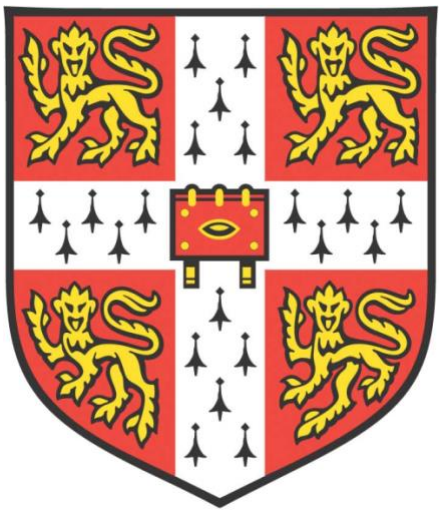
QKD and high-speed classical data hybrid metropolitan network



Han Qin

Hughes Hall

Department of Engineering

University of Cambridge

This dissertation is submitted for the degree of Doctor of Philosophy

May 2020

Declaration

This thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text. 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. It does not exceed the prescribed word limit for the relevant Degree Committee'.

The dissertation does not exceed the word limit requirement for Engineering Committee. It contains 39133 words and 87 figures.

HAN QIN

May 2020

QKD and high-speed classical data hybrid metropolitan network

Abstract

Quantum Key Distribution (QKD) is currently receiving much attention as it provides a secure source of encryption keys [1-3]. Discrete-Variable QKD (DV-QKD) is possible for single photon transmission in QKD to-coexist with and encode classical wavelength division multiplexed (WDM) data with appropriate system design. Nevertheless, previous QKD field trials adopted either or both of key relay via trusted nodes and transparent link via optical switching. The former requires guaranteed physical security of the relay nodes, but can expand key distribution distance arbitrarily [4]. The latter can realize key establishment for more users with less complexity of key management over an untrusted network. To realise the adaption of the QKD system for future high speed and long distance metropolitan world exploitation at lower cost, there has to be investigations on existing fibre infrastructures.

Prior to this work, previous researches over similar distances feature extremely low secure key rates. For example, the Swiss Quantum Network between three sites displayed secure bit rates of 2.5 kbps at a fibre length of 17km [5]. Quantum Key distribution within the 25km Cambridge Quantum Network have demonstrated the highest long-term secure key rates yet demonstrated in a field trial of at least 2.5Mb/s which is the fastest and much higher than 0.8 kbps which was reached over the similar channel loss field trial up to date [6]. Additional field trials have been performed on the UK Quantum Network using a 66km path having 16dB loss. Combined wavelength division multiplexed 2 x 100 Gb/s traffic encrypted using QKD co-existing on the same fibres has operated for several months, with a long-term key rate of 80kb/s that is also faster than any other similar long-term QKD trial systems [7, 8].

In addition to this advanced commercial QKD system, there have been secure key rate analysis comparisons between laboratory fibre coils and practical field trials more than field trials only conducted before [4] [6] [7] [9]. These comparisons help to identify factors that limit future QKD network scale in both quantity and quality aspects. Also, the limit for the highest secure key rate at longest fibre length QKD in the multiplexing environment is discussed and determined in this research thesis.

Nevertheless, in this thesis, improvements have been made to minimise the corresponding negative effects by investigations on the dependence of temperature have been done in order to ensure system operation environment effects. It was found from the trial results that there

exists a relationship between temperature and secure key rate [4] [6] and further study has been done to evaluate the system sensitivity to operating temperature. Although the conventional DV-QKD system, original BB84 coding scheme, was designed to exploit the quantum properties of single photon polarization states, the trial equipment operates based upon the phase coding schemes. These coding schemes are based on the properties of interferometers and the coding is implemented by changing the relative optical path lengths or phase between the internal arms of the interferometer, while in the real transmission environment, temperature or polarization variation happens unpredictably.

The existing polarisation controllers operate at relative low speed align within the interferometer, which slows to operation environment such as a punch to fibre causing phase difference. Therefore, in this project, there has been an improvement in the QKD-WDM system performance by adding an external polarization controller to minimize the Raman noise and increase the secure key rate at the longest fibre length up to date.

In Summary, transmitting quantum keys over a coil of fibre in the lab differs a lot from actually putting it in the ground. This work contrasts the world fastest QKD system at the longest distance in field trials with lab fibre reels and then characterises and identifies two of the key factors, temperature and polarizations, influencing performance in practical wavelength-multiplexed secure communication systems. This is a significant step towards the coexistence of the quantum and conventional data channels on the same fibre for metropolitan networks and paves a way for an information-secure communication infrastructure.

Acknowledgements

This research and thesis could not be finished without the help from numbers of people. I would like here to express my gratitude to a number of people, organisations and intuitions. In particular I would like to appreciate and thank,

Professor Richard Penty for giving me lots of help during my last year especially during Covid-19 lock down time; always giving feedback during my entire PhD period.

Professor Ian White for giving me the opportunity to study and research in the group of Centre for Photonic System, Electrical Division, University of Cambridge; for sparing no effort to guide me since my first year with my research, proof reading my publications and this thesis.

Adrian Wonfor for assisting me with laboratory set-ups, equipment purchasing, discussing series of questions along my research.

Dr Shuai Yang for his help in preparing for conducting experiment and safety checks.

Marco Lucamarini for his explanation for using and solving problems when using Toshiba QKD devices during this research.

Victoria Rose for sorting the administrative problems in CAPE.

Dr Carole Sargent for helping me to overcome a number of difficulties in college and universities lives.

Everyone in Hughes Hall for providing a friendly and helpful environment through the time in Cambridge.

Everyone in St Andrews the Great for their prayers for me and helping me when I feel stressful and depressed.

Everyone in the group of CPS for giving me advices not only in academic field but also in life during the four years at CAPE.

My landlord, Mr and Mrs Robinson, for their lovely house and environment when I was at my thesis writing up stage.

Yuxuan Chen for his help with my coding skills and encouragement when I was in a bad mood.

Gaomin Liu for her friendly company during the period in Cambridge so that I can have a good mood to face the academic and life pressures.

Shilei Chen for her company outside of the academic world, which helps me to live and study with a more positive attitude.

My Mom and Dad, who have been an inspiration for me, continuous psychological and financial support since my first year abroad help me to deal with and overcome numerous difficulties.

Publication List

A Wonfor, H Qin et al., *High performance field trials of QKD over a metropolitan network* ,**Qcrypt 2017**

A Wonfor, H Qin et al., *Field trial of a QKD and high-speed classical data hybrid metropolitan network* ,**SPIE Photonic West 2018**

H Qin, A Wonfor et al., *Raman scattering effect on a QKD and high speed classical data hybrid link* ,**SIOE 2019**

Table of Contents

List of figures

Chapter 1. Introduction

Cryptography is an art of keeping information secret, which has special historical significance. In more recent times, since the second world war, cryptography has become an indispensable feature of today's society [10]. Cryptography is a branch of a larger field called cryptology. The other branch of cryptology is cryptanalysis, which is associated with code breaking.

Cryptography is aimed at encoding and decoding information, in a way that cannot be understood by a third party [1]. Conventionally and traditionally, the sender is named as 'Alice', the receiver is named as 'Bob' and the third party trying to intercept their secret communication is commonly referred to as 'Eve'. As shown in Figure 1.1, Alice encodes her secret message (plaintext) using a cipher (algorithm) and a key to produce a message (cipher text) and sends it to Bob. Bob then decrypts the message using the cipher and the key to retrieve the secret information. The 'one-time-pad' (OTP) cipher is a known encoding method with provable security. It was first introduced by Gilbert Vernam in 1926 [11] and the security of this cipher was proved by Claude Shannon in 1949 [12]. OTP is a symmetric cipher and the key is as long as the information to be sent. Information is secure provided that the key material is never reused. With a provably secure cipher, the problem of secure communication is reduced to how to distribute secret keys.

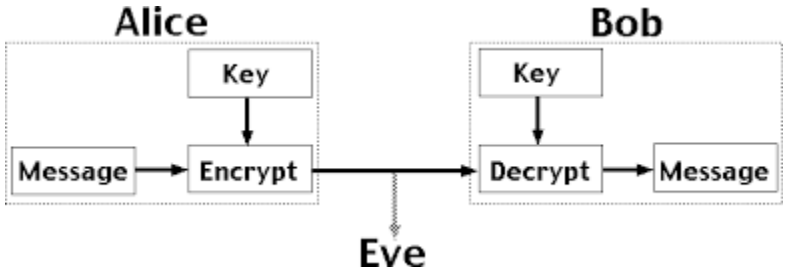


Figure 1.1 Encryption process

In general, the principle of a conventional network is to communicate between users by replicating data and then transmitting the resultant copy, however, the quantum mechanics differs from these rules significantly, as it prevents directly creating any corresponding unknown, arbitrary and independent copies of quantum states. Whereas in classical communications where valuable data can be unknowingly intercepted, fragile quantum data can only be unique unless the network can use teleportation or perform teleportation-derived techniques [13]. In a word, quantum communication is to exchange the quantum states over

links, typically using optical fibre and it cannot be easily realized without the support of substantial conventional communication.

1.1 Overview of Cryptography

1.1.1 Classical Cryptography

In classical cryptography, there are two main methods of distributing cryptographic keys. One is a trusted messager, and the other one is a public key encryption systems [14]. It is unrealistic for couriers to hand out keys because it depends on the delivery logistics and their efficiency. Although control measures can be taken, there is no absolute way to know if critical material has been tampered with [15].

In public key cryptographic systems, keys used for encoding and decoding are different. In such systems Bob chooses a private (decoding) key, from which he derives, through calculation the corresponding public (encoding) key which is announced publicly [16, 17]. Anyone interested in communication with Bob, for instance Alice, encodes her information using this public key and only Bob is able to retrieve this secret information since he possesses the private key for decoding. Anyone else not possessing the private key has to face a complex calculation to decrypt the information. The security of such algorithms is then based on calculating some complex, one-way mathematical functions. In public key cryptography, the encryption key is public, unlike the secret decryption key. The users create and publish a public key based on two large prime Numbers and a secondary value. Primes are secret. Anyone can encrypt a message through the public key, but it can only be decoded by someone who knows the prime number. This is the case for the RSA algorithm [1, 10, 18], introduced by Ronald Rivest, Adi Shamir and Leonard Adleman in 1977, whose security is based on factoring large integer numbers.

However, these algorithms have not been proven secure and any development in algorithms to factor large numbers may hold serious implications for security. Fast factorisation has already been shown to be possible with a quantum computer [19] and major efforts are continuing to be made in this field. So, either an overnight mathematical discovery or a breakthrough in quantum computers would impose a serious threat on information security.

Symmetric cipher cryptographic systems widely used by society at large are the Data Encryption Standard (DES) [20] and the Advanced Encryption Standard (AES) [21]. The

length of the key is of the order of a few hundred bits. Again, this key is encrypted with the plaintext in a mathematically complicated manner with permutations and nonlinear functions and provides computational security [22].

The fibre industrial of America began in the early 1980s. At that time, systems could was able to operate at 90 Mb/s. At this level of data rate, a single optical fibre was able to handle about 1300 voice channels at the same time. Nowadays, communication systems are about to typically operate at 10 Gb/s and even higher. That means it can support the capacity of more than 130,000 simultaneous voice channels. Over the past five years, new technologies have been developed and improved such as dense wavelength-division multiplexing (DWDM) and erbium-doped fibre amplifiers (EDFA) have been used successfully used to further increase data rates to more than a terabit/second (>1000 Gb/s) over distances in excess of 100 km [23].

However, by adopting QKD today, organisations can protect their communication infrastructure from the massive and changing cyber threats not only today but also those of tomorrow. Already, hackers have used techniques such as harvesting and decrypting, today scraping and storing data for decryption once they have the ability to do so through advances with supercomputers, implementing quantum computers or newly discovered cryptographic techniques. Therefore, with quantum cryptography solutions such as QKD, any data that requires long-term protection is not only secure in today's IT environment, but also secure in the future in the coming quantum age.

1.1.2 Quantum Cryptography

Based on quantum mechanical principles, quantum key distribution (QKD) promises a solution to the problem of the distribution of keys. For the first time, security can be proven and quantified. The information is represented in a physical form e.g. the quantum state of a photon known as a quantum bit or 'qubit'. Security arises from the measurement principle of quantum physics [24], which states "Measurement of a quantum system in general disturbs the state of the quantum system." [1] Furthermore, the 'no cloning theorem' in quantum physics states that "It is not possible to duplicate unknown quantum states." Therefore eavesdroppers cannot faithfully copy the quantum information, which is otherwise possible in the classical world [1, 10]. For instance, when an eavesdropper tries to glean the quantum communication information between Alice and Bob, she inevitably introduce perturbation to the quantum communication system and thus her presence is revealed. This is the unique feature of a QKD system as it provides not only unconditional security but also the ability to detect eavesdropping.

Unconditional security is defined as security which is independent of the computational power and resources available to an eavesdropper.

QKD protocols can be divided into three types of protocols, namely discrete variable (DV), continuous variable (CV) and distributed phase reference protocols. These protocols are described in the review article by Scarani et al [2]. Irrespective of the protocol implemented, the essence of the security of a QKD system is based on encoding upon non-orthogonal quantum states [25, 26]. The protocols differ mainly on the detection schemes used for their implementations. DV-QKD and distributed phase reference protocols utilise photon counting while CV-QKD uses mainly homodyne detection. CV-QKD benefits from the relatively low cost p-i-n diodes for the detection [27]. However, this benefit is outweighed by their significant overhead cost for error correction [2].

1.2 Protocols of Quantum Key Distribution

Detecting the existence or non-existence of an eavesdropper based upon quantum mechanics is the main idea of Quantum Key Distribution. Alice and Bob, that is transmitter and receiver respectively, exchange quantum states in the link during the protocol. Basically, an eavesdropper (Eve), will measure and evaluate the states that have been or are being exchanged to understand the corresponding data values. Such a process is known as surveillance or hacking and should be avoided for security purpose in practical applications. And the eavesdropper's measurements do cause the collapse of the quantum state. It has been proposed that, in theory, sensitive statistical methods could reveal the changes caused by Eve's measurements, and even if Eve tried to reduce or constrain her measurement; there has implications for the state. In addition, the longer time Eve attempts to measure and learn, the more likely and chances she is to be detected [28]. As time goes, it is not of any possibilities for Eve to be unnoticed at all. In a word, QKD is therefore an unconditional approach by all means [29-31].

1.2.1 BB84 protocol

The Bennett-Brassard protocol [32], which is also known as BB84 was proposed and published in 1984 by Charles Bennett and Giles Brassard, here Alice transmits a series of individual photons to Bob who aims to measure the photons once they arrive the end. Definitely, there will be a numbers of photon that never reach the end and cannot be detected. For those that

have been arrived, some of the signals are kept and treated as key material while rest of them are utilized to find out where Eve is and how she works [33].

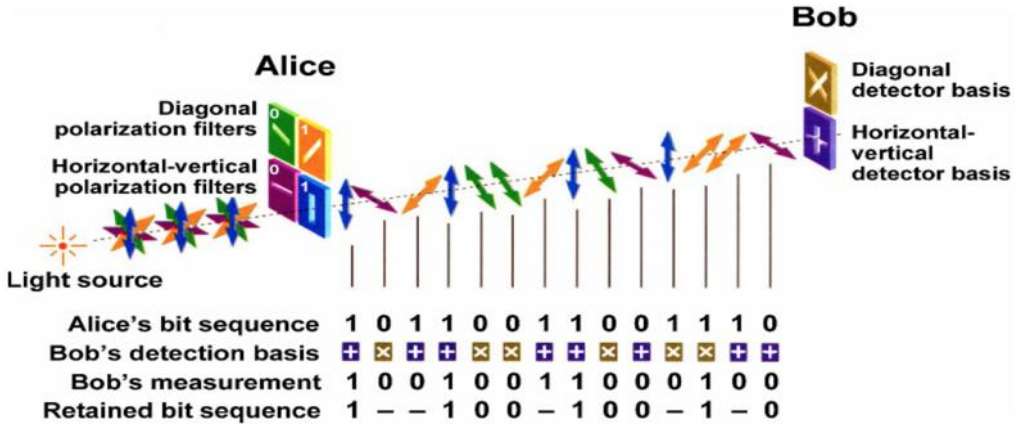


Figure 1.2.1.1 Schematic of BB84 protocol (taken from [25])

Figure 1.2.1.1 illustrates the fundamental BB84 protocol principle, here Alice can theoretically encode a bit using a qubit based upon any basis. Alice's original conventional bit will be detected when measure in the original basis. However, the state of the qubit will be altered if measurement in a distinct basis hence as a consequence a subsequent measurement may possibly lead to a different bit. Therefore, if a wrong basis is used for Eve's measurement because it passes her and the information will be let to go on to Bob who will measure it based upon the right basis and distinguish the qubit that has been altered during the process [34].

In theory, polarization is the most straightforward and simplest approach that Alice could utilize and the protocol runs in several steps as follows:

1) Alice sends quantum states to Bob, utilizing two bits which are of classical form. For each qubit she sends to select both the encoding basis she has used (+ or ×) and the bit she has sent (0 or 1);

2) Bob receives and measures the qubits that has sent by Alice, and Bob uses an arbitrary classical bit or quantum effect to determine the measurement basis;

3) The qubits Bob has received will be informed by Alice over a public channel;

4) Both the bases used by Bob and Alice will be exchanged via a public channel while Bob's messages could be combined with step 3). The measured bit will be kept if and only if both Alice and Bob chose the same basis. Otherwise it is sifted.

At this stage, both Alice and Bob have their own set of optical quantum bits. If there were no eavesdroppers, the two sets would theoretically be the same. In practice, however, two things are required to ensure that if these sets of quantum bits are designed as an encryption key. One is to perform the real eavesdropping detection and error correction on the remaining quantum bits. A standard classical error correction should be applied to the rest of the key. Finally, it should use this technique to remove the last bit of doubt. It's called privacy amplification, and it's based on classical information theory.

The protocol begins when Alice sends Bob a very large number of qubits over the quantum channel. Bob will record all the bits arrive at his end and measure each qubit by using randomly bases. Statistically, an average 50% possibility of Bob's measurements will be correct for the remaining bits.

However, if Eve exits and tries to intercept some of the qubits at any point between Alice and Bob, Eve has to make random choice from either of the base to measure the qubits that she want to measure. Thus because Eve intercepts and hacks 50% of the qubits and then only the other 50% will be sent to Bob. When Eve measures, copies, and re-sends this hacked information to Bob, only 50% would be the same as the original information theoretically. As a consequence, 75% (i.e. 50% + 50%*50%) of the qubits will technically get to the Bob end which are the same as Alice's intensions. At this point, once Bob receives and measures the qubits randomly as before, it will lead to a new accuracy of 62.5%. Whereas Bob doesn't know the existence of Eve at this stage, so he and Alice have to send each other some information to figure out how accurate the information Bob has received. And this step is called error correction. Once Bob has measured all the qubits he has received, he will turn to the classical channel and send Alice a string of bits, telling her which bases he has used to measure each of the qubits. Once Alice receives the message from Bob, she checks her personal record and sends message to Bob, telling him which quantum bit bob has finally measured correctly.

In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In QKD schemes the quantum signals are used to generate the shared secret key rather than to encode the message itself, which is subsequently communicated using the classical one time pad scheme. Providing Alice and Bob wish to transmit secure information between each other, the only way that they both can be absolutely sure there is no eve between them is to use a one-time pad and no key will be reused. Now Bob can abandon the distinct

qubits, and Alice can do the same so the whole process is a one-time pad which means no key is reused in order to reduce the copy and resend attacking probability.

