are calculated as 1.9×10^4 bits/s, 1.6×10^6 bits/s, 2.9×10^6 bits/s, 2.5×10^6 bits/s and *Null* for repetition rates of 1 MHz to 100 MHz, 250 MHz, 500MHz and 1 GHz, respectively. It can be predicted that, the secure key rate can be optimised with system repetition rate at certain transmission range. For example, in our simulations, within the transmission range between 40 km and 60 km, systems with a 250 MHz repetition rate are feasible and offer better performance. However, longer distance key transmission needs to be achieved by using a lower repetition rate.

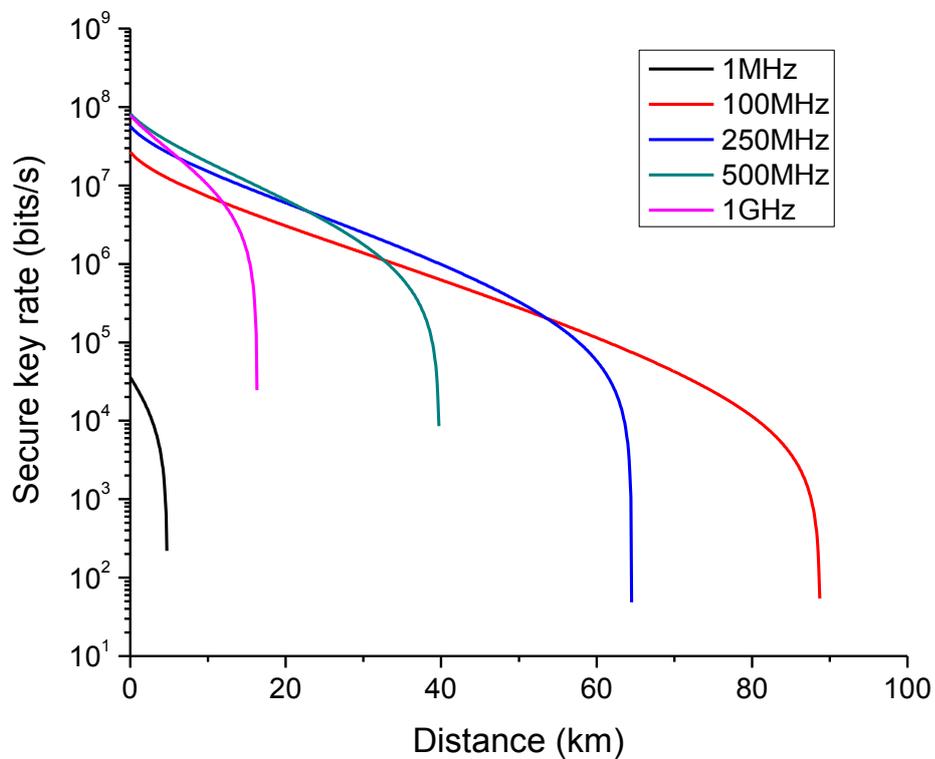


Figure 5.3 Secure key rate as a function of distance at clock rate of 1 MHz 100 MHz, 250 MHz and 1 GHz in a CVQKD system with an LLO scheme

The secure key rates for a LLO CVQKD system is plotted in Figure 5.3. the excess noise can be estimated as 0.249 SNU, 0.030 SNU 0.047 SNU, 0.085 SNU and 0.165 SNU for repetition rates of 1 MHz to 100 MHz, 250 MHz, 500MHz and 1 GHz, respectively, based on the above noise analysis. Firstly, the effect of phase noise in the LLO case results in a lower transmission distance compared with the TLO scheme. The lower speed repetition rate is thus not practical for LLO schemes, due to the challenge of minimizing phase noise between the two independent

lasers. Thus, as predicted in our simulations, the 1 MHz repetition rate has the worst performance among these cases.

As the repetition rate increases from 1 MHz to 100 MHz in our simulation, the phase noise decreases, and hence better performance can be achieved for a given laser linewidth, $\Delta\nu$. When the clock rate is further increased, the phase noise decreases and becomes less dominant in the total excess noise, and then the excess noise due to the modulation error starts to degrade the system performance. In turn, the maximum distance decreases with an increased repetition rate. Although the maximum key rate is boosted by the repetition rate, the transmission distance becomes limited at higher speeds. The maximum transmission distances are calculated as 89 km, 65 km, 40 km and 16 km for repetition rates of 100 MHz, 250 MHz, 500 MHz and 1 GHz, respectively. Similar to TLO schemes, the repetition rate needs to be carefully selected for the required transmission range. Our simulation predicts that 250 MHz is feasible for the range of a metro network area.

5.3 Experimental demonstration of a GHz CVQKD detector

In this section, we experimentally demonstrate a GHz BHD system for CVQKD systems, built from modified commercial components. We experimentally test the performance of the BHD using the setup shown in Figure 5.4. A CW laser source operating at a wavelength of 1550 nm is externally modulated by a 10 GHz amplitude modulator driven by an electrical signal to generate 0.4 ns width optical pulses at a repetition rate of 250 MHz. A variable attenuator is used to control the LO power launched into the balanced detector, and the power is monitored by a power meter together with a 99/1 beam splitter. The LO is then coupled into two reverse biased InGaAs PIN detectors. The tuneable optical delay is realized by a fibre stretcher, which is installed in one of the paths to ensure the same arrival time from two arms. A variable attenuator is used to guarantee balance between the same intensity being incident on each detector, and a CMRR of 51 dB is obtained. The differential output current from the photodiodes is then amplified by a modified commercial 1 GHz bandwidth transimpedance amplifier. The data acquisition is done in real-time via a 20 GS/s oscilloscope. As mentioned above, the voltage fluctuations on the power supply enhanced the electronic noise of TIA. This effect can be practically expressed as Power Supply Rejection Ratio (PSRR) ratings which are normally published by manufacturers for their circuits. To reduce the PSRR of our TIA and hence minimise the electronic noise in our BHD system, we powered the TIA by a 12 V battery instead of AC power. The reduction in electronics noise is measured to be about 2 dB. The

linearity of BHD is investigated by shot noise measurement at different LO powers. The variance of the electronic noise is determined by setting the power of the LO to 0 mW.

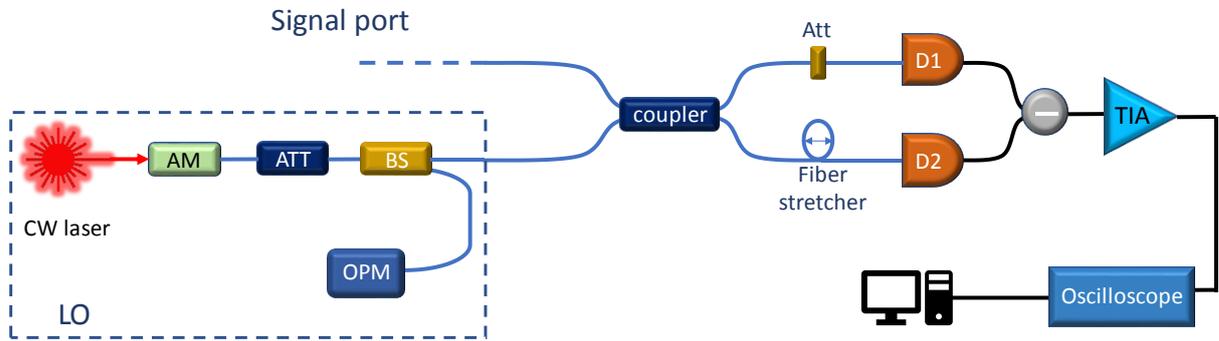


Figure 5.4 Balanced Homodyne detector experimental setup. AM: amplitude modulator; ATT: variable optical attenuator; BS: 99/1 beam splitter; D1 and D2: PIN detectors; TIA: Transimpedance amplifier. OPM: Optical power meter.

To meet the Gaussian linearity model for the GMCS protocol, the linearity of the built BHD has been tested via measuring the output noise variance with increasing LO from 0 to 1×10^7 photons per pulse. The measurements are shown in Figure 5.5. The total output variance is a sum of the shot noise variance and electronic variance. When the LO power is set lower than about 1.5×10^6 photons per pulse, the output variance is dominated by the electronic noise, as shown in the black dotted line. The electronic noise in the system is about 0.0004 mV^2 and is not changed by the LO power. As the power of LO increased to about 3×10^6 photons per pulse, the output variance from BHD started to be dominated by the shot noise. As shown in the plot, the region between 4×10^6 to 1×10^7 could be feasible for detecting CVQKD signals using the GMCS protocol, which requires a linear relationship between input and output of the detector. The shot noise to electronic noise ratio can be obtained as about 9.5 dB, 13.9 dB, 16.8 dB, and 18.6dB, which correspond to electronic noise values $N_{ele} = 0.11, 0.04, 0.02, \text{ and } 0.01 \text{ SNU}$, at $4.4 \times 10^6, 6.2 \times 10^6, 8.1 \times 10^6, \text{ at } 1.0 \times 10^7$ photons per pulse, respectively.