The photon number splitting (PNS) attack is one example of a loophole based attack on the standard BB84 protocol. It was first introduced by Brassard et al. [35]. The problem here is that the photon source used by Alice is not a truly single photon source as assumed by the protocol. In fact, pulsed attenuated laser sources are usually employed in QKD systems. Such sources always have a non-zero probability of emitting a pulse with more than one photon. These multi-photon pulses can be exploited by an eavesdropper in the PNS attack. In this attack, when a multi-photon pulse is discovered from the incoming stream of photon pulses emitted by Alice, Eve splits the pulse and stores it in her quantum memory and forwards the rest to Bob. Later on when Alice and Bob carry out bases reconciliation, Eve can obtain enough information to reconstruct part or all of the final key; crucially without detection[36].

To discuss the security of quantum cryptography, here is a simple example of an intercept-resend attack by Eve, who measures each photon in a randomly chosen basis and then resends the resulting state to Bob. For instance, if Eve performs a rectilinear measurement, photons prepared by Alice in the diagonal bases will be disturbed by Eve's measurement and give random answers. When Eve resends rectilinear photons to Bob, if Bob performs a diagonal measurement, then he will get random answers. Since the two bases are chosen randomly by each party, such an intercept-resend attack will give a bit error rate of 50% × 50% + 50% × 0 = 25%, which is readily detectable by Alice and Bob. Complicated attacks against QKD do exist but fortunately, the security of QKD has now been proven [37].

Traditionally, cryptography has been a continued battle between the hackers and the programmers. On one hand, hackers try to exploit the system loopholes and breach the security while programmers try to come up with a solution to counteract the attack on the system. A solution to the PNS attack was found around a decade ago by a modification of the standard BB84 protocol. This is now known as the 'Decoy protocol'.

1.2.2 Decoy state protocol

This protocol is attractive since its implementation only requires a minimal modification of the existing hardware used for the BB84 protocol. This idea was first introduced by Hwang [20]. 'Decoy' pulses here are simply photon pulses from an attenuated laser with a different mean photon number. These pulses are in addition to the photon pulses used to transmit the usual

key information (termed ‘signal pulses’) [38]. Decoy pulses are randomly interleaved in the signal pulse stream. This time the PNS attack by Eve fails in the following way. Again, Eve tries to implement the PNS attack by completely blocking the single photon pulses and splitting the multi-photon pulses. Eve stores one photon from the multi-photon pulses in her quantum memory and forwards the remaining photons to Bob. However, Alice has intentionally introduced decoy pulses along with the signal pulses [39]. As the decoy pulses are randomly distributed in the signal pulses Eve cannot distinguish between them. By analysing the transmission and QBERs of the decoy pulses, Alice and Bob can detect Eve’s presence even though a true single photon source is not used [40].

With the decoy state protocol not only unconditional security but also transmission distances in excess of 140 km can be achieved as shown by Lo et al [39]. Another big advantage of the decoy protocol is that higher mean signal photon numbers can be used, which increases the secure bit rate. It was also suggested that for implementing the practical decoy protocol only two classes of decoy pulses are sufficient. Each class has a different mean photon number. More rigorous security proofs can be found in the paper by Ma [41].

1.2.3 T12 protocol

Practical experimental components are not perfect and this has to be taken into account in the security proof. For example, most security proofs assume a single photon source. However, the attenuated laser source with the decoy technique was used in the experimental work. Also, it is often assumed that the amount of data available to the experimentalist is infinite. This is described as the ‘asymptotic scenario’. However, a real system deals with only finite data samples and thus the description in the asymptotic scenario has to be replaced by one in the finite size regime instead. If the finite size effect is ignored, the secure key rate is overestimated, because there is an assumption that the acquisition accuracy of QKD parameter is infinite, where there are errors in the actual applications. Due to statistical fluctuations of the sample, this type of error needs to be accurately quantified and included in the security proof. Finally, the technical progress in the QKD field requires high efficiency protocols hence the efficient BB84 protocol has to be implemented. To address these issues, a new ‘T12’ protocol was introduced by *Lucamarini* et al. [42], which is quantifiably secure in the finite size scenario as well as efficient. At the same time, it removes a few idealisations and bridges the gap between theory and practice.

The security proof of T12 protocol is based on the finite size security proofs described in [43-45] and offers several advantages. Firstly, it provides universally composable security [46, 47], which implies the key is secure irrespective of the application it is used for. Secondly, it neither requires a random permutation of the users' string prior to the classical post processing stage nor to encrypt error corrected information [48, 49].

1.3 The quantum bit and properties

For the BB84 protocol, Bob randomly switches between the rectilinear and diagonal of his basic states and then measures the photons sent by Alice. These detected events form the 'raw key'. When Alice and Bob use the same bases, their results are correlated. Otherwise they will get uncorrelated or irrelevant results and they discard these type of quantum bits in the end. The sequence of retained bits is known as the 'sifted key'. Although the sifted keys are highly correlated, they differed in some bits, i.e., quantum bit errors, resulting from either the system imperfections, such as detector dark counts, or eavesdropping. The ratio of the number of errors to the total number of sifted bits is defined as the quantum bit error rate (QBER).

In order to predict the performance of a given QKD scheme, the key distribution rate before error correction and privacy amplification R_{raw} can be estimated by experimental parameters and the formula is as follows [1, 2, 50],

$$R_{raw}=q\mu v\eta_t\eta_d \qquad \text{Eq (1)}$$

q is a systematic factor which depends on the implementation chosen. For instance, in the case of the BB84 four states protocol, it is equal to $\frac{1}{2}$, because the bases that Alice and Bob randomly selected are incompatible half the time, μ is the average number of photons per pulses. In a more rigorous treatment, this quantity should be replaced by the probability of a pulse containing at least one photon. Assume it is small, it is well approximated by the average of the Poisson distribution. v is the repetition frequency and η_d is the detector efficiency. Finally, η_t is the transfer efficiency between Alice's output and Bob's detectors, which can be defined as:

$$\eta_d = 10^{\frac{-(L_f l + L_B)}{10}} \qquad \text{Eq (2)}$$

where L_f corresponds to the attenuation in the fibre in dB/km, l to the length of the link in km and L_B to Bob's internal losses in dB.

The QBER stated above can be evaluated as the ratio of the probability of getting a false detection to the total probability of detection per pulse:

$$\text{QBER (q)} = \frac{\pi_{opt} p_{phot} + p_{noise}}{p_{phot} + 2p_{noise}} \cong \frac{p_{noise}}{p_{phot}} + \pi_{opt} = QBER_{det} + QBER_{opt} \quad \text{Eq (3)}$$

p_{noise} and p_{phot} are the probabilities are the probabilities of recording counts caused by noise and photons, respectively, while $p_{phot}$is the probability of photons reaching the unexpected detector. The value of QBER consists of two parts. The first one, called $QBER_{det}$, is caused by the noise counts, mainly due to the dark counts from detector. The second part $QBER_{opt}$ is the propagation of photons to the wrong detector due to incorrect phase or polarisation measurements. When the transmission distance goes up, the transmission efficiency $\eta_t$becomes lesser, while p_{noise} will not change. This leads to an increase of $QBER_{det}$, which imposes the principal limitation on long distance QKD. ***Gisin*** et al. [1] shown that QBER is lower than 15% and can establish security key immunity against any personal attack by means of error correction and privacy amplification. However, the individual attack is not the most powerful attack against the BB84 Protocol actually compared to the asymptotic scenario. Walter O. Krawec et al. [51] derived a new proof of security and key-rate bound for a three state BB84 protocol. They showed that this new key rate bound, in addition to the use of mismatched measurement outcomes, can tolerate the same maximal noise level as the four state BB84 (i.e., the key rate is positive for all Q $\leqslant$ 11%) in the asymptotic scenario [52, 53].

In a word, the threshold of QBER=15% corresponds to the security of the BB84 protocol against the so-called "individual attacks", which is NOT the most powerful attack against the BB84. When consider attacks more powerful than the individual attack, the security threshold decreases to 11%, but only in the so-called "asymptotic scenario", i.e., when acquire data "for an infinitely long time". This is clearly impossible in a real experiment, where data can be acquired only for a finite amount of time (e.g. 10 seconds or 10 minutes...). When take this "finite-time scenario" into account, the threshold decreases again, and can easily reach 6-7%, depending on the amount of data acquired in the finite time. Toshiba's system takes all these things into account, which is why you can experience a zero rate when the QBER is about 7% [42, 54].

As is described in previous sections, with the help of formulas, the raw key creation rate R_{raw} and QBER are given experimental conditions. Since the errors in the raw bit sequence are suppressed during key distillation, the useful key creation rate R_{useful} which follows the error correction and privacy amplification – forms the only truly significant value. Therefore, it is necessary to determine to what extent R_{raw} is reduced by the key distillation procedures, as a function of the QBER. The number of bits lost in the process of error correction as a function of the QBER is given for long strings (> 100 bits) by [51]:

$$R_{ec} = \frac{7}{2} QBER - QBER log_2^{QBER} \qquad \text{Eq (4)}$$

This expression is valid for small QBER. Rec increases with the error rate, which implies that it is important to keep it low. On the other hand, the fraction of bits lost through privacy amplification can be estimated by

$$R_{pa} = 1 + log_2(\frac{1+4QBER-4QBER^2}{2}) \qquad \text{Eq (5)}$$

Assuming that all the errors are caused by Eve's tampering and she can gain the information of 4 QBER / $\sqrt{2}$ or about 2 QBER / ln2 at most. This assumption demonstrates that the average number of photon per pulse μ is as usually small as 0.1 to ensure that the lower ratios of the pulses contains more than one photon. If this condition is not reached, the estimate does not apply in this case.

Finally, the useful key creation rate can be estimated:

$$R_{useful} = R_{raw}(1 - R_{ec})(1 - R_{ec}) \qquad \text{Eq (6)}$$

$$\frac{final\ bit\ rate}{sifted\ key\ rate}\% = (1 - r_{ec})(1 - r_{pa}) \qquad \text{Eq (7)}$$

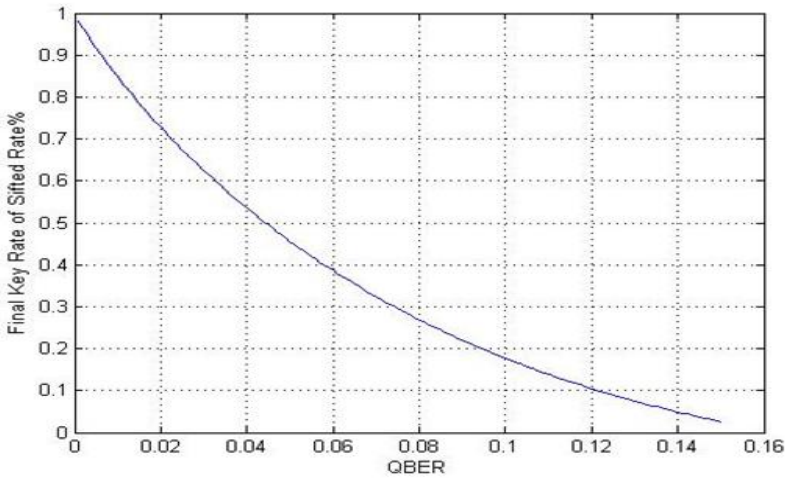


Figure 1.3 Theoretical simulation of Final key rate of sifted rate vs QBER

1.4 Motivation for the research in this thesis

The potential for general purpose quantum computers to be able to break the cryptographic systems currently used to secure networks has resulted in increased interest in quantum cryptography for secure data transmission. QKD provides an inherently secure method of cryptographic key generation at distant points on a network. This thesis focus on using DV-QKD to provide keys for high data rate classical WDM transmission secured by the [22] AES standard. The challenge is simultaneous transmission of single photon QKD signals in the same fibre as 100Gb/s coherent WDM signals, which are more than 60dB higher power.

QKD must be designed to operate at telecommunication wavelengths and have high secure bit rates so as to coexistence with exiting telecommunication links at low cost [55]. The secure key rate of QKD systems was often limited to a few kbps due to poor performance of the single photon detectors. Higher secure key rates are demanded for scenarios such as a network shared by many users or high bandwidth applications such as video transfer and the performance of the single photon detector has been dramatically improved for DV-QKD system [56]. Hence, it is necessary to have the hybrid system on trial and then study the restrict factors for real QKD network links compared with laboratory demonstrated experiments.

Although the traditional DV-QKD system, the original BB84 coding scheme, was designed to take advantage of the quantum properties of single-photon polarization states, the experimental equipment operates based upon the phase coding schemes. These encoding schemes are based on the properties of interferometers and the encode by changing the relative optical path lengths or phase between the arms of the interferometer. However in actual transmission environment, the change of temperature or polarization is unpredictable [57].

Raman noise has to be greatly drawn attentions in such a hybrid link rather than traditional communication systems, because the classical channel power in hybrid link is as 70 dB higher as quantum channel. And such a huge difference will lead to unexpected noise photons arrive at detector and therefore increase the QBER and reduce the secure key rate.

1.5 Summary

So far, most experiments and field trials have been conducted on dark fibre only. Since dark fibre is a scarce and expensive resource, it is urgent to make QKD coexist with data signals on the same fibre to build a hybrid quantum network. However, studies conducted before this research have been limited to very low bit rates, short fibre lengths, and/or one-way data communications. With the adoption of new protocol (i.e. T12) and commercial equipment, this research demonstrates that QKD has error-free bidirectional Gbps data transmission with a secure bit rate three orders of magnitude higher than previously reported and figured out factors that affect the hybrid quantum network followed by an optimisation method.

Chapter 1 was a brief introduction to classical and quantum cryptography techniques. The novel key distribution method based on quantum physics, followed by explanations of the various protocols including BB84, decoy BB84 and T12 were introduced in some detail. Serval key parameters such as QBER used for describe QKD system performance were briefly discussed here. Moreover, the motivations for pursuing the research were elaborate and thesis framework was stated in the end.

Chapter 2. Quantum Network Characterisation

Chapter 1 compares conventional cryptography with quantum cryptography in terms of data rate, limitations and practical application ranges. And also the significance of quantum key distribution is to improve the security level of the existing encryption measures, but also to prepare for the future emergence of the quantum computer to prevent threats to the security of the existing communication encryption technology. Hence ***Chapter 2*** aims to demonstrate the general components and system implementation of a high speed communication channel encrypted upon quantum key distribution.

2.1 Introduction to quantum network

Quantum cryptography, or quantum key distribution, offers the possibility of secure key distribution that guarantees confidentiality through quantum mechanics [58]. This opens up the interesting possibility of communication systems rely solely on fundamental laws of physics to provide security, rather than on the principles of mathematical complexity that underlie today's cryptography. Most of the studies on actual QKD systems focus on extending the transmission distance of point-to-point optical fibre and free space optical links, with the purpose of establishing national or global-scale security key exchange and management network [59-62].

So far, there has not enough attention been drawn to the development and establishment of QKD access networks, especially metropolitan quantum networks or larger-scale QKD secured access networks, which aims to connect end users to these secure network infrastructures. In principle, a broad access network topology is feasible for QKD [63], but standardized solutions developed primarily for traditional high-speed communication requirements are likely to end up providing the lowest cost and thus the most practical solution.

Therefore, the encryption method of QKD on existing conventional communication infrastructures which is also constructing quantum network is feasible and low-cost. The data speed has exceeded 100Gbps over tens or even hundreds of kilometres of point-to-point single-mode optical fibre communication. If the encryption technology of QKD can be combined with this high-transmission rate optical fibre communication, it is the foundation for the construction of a high-speed transmission network without security risks in the future against quantum

computer's threat. Then, the following will cover the basic components of a quantum network and the constraints that can actually be encountered [64].

2.2 System characterisation

2.2.1 Single Photon Source

Attenuated pulsed lasers are promising light sources for QKD. Although they emit multi-photons as well as single photons, their performance approaches that of a true single photon source when used for example in a decoy protocol system (described in Chapter 1) [39]. With present technology, a commercial-available laser is able to offer many benefits such as compact packaging, cryogenics-free, operation at telecommunication wavelengths, low power consumption and low cost [65].

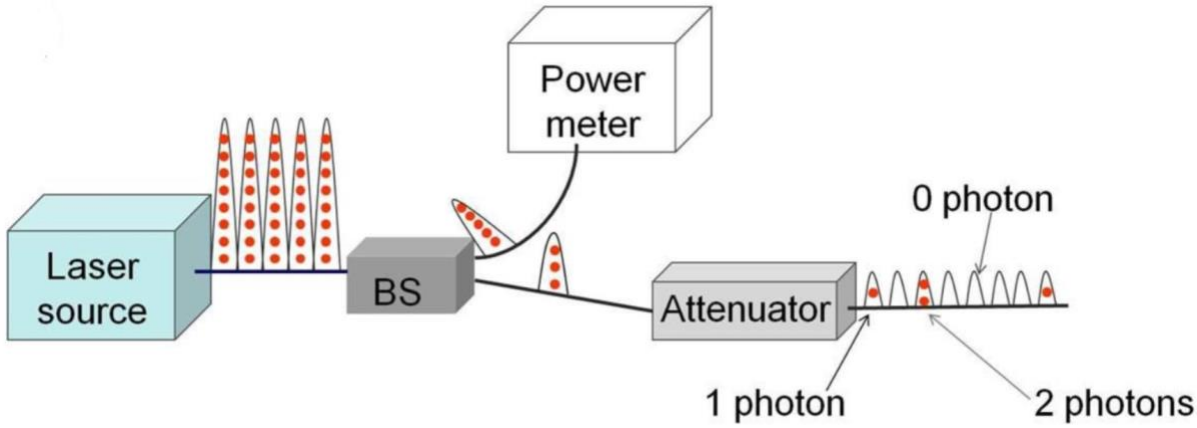


Figure. 2.2.1 Schematic of an attenuated light source QKD system

The schematic for an attenuated light source based on a pulsed laser is shown in Figure 2.2.1. Coherent pulses of light are emitted from the laser and the light is split into two parts by a beam splitter (BS). One path is monitored using a power meter and the other part goes into a calibrated attenuator. The attenuator is used to reduce the photon flux of the laser pulses down to the single photon level. The power meter is used for calibration of the photon flux. In practice, a pulse might contain two or more photons. This is because the distribution of the photons in a pulse follows Poissonian statistics and is given by [1, 66]:

$$p(k,\mu) = e^{-\mu}\frac{\mu^k}{k!} \qquad \text{Eq (8)}$$

where μ is the average number of photons per pulse and k is the actual number of photons in a pulse. For instance, for μ=0.2,then $p(0,0.2)=0.82$, $p(1,0.2)=0.16$ and $p(2,0.2)=0.02$. As is

introduced, $p(1,0.2)=0.16$, such a source is vulnerable to the PNS attack when used in a QKD system [36, 67]. The eavesdropper could split the multi-photon pulse in order to acquire information without detection. To overcome this problem, the decoy technique has been implemented as described in Chapter 1. For the experiments described in this thesis, a 1 GHz pulsed laser source has been used and embedded into a Toshiba QDK system.

2.2.2 Communication Channel

Transmission media for QKD include free space channels, ground to satellite communication channels, and fibre-based point-to-point links. In this section, free space channels and ground to satellite communication channels are briefly summarised before describing in detail fibre-based point-to-point links, which are utilised in this thesis.

An example of a free space QKD experiment is a single photon entanglement-based free space QKD demonstration over a distance of 144 km using polarisation encoding and closed loop tracking at the receiver [61]. In 2007, a QKD experiment was carried out using the decoy state BB84 protocol over a similar free-space link, yielding a secure rate of 12.8 bit/s with a channel attenuation of 35 dB. In this case at the receiver end, the light was collected by two telescopes using an active tracking technique in order to ensure optimal coupling [68-70].

In an attempt to extend the transmission distance, in-orbit satellites are used to allow quantum communication between the receiver ground stations via the satellite [71]. This is the most basic arrangement; however, variations have been studied. Recently, researchers have explored QKD performance when the transmitter and/or receivers' platforms are moving. This was accomplished by utilising an airplane moving at 290 km/h separated by a distance of 20 km from the ground. The mean sifted bit rate and QBER were 145 bit/s and 4.8% respectively using the BB84 protocol with a predicted secure bit rate with the decoy protocol of 7.9 bit/s [72]. Also, ground station to satellite QKD has been extensively tested in different test beds, for example, using a transmitter on a turntable to simulate an orbiting satellite. Another example is placing the transmitter in a hot air balloon to explore the effect of a vibrating or floating platform. This experiment also explored the effect of a high loss environment where the transmitter and receiver were separated by 96 km with a loss of 50 dB. In the floating and moving platforms, secure key rates of 150 bit/s were obtained on average with a QBER of 2.8%, while in the 96 km case the rate fell to 48 bit/s owing to a QBER of 4% [73].

In both free space and satellite based QKD a direct line of sight and favourable weather conditions are required. This is because the results of the system can be affected by temperature, humidity gradients and wind speeds. The alignment of such systems is challenging and they are also inefficient in terms of secure key rates.

The electronic polarization controller (EPC) can be used before the interferometer in the QKD receiver in order to compensate for the constant rotation of the output polarization caused by the birefringence of the transmission fibre and environmental motion and expansion. The EPC is continuously driven based on the feedback signal provided by the detector count rate.

The stabilization subsystem is related to the time variation of the photon during transmission, which is mainly caused by the expansion and contraction of the fibre due to the change of the ambient temperature. The clock delay of the receiver is adjusted according to the detected photon count rate so that the arrival time of the photon is always matched with the detector's gate cycle centre and the phase modulator cycle centre.

In this thesis, an optical fibre-based point-to-point link QKD configuration has been used. Silica optical fibre has emerged as an attractive choice as a transmission medium because of low signal attenuation, immunity to electromagnetic interference, high transmission bandwidth, low raw material cost and long haul transmission [74]. Some of the practical aspects of the fibres are discussed here.

The fibre output optical power, P_{out} , as a function of fibre distance, L, can be expressed as $P_{out} = P_{in}e^{-\alpha L}$, where P_{in} is the input optical power, α is the fibre attenuation coefficient expressed in the unit of km^{-1}. The loss of the silica single mode (SM) fibre is dependent on the wavelength as shown in Figure 2.2.2. Typically, the loss of the fibre at 1550 nm is 0.2 dB/km [75]. The three distinct absorption peaks in the loss spectrum occur due to interaction of OH ions with Silica. The dominant remaining factors for the loss in the fibres are material absorption and Rayleigh scattering. Rayleigh scattering is a loss mechanism in the fibre, which is due to local fluctuations in the refractive index that are smaller than the wavelength of the light. The Rayleigh dependant loss scales with wavelength as λ^{-4}.

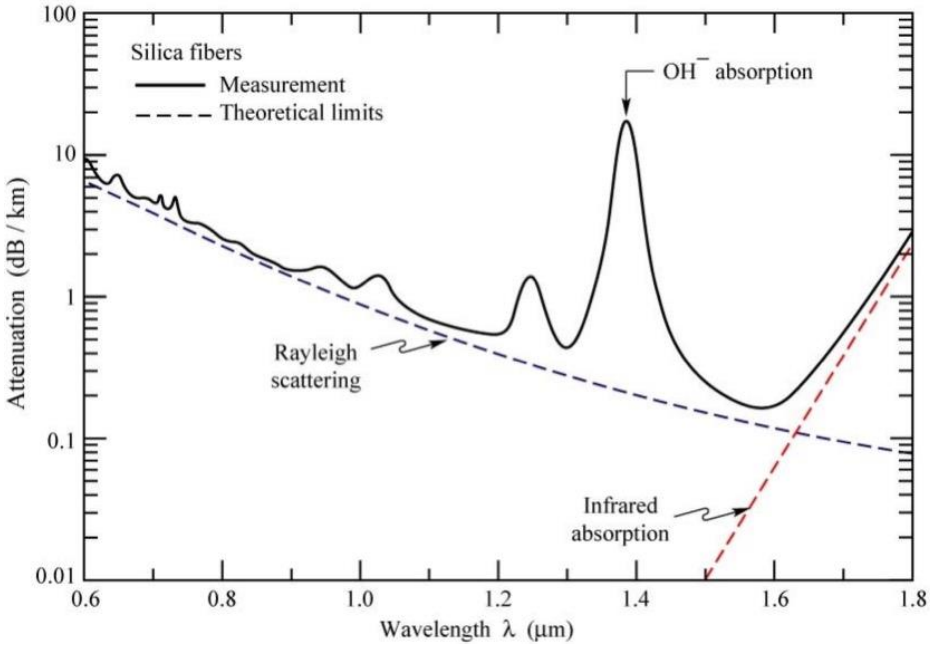


Figure 2.2.2 Attenuation in silica fibre (directly taken from[75])

2.2.3 "Plug and play" QKD system

A traditional experimental QKD system called *"plug&play"* first suggested in 2002 by Stucki *et al [76]*. "Plug&play" scheme is a two-pass auto-compensating scheme, which is commonly used when phase encoding [77]. Figure 2.2.3 demonstrates a schematic diagram of the optical part which consists of a transmitter (Alice), receiver (Bob) and quantum channel (SMF).

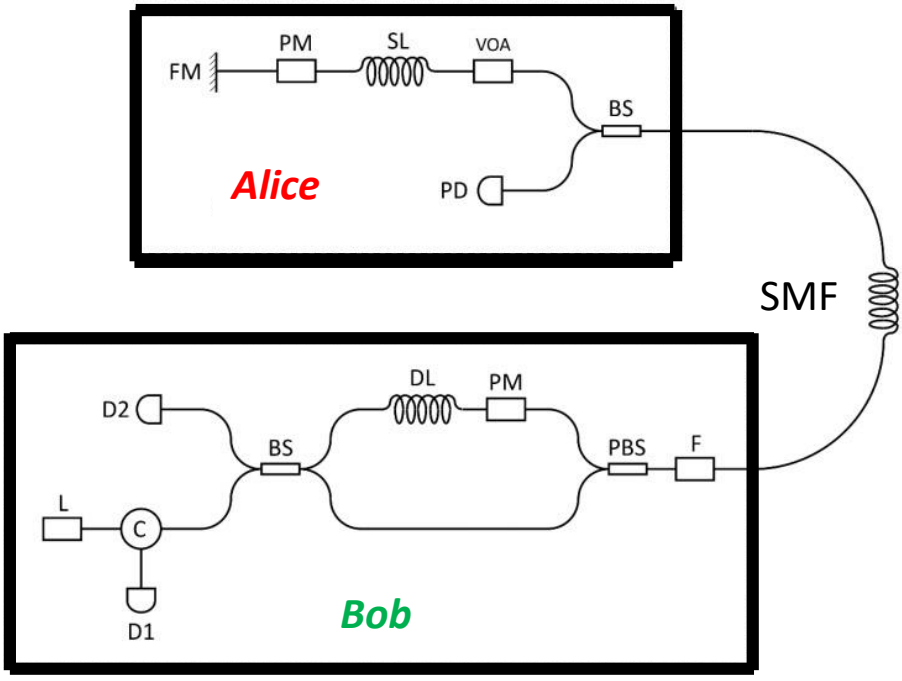


Figure 2.2.3 Schematic diagram of the optical component of plug and play QKD

Receiver Bob is the multi-photon light pulse source generated by laser. The wavelength of light is 1550.86 nm, and the laser pulse duration is 5 ns. First, the light pulse passes through a circulator C and enters a 50/50 beam splitter b. Half of the pulse passes through the short arm of the Mach Zehnder interferometer into the polarization splitter (PBS). The second part passes through the long arm of the interferometer, which consists of a delay line (DL) and a phase modulator (PM), and then also enters PBS.

After passing through PBS, the two parts of the pulse pass through the quantum channel SMF to the transmitter Alice, where they pass through the variable optical attenuator (VOA), the memory line (SL), and the phase modulator (PM). After reflection mirror Faraday (FM), rotating light polarization, again in 90° to the exit at the end of the optical pulse reach Alice.

The advantage of the scheme is that the interferometer can be automatically compensated, and the interferometer can work without feedback system, so as to compensate the uncontrollable phase change of the optical signal from the sending end to the receiving end. However, since the light signal travels in both directions, reverse Rayleigh scattering reaches the receiver's single-photon detector, which can significantly increase the noise level [78].

2.3 Technique for a hybrid QKD with classical data communication system

Optical wavelength division multiplexing (WDM) is a technology capable of explosive growth of Internet and telecommunication traffic in wide fibre communication networks, metropolitan scale optical communication networks and local communication networks. The WDM is used to divide the 50 Hz bandwidth of a single fibre into different wavelength channels and multiple non-overlapping frequencies. Each WDM channel can operate at any speed, for example, a peak electron speed of several thousand megabits per second (Gbps). At the current stage, commercially available optical fibres can provide more than 100 of these wavelength channels, all of which are capable of speeds in excess of a gigabit per second [79-81].

However, even though a single fibre strand has a wavelength channel that has speed over gigabit-per-second and over a bandwidth over terabit-per-second, to support the traffic connections, a rate that is lower than the full wavelength capacity may still be required by the network. These low-rate traffic connections can have minimum capacity as 51.84 Mbps or even lower and maximum capacity to full wavelength. For network operator, being able to groom the multiple low-speed traffic connections onto high-capacity circuit pipes is very vital if the performance improving and saving network cost are needed. In transport systems, when

operating cross-connections of conversions, whether between multiple systems or within same system, grooming is used to describe the optimization of capacity utilization.

The process of mounting many wavelengths onto a single fibre is called wavelength division multiplexing. Wavelength division multiplexing is able to equip multiple independent and separate channels onto optical fibre, which is also can be called as Analog multiplexing technique. Hence, WDM technology can be used to increase total communication bandwidth. By reducing the channel spacing and increasing the bit rate, one can increase the transmission capacity of wavelength division multiplexed systems. In order to increase the extent of broadband information distribution, normally an erbium-doped fibre amplifier to boost signal power is used in WDM systems as well as low dispersion fibres. Figure 2.3(a) shows the schematic of a wavelength division multiplexing technique where N channels which are all different wavelength/frequency are combined by an optical multiplexer and then transmitted onto a single fibre and de-multiplexed at the end of the fibre [79, 82].

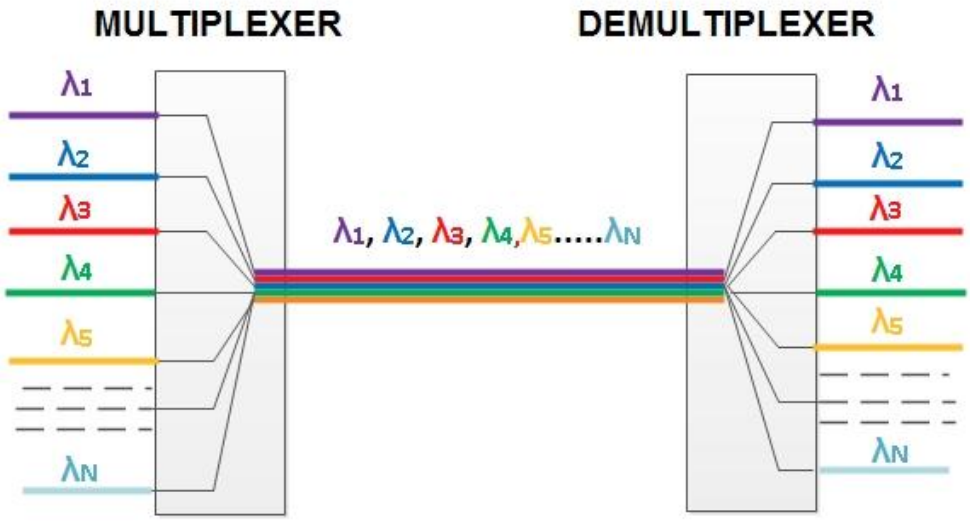


Figure 2.3(a) Schematic of wavelength division multiplexing and de-multiplexing

Wavelength division multiplexing has had great impact in high capacity transmission systems with large capacity in recent years. The first wavelength division multiplexing systems only carried two signals however wavelength division multiplexing systems nowadays can carry up to 160 signals. Multiplexer is adopted in the transmitter-ended systems to combine multiple signals together. On the contrary, De-multiplexer is adopted at the receiver-ended systems to separate those signals. Generally, two types of wavelength division multiplexing are used extensively, Dense wavelength division multiplexing(DWDM) and coarse wavelength division multiplexing(CWDM) [79, 83].

DWDM shown in Figure 2.3(b) is the a type of wavelength division multiplexing for optical fibre communication technique and is designed for long distance transmission where wavelengths are densely integrated together. Dense wavelength division multiplexing is the process of multiplexing multiple signals onto a single fibre where each fibre has a series of parallel optical channels. Each optical channel is using many different light wavelengths that can transmit data serial-by-character or parallel-by-bit. CWDM (coarse wavelength division multiplexing) does not span long distance since the light signal of coarse division multiplexing is not amplified. Therefore, the cost is reduced but also propagation distances are limited to maximum value. Compared with DWDM, the channels used in coarse division multiplexing are often fewer. Additionally, for metro carriers who prefer to start small and expand as the demand increases, these channels may be sufficient. With retaining high loss tolerance, the cost has been kept down by the signalling systems. Every time when implementing a trade-off between the capacity and distance a non- amplified signal is used. Filtering of light and multiplexing or de-multiplexing of different wavelengths are the two functions performed by CWDM and both of them are travelling in a same medium [84, 85].

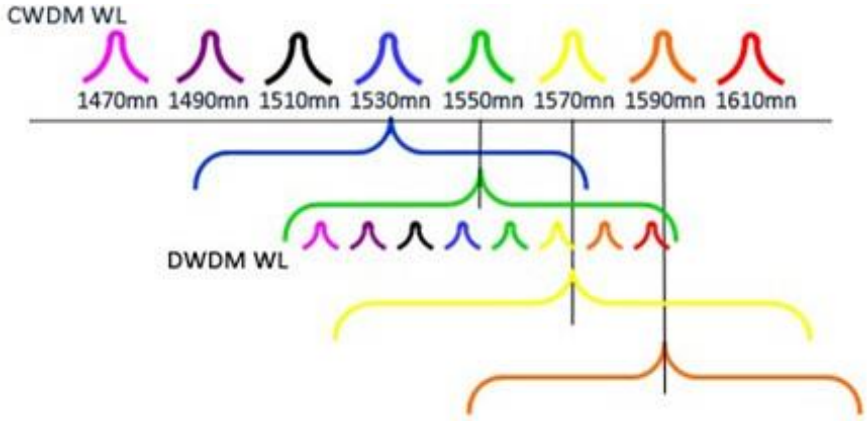


Figure 2.3(b) Wavelength for CWDM and DWDM

Types	CWDM	DWDM
Channel Spacing	20 nm	100 GHz/ 50 GHz/ 25 GHz
Laser	Un-Cooled Laser	Cooled Lasers
Capacity(Max.)	18×10 Gbps	192×10 Gbps
Application	100 km	5000 km

Table 2.3 Comparison between CWDM and DWDM performance [84]

2.4 Review of Quantum networks

2.4.1 Overview of QKD systems

Early QKD systems required dark optical fibre connections to avoid light-polluting sensitive quantum signals from other data transmissions. Putting a fibre in this way means huge deployment costs, and it makes commercial sense to be able to send quantum signals along the same fibre as traditional data [72, 86-88].

Implementations of QKD are more than only the experimental phase. A series of Quantum key distribution systems have been demonstrated in laboratories all over the world in recent years and also some of the laboratories are supported and funded by governments, for instance, NIST and LANL in the United States [60] and NICT in Japan [89], and at corporate laboratories, such as HP, IBM, NEC, NTT and Toshiba. MagiQ Technologies [3] and id Quantique [76], are two of the largest companies in the world who had commercialised Quantum Key Distribution gateways for several years and the products from both companies incorporate classical encryption for the bulk data as well as providing the QKD itself. Metropolitan-area testbed networks have been built in Boston, Vienna, Geneva, Barcelona, Durban, Tokyo, P.R China and elsewhere in the world [90-92].

Toshiba has developed a system that can transmit quantum keys over optical fibre, as well as classical data. In core and metro networks, high data rates and performance are key issues, while in access networks, it is important to limit the cost of providing services to a large number of users, so these technologies are optimized. Reducing the cost of delivering QKD services to end users can be achieved by using a quantum access network, where many users are serviced by a quantum receiver. In figure 2.4.1(a), multiple users share a photon detector. Customers need only cheaper components to send to quantum receivers. The standard passive fibre combiner is widely used in fibre to enterprise and fibre to home applications.

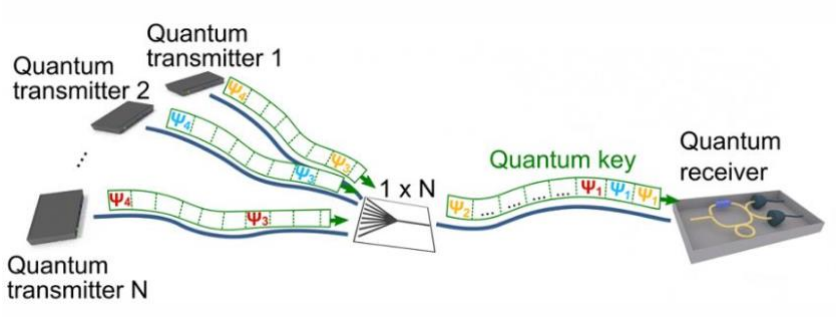


Figure 2.4.1 (a) Access Quantum Network Schematic (directly copy from [93])

2.4.2 Tokyo QKD network

The Tokyo QKD network which is shown in Figure 2.4.2(a) is based on JGN2plus (Japan's Gigabit Network) [94]. Overall, JGN2plus is an open testing network with more than 100 research projects using JGN2plus's services. The network can be viewed as a star network, connecting the operations centre in Otemachi with NICT's headquarters in Koganei, as well as the university of Tokyo in Hongo and NICT's research facility in Hakusan[94]. The QKD network field trial in Tokyo has demonstrated a QKD system with a bit rate of more than 1Mbit/s. This allows high-bandwidth applications such as high-speed video encryption to be secured using quantum methods. Secure video encryption and intercepted eavesdropping attacks have been demonstrated. Long field trials were also carried out. The transmitter was installed in the server room of a high-rise building in central Tokyo's Otemachi district. The recipient is located at NICT's Koganei facility in the greater Tokyo area. The two ends are connected by a 45-kilometer urban fibre optic cable. Although approximately 50% of this fibre is ground routed on poles and is therefore subject to weather and traffic interference, it was found that the safe bit rate of QKD is very stable in [94-96].