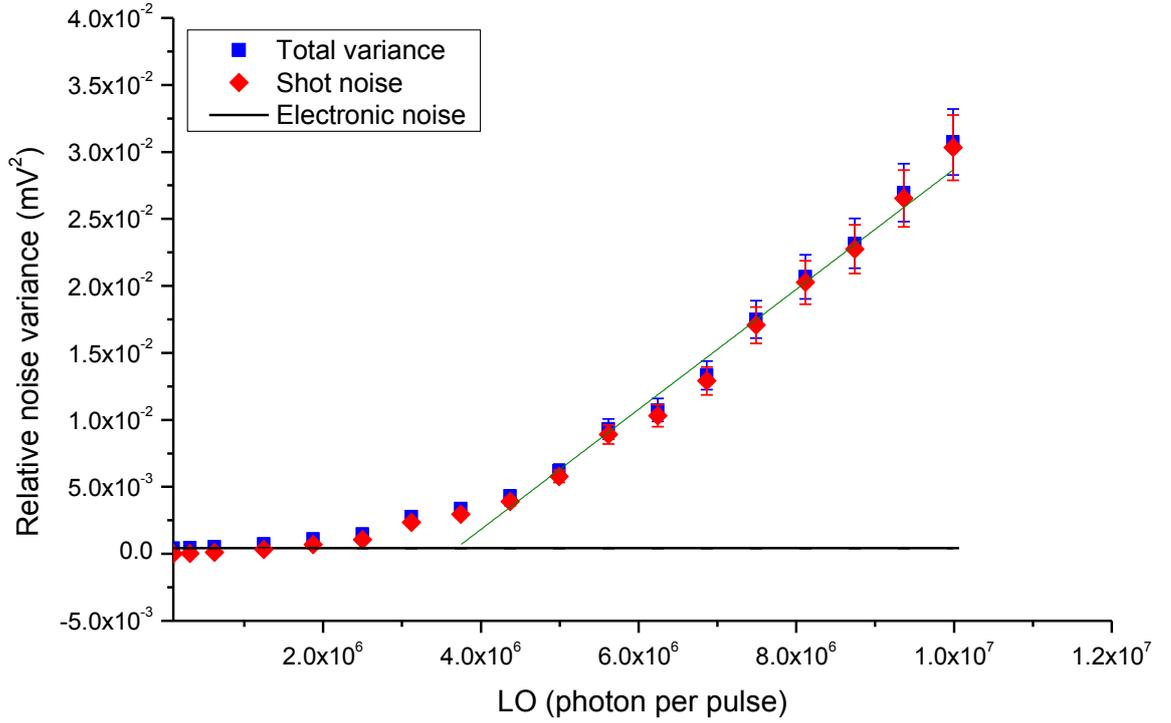


Figure 5.5 Output variance measurement as a function of LO power. The green line shows the region where the output variance is approximately linearly proportional to LO power.

5.4 Feasibility of optically Switched CVQKD systems

The secure key analysis model for a GMCS CVQKD system was introduced in Chapter 2. The model needs to be modified for a multi user CVQKD system by introducing optical switches with additional loss and crosstalk. Thus, the transmission T and excess noise ξ used in Eq. (2.32)–(2.34) need to be modified as (in SNU):

$$\frac{1}{T_{new}} = \frac{1}{T} + \frac{1}{T_s} \quad (5.10)$$

$$\xi_{new} = \xi + \xi_s \quad (5.11)$$

where $1/T_s$ is the insertion loss of the optical switch, and ξ_s is the additional excess noise due to the crosstalk effect. However, unlike the SPD in DVQKD systems, only the portion of crosstalk photons which are in the same spatiotemporal and polarisation mode as the LO

contributes to excess noise in the desired path [146]. The excess noise ξ_s caused by noise photons in the matched mode can be expressed as [47]:

$$\xi_s = \frac{2\langle N \rangle}{\eta_B T} \quad (5.12)$$

where $\langle N \rangle$ is the average number of noise photons in the matched mode with LO. In our case, this is the noise photons from the crosstalk from other paths. Due to the independent free running laser sources used in different Alices, the crosstalk in an optically switched CVQKD system would not be significant and so can be neglected.

A basic optically switched GMCS TLO CVQKD system has been experimentally conducted. The experimental setup and the equivalent schematic diagram of the optically switched system are shown in Figure 5.6. In Alice, the pulse trains with a repetition of 250 MHz from a directly modulated laser are split to signal pulses and stronger LO pulses by a 90/10 beam splitter. The pulse width is set to about 400 ps. The x and p quadratures of the signal pulses are modulated by an amplitude modulator and a phase modulator, using the modulating signal from arbitrary waveform generators (AWGs). Specifically, two set of random numbers as quadrature values following the Gaussian distribution are generated by the software in advance, and the corresponding voltage values for amplitude and phase modulations are then prestored in the AWG and used upon request. A 99/1 beam splitter is used for monitoring the signal power output from Alice, and a variable optical attenuator is used to adjust the signal variance to the desired level with respect to the shot noise. The time delay between the signal and LO is adjusted by a delay line, in cooperation with a Faraday mirror and a polarisation beam splitter. Thus, the LO pulses and signal pulses are then multiplexed in both time and polarisation at the polarisation beam splitter and sent out from Alice.

The pulses from Alice are sent to Bob via a 1x2 Optic-Mechanical switch, which had a crosstalk of -75 dB and loss of 1 dB. Due to resource constraints, different Bobs are virtualised using one detection system by using an optical combiner at the outputs of the optical switch. A different attenuation is applied to the two paths using optical attenuator to simulate different transmission distances. The total transmission losses of the two paths are about 4 dB and 7.5 dB.

At Bob, a dynamic polarisation controller is used to compensate for the polarisation drift during transmission. The LO pulses and signal pulses are then demultiplexed from the polarisation beam splitter into different optical paths. A phase modulator in the LO path is used so that Bob

could randomly choose to measure either the x or p quadrature of each pulse. The polarisation and arrival time of the LO pulses are adjusted to match the signal pulses before being input to the BHD, using another delay line with a Faraday mirror and polarisation beam splitter. The 1 GHz BHD demonstrated in Section 5.3 is used to detect the quadrature values, which are captured by a software controlled oscilloscope.

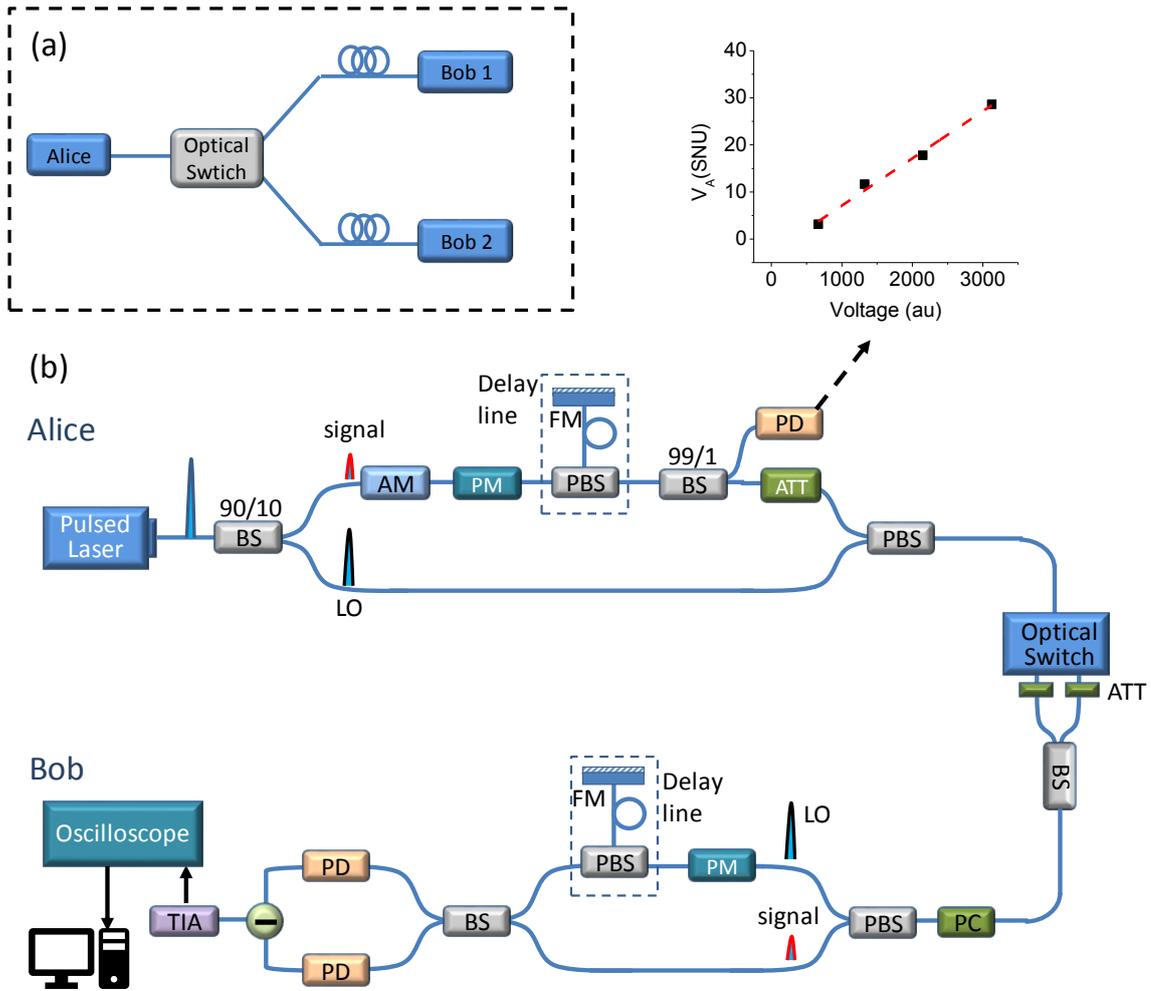


Figure 5.6 (a) Equivalent schematic diagram of the optically switched system. (b) Experimental setup for the reconfigurable CVQKD systems. All the fibre optic components within Alice and Bob are pigtailed with polarisation mentioning (PM) single mode fibres. PD: photodiode; PBS: Polarisation beamsplitter; TIA: Transimpedance Amplifier; AM: amplitude modulator; PM: Phase modulator; ATT: optical attenuator; PC: polarisation controller. FM: Faraday mirror. The inset shows the Calibration of V_A . (V_A values are fitted as a linear relation with the monitored voltage on an oscilloscope)