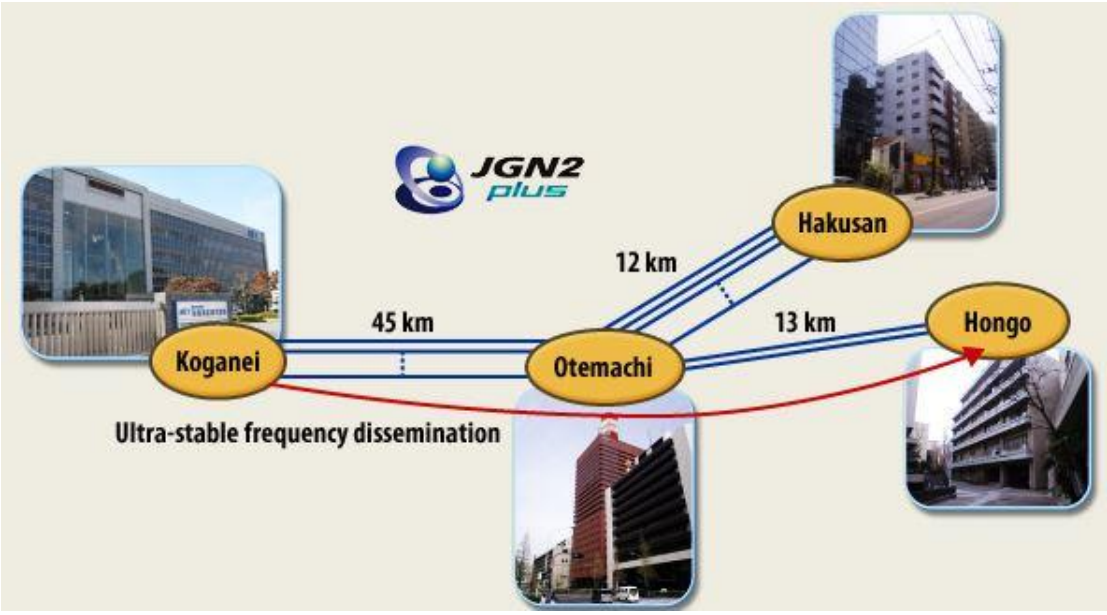


Figure 2.4.2(a) Tokyo QKD Network (Directly copy from [94])

2.4.3 Untied States QKD

Figure 2.4.3 illustrates a structure of Boston-rea network supported by DARPA [97] that was the world's first Quantum networking deployed QKD network. Basically, there exists 10 nodes in the DARPA QKD network shown below, running several distinct QKD implementations.

Single photons are generated by the laser with attenuated and weak coherent pulses from the first four nodes which is Bob, Alice, Anna and Boris. And both Alice and Anna are technically transmitters while Bob and Boris are the receivers at this stage.

It is reported that there exists a typical error rate around 5% in one of the links in the DARPA network hence the substantial error detection and correction are extremely desired to be taken into account for QKD implementations. One of the protocols that can be used to overcome and manage the errors is the cascade protocol developed by ***Brassard*** and ***Salvail*** [98].

The most common protocol for managing these errors is the Cascade protocol developed by ***Brassard*** and ***Salvail*** [99]. BBN implemented both Cascade and their own Niagara forward error correction (FEC) protocol and it results in a bit error rate of 3%.

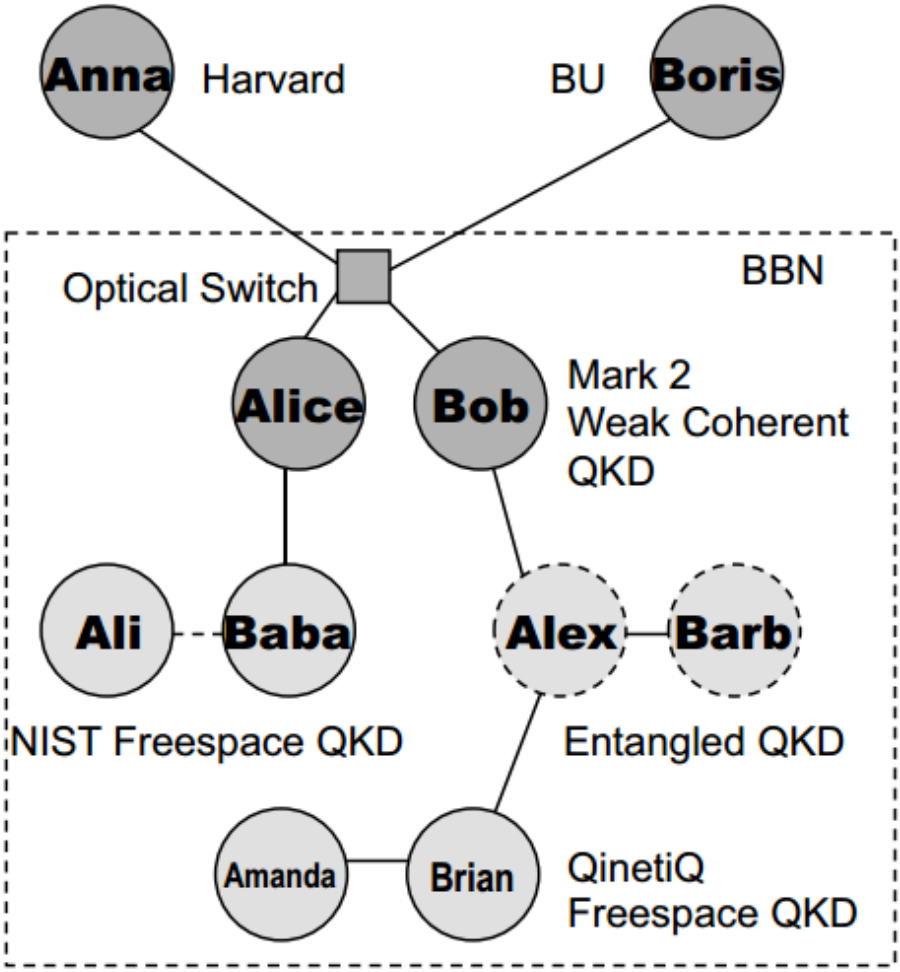


Figure 2.4.3 US QKD network[97]

2.4.4 UK and Cambridge QKD network

In this thesis, the Toshiba QKD system, which is introduced in previous section, has been utilized for research. Toshiba's prototype Quantum Key Distribution (QKD) system delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages. The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100 km in length and bit rates sufficient to generate 1 Megabit per second of key material over a distance of 50 km — sufficiently long for metropolitan coverage.

Beyond a Point-to-Point network and adopting to the existing infrastructure of current conventional data system is more reasonable and many research organizations are making their own efforts. It also has been demonstrated and been building a network based key distribution (>Mb/s) and quantum encryption over the Cambridge Quantum network [81]. The general geographical illustration is shown in Figure 2.4.4(a). The networks consist of several different transceiver ends including Centre for Advanced Photonic and Electronic (CAPE), TREL, Cambridge University Engineering Department, University CNF, BT and NDFIS at Duxford.

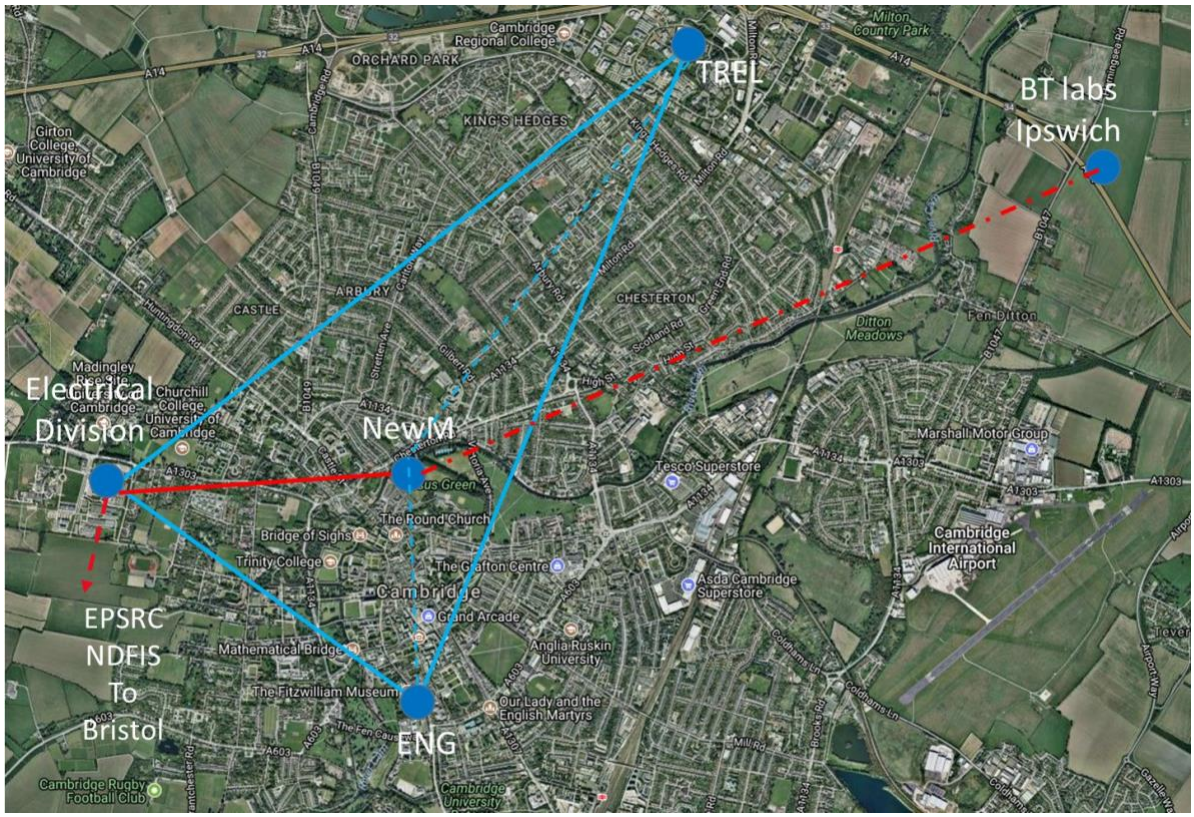


Figure 2.4.4(a) geographical illustration for UK and Cambridge QKD network

For the QKD network, the fibre links were populated with ADVA classical 10/100GbE networking equipment [100] shown in Figure 2.4.4(b). The QKD links between each node were tested progressively and will be discussed in next chapter. In other word, the initial test was a fundamental point-to-point QKD signal only test. Then a QKD point to point links with intermediate node (e.g. from CAPE to Engineering department and then to TREL) were tested. Next, 100 Gbps classic data signal were tested in the similar way to QKD signals and once the tests between each single link are completed, the combined conventional and QKD signals (100Gbps traffic + QKD) were combined together and run simultaneously on the fibre links.

Figure 2.4.4(a) UK and Cambridge QKD network set-up

Table 2.4.4 summaries some results for DV-QKD systems and it could be easily concluded that the secure rate decreases with the incensement of link length.

Author(s)	Distance(km)	Secure Bit Rate(kbps)
Dyes et al.	20	10
Rosenberg et al.	100	0.02
Sun et al.	25	805
Sun et al.	50	89.8
Dixon et al.	20	1020
Dixon et al.	100	10.1
Zhao et al.	15	165
Tanaka et al.	97	0.79

Table 2.4.4 Summary of Demonstrated DV-QKD System

	Tokyo	Geneva	China	This Research
Protocol	Decoy BB84	SARG	Decoy BB84	T12
Number of nodes	6	3	9	3
Longest Link	45km	14.4km	85.3km	10.6km
Highest key rate	300 kbps	2.4kbps	16.2kbps	2.5Mbps
Operation time	1 day	600 days	212days	580days
Data Mux	No	No	No	Yes
Data Bandwidth	No	No	No	200Gbps

Table 2.4.5 Summary of existing QKD system

2.5 Hybrid quantum network limitations and difficulties

2.5.1 optical fibre

Optical fibres suffer from dispersion that broadens the temporal duration of the optical signal pulse as it propagates through the fibre [101]. For high data rate classical communication this effect can be problematic. Due to dispersion in the high data rate regime the optical signals from neighbouring clock cycles can overlap causing adjacent bits to become indistinguishable. This is known as inter symbol interference (ISI), which deteriorates the quality of the optical signal [102]. Similarly, for quantum communication the effect of dispersion is problematic. If the detector active on time is long, dispersion can cause photons from adjacent clock cycles to be detected in the same gate period causing an increase in ISI and QBER.

Single mode (SM) optical fibre experiences non-uniform stress due to the fibre drawing process and/or environmental effects such as vibration and temperature. These effects break the circular symmetry of the SM fibre core resulting in cross sectional shape variation along the length.

Two orthogonally polarised modes will travel at different speeds and this is known as modal birefringence. The fibre can now support two orthogonal polarisation modes with differing group velocities, traditionally termed as the fast and slow axes modes. The axes alignment is not constant along the fibre and light launched into fibre transforms into an arbitrary polarisation state. The energy is interchangeably transferred between the fast axis and slow axis modes and this leads to polarization mode dispersion [101]. Typical values of PMD for modern fibres are less than 0.1 $ps/\sqrt{km}$. Since the PMD increases with square root of distance its contribution is comparatively smaller than chromatic dispersion [101].

In some special types of fibres, birefringence is maintained so that the two orthogonal polarization modes are not coupled. These are called polarization-maintaining (PM) fibres. Note that polarization-maintaining optical fibres do not polarize light as polarizers do. Instead, the PM fibre maintains the linear polarization of linearly polarized light, provided it is emitted into a fibre aligned with one of the fibre's polarization patterns. Shooting linearly polarized light into the fibre at different angles excites two polarization modes, transmitting the same wave at slightly different phase velocities. At most points along the fibre, the net polarization will be an elliptic polarization state, returning to the original polarization state after integer beat length. Thus, if a visible laser is fired into a fibre and two polarization modes are excited to observe the scattering of the transmitted light from the side, periodic light and shade patterns will be observed at each beat length, since the scattering is preferentially perpendicular to the direction of polarization. This may be used as a communication medium for the QKD channel, but it is not practical for real world fibre networks, as most installed fibre is SM [1].

2.5.2 WDM system

The coexistence architecture based on WDM technology was proposed by ***Townsend*** in the late 1990s [103] and studied later [87, 104-107]. These studies indicate that the existence of strong classical traffic may be detrimental to the QKD channel. This is because classical signals are usually many orders of magnitude stronger than quantum signals. Therefore, even a small crosstalk from a classic channel can override normal QKD operations. One possible method is to place the quantum signal in the "original" or o band of 1300 nm, and the classical signal in the "traditional" or c band of 1550 nm [87]. For such a large wavelength separation, both classical signal leakage and anti-stokes Raman scattering can be effectively suppressed to a tolerable level. In many cases, however, it is beneficial to have both quantum and classical signals in the c-band. For example, fibre loss is significantly lower in c-band than in o-band;

Therefore, the safe distance of QKD can be extended. In addition, this architecture is more compatible with today's fibre optic networks [108].

In a typical coexistence architecture based on WDM, the noise photons in the quantum channel can be contributed by several sources [87, 106, 107], including the leakage photons from classical channels due to the finite isolation of DWDM components, the 'in-band' noise photons generated in optical fibres from nonlinear processes, such as four-wave mixing (FWM) and spontaneous Raman scattering, and the in-band amplified spontaneous emission (ASE) photons generated by optical amplifiers. Here, in-band noise refers to noise photons within the spectral bandwidth allocated to the quantum channel. In this section, we quantify the noise photons contributed by each of the above sources based on a typical WDM configuration as shown in Figure 2.5.2. In the schematic, an erbium-doped fibre amplifier (EDFA) was employed to boost the optical power of classical channels before multiplexing with quantum channels. Furthermore, we assume that all the classical channels are placed at wavelengths longer than that of the quantum channels, since the spontaneous anti-Stokes Raman scattering (SASRS) is typically weaker than the spontaneous Stokes Raman scattering.

In this thesis, we assume that the eavesdrop (Eve) can control all the classical channels, but she cannot access the multiplexer (MUX) and de-multiplexer (DEMUX) used for multiplexing quantum signals with classical signals. A special case is that classical signals are actually used by Alice and Bob for authentication, error correction, and privacy amplification [107].

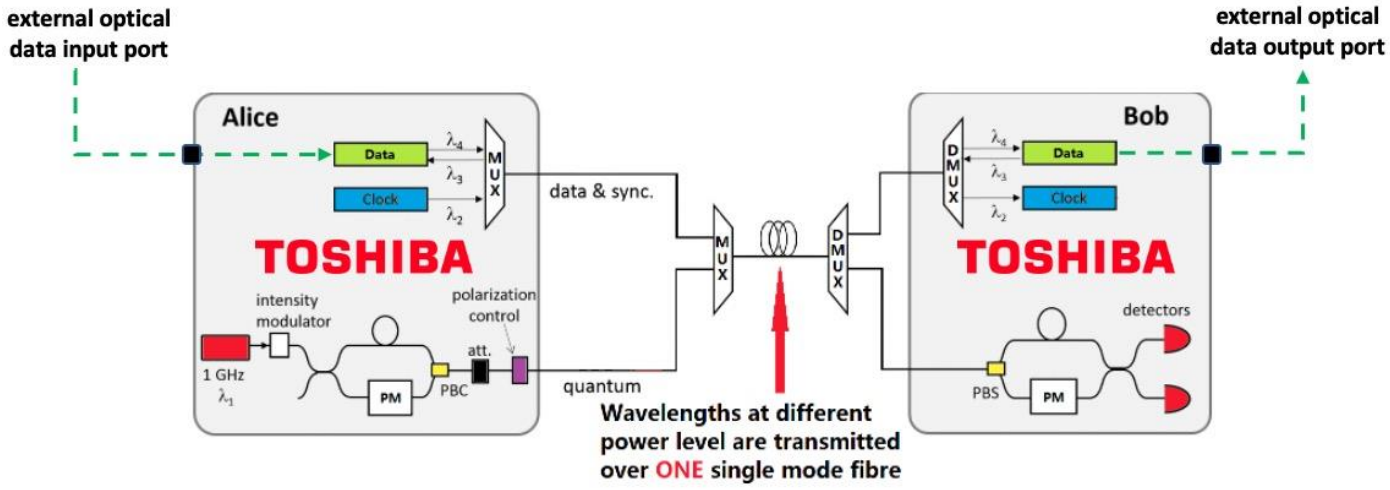


Figure 2.5.2 Scheme for multiplexing QKD with classical data

(NB: the two squares in the figure are the internal structures of Alice and Bob instruments, and there is an interface on Alice to inject optical data and one output port on Bob)

a) *Amplified spontaneous emission (ASE)*

As we all know, the ideal noiseless amplifier does not exist [109]. In the case of an optical amplifier, the basic noise comes from spontaneous emission. The ASE in the actual EDFA has a broadband bandwidth of tens of nanometers. Within the spectrum bandwidth of the quantum channel, it can be regarded as a broadband noise source with flat spectral power density. We note that a real laser source also has a wideband noise background, which can be simulated from a virtual optical amplifier as ASE.

The average ASE photon number in one spatiotemporal mode is given by [110]:

$$\langle N_{ASE} \rangle = 2n_{sp}(G-1)hv \qquad \text{Eq (9)}$$

Here factor 2 accounts for the two orthogonal polarization modes. *G* is the gain of the EDFA, and $n_{sp} \geq 1$ is the spontaneous emission factor. If spontaneous emission is the only noise source (no excess noise), $n_{sp} = 1$.

In practice, the excess noise of an EDFA is commonly quantified by its noise figure (NF). In the unsaturated regime, NF is related to n_{sp} by [110]

$$\mathrm{NF} = \frac{1+2n_{sp}(G-1)}{G} \qquad \text{Eq (10)}$$

In the high-gain range(G≫ 1), NF≅ $2\mathrm{n_{sp}}$.

In general, the ASE power is much lower than the classical signal. However, it's bandwidth is much wider and extends to the quantum channel. Therefore, ASE can cause in-band noise. Fortunately, the MUX used by the Alice end acts as a bandpass filter, greatly suppressing this in-band ASE noise. Given across the strait of isolation MUX is deduced ξ_1, in-band ASE photon number (per space-time mode) at the output of the MUX is defined as[110],

$$\langle N_{ASE}^{(A)} \rangle = 2\xi_1 \mathrm{n_{sp}}(G-1) \qquad \text{Eq (11)}$$

In this thesis, the “out-of-band” ASE noise were not taken into consideration since they are significantly weaker than the classical signals themselves.

b) *Leakage from the classical channel*

Although the wavelength of the classical signal is different from that of the quantum signal, due to the limited isolation of DEMUX, a small part of the classical signal will leak into the quantum channel. In the BB84 QKD system, this leakage leads to out-of-band noise, which

can be further reduced by using a spectrum filter at the receiver end. In the Gaussian modulated coherent state (GMCS) QKD system, this leakage puts the noise photon in LO's "mismatched mode".