Before signal transmission via a quantum channel, a calibration of V_A needs to be conducted via a direct connection between Bob and Alice, in order to practically determine the modulation variance V_A of the sending quantum signals at the output of Alice. Specifically, Alice sends the modulated signal with different variance to Bob, who then measures the corresponding variance using the BHD. The optical signal pulse train is monitored by the photodiode in Alice before the signal is highly attenuated by the optical attenuator, which is able to be read on an oscilloscope as electrical pulses. Four different pairs of V_A and the average pulse amplitude monitored on the oscilloscope are obtained, as shown in Figure 5.6(b). Thus, the value of variance V_A can be determined at Alice and will then be announced to Bob for parameter estimation after the signal transmission.

Next, as discussed in the previous section, while the transmission, a number of states are needed to be used for shot noise variance calibration and parameter estimation. In addition, pilot pulses with higher intensity are periodically sent along signal states from Alice to Bob for compensating relative phase drift between the signal and LO paths due to temperature and other environmental fluctuations. Therefore, the signal from Alice is sent in packets with a pattern illustrated in Figure 5.7. Each signal packet contains 400 laser pulses, out of which 36 pulses are used as pilot pulses and the rest are equally divided into two sections for the shot noise calibration and parameter estimation, respectively. Please note that in a complete CVQKD system, the packet should be equally divided into three sections instead of two, as one is used for the key generation. However, in this proof of principle demonstration, the post processing and the final key generation are not included.

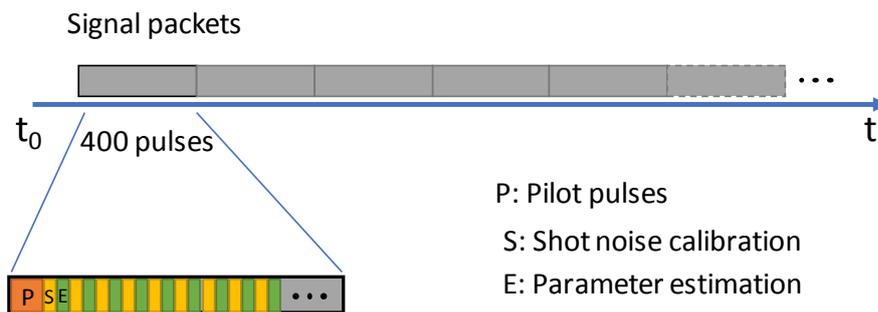


Figure 5.7 Illustration of the transmission pattern of signal packets

The pilot pulses in each signal packet are initially set to have three different phase rotations at the output of Alice (0° , 120° , and 240°), as shown in Figure 5.8. When they arrive at Bob, the phase is drifted and rotated by an arbitrary angle of θ_d with respect to the phase of the LO pulses.

Bob then estimates this angle using the measurement of the average X quadrature of those three sets of pilot pulses, namely X_1 , X_2 , and X_3 :

$$\theta_d = -\tan^{-1} \left[\frac{X_3 - X_2}{\sqrt{3}(2X_1 - X_2 - X_3)} \right] \quad (5.13)$$

Bob announces this angle to Alice, who will then accordingly offset and correct the phase of the transmitted data within this signal packet. Thus, the parameter estimation as well as the potential key generation will be in the same phase reference frame between Alice and Bob.

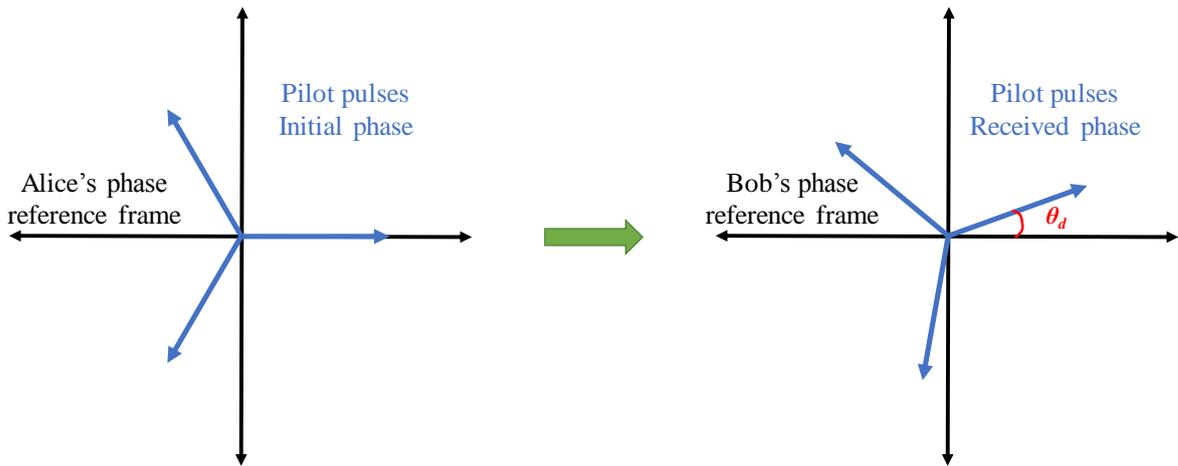


Figure 5.8 Illustration of phase drift in pilot pulses

In this experiment, the measurement of θ_d is shown in Figure 5.9. The discontinuity of the plot is caused by the reading from the oscilloscope. Owing to the lack of a continuous data acquisition system, the measurement is conducted via block by block data transfer from an oscilloscope to a PC. Each point on the plot corresponds to a phase estimation from the 36 pilot pulses, and therefore be used to correct the phase of the rest of the signal pulses (364 pulses) within the same packet. The plot shows that the measured θ_d randomly varies between 0 to 360 degrees. The estimated angles are then used for correcting the phase of Alice's sending states. The data points are an exponential moving average in order to increase the precise in estimation of θ_d .

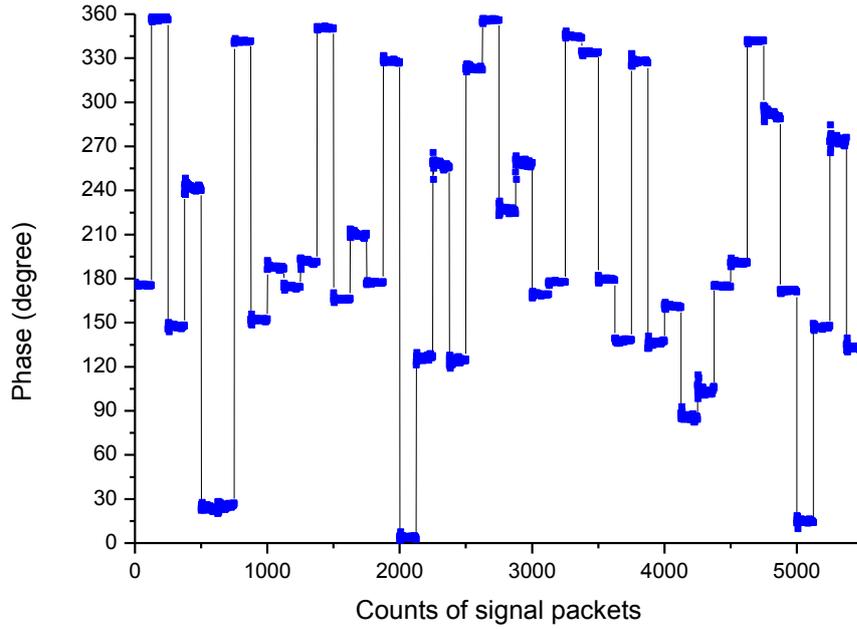


Figure 5.9 Experimental measurements on the phase drift within each signal packet

The system parameters are then estimated from successive sections in the signal packets using **Eq. (2.26)–(2.29)** in Chapter 2. V_A is calibrated to be around 3.5 in our experiment. In this demonstration of the feasibility of an optically switched system, the x quadrature of the receiving signal states is always measured. Estimations for the two optical paths of the optical switch are summarized in Table 5.1. The sampled data is transferred block by block from an oscilloscope to a PC, which limits the overall data acquisition speed. Each of the values in the table is evaluated from around 5×10^7 sampling points takes more than 40 mins. To estimate the secure key rate of this setup, the electronic noise is measured to be about 0.1 SNU and the reconciliation efficiency is assumed to be a typical value of 95%.

Table 5.1 Parameters and secure key estimations

	T	ξ	I_{AB}	χ_{BE}	Estimated Secure key rate
Path 1	0.06	0.08	0.07	0.06	1.0×10^5 bits/s
Path 2	0.16	0.06	0.16	0.14	1.2×10^6 bits/s

In this experiment, the signal transmission and parameter estimation can be immediately re-established when changing the switching state of the optical switch. Taking the channel transmission estimation as an example, Figure 5.10 shows continuous measurements at the transition of paths. Each point on this plot corresponds to the evaluation of a data block with

1×10^5 sampling points, which takes about 8 seconds. Although each individual point cannot be used for key estimation due to the statistical fluctuation, this plot illustrates the continuous signal transmission during optical switching.

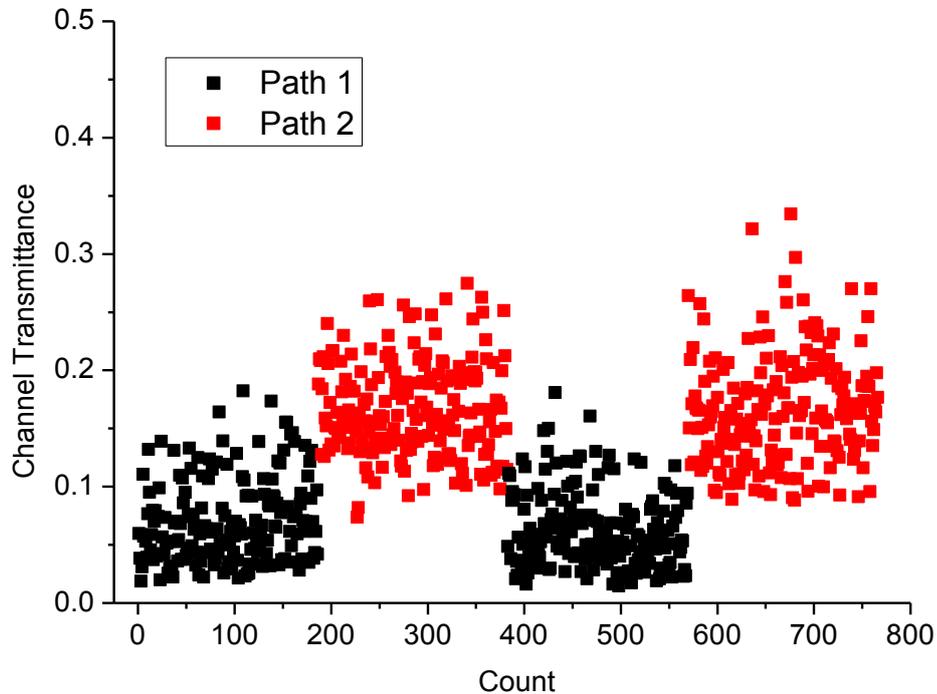


Figure 5.10 Continuous estimations on channel transmission with optical switching

Please note that the above experiment is not a complete CVQKD system but based on the optical layer setup in a lab condition. The devices in Alice and Bob are synchronized electrically. The postprocessing procedures for key distillation are not included, and the key rates are estimated based on the common security analysis introduced in Chapter 2. In addition, owing to the constraints of the lack of real-time feedback control, the above setup is not automatically operated with respect to mitigating the polarisation drift and temperature changes. The calibration is not dynamically adjusted in real-time while operating, which may have affected the estimation accuracy. Although we have demonstrated feasibility of the CVQKD transmission via an optical switch, addressing the above points would be an important part of the future work and more precise estimation could thus be obtained for a complete CVQKD system.

5.5 Equalization in CVQKD detection

In all the studies so far, bandwidth limitations in the detector have not been posed as an issue, as the case of insufficient bandwidth was not considered. In general cases, high bandwidth photodiodes require lower capacitance and hence a reduced active area, thus lowering their saturation power which in turn limits the power of LO in CVQKD system with either TLO or LLO schemes. In addition, BHD with a lower bandwidth normally offers lower electronic noise. Thus, it is more practical and cost-effective to design and use a lower bandwidth detector at higher rates.

However, as mentioned in Section 5.2, if a lower bandwidth detector is used at higher rates, then impaired performance may arise from enhanced noise and distortion due to the overlapping detected electrical pulses. This was first reported in a CVQKD experimental demonstration in [141]. Such an effect is similar to Inter-symbol interference (ISI) in conventional telecommunications, in which the spreading of the pulses due to a bandlimited receiver results in interference between neighbouring symbols.

In conventional telecommunications, equalization, either at the transmitter or receiver, can be used to mitigate ISI [147]. In this section therefore, after briefly introducing the principle of equalization, we propose the use of an equalizer for GMCS CVQKD detection to compensate for overlapping distortion. We have investigated the improvement in the quality of detected quadrature values of the quantum signal by the application of an equalization method. This in turn allows the use of lower bandwidth BHD for a higher repetition rate.

5.5.1 Equalization Principle

Feed Forward Equalization (FFE) is often used in communications. It uses an algorithm that reduces inter-symbol distortion using weighted linear combinations of delayed versions of the received signal. This enables one to overcome impairments caused by variations in the frequency and phase response of the system. This principle is illustrated in Figure 5.11. The received signal, $x(t)$, which is distorted by the effect of ISI, is input to an FFE with N steps of delay with a constant tap delay T_{FFE} . At the n th step, the magnitude of the delayed signal is weighted with a factor, a_n , known as the tap weight. Thus, the equalized output, $y(t)$, is the superposition of the weighted delayed versions of the received signal. The mathematical model of an FFE can be expressed as [147]:

$$Y(t) = \sum_{n=0}^{N_{FFE}} a_n \times x(t - n \times T_{FFE}) \quad (5.14)$$

The tap values need to be optimised to give the corrected values of $Y(t)$ at a point of interest by correlation with the original value at the transmitter. Optimisation is normally achieved using a training process, which commonly employs the steepest decent approach with the minimised mean square error (MSE) with k th steps, for which the algorithm can be written as [147]:

$$A(k) = A(k - 1) + \mu(X_{ref} - XA(k - 1))X^T \quad (5.15)$$

where $A=[a_0, a_1, a_2, \dots, a_n]$, μ is the rate of convergence to the optimal solution, and X_{ref} is the training sequence.

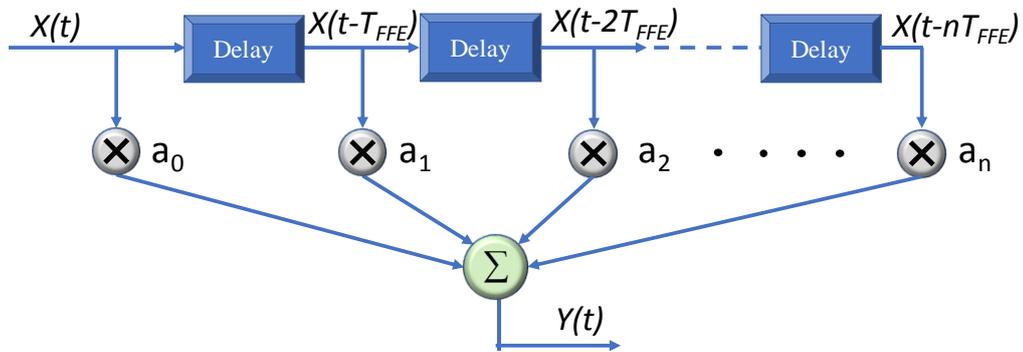


Figure 5.11 Illustration of the method of FFE. a_n is the n th tap and T_{FFE} is the delay between adjacent taps.

The equalization process overcomes impairments in the transfer function of the channel by effectively inverting this transfer function after detection. This process also enhances any electronic noise introduced by the receiver, as illustrated using the frequency response plot of the equalization process (Figure 5.12).

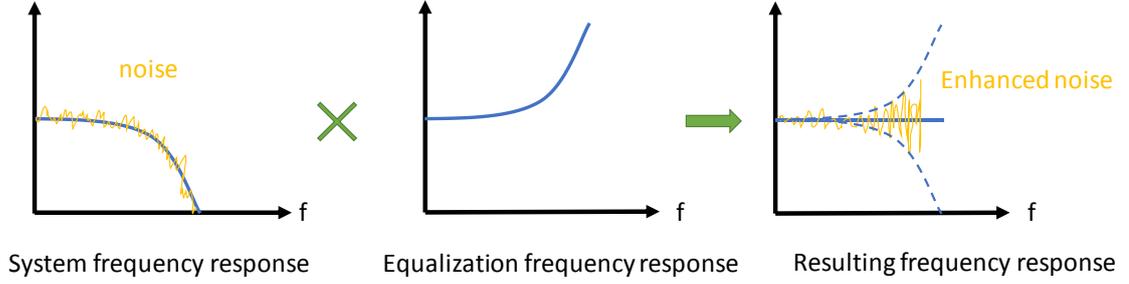


Figure 5.12 Frequency response resulted from system and equalization, illustrating the electronic noise enhancement.