We define the power of the classical signal output from the communication fibre as P_{out}. Given the isolation of the DEMUX ξ_2, the power of the leakage signal received by Bob is $P_{leak} = \xi_2 P_{out}$. The average leakage photon number per second is[110]

$$\langle N_{leak}^{(C)} \rangle = \frac{\xi_2 P_{out}}{h\nu} \qquad \text{Eq (12)}$$

Here h is Planck's constant and ν is the frequency of the classical signal.

c) Spontaneous Raman scattering (SRS)

When the strong classical signal is propagated along the optical fibre, noise photons of different wavelength will be generated through various nonlinear optical processes. If the wavelength of the noise photon is the same as the wavelength of the quantum signal, they cannot be filtered out at the receiving end, resulting in in-band noise. The results show that SRS is the main nonlinear process when the quantum channel is in the short wavelength of the classical channel [87] [107].

The spontaneous Raman scattering noise power within a bandwidth of $\Delta\lambda$ (measured at the end of optical fibre in Figure 2.4) is given by [87]

$$P_{SRS} = P_{in}\beta z \eta_{ch} \Delta\lambda = P_{out}\beta z \Delta\lambda \qquad \text{Eq (13)}$$

Here β is the spontaneous Raman scattering coefficient, P_{in} (measured at input of optical fibre in Figure 2.4) is the input power of the classical signal, z is the fibre length and η_{ch} is the transmittance of the optical fibre.

To estimate the noise photon number per spatiotemporal mode, we first use the relation $\nu = c/\lambda$ to determine the total mode number corresponding to a bandwidth of $\Delta\lambda$ and a time window of $\Delta t = 1s$ to be $N_{mode} = |\Delta\nu\Delta t| = \frac{c}{\lambda^2}\Delta\lambda$ and c is the speed of light in vacuum.

Given that the insertion loss of DEMUX is η_{DMU}, the in-band SRS photon number(per spatiotemporal mode) measured at the output of DEMUX can be quantified as [110]

$$\langle N_{SRS}^{(C)} \rangle = \frac{P_{SRS}}{h\nu N_{mode}} \eta_{DMU} = \frac{\lambda^3}{hc^2} P_{out}\beta z \eta_{DMU} \qquad \text{Eq (14)}$$

d) Four-wave mixing (FWM)

FMW is a third order nonlinear process produced by the χ^3 nonlinear fiber in the presence of two or more pumps. In order for the FWM process to be effective, phase matching conditions are required. Although FWM may be a major source of noise at very short distances, it is much weaker than Raman scattering at the actual fibre length [106]. In addition, FWM can be effectively suppressed by optimizing channel structure [106, 107] or adopting polarization multiplexing [78]. In this thesis, we simply ignored FWM.

2.5.3 Toshiba system specification and T12 protocol

This research project is a collaboration with organizations such as Toshiba European research centre and BT. Toshiba provides equipment for QKD parts, so before the start of the research, preliminary exploration and studies on the Toshiba system has been done.

For quantum communication systems, information is transmitted between a transmitter and a receiver by means of a single quantum encoded photon, such as a single photon state. Each photon carries a bit of information encoded on one of the properties of the photon, for instance its polarization, phase, or power level, known as a quantum signal. Photons can even carry more than one bit of information, for example, by using properties such as angular momentum [111]. For majority forms of quantum key distribution, Alice and Bob aim to encode quantum bit by using two or more non-orthogonal bases. Quantum mechanics indicates that the measurement of a photon by Eve, without knowing the encoding basis of each photon in advance, will definitely lead to a state changes for part of the photons. These changes in photon states will lead to errors in the bit values sent between Alice and Bob. By comparing parts of their original string of quantum bits, Alice and Bob can theoretically determine if Eve has captured the information from them.

Toshiba has been working to optimize the architecture of the quantum access network and reduce the scattering of light in optical fibres, so that the number of quantum users in the dual feeder network reaches 128. This access network provides connectivity between multiple user endpoints, each of which has a traditional GPON router and a core network or metro network, and each GPON router has a QAN transmitter for quantum key distribution. Optical networks (PONs) is an economical and efficient way of connecting passive power distributors to transmit signals from GPON network terminals (including QAN receivers) to GPON network terminals. Full power transmission of GPON signals allows for optimal compatibility with existing components [93].

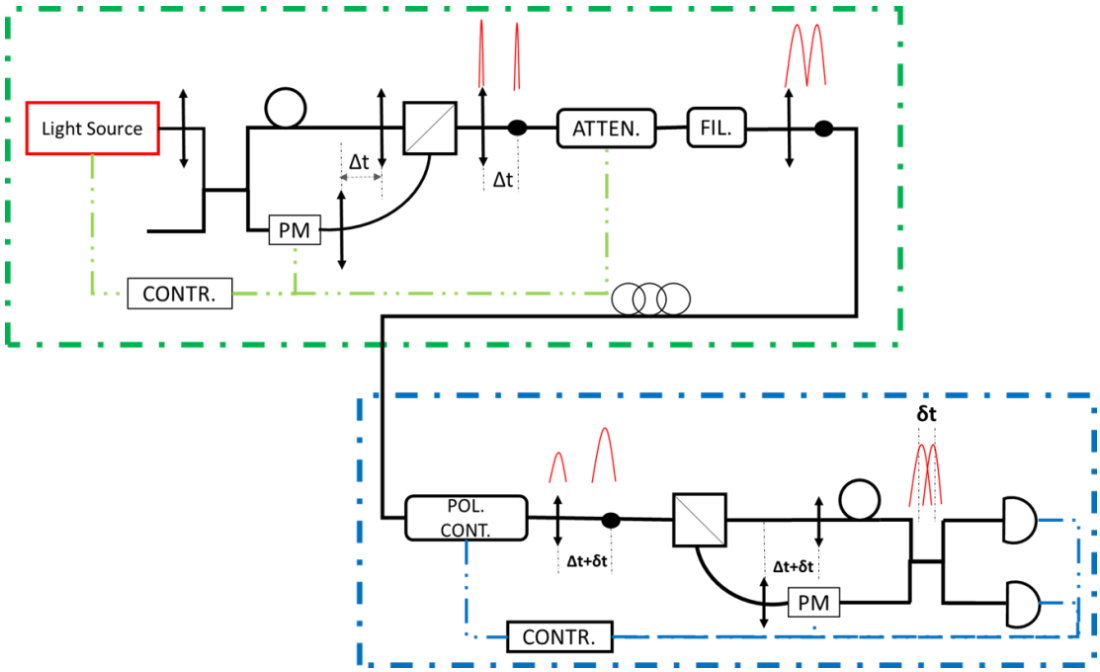


Figure2.5.3 Schematic of Toshiba QKD system

A schematic of a Toshiba quantum communication system having a band pass filter and an attenuator is shown in Figure 2.5.3 which is the system utilized in this thesis.

The upper half of the system is a transmitter, which includes a light source that generates short pulses of linearly polarized light that travel along the slow axis of the polarization-maintaining fibre. However, although in the system shown above, light travels along a slow axis, in other systems the light source can be coupled to the fibre, for example where light travels along a fast axis. The light pulse then enters an asymmetric Mach Zehnder interferometer (MZI), which in this case ACTS as a phase encoder encoding random critical information.

The Mach-Zehnder Interferometer is constructed using polarization maintaining fibre. First, the light pulses on entering the MZI pass through a coupler that splits the incoming light pulses into two paths. The first path comprises a longer arm (i.e. the upper arm in the diagram) of the interferometer using an optical delay loop. The other shorter path comprises a phase modulator that encodes random key information onto the light pulse. Due to the variation in the length of two arms, light pulses that follow either the short path and the long path suffer a temporal separation Δt. This temporal separation may be set to $\frac{1}{2}$ the inverse clock rate of the QKD system. The pulses are then combined at a polarizing beam splitter (PBS). The PBS has the property that one of the input arms polarization is rotated by 90 degrees. This results in an output which has a polarization that can be decomposed into two orthogonal polarizations

separated by a short time Δt. The pulses are then attenuated to the single photon level using an optical attenuator resulting in single photon pulses and before being emitted from the transmitter into an optical channel which is the optical fibre in this thesis.

The light pulse from the communication channel enters the receiver, the lower half as shown in the figure above. First, the pulse enters the polarization controller and is sent through PBS. The polarization controller is adjusted to correct any rotation of polarization that occurs during fibre optic transmission. This resulted in two orthogonal light pulses colliding with these polarizations into PBS.

The polarization beam splitter directs the light pulse to the long or short arm of the MZI containing the phase modulator based on the input polarization of the light phase. The receiving terminal phase modulator is used to decode the random key information on the optical pulse. In the PBS inside the transmitter, the PBS rotation at the receiver end comes from the polarization of the different arms. Therefore, the two outputs have the same polarization. With the correct input polarization, one of the two light pulses travels along the long arm of the transmitter interferometer and the other along the short arm. Thus, the delay loop cancels out the time difference between the two light pulses Δt, and since the two light pulses completely overlap, the optical interference results in the final beam-splitter.

In the above described system function ideally, there are the following assumptions:

(i) The two optical pulses from each arm of the decoder arrive at the same time at the final beam splitter;
(ii) The optical frequency of the light source does not time vary across the optical pulse;
(iii) The two optical pulses from each arm of the decoder arrive at the final beam splitter with the same intensity.

Requirements (i) - (iii) shall be satisfied to maintain high interferometric visibility. However, if there is a polarization degradation mechanism in the fibre link, these requirements may not be fully met. Polarization degradation mechanisms include polarization rotation, polarization mode dispersion and polarization dependent loss.

Each optical element in the transmitter is controlled by an electronic controller whose purpose is to control the attenuator in real time, for example by monitoring the qubit bit error rate (QBER).

2.5.4 Phase modulation scheme

Figure 2.5.4 illustrates a fundamental Mach-Zehnder interferometer set-up. This set-up comprises two beam splitters and mirrors and a phase modulator. The light is split and recombined by the beam splitter. Two detectors are placed at the two output ends of the interferometer to measure this interference. It is worth noting that any phase change between the transmitted beam and the reflected beam at the beam splitter is possible, but for simplicity we assume that the phase change is π and 0 when the beam is reflected at the beam splitter along the transmission.

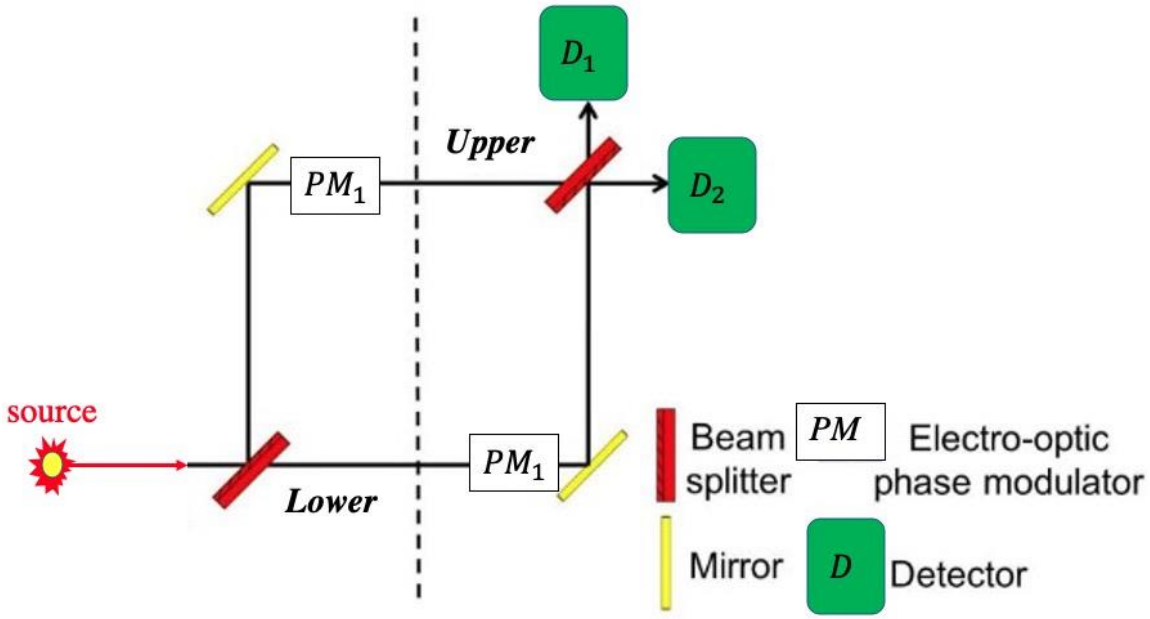


Figure 2.5.4 Mach-Zehnder interferometer

Now, different contributions to each detector are considered. Initially, we assume that the phase modulator are set to zero phase change to the light,

Detector D_1: For the upper path, a phase shift π comes from the reflection first beam splitter and another π from the mirror, giving a total phase shift of 2π. For the lower path, a phase shift π reflection is from the mirror. These two phase shift are out of phase and hence will add destructively resulting no light at Detector 'D_1'.

Detector D_2: For the upper path, a phase shift π comes from the reflection first beam splitter and another π from the mirror, giving a total phase shift of 2π. For the lower path, a phase shift π reflection is from the mirror and another π comes from the final beam splitter. These two phase shift are in phase and hence will add constructively interference at Detector 'D_2'.

Providing the phase modulators $PM_1 PM_2$ apply phase shifts of π and 0 respectively, then the results can be reversed which will be constructive at D_1 and destructive at D_2. So, changing the phase shifts can result in reversed output.

This set-up was designed for conventional optical communication but also applies to single photon level quantum key distribution. For the BB84 and T12 protocol introduced in previous sections, two orthogonal bases are used. In these cases, Alice encodes bit values 0 and 1 onto 0 and π for the first set of basis and $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$ for the other set of basis. On the contrary, Bob will measure each of the photon by using either 0 phase shift for the first set of basis and $\frac{\pi}{2}$ for the other set.

Input qubit	$\boldsymbol{PM_1}$	$\boldsymbol{PM_2}$	$\boldsymbol{PM_1 - PM_2}$	**Output qubit**
0	0	0	0	0
0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	
1	π	0	π	1
1	$\frac{3\pi}{2}$	0	$\frac{3\pi}{2}$	
1	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	π	1
1	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	
0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0
0	0	$\frac{\pi}{2}$	$\frac{3\pi}{2}$	

When the phase difference term $(PM_1 - PM_2)$ is $\{0\,\pi\}$, the outcome can be speculated and confirmed as shown in the table above and this occurs when both Alice and Bob use the matching bases. On the other hand, when the phase difference is $\{\frac{\pi}{2}, \frac{3\pi}{2}\}$, a random result is obtained since there is equal probability that the photon is either measured by detector 'D_1' or 'D_2' when incident on the final beam splitter.

This phase modulation scheme is for a free space system and becomes an optic-fibre-based phase modulation system when upper and lower paths are replaced with fibres. However, practical Alice and Bob are separated at least few kilometres away and such a distance is much longer than the theoretical two path/fibre difference. Hence, the asymmetric Mach-Zehnder interferometer for both Alice and Bob were proposed and improved to Toshiba system as shown in Figure 2.5.3.

2.6 Summary

The recent advancement in the field of QKD includes Mbps secure key rates [112, 113], long term operation [114] and the coverage of fibre length up to 260 km [6, 115]. A high bit rate QKD system was briefly introduced. QKD has also been realised in numerous network field trials [94, 97]. But QKD protocol execution involves steps such as authentication, error correction and privacy amplification and these are carried out on a separate public channel. Also, subsequent applications require support of classical data communications.

One option is simply to use separate fibres for the quantum and classical, that is data channels. However, in this case, the quantum fibre does not contain any other signal traffic and is referred to as dark fibre. The data channel fibre need not be dark and can contain many data signals. It is preferable for data and quantum signals to be simultaneously transmitted through a single fibre. Nevertheless, to date, most experiments and field trials have been performed on dark fibres. As dark fibre is a scarce and expensive resource, there is a pressing need to enable the coexistence of QKD with data signals on the same fibre.

Optical signals can be combined on a single optical fibre using wavelength division multiplexing technology utilising various wavelength of light. This technology supports bi-directional communication as well as boosts the information carrying capacity of an optical fibre [74]. White light is made up of different wavelengths and in a WDM system, at the transmitter side the wavelengths can be combined by using a prism or a diffraction grating type optical filter and sent through the optical fibre. One the receiver side, the same filters can be used in reverse to separate these distinct colour/wavelengths.

Iris Choi et al have presented results from the first field trial of a quantum secured DWDM transmission system with real-time 10Gb/s layer-1 data encryption over installed fibre of 26 km. Coexistence of quantum keys and up to 4 × 10Gb/s encrypted data is demonstrated over a single installed fibre. Secure key rate of 160 kbps has been achieved in presence of error free 4 × 10Gb/s data. A system power margin of > 10dB for the 10Gb/s channels was maintained throughout the field trial providing ample margin for further capacity and reach increase. This also confirms the robustness and ease of implementation of QKD systems. The experimental results represent an important step towards mass deployment of ultra-secure high speed data networks employing novel quantum technologies [116].

K. A. Patel et al have shown that single-photon based QKD systems can be deployed in a DWDM environment. In these systems, temporal filtering is intrinsic to the single photon detectors and spectral filtering is achieved with low-cost off-the-the-shelf telecom components. Our QKD system allows a secure key rate of 2.38 Mb/s over 35 km fibre and a maximum length reach of 70 km, in the presence of error free bidirectional 10 Gb/s data. They have also demonstrated high bit rate QKD with the standard data laser power of 0 dBm. These positive results show the potential of high speed QKD for securing future communication infrastructures.

In a word, QKD has huge potential and is valuable to be combined with exist infrastructure of classical data system even though there are still distance, secure rate, noise etc. limitations. It is then well worth to studying the effect of each factor on system performance and corresponding optimisation method.

Chapter 3. Characterisation for a Hybrid QKD Network

Specifications of the quantum system and the QKD protocols which are used in this research have been described in Chapter 2. However the practical operation of the system can be affected by different internal and external factors and it is very important to target the adverse impact. In addition, one must optimise the system performance for future larger scale hybrid quantum network implementations. Thus, this chapter discusses how the secret bit rate and the optimized parameters are dependent on various system properties, such as detector dark count, transmission loss, and noises.

3.1 Calculating the rate

For any given protocol, there is a simple linear program that can be used with some statistics from Bob's data to strictly limit the maximum number of secure single-photon signals (SPS). Therefore, there is also a quadratic programming to determine the limit of bit error rate (BER) in SPS. In both cases we assume that the intensity j is clear. The length of the generated secret key is made up of SPS plus a dark count [117] minus the amount of information displayed during the error correction process, minus the amount of privacy restrictions required. The secret key rate formula we use in the system is very similar to the form of GLLP [3], but its security is actually a limited statistical derivation of Koashi's security proof [118]. For the numerical study reported in this work, we use:

$$\mathrm{K} = \mathrm{RN} = \sum_j (S_j + D_j - f_{EC} \cdot C_j \cdot H_2(BER) - f_{PA} \cdot S_j \cdot H_2(b_1^{max})) \qquad \text{Eq (15)}$$

where the summation is only of the j's that label the signals that encode secret key bits, K is the length of the key, R is the key rate, N is the session length measured in the number of signals sent, S_j is the lower bound on the SPS and D_j is the lower bound on the dark counts, C_j is the number of total signals that Bob received from decoy state j, $H_2(\cdot)$ is the binary Shannon entropy function and b_1^{max} is an upper bound on the bit error rate of only the SPS. Efficiency factors f_{EC} and f_{PA} respectively relate how close error correction and privacy amplification are to the Shannon limit. The simulations here use f_{EC} = 1.2 and $f_{PA} = 1 + 1.53(b_1^{max})^{-0.54} S^{-0.44}$, where S = $\sum_j S_j$ is the bound on the total number of SPS contributing to the secret key. (The expression for f_{PA} is a rough numerical fit we have derived for calculating the typical number of strings needed to describe the output of a binary symmetric

channel with high confidence, as needed for computing privacy amplification in Koashi's approach [18].)