5.5.2 CVQKD detection with Equalization

The ISI occurs in the detection of higher rate CVQKD signals when using a lower bandwidth BHD. Due to the bandwidth limitations of the receiver, the high-rate laser pulses carrying the key information are distorted by the transfer function of the balanced homodyne detector. As a result, every detected electrical pulse is spread across adjacent pulses, which can result in additional distortion due to the overlapping detected electrical pulses. This causes an increase in ξ through a term ξ_{ISI} , due to ISI and hence reduces the secure key rate. With the aim of mitigating this noise term and hence increasing the secure key rate of a CVQKD system with a bandlimited balanced homodyne detector, we proposed to use equalization in the CVQKD detection system. The schematic of the analytical model is shown in Figure 5.13. When the quantum signal arrives at Bob, the Gaussian modulated optical signal is first detected by a balanced homodyne detector with a fixed bandwidth (BW). The amplitude and phase values are determined at the peak of each measured output from the detector. We have considered Gaussian-shaped pulses in [141] with $\tau=1/BW$ and used our analytical model to show the improvement in CVQKD detection by the use of equalization. CVQKD signal pulses with a variance V_a of $20 N_0$, are sent from Alice to Bob over a 20 km long fibre channel. Electronic noise in the balanced homodyne detector is assumed to be $0.01 N_0$. A 5-tap FFE is applied to the detected pulses. Prior to detection, a training process is conducted for the FFE using a training sequence of 10^3 reference pulses with 20 dB higher intensity to obtain the optimised tap values.

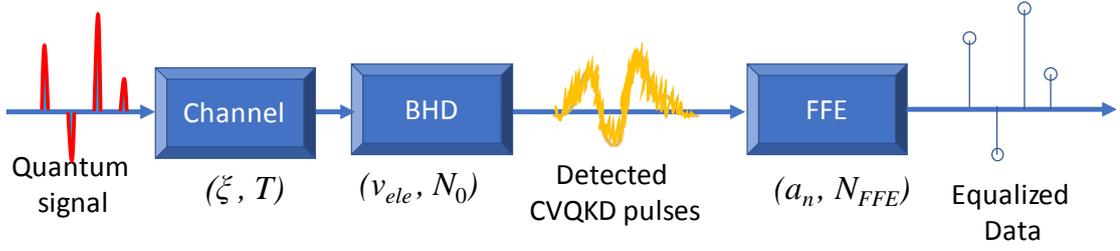


Figure 5.13 CVQKD detection system with equalization. The fibre channel is practically modelled as noise and loss, and the electronic noise N_{ele} is added into the detected signal. The downward pulse indicates a negative phase value.

The cross-correlation due to the ISI between the quadrature values is estimated at different repetition rate to bandwidth ratios, with and without equalization. Figure 5.14(a) shows that interference between adjacent pulses began to occur at a repetition rate about one-third of the bandwidth. At greater frequencies the introduction of equalization significantly reduced the cross-correlation. We estimated the ISI noise, ξ_{ISI} , as a function of the cross-correlation C :

$$\xi_{ISI} = \frac{2V_B C^2}{\eta_B T} \quad (5.16)$$

In Figure 5.14(b), ξ_{ISI} is plotted for varying repetition rates. For conventional CVQKD detection without equalization, ξ_{ISI} increased sharply at a repetition rate about one-third of the bandwidth which is hence the highest repetition rate bandwidth ratio (the minimum bandwidth of the BHD) that should be used in the link without the external excess noise ξ_{ISI} . It clearly shows that the use of equalization enables the lower bandwidth BHD to be used with same level of ξ_{ISI} , and that the bandwidth can be reduced from 3.3 times to twice the system repetition rate. For a CVQKD with a 250 MHz repetition rate, the minimum bandwidth of BHD required for $\xi_{ISI}=0$ can be reduced from 825 MHz to 500 MHz.

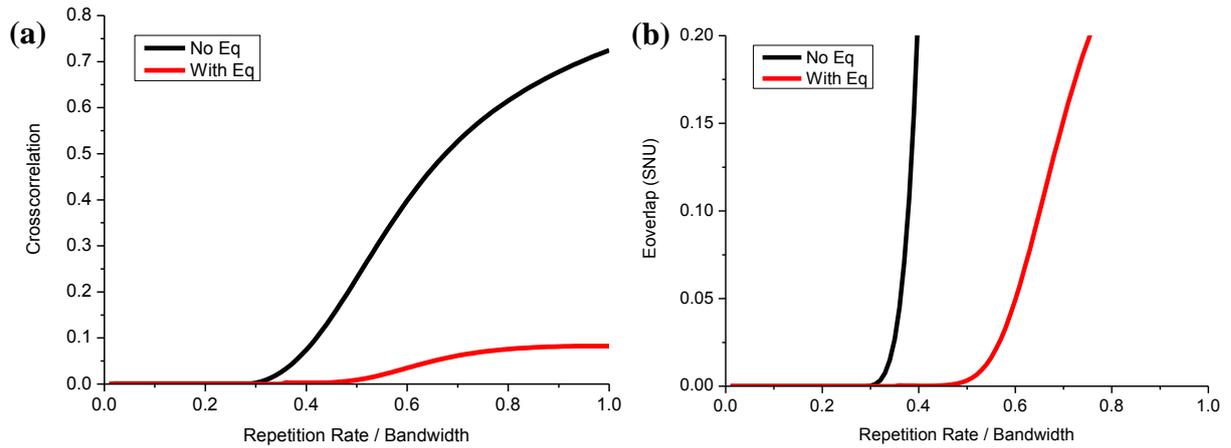


Figure 5.14 Simulated (a) cross-correlation and (b) ζ_{ISI} of the detected quadrature values with and without the application of equalization.

5.6 Summary

This chapter presents a theoretical model which analyses noise behaviours in a high bit rate CVQKD system. The repetition rate-dependent noise performance has been firstly investigated and discussed with corresponding secure key rates at different transmission distances for a GMCS CVQKD system with both TLO and LLO schemes. The repetition rates of 1 MHz to 100 MHz, 250 MHz 500MHz and 1 GHz are examined. A trade-off between the noise influence and system speed is shown for maximizing secure key generation at given transmission distances. Our noise analysis predicts that a CVQKD system with a repetition rate of 250 MHz can be feasible and provides a higher secure key rate for the range of a metro network area. A GHz BHD is then built using modified commercial components, and the feasibility of its application in a GMCS protocol is experimentally tested. The feasibility of an optically switched CVQKD system is experimentally demonstrated. The secure key rates are predicted to be 1.0×10^5 bits/s and 1.2×10^6 bits/s for the two paths with estimated transmittance of 0.06 and 0.16. A proposal of using equalization in a CVQKD detection system is presented. With FFE equalization, the mitigation of inter-symbol-interference noise caused by limits on the bandwidth of balanced homodyne detectors is investigated. For a fixed repetition rate, introducing equalization can reduce the bandwidth requirement by nearly half. We hope that this work will encourage research to explore the applications of classical communication tools in quantum communications.

Chapter 6 Conclusion and Future work

6.1 Conclusion

QKD has been shown to be a promising approach that can provide unconditionally secure communications in combination with classical encryption methods. Unlike conventional cryptography, where the security is based on computational and mathematical complexities, the security of QKD relies on the quantum physical properties of light. Since its first introduction in 1984, various QKD protocols have been proposed and demonstrated, which fit into two categories: DV and CV QKD. Experimentally, point to point DV and CV QKD links have been widely demonstrated over standard single mode fibres, and their performance in terms of transmission distance and secure key rate has been significantly improved.

The maturation of this technique has potentially enabled the use of QKD in today's metro and access telecommunication networks. Therefore, more research has been drawn to realizing QKD between multiple users. Optical switching has been shown to be a promising technique for establishing cost-effective reconfigurable QKD networks. This thesis has studied optically switched QKD in the context of its practical and highly reconfigurable use in the current metro network.

This thesis first reviewed practical point-to-point fibre-based QKD links with different protocols. Single photon techniques in DVQKD links were introduced in terms of generation and detection. Owing to the immaturity of truly single photon generators, single photons in a DVQKD link are practically generated using a highly attenuated laser. The accompanying problem of a PNS attack can be mitigated by introducing decoy states. The use of the APD in DVQKD detection was discussed, along with its main characteristics. The widely used implementation configurations were introduced for the representative DV protocols, BB84 (with and without decoy states) and COW. Secure key analysis was studied, based on which the distance-dependant secure key rates were calculated for these protocols. The review of CVQKD links began with the introduction of the detection technique: BHD, which is the most distinctive difference from a DV QKD link. Practically, the LO can be either transmitted from Alice or locally located in Bob. The practical implementation of CVQKD links using the GMCS protocol based on either the TLO or the LLO scheme was reviewed and discussed.

Similarly, secure key generation was analysed using the common mathematical model for a GMCS CVQKD link.

6.1.1 Feasibility and limitation of optically switched QKD

Among the different scenarios for establishing multi-user QKD systems, optically switched QKD shows the greatest potential for network integration since it is cost-efficient, and offers lower transmission loss and higher flexibility. After a detailed introduction to optical switching techniques, optically switched QKD was investigated in terms of its feasibility and issues.

A mathematical model describing a multiuser QKD system with optical switching elements was derived from the common secure key analysis for point to point QKD links. This model was then used to theoretically evaluate the performance of a multiuser QKD system with optical switching elements. The degradation of secure key generation due to the loss and crosstalk introduced by the optical switching element was comprehensively investigated using this model. In addition, this model was verified with a series of proof-of-concept experiments. The QKD performance in term of QBER was estimated for a basic QKD setup with different level of loss and crosstalk an optical switching element would introduce.

The work presented in Chapter 3 is essential to building reconfigurable optically switched multiuser QKD systems. Both theoretical estimation and experimental results indicate that the loss must be carefully minimised and the crosstalk needs to be kept below about -20 dB when designing or selecting optical switch elements for a practical optically switched QKD system.