3.1.1 Sifting

In the sifting step, Alice and Bob use a public channel to communicate information related to their measurement, in particular what basis they used to prepare or measure their qubits and at what times they registered a detection event. They do not disclose the measurement result. As it is introduced in Chapter 1, it follows that whenever Alice and Bob use the same basis, they should get correlated bits. The process of discarding the bits in the cases where they used different bases is called sifting. The ensemble of bits remaining after this basis reconciliation forms the sifted key. The sifted key generation rate is given by:

$$R_{sifted} = sR_{raw} \qquad \text{Eq (16)}$$

where s is the sifting parameter, that is the fraction of bits for which the bases were the same.

If there are no errors in the quantum cryptography system, then a potential eavesdropper, referred to as Eve, cannot intercept the transmission and make a measurement that will yield information on the quantum state of the system without causing an unavoidable back action. This will introduce errors in the transmission and will therefore reveal the presence of the eavesdropper. In this case, the sifted key is unconditionally secure. In any practical communication system, however, errors naturally occur due to imperfections in the individual components, such as the transmission line or the detectors. Errors caused by the system cannot be distinguished from errors due to eavesdropping. Thus, in practical systems, the statement that any eavesdropping will unavoidably cause errors and reveal the eavesdropping, is not a sufficient security proof. There is always a baseline system error rate, so we must ensure that some information about the quantum transmission has been leaked. Consequently, we must be able to put a bound on the amount of information leakage given the error rate. Practical QKD systems handle system errors and eavesdropping by complementing raw quantum transmission and sifting with two important additional steps: error correction and privacy amplification. Processing in both of these steps can be performed using a public channel, it does not require the exchange of additional qubits [119]. These steps are described in the following section.

3.1.2 Error detection

The dual purpose of the error correction step is to correct all error received bits and give an estimate of bit error rate. In particular, Alice gives Bob some additional information about her key, which will allow Bob to find and correct all the wrong bits. For example, Alice and Bob can group their bits into segments and check parity for each segment, optimizing the size of the segment as the error correction process continues. Since this information is sent over a public channel, error correction inevitably reveals other information to the eavesdropper. This information leakage must be kept as small as possible. The minimum number κ of bits that Alice and Bob must exchange to publicly correct their strings is a result of a central classical information theory, Shannon's silent encoding theorem [120]. In the case we are interested in, each bit of transmission is incorrect, and the error probability of each bit of transmission is e, the theorem asserts [121]:

$$\lim_{n\to\infty} \frac{k}{n} = -e \log_2 e - (1-e)\log_2(1-e) \equiv h(e) \qquad \text{Eq (17)}$$

where n is the length of the sifted key. Unfortunately, Shannon's theorem has a non-constructive proof, which means that we know there exists an error correction scheme disclosing only κ bits but the theorem does not provide an explicit procedure for this scheme. An error correcting algorithm should ideally operate very close to this limit. At the same time the algorithm should be computationally efficient otherwise the execution time may become prohibitively long [62, 121].

Error correction algorithms can usually be divided into two classes, unidirectional and bidirectional. In a unidirectional algorithm information flows only from Alice to Bob. Alice provides Bob with an additional string which he uses to try to find his errors. This makes it difficult to design algorithms that are both computationally efficient and operate near the Shannon limit [122, 123]. In a bidirectional algorithm information can flow both ways, and Alice can use the feedback from Bob to determine what additional information she should provide him, which makes it easier to approach the Shannon limit. These two error correction algorithms classes can be further subdivided into algorithms that discard errors and algorithms that correct them. Discarding errors is usually done to prevent additional side information from leaking to Eve. By correcting the errors, we allow for this additional flow of side information, which can be accounted for during privacy amplification. Since privacy amplification is typically a very efficient process, algorithms which correct the errors tend to perform better [124].

3.1.3 Privacy amplification

In order to interpret the information leaked in the original quantum transmission process, the last step of privacy amplification is to carry out in the error correction process. In privacy amplification, the error-corrected key is compressed into a final security key that can be encrypted as needed. The compression required depends on how much information have been possibly leaked to the eavesdropper in the previous phase of transmission [125-127].

For security to be useful, it must limit the amount of information leaked during quantum transmission and error correction, and relate it to the amount of compression that must be applied in privacy amplification. For the most deeply studied protocol, the BB84 protocol, the earliest work in this area was considered to be the simplest type of attack, known as interception and replay attacks [127-129]. Three types of generalized attacks have been considered: individual, collective, and concerted. In a single attack, the eavesdropper is limited to wrapping a quantum probe independently around each qubit. The probes are stored in quantum memory until the measurement benchmark is published, and then each probe is measured independently. Any measurement not prohibited by quantum mechanics is allowed. For the BB84 protocol, security against such attacks has been demonstrated in [46, 123, 130, 131], and these proofs have been extended to actual photon sources in [54]. Collective attacks are similar to individual attacks, but Eve can now use a quantum computer to make global measurements of all the probes that are considered to be a single quantum system. This enabled her to take advantage of the relevance introduced in the privacy amplification process of error correction and information exchange. Such correlations could potentially perfect the eavesdropper's quantum measurements. Security against collective attacks has been proven against BB84 in [132]. The most common type of attack is the coherent attack, in which eavesdropping treats the entire quantum transmission as a system entangled with a very large dimensional probe in any initial state. For the most general scenario, an security proof for an idea [46] [118] and an actual qubit source [133] have been proposed and proved. Security proof for individual, collective, or coordinated attacks, as well as several assumptions about the BBM92 protocols [37, 133-135] and B92 protocols [136], also have been conducted.

In this work, practical quantum communication systems and network are necessary. However, the ability to perform collective or coherent attacks is well beyond today’s technological capabilities or even in the foreseeable future. As a consequence, we will restrict our discussion in this thesis only to individual attacks. Even these attacks assume very advanced capabilities

because Alice and Bob can delay the public base announcement for an arbitrarily long time, thus Eve is assumed to possess a quantum memory with an infinitely long coherence time, which is not available today. Nevertheless, general individual attacks are close to being realistic so it is very important to prove the security of a quantum key distribution algorithm against these attacks. Thus, in the following, Eve is restricted to attack individual qubits, and she is not allowed to perform a coherent attack consisting of collective quantum operations and measurements of many qubits with quantum computers. This not only corresponds to a realistic scenario but it also makes the mathematical treatment of the problems we will consider simpler and more intuitive.

The role of the privacy amplification step is to deduce the shrinking factor τ by which the error corrected key has to be compressed, given the error rate calculated in the error correction step and the bound on the amount of information leaked during the previous phases of the transmission, so that Eve's information about the final key is lower than a specified value. This calculation is performed using the methods of the generalized privacy amplification theory [137], which makes the worst case assumption that all errors are potentially caused by eavesdropping. The result of this theory states that the length of the final key should be set to [137]:

$$r = n\tau - k - t \qquad \text{Eq (18)}$$

where n is the length of the sifted key, k is the number of bits disclosed during error correction, t is a security parameter, and the shrinking factor τ is given by the expression[137]:

$$\tau = -\frac{\log_2 p_c}{n} \qquad \text{Eq (19)}$$

In the above expression, p_c is the average collision probability, an important quantity in the analysis of privacy amplification, which is a measure of Eve's mutual information with Alice and Bob.

Instead of the length of the final secure key given above, it is more useful to calculate the normalized communication rate in units of bits/s.

If N is the length of the transmission, then $n = NR_{sifted}$, and the communication rate, or else secure key generation rate, is defined as[137]:

$$R = \lim_{N\to\infty} \frac{r}{N} = \lim_{n\to\infty} R_{sifted}\left(\tau - \frac{k}{n} - \frac{t}{n}\right) \qquad \text{Eq (20)}$$

However, an algorithm that is computationally feasible and works at this ideal limit does not exist. All practical algorithms are inefficient to some extent, and this is accounted for by introducing a function f(e), defined as the ratio of the algorithm performance to that of the Shannon limit. Thus,

$$\lim_{n\to\infty} \frac{k}{n} = -f(e)[e\log_2 e + (1-e)\log_2(1-e)] = f(e)h(e) \qquad \text{Eq (21)}$$

Combining the above, the final expression for the secure key generation rate is,

$$\mathrm{R} = R_{sifted}\{\tau + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\} \qquad \text{Eq (22)}$$

where R_{sifted} and τ depend on the QKD protocol and system parameters.

3.2 Detector characterisation

3.2.1 Performance parameters of an APD

Here, the key figures of merit for APDs are summarised.

Single photon detection efficiency: The single photon detection efficiency is defined as the probability of detection given that a photon is incident on the device [138-140].

Dark count probability: The dark count probability is defined as the probability of detection in the absence of a photon. Dark counts in semiconductor devices are stimulated by defects. Dark counts can derive from either thermally or tunnelling generated carriers. In the case of thermal generation, the carriers move from valence band to conduction band either directly or via a defect state due to thermal excitation. On the other hand, tunnelling generation is due to carrier tunnelling from either valence band to conduction band or defect to conduction band [141]. The dark count probability P_D is directly proportional to the temperature, T, and given by [142, 143]:

$$P_D \propto \frac{n_i}{\tau_e} \propto T^2 e^{\left(\frac{-E_\alpha(T)}{kT}\right)} \qquad \text{Eq (23)}$$

where n_i is the APD material intrinsic carrier density, τ_e is the effective lifetime of the carriers, $E_\alpha(T)$ is the carrier thermal activation energy and k is the Boltzmann constant. From the equation above, the dark count level can be controlled by tuning the temperature T of the device. The APDs are thermoelectrically cooled to -30°C and the source of dark counts is predominantly due to thermal generation of carriers.

After-pulsing: After-pulsing is the creation of false counts that arise from the emission of carriers, which are trapped in the multiplication region during a previous detection event. During the avalanche development in an APD, carriers generated can be trapped in defects within the bandgap. These defects (energy states) in the semiconductor can be classified as donor states for electron defects (or traps) and acceptor states for hole defects (or traps), as shown in Figure 3.2.1.1. As this process is thermal, the timescales for de-population are long, which prevents the operation of the APDs at high frequencies. After-pulsing, P_A, can be expressed as a function of time, t ,[140, 144, 145]

$$P_A(\mathrm{t}) = P_{ava}\frac{N_{ft}}{\tau_{trap}}e^{(-\frac{t}{\tau_{trap}})} \qquad \text{Eq (24)}$$

where $P_{ava}$is the avalanche probability, N_{ft} is the number of filled traps, τ_{trap} the de-trapping lifetime and this de-trapping lifetime is related to temperature as follows

$$\tau_{trap} = \frac{1}{\sigma\nu N}e^{(\frac{E_{trap}}{kT})} \qquad \text{Eq (25)}$$

where σ is the trapping cross section, ν is the average thermal velocity of carriers ($\nu \propto T^{1/2}$), N is the effective density of states ($N \propto T^{3/2}$), and E_{trap} is the activation energy of the traps. As a result, the de-trapping time τ_{trap} is inversely proportional to T^2 and hence at lower T the detrapping lifetime increases as does the after-pulse rate.

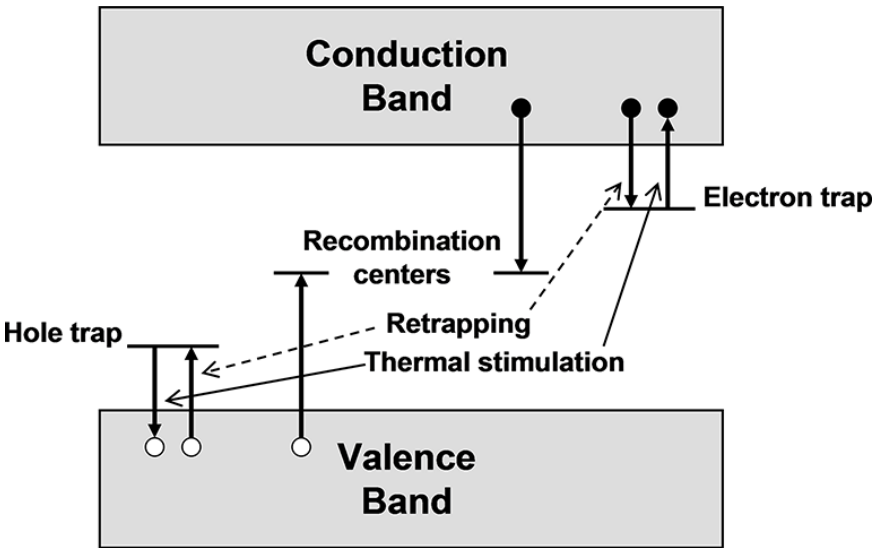


Figure 3.2.1.1 Schematic of Band energy diagram including the trap energy states

On the other hand, dark counts decrease with temperature. Hence, there is a trade-off when optimising the operating temperature of the device. As is the case of dark counts, afterpulsing depends on the defect concentration in the material. So in order to reduce afterpulsing, the

material quality should be improved or the carriers flowing through the device should be minimised using suitable quenching circuits.

Timing jitter: This is the uncertainty in the detection time of a photon impinging on the device. It usually stems from the avalanche noise due to the APD avalanche process [146, 147].

Dead time: This is usually regarded as the time after a photon detection event during which the detector is unable to register a count [148].

3.2.2 Impact of the dark count effect in QKD

The dark count rate varies with the material used for the detector. Detectors for telecommunication wavelengths are typically based on germanium and InGaAs/InP. These materials do suffer from high levels of impurities due to the crystal growth process. That said, APDs should be operated at lower temperatures so as to reduce dark counts caused by thermal excitations. However, too low a temperature might lead to higher after-pulsing probability because cooling slows the rate at which the traps release the charge carriers [149, 150].

The inefficient dark counts of the detector will also affect the security of the QKD system. Eve may use this imperfection to cover the error she introduces from her measurement of the single photon state. In other words, the key problem here is that Bob does not know whether his detection events arise from: single photon detection, multi photon detection, or dark counts. as a "scope" telling Alice and Bob which state comes from single photon, multi photon or dark count [151].

The performance of a single-photon detector on QKD should be evaluated by use of a quantum-bit-error rate (QBER) introduced in Chapter 1, given by [151, 152],

$$\begin{aligned} \text{QBER} &= \frac{P_{opt}P_{phot} + P_{dark}}{P_{phot} + 2P_{dark}} \\ &\cong \mathrm{P}_{opt} + \frac{P_{dark}}{P_{phot}} \\ &= P_{opt} + \frac{P_{dark}}{\mu\eta_t\eta_d} \end{aligned}$$

where P_{dark}, P_{phot}, and P_{opt} are the probabilities of getting a dark count, of detecting a photon, and that a photon went to an erroneous detector, respectively. μ is the probability that an emitted pulse will contain at least one photon. η_t is the transfer efficiency from a sender to a detector, and η_d is the quantum efficiency of the detector. The QBER that is due to the

imperfect single-photon detection is given by the ratio of the dark-count probability per gate, P_{dark}, to the quantum efficiency of a detector, hd. The transmission distance is limited by the condition that the QBER is below 15% (for a different assumption of the eavesdropper's ability, the QBER must be below 11.5%) [152]. Therefore the maximum transmission distance is obtained when P_{dark}/η_d is minimum.

Here we assume that the effect of afterpulses is negligible. The probability that a photon goes to an erroneous detector P_{opt} is expressed by

$$P_{opt} = \frac{1-V_c}{2} \qquad \text{Eq (26)}$$

where V_c is the fringe visibility of an interferometer used for QKD [153]. Transfer efficiency η_t is given by

$$\eta_t = 10^{-(L_f l + L_r)/10} \qquad \text{Eq (27)}$$

where L_f is losses in the fibre, in decibels per kilometre, l is the transmission distance, in kilometers, and L_r are internal losses in the receiver system, in decibels. Then the maximum transmission distance l is given by [77]

$$l = -\frac{10}{L_f}\log\{\frac{P_{dark(1-2e)}}{\left[e-\left(1-\frac{V_c}{2}\right)\right]\mu\eta_d 10^{-\left(\frac{Lr}{10}\right)}}\} \qquad \text{Eq (28)}$$

And this equation is used for distance prediction in the following chapters.

3.3 Noise characterisation

Due to photon–phonon interactions, photons can change their wavelength and thus compromise other channels. Depending on whether a phonon gets excited or de-exited, photons at wavelengths above (Stokes) and below (anti-Stokes) the initial wavelength are generated. Scattering off acoustic phonons (Brillouin scattering) is not critical, since the maximal frequency shift of the scattered photons is small (10GHz, in the backward direction) and therefore cannot reach adjacent channels on a 100 GHz grid. By contrast, scattering off optical phonons (Raman scattering) can lead to significant frequency shifts covering the entire C-band[103], having an intensity maximum at a shift of about 13 THz (corresponding to a wavelength shift of 100 nm at 1550 nm). Different from acoustic phonons, the more or less flat dispersion relationship of optical phonons results in frequency shifts independent of the scattering direction. This means that a wide spectrum of photons can be produced in both the

co-propagation direction and the counter-propagation direction (as opposed to the excitation signal).

As discussed in the previous chapters, transferring quantum and classical data is less costly and efficient. To execute this process correctly, Bob and Alice need to synchronize; This can be done by sending strong pulses of light between them. In order to optimize resource utilization, these classical channels should share the transmission fibre with QKD photon. In addition, from the perspective of optical networking, it is very practical to combine QKD with classical WDM optical channels [154]. Some photons in the classical channel can be spontaneously inelastic Raman scattering into the quantum channel bandwidth. This effect is characterized by bandwidth, which is proportional to the total power of the traditional channel and depends on the length of the fibre link. Another noise mechanism involves Rayleigh backscattering of the quantum channel itself. Since QKD involves the detection of a single photon, very sensitive detectors are required [115], and any background light in the fibre increases the noise level of the system and limits its performance.

Based on the model in [41] [39], the effect of spontaneous Raman scattering (SRS) generated by classical flow on the QKD system is analysed. This model is applied to the BB84 system with a weak laser source with a decoy state. This means that the strength of the quantum source is assumed to vary randomly to test whether the channel is disturbed by eavesdropping. It allows longer distances to be reached and analyses the results in a safe key-rate value, bounded below the model. Here we conservatively assume the use of infinite deceptions, and the analysis depends on the average number of photons emitted per time interval, channel losses, in-band generation of SRS, and the efficiency of the detection equipment.
The channel transmittance between Alice and Bob depends on the fibre length L, which is determined by [41]

$$\eta = \exp(-\alpha L) \times \eta_{bob}\eta_{SPD} \qquad \text{Eq (29)}$$

where α is the fiber attenuation coefficient at the quantum channel [km^{-1}], η_{bob} is the transmittance of Bob's equipment and η_{SPD} is the SPD detection efficiency. The yield of a number state containing n photons, defined as the conditional probability of a detection event at Bob's side given that Alice sends out an n-photon state, can be written, for small values ηY_0, as [41]

$$Y_n \approx Y_0 + 1 - (1-\eta)^n \qquad \text{Eq (30)}$$

where the yield for vacuum state (Y_0) is the system noise, composed by the SRS noise and the dark counts of the SPDs. For a BB84 system with two SPDs [1], $Y_0 = 2P_{dark} + \kappa P_{srs}$, i.e.,

twice the dark count probability (P_{dark}) of one detector, and the unpolarized SRS noise is assumed to be split between the two devices. The factor κ depends on the modulation format assumed for the telecom traffic and is related to its duty cycle. For phase shift-keying-based (PSK) format, this factor is 1, while for on-off keying (OOK) with return to zero (RZ), κ is $\frac{1}{4}$. The PSK-based format family represents the worst case, when the intensity of the parallel traffic is continuous in time, while in the RZ-OOK, half the bits are zero and the bits occupy half of each bit slot, which results in a smaller average optical power and a reduction of the SRS.