6.1.2 Reconfigurable Quantum-safe metro network

A novel quantum-safe network solution was addressed in Chapter 4, in which the reconfigurable QKD is smoothly and cost-effectively integrated into existing metro telecommunication networks to protect classical data traffic. Quantum signals are transmitted with classical data along the same fibre between network nodes. The effective encryption topologies based on PTP and ETE were presented. The network solution also considered the system reconfiguration time, which is the time required to produce secure key material when setting up a new connection. It was thoroughly discussed as it limits the reconfigurability and hence the overall secure key rate in the network. In the proposed network structure, the system reconfiguration time can be effectively reduced by broadcasting a master clock signal to all endpoints from a single source.

The feasibility of this network was experimentally examined with commercial QKD boxes and opto-mechanical switches. Classical data and control signals in the C-band are wavelength-multiplexed with 1310 nm quantum signal and transmitted along the same fibre between different network nodes. The secure keys were continuously distributed between the common Bob with four virtual Alices, via different channel attenuations corresponding to transmission distances of 30 km, 31.7 km, 33.1 km, and 44.6 km. The QBER measurements for the four paths were 2.6%, 3.2%, 3.6% and 4.1%, with secure key rates of around 1.8×10^3 , 1.6×10^3 , 1.3×10^3 , and 0.7×10^3 bits/s obtained, respectively. The continuous measurements were conducted in the proof-of-concept experiments with software-enabled virtual Alices, and a maximum reconfiguration time of 20 s can be predicted for physically distinct Alices in the proposed quantum safe metro network. This improves the network reconfigurability and hence result in an increased overall secure key rate between multiple QKD users.

6.1.3 Towards a reconfigurable CVQKD network

CVQKD is a relatively younger technique but has been shown as a promising alternative to DVQKD. Although it has not been commercialized and not been demonstrated with optically switched configurations, the advantages of point to point CVQKD using the widely used and studied GMCS protocol have been shown such as its tolerance in noisy environments, compatibility with classical communication elements, and relative low cost. With the aim of supporting a reconfigurable CVQKD system in our proposed network, the following main works were conducted in Chapter 5 of this thesis.

Firstly, CVQKD systems suffer from a lower raw data rate. In order to meet the demands of encrypted classical data traffic in a metro network, the feasibility and issues of high speed CVQKD in term of noise performance was investigated. The repetition rate-dependent noise performance was theoretically analysed for the first time. Based on this analysis, the noise behaviour as well as the corresponding secure key rate of CVQKD with both TLO and LLO schemes at higher repetition rates of 100 MHz, 250 MHz, 500 MHz, and 1 GHz were investigated. A trade-off between noise level and repetition rate was observed when optimising the secure key rate.

Secondly, a GHz BHD has been built and its feasibility in the GMCS CVQKD detection has been experimentally demonstrated. Following this, a proof of principle experiment of an optically switched CVQKD system with an opto-mechanical switch was conducted. With an

optical layer setup of GMCS CVQKD, the quantum signal transmission is routed between two virtualised Alice-Bob pairs. The secure key rates were estimated to be 1.0×10^5 bits/s and 1.2×10^6 bits/s for the two paths with estimated transmittance of 0.06 and 0.16.

Thirdly, a method of using equalization in the CVQKD detection was proposed, and the effective reduction of the ISI due to the bandwidth limitation of BHD was analytically investigated. FFE, which is the common equalization method used in conventional communication, was applied for the first time to improve the quality of CVQKD detection. As a result, BHD with lower bandwidth, which is more practical due to its better noise performance, higher saturation power, and lower cost, can be designed and used in high speed CVQKD detection. This work also aimed to encourage research to explore the applications of classical communication tools in quantum communications.

The work and achievement in this thesis will greatly support ongoing research into the practical application and integration of highly reconfigurable optically switched QKD in the present metro network.

6.2 Future work

There are several possible works that can be conducted in the future to take the field forward.

The feasibility of our proposal of a quantum-safe metro network solution with an optically switched QKD system has been experimentally demonstrated with a reduced reconfiguration time. A pair of commercialized DVQKD systems was in use. As an extension work, more QKD devices could be employed in the future and hence the practical implementation of our proposed structure with physically distinct Alice/Bob elements could be conducted. In addition, the proposed modification of the provided QKD system, including implementation of saving/reloading system parameters and the separation of the clock signal from the service channel, could be also carried out after discussion with the supplier.

The development of the routing mechanism could be another important aspect in the practical deployment of reconfigurable QKD in our network [148, 149]. The network path optimisation principle could be used to reduce the number of necessary QKD devices (Alices or Bobs) in the proposed network structure to further reduce the overall cost.

The 250 MHz CVQKD system experimentally demonstrated in this thesis is based on the conventional TLO design. Recently, LLO CVQKD has attracted much research interest due to its advantages, including enhanced security and mitigation of the power constraints on LO affected by channel attenuation [88]. Experimentally, LLO design is challenged by the difficulty of agreeing a common phase reference between the two individual lasers, which results in increased phase noise. Fortunately, this problem can be solved by increasing the system repetition rate, as illustrated in Chapter 5. The establishment of high-speed reconfigurable CVQKD with an LLO scheme to be tested within our proposed network could be one promising future work.

With regard to electronic noise suppression in the built BHD, electronic noise was reduced by 2 dB by replacing the AC power supply with a DC battery. Further improvements are likely to be obtained by the use of a cooling system. In a preliminary test, a dual radiator liquid CPU cooler together with several Peltiers was attached to the outer case of the TIA of a BHD, and a slight decrease in electronic noise was obtained. Further enhancements can be predicted when installing the cooler inside the device, close to the electronic amplifier components.

The CVQKD experiment presented in this thesis focused on the feasibility study for the optical switched system, which is built with a basic optical layer setup. Although it is beyond the scope

of this thesis, further improvements to the system could be conducted through post processing and key distillation. In addition, the use of automated real-time feedback control and a fast data acquisition system (using a high-speed DIO card instead of AWG and Oscilloscope) are likely to be future works to improve the practicability and stability of the system, which could be the next step towards to the practical deployment of reconfigurable CVQKD in our proposed network structure.

The research into using the equalization methods for CVQKD detection could be further investigated. This is an important research direction as it opens the gateway to exploring the applications of classical communication tools for quantum cryptography. In Chapter 5, the standard FFE equalization algorithm was employed in the recovery of overlapping CVQKD signals. Further improvements are likely to be obtained by using other algorithms. Unlike the FFE, which corrects the received signal based on the weighted sum of delayed points of the signal itself, Decision-Feedback Equalization (DFE) is an algorithm that recovers the current sampling value by eliminating the effect of ISI based on several previously correctly-decided sampling point values [147]. The FFE and DFE methods can be used together to mitigate both pre-cursor and post-cursor distortion in classical data communication. However, the logical decision circuit used in DFE's feedback loop cannot be applied to CVQKD signals, as the quantum signal is modulated with a Gaussian distribution instead of a finite set of levels. However, it may be feasible to develop a DFE-like algorithm with offline data processing in software, which is not limited by the number of decision levels. At a minimum, it would be expected that the DFE like algorithm would provide a performance comparable to the FFE algorithm. This is because the DFE section would simply replace the weighted sum of the received waveform with the weighted sum of an appropriately selected synthetic waveform. Such a development might provide further improvements of the quality of the recovered CVQKD signals, and further mitigate ISI noise occurring in the higher rate detection when using a lower bandwidth BHD.

References

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, pp. 145-195, 2002.
- [2] A. Slinko, "Cryptology," in *Algebra for Applications: Cryptography, Secret Sharing, Error-Correcting, Fingerprinting, Compression*, ed Cham: Springer International Publishing, 2015, pp. 37-71.
- [3] P. Jouguet, "Security and performance of continuous-variable quantum key distribution systems," PhD thesis, Télécom ParisTech, 2013.
- [4] A. Kerckhoffs, "la cryptographie militaire," *Journal des Sciences Militaires*, vol. IX, pp. 5-38, 1883.
- [5] B. Qi, L. Qian, and H.-K. Lo, "A brief introduction of quantum cryptography for engineers," *arXiv:1002.1237*, 2010.
- [6] G. S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295-301, 1926.
- [7] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.
- [8] W. Diffie and M. E. Hellman, "Privacy and authentication: An introduction to cryptography," *Proceedings of the IEEE*, vol. 67, pp. 397-427, 1979.
- [9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120-126, 1978.
- [10] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comput.*, vol. 26, pp. 1484-1509, 1997.
- [11] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134.
- [12] H.-K. Lo and Y. Zhao, "Quantum cryptography," in *Computational Complexity*, ed: Springer, 2012, pp. 2453-2477.
- [13] C. H. Bennet and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing," in *Proceedings of the IEEE international conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984.
- [14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301-1350, 2009.
- [15] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802, 1982.
- [16] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3-28, 1992.
- [17] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum cryptography," *Applied Physics B*, vol. 67, pp. 743-748, 1998.
- [18] K. A. Patel, "Multiplexing High Speed Quantum Key Distribution with Conventional Data on a Single Optical Fibre," PhD thesis, University of Cambridge, 2014.
- [19] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited Review Article: Single-photon sources and detectors," *Review of Scientific Instruments*, vol. 82, p. 071101, 2011.
- [20] A. Lohrmann, B. C. Johnson, J. C. McCallum, and S. Castelletto, "A review on single photon sources in silicon carbide," *Reports on progress in physics. Physical Society (Great Britain)*, vol. 80, p. 034502, 2017.
- [21] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," *Physical Review Letters*, vol. 85, pp. 1330-1333, 2000.