A laser source can be approximated to a weak coherent state, which exhibit Poisson distribution of the number of photons n per time interval, i.e., $P(n|\mu) = \exp(-\mu)\,\mu^n/n!$, given an average number of photons in each interval. The channel gain Q is composed by the sum over the gain values for each photon-number state, i.e. the probability that Bob yields a detection event given that Alice has sent an n-photon pulse [41],

$$Q = \sum_{n=0}^{\infty} Y_n\, P(n|\mu) = Y_0 + 1 - \exp\,(-\mu\eta) \qquad \text{Eq (31)}$$

Since each vacuum yield can randomly generate a count in any detector, the associated quantum bit error rate (QBER) is $\frac{1}{2}$. Furthermore, misalignment of the optical components (γ) can bring non-vacuum states to cause erroneous detection. The overall QBER can be calculated by summing over the contribution of each photon-number state relative to the overall gain [41], i.e.,

$$QBER = \frac{\frac{1}{2}Y_0 + \gamma[1-\exp(-\mu\eta)]}{Q} \qquad \text{Eq (32)}$$

The lower bound for the final secure key rate is finally written as [41]

$$Secure\ Key\ Rate\ (R) > \frac{1}{2}\{Q_1\left[1 - H_2\left(\frac{\frac{1}{2}Y_0 + \gamma\eta}{Y_1}\right)\right] - Qf(E)H_2(E)\} \qquad \text{Eq (33)}$$

and depends on the single-photon gain Q_1 and the Shannon entropy of the error $H_2(E)$. A quantum error correction inefficiency factor $f(E)$ is usually considered, which reduces the final key rate.

3.4 Hybrid system specification

For an original BB84 protocol, the coding scheme was designed to develop the quantum properties of any single photon polarization states, however phase coding schemes can also be realized [78]. These coding schemes are based on the properties of interferometers and the coding is implemented by changing the relative optical path lengths or phase between the internal arms of the interferometer which is referred to Toshiba instrument and will be introduced in Chapter 4.

The commercial QKD system used in this study comes from a Toshiba device shown in Figure 3.4.1 that reached an advanced level of secure key rate. Essentially, the way to use this in high data rate transmission is to use Toshiba transmitter and receiver (i.e. Alice and Bob), in this case. These series of Alice of Bob are used to generate key pairs and take the key pairs out of them and input them into the line card. These are 100 gigabit polarization multiplexed quadrature phase shift keying (PolMux QPSK) standard transmission systems encrypted with AES 256.

Figure 3.4.1 Toshiba Alice/Bob device

Typically, AES 256 encryption is derived from both ends using the standard Diffie-Hellman technique. But in this case, instead of using Diffie-Hellman and the current standard method, this study provides the feeding QKD signal directly from the QKD system. In the thesis, as shown in the figure below, two wavelengths were injected into Alice. And then it combines with other wavelengths, like QKD. And then on the far side, they get de-multiplexed again.

In this study, wavelength at 1530 nm is allocated for the classical wavelengths and 1550 nm for the QKD wavelengths. And due to fairly careful frequency and time domain filtering in the receiver Bob, we can operate at these enhanced key rates.

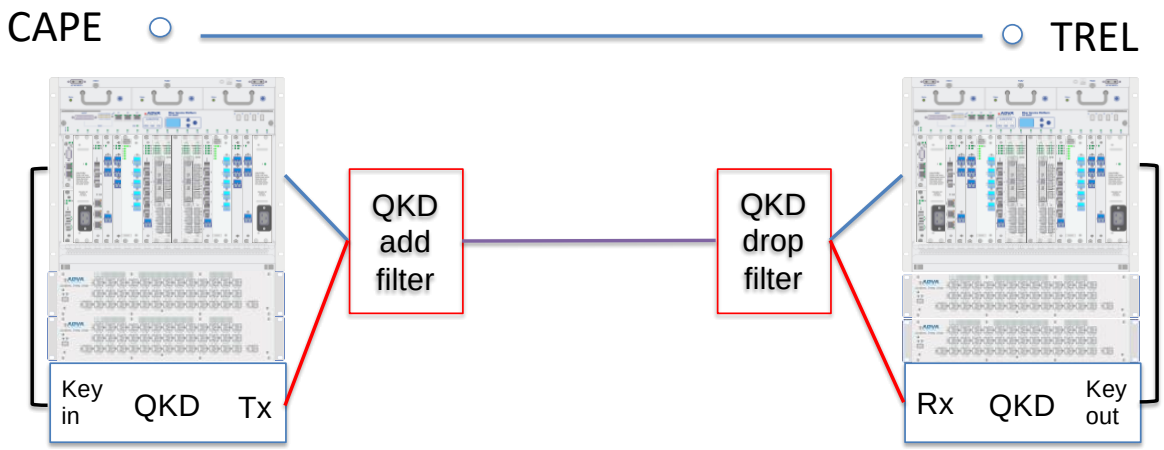


Figure 3.4.2 QKD with gigabit data line card

Figure 3.4.2 illustrated one of the links where one pair of Alice and Bob locate in this study. Data at different wavelengths including gigabits QPSK classical data at high power level and QKD keys data are transmitted straight across the three-node Cambridge quantum network without any need to regeneration.

Figure 3.4.3 Laboratory view of hybrid system

We note that network key management QKD was developed by ***Peev*** et al. [90], ***Sasaki*** et al. [94], and ***Stucki*** et al [115]. However, in this study we used ***Tanizawa*** et al. [155], a recent design which features major advantages than other network key management architectures, particularly high-speed, Mbps operations compatible with our network bandwidth.

Figure 3.4.4 shows the basic idea of the network key delivery layer, or key management. Assume that each node is trusted and can generate a "global key" buffer that is shared with peers using a one-time encryption (OTP) tunnel encrypted based upon the QKD key. In this way, the global key is quantum secure and can be used by an application through a dedicated application interface (API) based on representational state transfer (REST).

As a sample application, we used two pairs of ADVA FSP3000 racks (figure 3.4.3) installed on the CAPE-TREL link with a classic ADVA 100G cryptographic line card. Due to the bidirectional nature of the line cards, each card has an AES encryptor in one direction and an AES decryptor in the opposite direction. Each pair of line cards requests a global key from its local node approximately every 4 seconds, in other word, QKD links provide a global key every 2 seconds on average (because there are two pairs of line CARDS). The global key replaces the normal AES key normally used to encrypt 100G of data traffic. It has been calculated that the key refresh rate of a global key every 4 seconds is equivalent to the (global) bit rate of about 100 BPS. The current key exchange frequency is not limited by the AES hardware, but by the speed of the REST API, which passes each key from the QKD device to the AES engine separately. Acceleration can be achieved, for example, by transferring multiple keys and optimizing the protocol runtime. Note: the standard c-band transmission system design allows a fully loaded system to work by collecting QKD keys in parallel without any further changes.

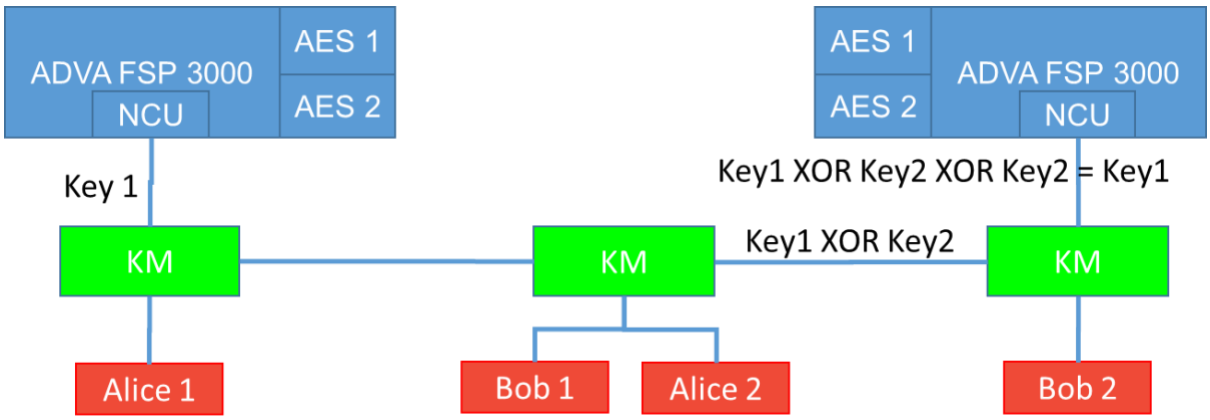


Figure 3.4.4 Key management

3.5 Summary

Chapter 3 presented the characterisation of a hybrid QKD network. Firstly several key rates in a QKD system have been derived. Because a single photon is highly susceptible to noise hence the influence and noise analysis of the single photon receiver in the system are discussed. In addition, it has introduced the noise likely generated in the hybrid system including Raman noise from high optical classical channel. The specification of the three-node ring QKD network are included as well as preliminary key-management.

Chapter 4. Hybrid QKD system performance of field trial and laboratory fibre reels

The previous chapters introduce the research background and related fundamental knowledge of this thesis such as early quantum key distribution protocol BB84. Chapter 4 describes the establishment of a preliminary model of the quantum network in Cambridge and the United Kingdom, followed by a point-to-point field trial. In addition, the comparison between the system built in the laboratory and the trial system shows that the hybrid communication system can reach the current maximum speed and high stability of the same fibre length in the actual QKD encryption communication process.

4.1 Motivation

The communication of optical fibre network is an important part of modern society. Social activities, from everyday life such as social software to public security such as banking systems, are increasingly linked to fibre-optic communications. As the importance of these networks grows, it needs to secure information between them to ensure that users can identify from each other and the data is secure so that data cannot be intercepted or eavesdropped. Quantum key distribution has been proved to be able to secure data not only to improve the security of today's communications systems [25, 132] but also to be able to cope with future eavesdropping techniques after the advent of quantum computers.

However, there are several challenges to developing a practical QKD system from a laboratory to the real world. Due to changes in environmental conditions and physical stresses, the installed fibre is always subject to stronger perturbations, which in turn cause perturbations of the transmitted quantum state. Installed fibre also suffer higher losses due to splicing, sharp bends, and inter-fibre coupling. The software and hardware of the QKD device must not only be designed to cope with all the conditions affecting the transmission fibre, but must also operate in the premises designed for standard telecommunications equipment. In addition, because systems should run continuously, they should also be designed to automatically recover from errors and protect end users from service outages.

The equipment required for the generation and reception of cryptography quantum state is designed and provided by Toshiba. The basic principles of the instrument have been introduced in the previous chapters. Using this equipment to carry out experimental analysis and actual

network construction from the most basic point-to-point model of the network is the premise of building a larger and more complex network in the future.

4.2 System theoretical limitations

4.2.1 Ideal and Poisson source performance

As described in the previous chapter, QKD is based on the production of a single photon. Unfortunately, all recent experiments are, in principle, unsafe due to real-life imperfections [39]. However, in the QKD system, the highly attenuated laser is often used as the source of single-photon generation. However, these sources sometimes produce signals that contain more than one photon. Multiphoton signals open the door to powerful new eavesdropping attacks, including photonic fission attacks. For example, Eve in principle can measure the number of photons per signal sent by Alice and selectively suppress the single photon signal. She separated the multi-photon signals, kept one for herself, and sent one to Bob. Now, because Eve has the same copy as Bob, the unconditional security in QKD [for example, the standard BB84 protocol [58] is completely compromised. To sum up, in the standard BB84 protocol, only the signal from the single photon pulse emitted by Alice is guaranteed to be secure.

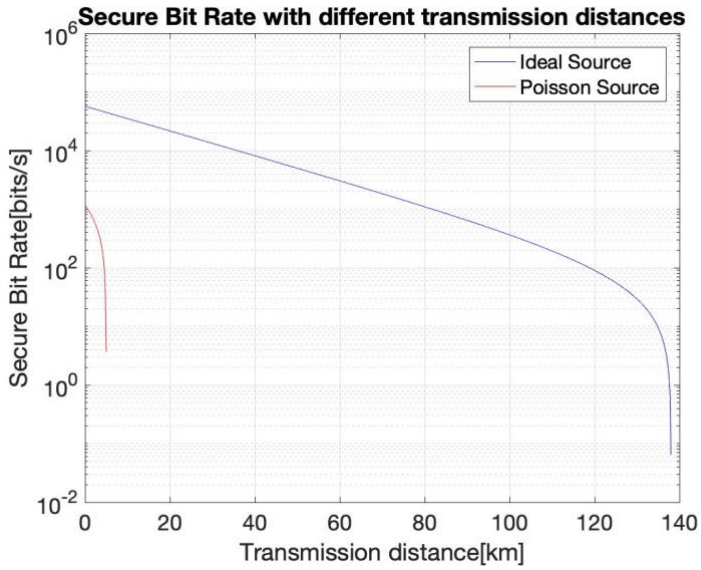


Figure 4.2.1(a) Theoretical simulation of BB84 protocol performance with perfect and Poisson source

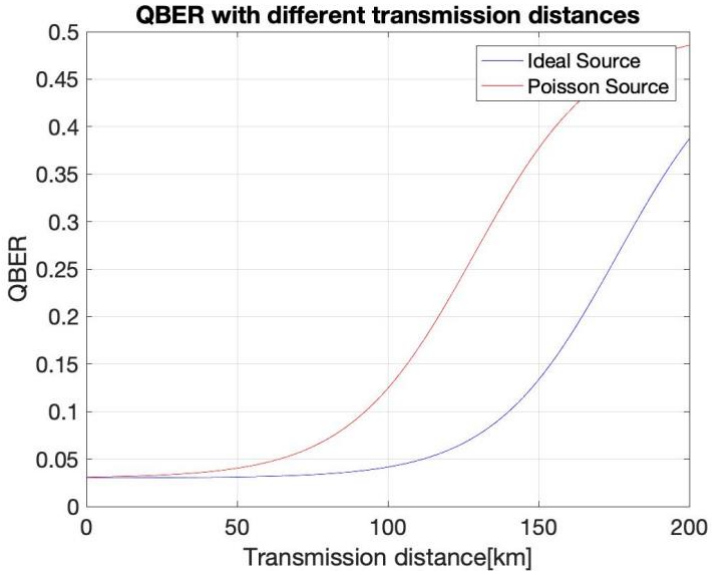


Figure 4.2.1 (b) Theoretical QBER of BB84 protocol performance with perfect and Poisson source

Theoretical plots of ideal single photon source and attenuated laser source, which is Poisson source, are shown in figure 4.2.1 plotted by ***Matlab***. Here, the communication length limit of the ideal single-photon light source system is about 130 km when only fibre loss is considered. Although the quantum bit error rate is only 5%, the secure key rate is less than 100 bit per second which is hardly possible to be utilized in real system. When using a Poisson light source, the system can only work up to few kilometres.

The parameters are as follows and works on the simulation of idea source and Poisson source.

Wavelength	1550nm
Channel loss	0.21 dB/km
Transmittance on Bob side	0.1
Error detection probability	0.03
Count probability for vacuum pulse	2e-5
Laser pulse repetition rate	2e6
Average photon number of signal states	0.1
Error rate of vacuum state	0.5
Reconciliation factor of BB84	0.5

Table 4.2.1 Specifications of ideal and Poisson source simulations

4.2.2 Decoy state QKD

The decoy-state quantum key distribution protocol (QKD) is the most widely used QKD scheme based on the basic BB84 protocol. Compared with the standard BB84 protocol, the actual QKD systems use multiple photon sources, which makes them vulnerable to photon number division (PNS) attacks. This will greatly limit the actual QKD system's secure transmission rate or maximum channel length. Using decoy technique [156], this basic weakness of the actual QKD system is generated by the use of multiple transmitter sources of intensity levels, i.e., qubits are randomly selected through the Alice intensity level (a signal state and several states of decoy), resulting in different photon counts for the entire channel. At the end of the transmission, Alice publicly announces which intensity level was used for each qubit transmission. A successful PNS attack needs to maintain the bit error rate (BER) at the receiver end, which cannot be achieved by multi-photon counts. By monitoring BERs associated with each intensity level, the two legitimate parties will be able to detect PNS attacks with a highly increased security transmission rate or maximum channel length, making the QKD system suitable for practical use. Figure 4.2.2 shows the simulation performance of the decoy state protocol, which can increase the transmission length to 100 km. However, the security key rate of tens of thousands of bits/second is still relatively low for the actual quantum network link application.

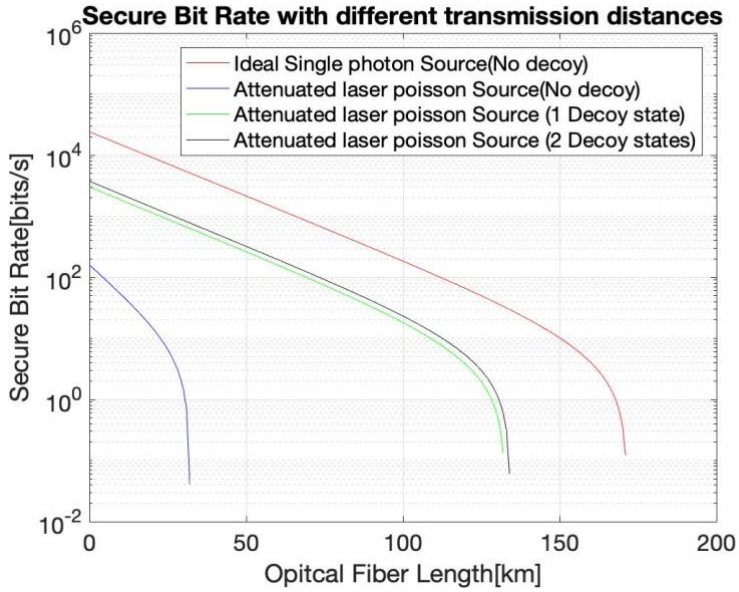


Figure 4.2.2 Theoretical simulation of Decoy state protocol performance

Wavelength	1550nm
Channel loss	0.21 dB/km
Transmittance on Bob side	0.045
Error detection probability	0.033
Count probability for vacuum pulse	1.7e-6
Laser pulse repetition rate	2e6
1 decoy state average photon number	0.12
2 decoy state average number $1^{st}/2^{nd}$ decoy	0.05/0
Average photon number of signal 1 decoy state 2 decoy state	 0.24 0.48

Table 4.2.2 Specifications of decoy state simulations

4.2.3 Cambridge quantum network

TREL have investigated the finite-size security of the efficient version of the decoy-state BB84 protocol, implemented with an attenuated laser and a decoy state technique called the T12 protocol which has advantages over the classical BB84 protocol and decoy state protocol discussed in previous chapters [42]. T12 Protocol is implemented by Toshiba's QKD device and continued to be applied in the following studies.