- [22] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters*, vol. 91, p. 057901, 2003.
- [23] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, p. 230504, 2005.
- [24] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, *et al.*, "Efficient decoy-state quantum key distribution with quantified security," *Optics Express*, vol. 21, pp. 24550-24565, 2013.
- [25] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, p. 194108, 2005.
- [26] X. Tang, A. Wonfor, R. Kumar, R. Penty, and I. White, "Quantum-safe Metro Network with Low-Latency Reconfigurable Quantum Key Distribution," *Journal of Lightwave Technology* vol. 36, pp. 5230-5236, 2018.
- [27] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical review letters*, vol. 85, pp. 441-444, 2000.
- [28] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology*, vol. 18, pp. 133-165, 2005.
- [29] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photonics*, vol. 9, p. 163, 2015.
- [30] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, p. 010303, 1999.
- [31] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Physical Review Letters*, vol. 88, p. 057902, 2002.
- [32] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," *Physical Review Letters*, vol. 93, p. 170504, 2004.
- [33] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," *Physical Review A*, vol. 79, p. 012307, 2009.
- [34] A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," *Physical Review Letters*, vol. 102, p. 180504, 2009.
- [35] D. Sych and G. Leuchs, "Coherent State Quantum Key Distribution with Multi Letter Phase-Shift Keying," *New Journal of Physics*, vol. 12, p. 053019, 2010.
- [36] F. Grosshans, "Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution," *Physical Review Letters*, vol. 94, p. 020504, 2005.
- [37] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of Continuous-Variable Quantum Key Distribution Against General Attacks," *Physical Review Letters*, vol. 110, p. 030502, 2013.
- [38] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, pp. 623-656, 1948.
- [39] K. Rupesh, Q. Hao, and A. Romain, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New Journal of Physics*, vol. 17, p. 043027, 2015.
- [40] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electronics Letters*, vol. 32, p. 1645, 1996.
- [41] E. Diamanti and A. Leverrier, "Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations," *Entropy*, vol. 17, 2015.
- [42] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM journal on Computing*, vol. 17, pp. 210-229, 1988.
- [43] X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, "Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution," *Physical Review A*, vol. 95, p. 022318, 2017.

- [44] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, *et al.*, "Room temperature single-photon detectors for high bit rate quantum key distribution," *Applied Physics Letters*, vol. 104, p. 021101, 2014.
- [45] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, pp. 378-381, 2013.
- [46] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Scientific Reports*, vol. 6, p. 19201, 2016.
- [47] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, *et al.*, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," *Optics Express*, vol. 23, pp. 17511-17519, 2015.
- [48] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," *Nature*, vol. 385, p. 47, 1997.
- [49] P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," *Journal of Lightwave Technology*, vol. 23, pp. 268-276, 2005.
- [50] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive Optical Network Approach to Gigahertz-Clocked Multiuser Quantum Key Distribution," *IEEE Journal of Quantum Electronics*, vol. 43, pp. 130-138, 2007.
- [51] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, p. 69, 2013.
- [52] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W. B. Tam, Y. Zhiliang, *et al.*, "Quantum secured Gigabit Passive Optical Networks," in *Optical Fiber Communications Conference and Exhibition (OFC)*, 2015, pp. 1-3.
- [53] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, *et al.*, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, p. 075001, 2009.
- [54] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express*, vol. 19, pp. 10387-10409, 2011.
- [55] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, p. 123001, 2011.
- [56] P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photonics Technology Letters*, vol. 15, pp. 1669-1671, 2003.
- [57] T. Honjo, K. Inoue, A. Sahara, E. Yamazaki, and H. Takahashi, "Quantum key distribution experiment through a PLC matrix switch," *Optics Communications*, vol. 263, pp. 120-123, 2006.
- [58] A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, Y. Nambu, and A. Tomita, "Recent Progress in Quantum Key Distribution Network Technologies," in *European Conference on Optical Communications*, 2006, pp. 1-3.
- [59] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network (Invited Paper)," in *Quantum Information and Computation III*, 2005.
- [60] L. Ma, A. Mink, H. Xu, O. Slattery, and X. Tang, "Experimental demonstration of an active quantum key distribution network with over gbps clock synchronization," *IEEE Communications Letters*, vol. 11, pp. 1019-1021, 2007.
- [61] T. E. Chapuran, P. Toliver, N. A. Peters, J. Jackel, M. S. Goodman, R. J. Runser, *et al.*, "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics*, vol. 11, p. 105001, 2009.
- [62] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, *et al.*, "Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources," *Journal of Lightwave Technology*, vol. 35, pp. 1357-1362, 2017.

- [63] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, pp. 27217-27225, 2010.
- [64] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," *Optics Letters*, vol. 41, pp. 3511-3514, 2016.
- [65] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, *et al.*, "A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing," *New Journal of Physics*, vol. 16, p. 013047, 2014.
- [66] C. Iris, J. Y. Robert, and D. T. Paul, "Quantum information to the home," *New Journal of Physics*, vol. 13, p. 063039, 2011.
- [67] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, *et al.*, "Multiplexed classical and quantum transmission for high bitrate quantum key distribution systems," in *2012 Conference on Lasers and Electro-Optics (CLEO)*, 2012, pp. 1-2.
- [68] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," *Optics Express*, vol. 23, pp. 10359-10373, 2015.
- [69] S. Aleksic, D. Winkler, F. Hipp, A. Poppe, G. Franzl, and B. Schrenk, "Towards a smooth integration of quantum key distribution in metro networks," in *2014 16th International Conference on Transparent Optical Networks (ICTON)*, 2014, pp. 1-4.
- [70] B. Qi, L. Qian, and H. K. Lo, "Quantum Encryption," in *Optical and Digital Image Processing: Fundamentals and Applications*, ed New York: Wiley-VCH, 2011, pp. 769-787.
- [71] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Unconditionally secure one-way quantum key distribution using decoy pulses," *Applied Physics Letters*, vol. 90, p. 011118, 2007.
- [72] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," *Applied Physics Letters*, vol. 91, p. 041114, 2007.
- [73] N. Namekata, S. Adachi, and S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," *Optics Express*, vol. 17, pp. 6275-6282, 2009.
- [74] T. F. d. Silva, G. B. Xavier, and J. P. v. d. Weid, "Real-Time Characterization of Gated-Mode Single-Photon Detectors," *IEEE Journal of Quantum Electronics*, vol. 47, pp. 1251-1256, 2011.
- [75] G. Humer, M. Peev, C. Schaeff, S. Ramelow, M. Stipčević, and R. Ursin, "A Simple and Robust Method for Estimating Afterpulsing in Single Photon Detectors," *Journal of Lightwave Technology*, vol. 33, pp. 3098-3107, 2015.
- [76] A. R. A. Gaya, D. C. Díaz-Aldagalán, V. G. Muñoz, A. M. García, W. A. A. Ocampo, J. G. R. Chicue, *et al.*, "Practical Quantum Key Distribution based on the BB84 protocol," *Waves*, vol. 1, pp. 4-14, 2011.
- [77] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, pp. 3121-3124, 1992.
- [78] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Unconditionally Secure One-Way Quantum Key Distribution Using Decoy States," in *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies*, Baltimore, Maryland, 2007, p. QML3.
- [79] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug and play' quantum key distribution," *Electronics Letters*, vol. 34, pp. 2116-2117, 1998.
- [80] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, *et al.*, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," *New Journal of Physics*, vol. 11, p. 075003, 2009.
- [81] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium on Information Theory, Proceedings.*, 2004, p. 136.

- [82] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," *Applied Physics Letters*, vol. 92, p. 201104, 2008.
- [83] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, p. 012326, 2005.
- [84] X. Ma, "Unconditional security at a low cost," *Physical Review A*, vol. 74, p. 052325, 2006.
- [85] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Optics Express*, vol. 16, pp. 18790-18797, 2008.
- [86] S. Kleis, R. Herschel, and C. G. Schaeffer, "Coherent receiver architectures for secure key distribution using faint optical multilevel signals," in *SPIE OPTO*, 2015, p. 7.
- [87] T. Gerrits, S. Glancy, and S. W. Nam, "A balanced homodyne detector and local oscillator shaping for measuring optical Schrödinger cat states," in *SPIE Defense, Security, and Sensing*, 2011, p. 7.
- [88] A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," *Physical Review A*, vol. 95, p. 012316, 2017.
- [89] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," *New Journal of Physics*, vol. 11, p. 045023, 2009.
- [90] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Physical Review A*, vol. 76, p. 052323, 2007.
- [91] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the Local Oscillator ``Locally'' in Continuous-Variable Quantum Key Distribution Based on Coherent Detection," *Physical Review X*, vol. 5, p. 041009, 2015.
- [92] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, *et al.*, "Self-Referenced Continuous-Variable Quantum Key Distribution Protocol," *Physical Review X*, vol. 5, p. 041010, 2015.
- [93] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Optics Letters*, vol. 40, pp. 3695-3698, 2015.
- [94] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Review A*, vol. 76, p. 042305, 2007.
- [95] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 42, p. 114014, 2009.
- [96] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0204127*, 2002.
- [97] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii*, vol. 9, pp. 3-11, 1973.
- [98] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, *et al.*, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation--The Theory of Practical Implementations," *arXiv preprint arXiv:1703.09278*, 2017.
- [99] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Applied Physics Letters*, vol. 112, p. 051108, 2018.
- [100] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, *et al.*, "Metropolitan Quantum Key Distribution with Silicon Photonics," *Physical Review X*, vol. 8, p. 021009, 2018.
- [101] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, *et al.*, "Continuous high speed coherent one-way quantum key distribution," *Optics Express*, vol. 17, pp. 13326-13334, 2009.

- [102] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, *et al.*, "High key rate continuous-variable quantum key distribution with a real local oscillator," *Optics Express*, vol. 26, pp. 2794-2806, 2018.
- [103] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, *et al.*, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *arXiv preprint arXiv:1712.10242*, 2017.
- [104] J. Bogdanski, N. Rafiei, and M. Bourennane, "Multiuser quantum key distribution over telecom fiber networks," *Optics Communications*, vol. 282, pp. 258-262, 2009.
- [105] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, *et al.*, "Using quantum key distribution for cryptographic purposes: A survey," *Theoretical Computer Science*, vol. 560, pp. 62-81, 2014.
- [106] C. Yang, H. Zhang, and J. Su, "The QKD network: model and routing scheme," *Journal of Modern Optics*, vol. 64, pp. 2350-2362, 2017.
- [107] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, *et al.*, "Demonstration of an active quantum key distribution network," in *Quantum Communications and Quantum Imaging IV*, 2006, p. 630506.
- [108] Q. Cheng, "Design and Experimental Characterisation of Scalable, Low-Energy Optical Switches," PhD Thesis, The University of Cambridge, 2014.
- [109] S. Bregni, G. Guerra, and A. Pattavina, "State of the art of optical switching technology for all-optical networks," *Communications World*, 2001.
- [110] R. Prasanth, J. E. M. Haverkort, and J. H. Wolter, "Compact polarization-independent Mach-Zehnder space switch combining carrier depletion and the quantum confined Stark effect," *IEEE Journal of Quantum Electronics*, vol. 39, pp. 379-383, 2003.
- [111] S. Nakamura, K. Tajima, and Y. Sugimoto, "Experimental investigation on high-speed switching characteristics of a novel symmetric Mach-Zehnder all-optical switch," *Applied Physics Letters*, vol. 65, pp. 283-285, 1994.
- [112] J. C. Campbell, F. A. Blum, D. W. Shaw, and K. L. Lawley, "GaAs electro-optic directional-coupler switch," *Applied Physics Letters*, vol. 27, pp. 202-205, 1975.
- [113] T. Shibata, M. Okuno, T. Goh, T. Watanabe, M. Yasu, M. Itoh, *et al.*, "Silica-based waveguide-type 16 x 16 optical switch module incorporating driving circuits," *IEEE Photonics Technology Letters*, vol. 15, pp. 1300-1302, 2003.
- [114] A. Densmore, S. Janz, R. Ma, J. H. Schmid, D.-X. Xu, A. Delâge, *et al.*, "Compact and low power thermo-optic switch using folded silicon waveguides," *Optics Express*, vol. 17, pp. 10457-10465, 2009.
- [115] A. M. Al-Hetar, A. B. Mohammad, A. S. M. Supa'at, and Z. A. Shamsan, "MMI-MZI Polymer Thermo-Optic Switch With a High Refractive Index Contrast," *Journal of Lightwave Technology*, vol. 29, pp. 171-178, 2011.
- [116] M. Haruna and J. Koyama, "Thermo-optic effect in LiNbO₃, for light deflection and switching," *Electronics Letters*, vol. 17, pp. 842-844, 1981.
- [117] G. I. Papadimitriou, C. Papazoglou, and A. S. Pomportsis, "Optical switching: switch fabrics, techniques, and architectures," *Journal of Lightwave Technology*, vol. 21, pp. 384-405, 2003.
- [118] D. A. Smith, R. S. Chakravarthy, Z. Bao, J. E. Baran, J. L. Jackel, A. d'Alessandro, *et al.*, "Evolution of the acousto-optic wavelength routing switch," *Journal of lightwave technology*, vol. 14, pp. 1005-1019, 1996.
- [119] A. Wonfor, H. Wang, R. Penty, and I. White, "Large Port Count High-Speed Optical Switch Fabric for Use Within Datacenters [Invited]," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 3, pp. A32-A39, 2011.
- [120] R. Spanke, "Architectures for guided-wave optical space switching systems," *IEEE Communications Magazine*, vol. 25, pp. 42-48, 1987.
- [121] R. Spanke, "Architectures for large nonblocking optical space switches," *IEEE Journal of Quantum Electronics*, vol. 22, pp. 964-967, 1986.

- [122] H.-Q. Ma, K.-J. Wei, J.-H. Yang, R.-X. Li, and W. Zhu, "A full quantum network scheme," *Chinese Physics B*, vol. 23, p. 100307, 2014.
- [123] M. Bahadori, S. Rumley, R. Polster, and K. Bergman, "Loss and crosstalk of scalable MZI-based switch topologies in silicon photonic platform," in *Photonics Conference (IPC)*, 2016, pp. 615-616.
- [124] D. E. Comer, *Internetworking with TCP/IP. Vol. 1, Principles, protocols, and architecture*, 5th ed.: Upper Saddle River, NJ; London : Pearson Prentice Hall, 2006.
- [125] Q. Cheng, A. Wonfor, R. V. Penty, and I. H. White, "Scalable, Low-Energy Hybrid Photonic Space Switch," *Journal of Lightwave Technology*, vol. 31, pp. 3077-3084, 2013.
- [126] J. Constantin, R. Houlmann, N. Preyss, N. Walenta, H. Zbinden, P. Junod, *et al.*, "An FPGA-Based 4 Mbps Secret Key Distillation Engine for Quantum Key Distribution Systems," *Journal of Signal Processing Systems*, vol. 86, pp. 1-15, 2017.
- [127] A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, *et al.*, "Quantum metropolitan optical network based on wavelength division multiplexing," *Optics Express*, vol. 22, pp. 1576-1593, 2014.
- [128] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, p. 063027, 2010.
- [129] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, *et al.*, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, p. 041010, 2012.
- [130] A. Poppe, S. Aleksic, and V. Martin, "Integration of Quantum Key Distribution in Metropolitan Area Networks," in *Research in Optical Sciences*, Messe Berlin, Berlin, 2014, p. QW4A.6.
- [131] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp, "Quantum key distribution over optical access networks," in *Proceedings of the 2013 18th European Conference on Network and Optical Communications & 2013 8th Conference on Optical Cabling and Infrastructure (NOC-OC&I)*, 2013, pp. 11-18.
- [132] R. J. Runser, T. Chapuran, P. Toliver, N. A. Peters, M. S. Goodman, J. T. Kosloski, *et al.*, "Progress toward quantum communications networks: opportunities and challenges," in *Integrated Optoelectronic Devices*, 2007, p. 15.
- [133] A. Poppe, B. Schrenk, V. Martin, and S. Aleksic, "QKD in Classic Optical Networks: Two Different Worlds Forever? (invited)," presented at the International Workshop on Quantum Communication Networks Leeds, UK, 2014.
- [134] C. V. Raman, "A new radiation," *Indian Journal of Physics*, vol. 2, p. 387, 1928.
- [135] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, pp. 188-190, 1997.
- [136] *ID Quantique Clavis3*. Available: <https://www.idquantique.com/single-photon-systems/products/clavis3-qkd-platform/> (accessed on 25/07/2018)
- [137] *ID Quantique Clavis3 brochure*. Available: <https://marketing.idquantique.com/acton/attachment/11868/f-0216/1/-/-/-/-/Clavis3%20QKD%20Platform%20%26D%20Brochure.pdf> (accessed on 25/07/2018)
- [138] "ID Quantique private communication."
- [139] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, *et al.*, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, pp. 621-669, 2012.
- [140] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, pp. 6072-6092, 2015.
- [141] C. Yue-Meng, Q. Bing, Z. Wen, Q. Li, L. Hoi-Kwong, Y. Sun-Hyun, *et al.*, "A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution," *New Journal of Physics*, vol. 13, p. 013003, 2011.
- [142] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Physical Review A*, vol. 90, p. 042329, 2014.

- [143] X. Tang, R. Kumar, D. Cunningham, A. Wonfor, R. V. Penty, and I. H. White, "Inter-Symbol-Interference Reduction in Continuous Variable QKD using Equalization," in *IEEE Global Communications Conference*, Abu Dhabi, UAE, 2018.
- [144] R. H. Walden, "Analog-to-digital converter survey and analysis," *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 539-550, 1999.
- [145] A. V. Masalov, A. Kuzhamuratov, and A. I. Lvovsky, "Noise spectra in balanced optical detectors based on transimpedance amplifiers," *Review of Scientific Instruments*, vol. 88, p. 113109, 2017.
- [146] Q. Bing, Z. Wen, Q. Li, and L. Hoi-Kwong, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, p. 103042, 2010.
- [147] T. Wong and T. Lok, "Theory of Digital Communications," ed. Online: <http://www.wireless.ece.ufl.edu/twong/Notes/Comm/ch4.pdf> (accessed on 10/08/2018).
- [148] Q. Han, L. Yu, W. Zheng, N. Cheng, and X. Niu, "A novel QKD network routing algorithm based on optical-path-switching," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, pp. 13-19, 2014.
- [149] C. Yang, H. Zhang, and J. Su, "Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying," *China Communications*, vol. 15, pp. 33-45, 2018.