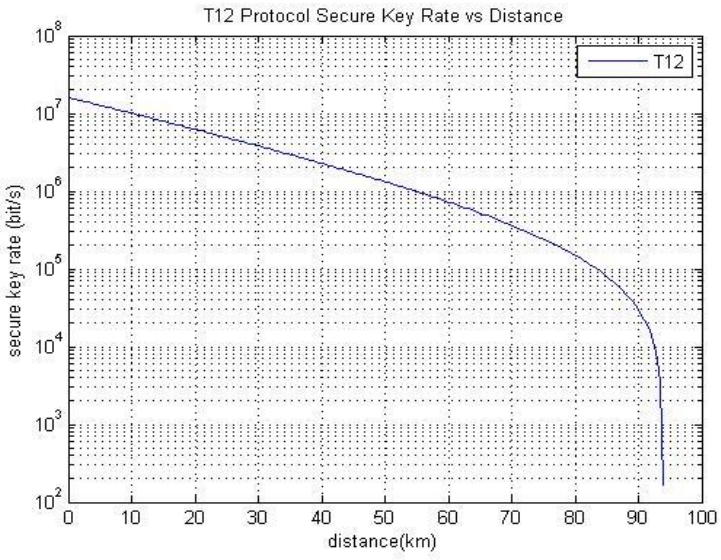


Figure 4.2.3. T12-protocol secure key rate vs distance simulation result

The secure key rate on a logarithmic scale as a function of the length of the optic fibre is plotted in Figure 4.2.3. The security key rate reduces exponentially as the fibre length increases and the trend is the same as standard BB84 and decoy state protocols. The exponentially reduce is because of the scattering in the optical fibre and loss of the standard optical fibre at 1550nm is 0.2 dB/km. Such attenuation is caused by the properties of the fibre and is often difficult to change. Some lower loss, such as 0.18 dB/km or 0.16 dB/km, can be used, but considering the cost and other factors, ordinary single-mode fibre are more widely used. In other words, an increase of 50km in the length of the fibre reduces the secure key rate by about a tenth.

All the above protocol simulations are theoretical results, and no additional several Gbps signals are combined with. In real communication systems, QKD aims to encrypt 100 Gbps classical data and both are transmitted through the same fibre. Hence noisy photons will weaken the theoretical limitations and are discussed in the following.

Wavelength	1550nm
Channel loss	0.21 dB/km
Dark count rate	2*5.9E-5
After pulse rate	0.0282
Bob efficiency	0.25
Average photon number of signal	0.42
Decoy average photon number of signal	0.042
Transmittance on Bob side	0.05
Error detection probability	0.031
Laser pulse repetition rate	1.036e9
Error rate of a vacuum state	0.5

Table 4.2.3 Specifications of T12 simulations

4.3 System experimental limitations

4.3.1 10 Gbps classical data

Figure 4.3.1 (a) shows the experiment setup to generate a 10 Gbps classical data. The traditional communication signals in the dotted box are pre-tested and calibrated before being fed into the transmitter, Alice.

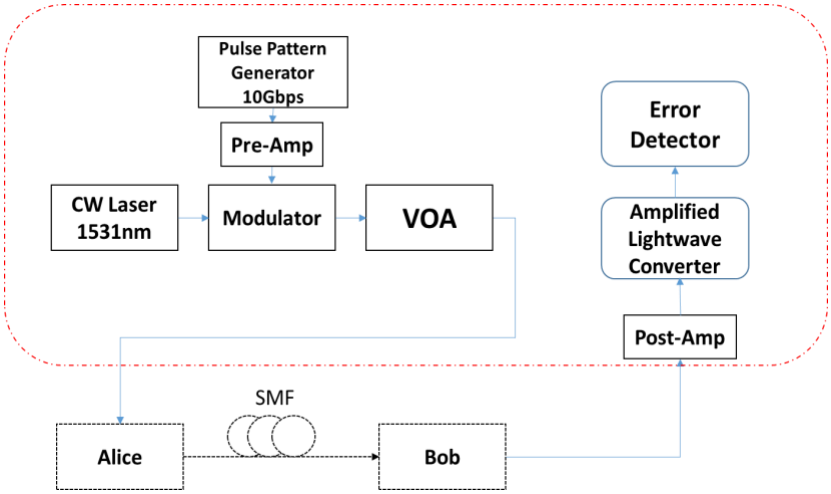


Figure 4.3.1(a)Diagram of adding external polarization controller

First, connect each instrument according to the figure above. The laser is selected for 1531nm with power less than -10 dBm to meet the requirements of the Toshiba system. The modulation mode is phase modulation and then VOA is used to protect the optical path. Two amplifiers are used in this optic circuit, where the pre-amplifier is an electronic-amplifier to match the signal power of the Pulse Pattern Generator (PPG) inject to the modulator, and the post-amplifier is an optical-amplifier aims to amplify the signal to monitor the error of the received signal.

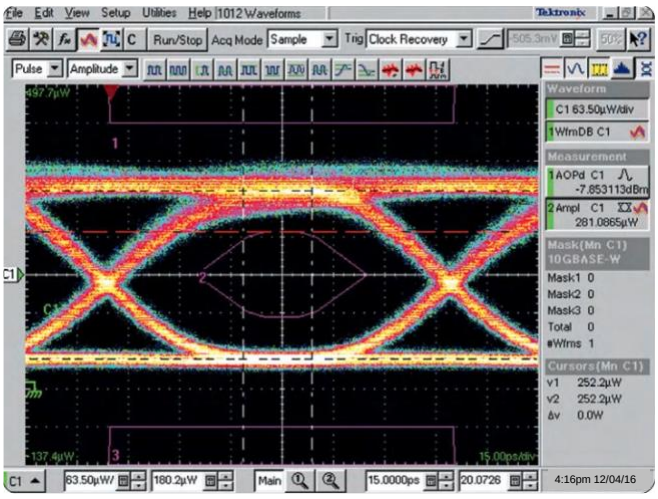


Figure 4.3.1(b) eye-diagram of the classical signal

In telecommunications, the eye diagram is an oscilloscope display in which the digital signal from the receiver is repeatedly sampled and applied to the vertical input, while the data rate is used to trigger the horizontal scan. It is a tool to evaluate the effect of channel noise and inter-symbol interference on the performance of baseband pulse transmission system. In the eye diagram, the greater the vertical opening of the eye, the clearer the edge, indicating that the received signal is more consistent with the original signal [157].

Remove Alice and Bob in the figure above and connect directly to different lengths of fibre reel. Changing the power of the incident laser, observe the changes of the eye diagram and the bit error rate. As a result, the data rate is set to be 10Gbps and the link is able to operate up to 25km (error free BER < 10^{-12}) and the power launches into fibre is up to $-8\ dBm$. However, since the input signal to Alice should not be greater than $-10\ dBm$, the optical signal is set to attenuate to $-10.2\ dBm$ before being sent to Alice, resulting in the bit error rate rising to 10^{-9}.

4.3.2 Commercial 10/100 Gbps classical data

In the actual communication process, besides ensuring low bit error rate, factors such as input signal power should be considered as well. Therefore, the above mentioned light path is difficult to be used in long-distance and high input power trial systems. In the following research, a set of commercial equipment ADVA is adopted. A pair of ADVA 10G classical encryption line cards are installed in two ADVA FSP3000 shelves and connected as shown in Figure 4.3.2 (a).

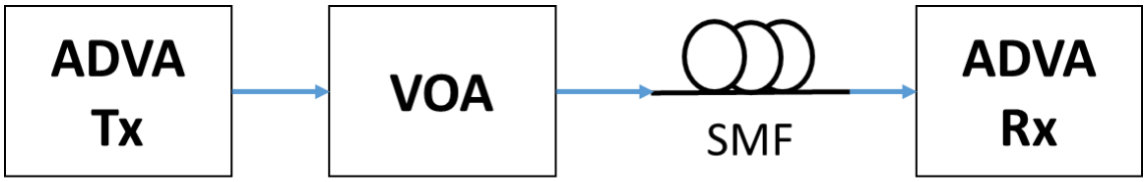


Figure 4.3.2 (a) Commercial classical data link test

As shown above, the transmitter is connected to a variable optical attenuator and then directly to the receiver. Change incident light power and record bit error rate. The attenuator is connected to a 15.6km optical fibre coil (~ 3.8dB loss), and then change the incident light power and record the corresponding bit error rate. And then replace the fibre with longer length and repeat the steps.

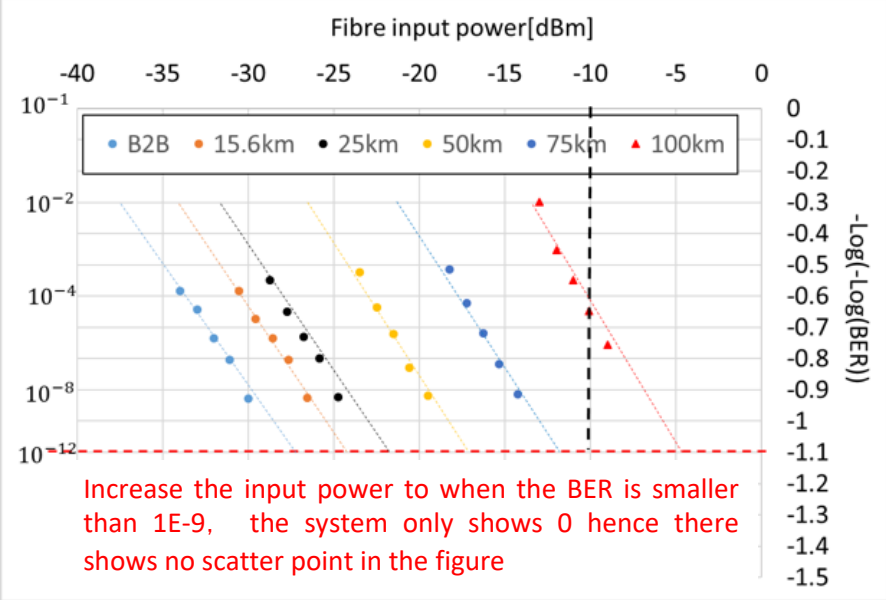


Figure 4.3.2 (b) performance of commercial sets

Figure 4.3.2(b) shows the plot of bit error rate as a function of fibre input power. For fibre with different length, the bit error rate decreases with the increase of incident power and is linearly proportional. The system is able to provide error free (BER < 10^{-12}) transmission through optical fibre length up to 75km without forward error correction. And the length can be extended to 100km with forward error correction.

4.4 Cambridge quantum network trial performance

In this study, the QKD link is shown in figure 4.4 (a). The network consists of a number of different transceiver nodes, including those of the advanced photonic electronics centre (CAPE), TREL and the engineering department (ENG) of the university of Cambridge. The optical fibre distance (loss) is 10.44 km (3.9 dB) [CAPE – TREL], 9.64 km (4.2dB) [TREL–ENGI] and 4.9 km (~2.5dB) [ENGI–CAPE]. The average fibre loss coefficient of all three links is 0.43dB/km, which is very similar to the dark fibre three-link quantum network demonstrated earlier [5]. There is a loopback link between CAPE and Duxford, which can test the link length up to 66km, with an overall link loss of 16dB and a dispersion of 1012ps/nm.

A long term field trial has been carried out over this network, for around 550 days, other tests have induced transmitting data from the electrical engineering building, to Toshiba labs, back to engineering, and finally back to the electrical engineering building.

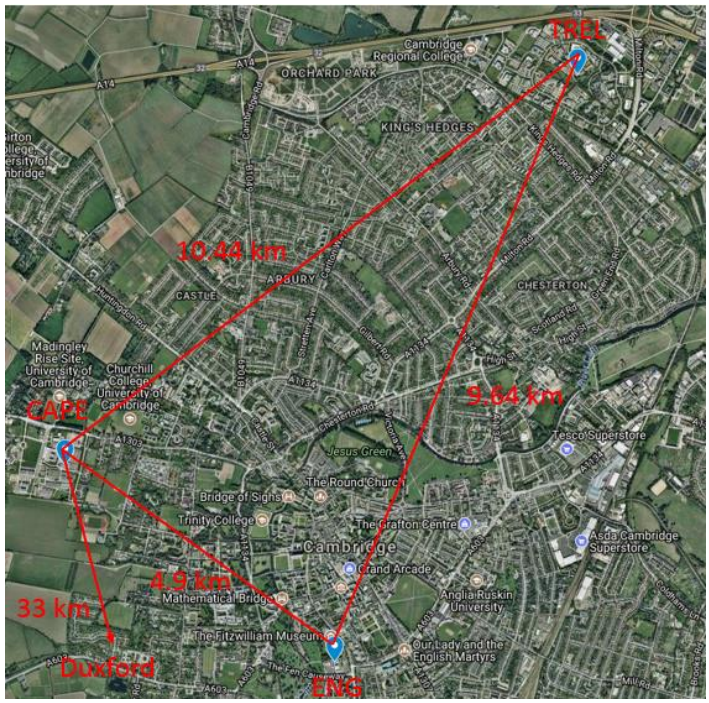


Figure 4.4 (a) The Cambridge Quantum Network Infrastructure

For simplicity, Figure 4.4(b) demonstrates the network structure both the QKD and classical data links. Each of these links has been a separate QKD node. There has been an Alice and a Bob up on each of the three links shown on the left. In addition, QKD links operate also in the presence of 200 gigabits of classical data, which are encoded and encrypted via the QKD and send high speed classical data through the whole network.

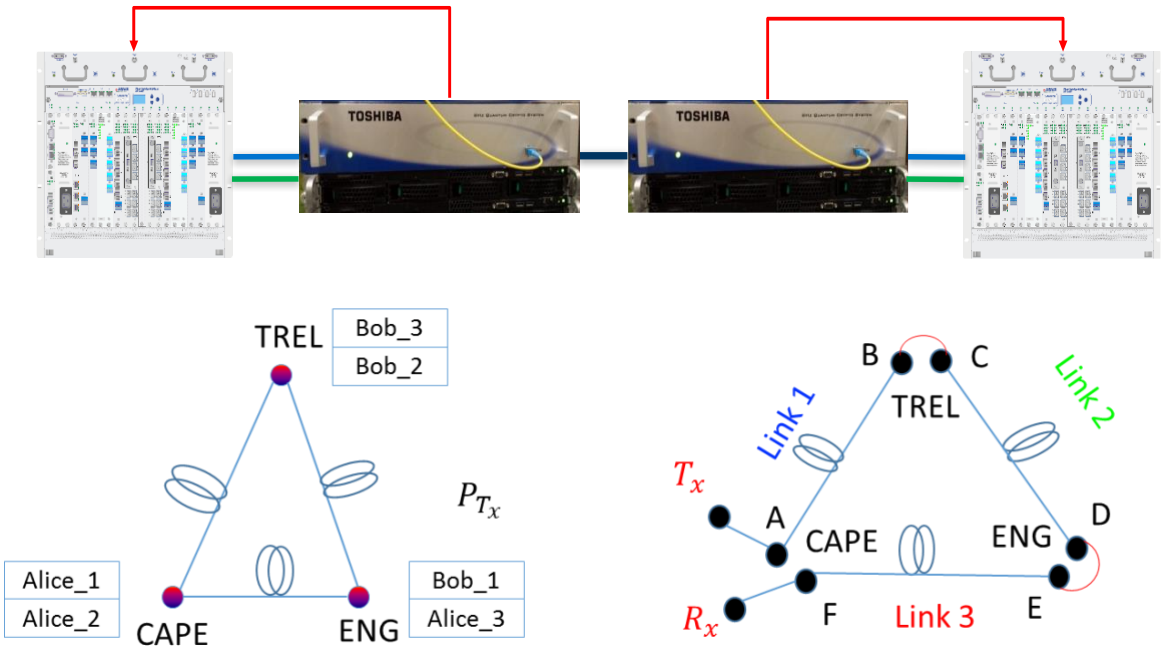


Figure 4.4 (b) Cambridge QKD network structure QKD links(left) Classical data links(right)

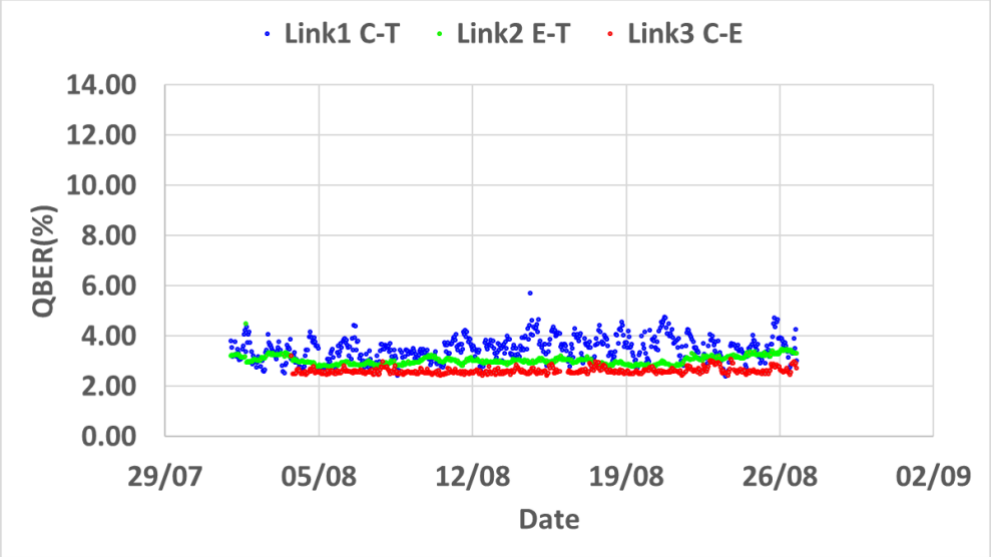


Figure 4.4 (c) long-term trial results of QBER within Cambridge QKD network

The results of the month-long experiment are shown in figure 4.4 (c) and figure 4.4 (d). The values of QBER maintains below 5% during the time. One of the links, Link 1 from CAPE to Toshiba laboratory, is showing a rather larger variation in QBER than the others. As it is described in figure 4.4(b), the way that the system is operating is to co-propagate QKD and high speed data along the same fibre. In other word, that is the highest intensity light, so that will suffer most degradation from scattering, from Raman and coupling as well which has been introduced in previous sections and will be discussed in details in Chapter 6.

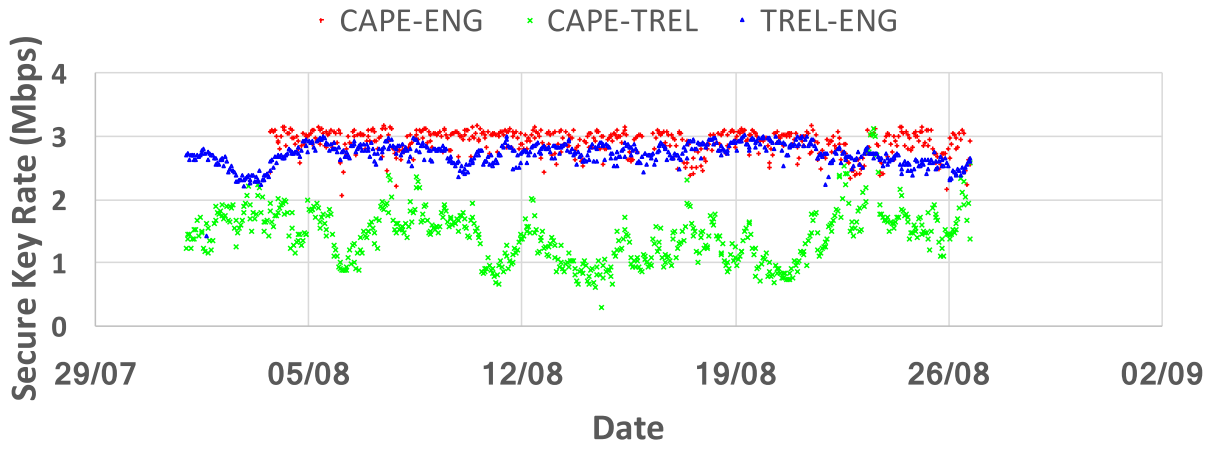


Figure 4.4 (d) long-term trial results of secure key rate of QKD network performance

Clearly, the network results in sustained key rates of the order of megabits per second and Figure 4.4 (e)shows the results in terms of the cumulative distribution functions which gives a better way demonstrating the fastest link at the same distance compared to many other systems[93, 97] due to the benefit of T12 protocol.

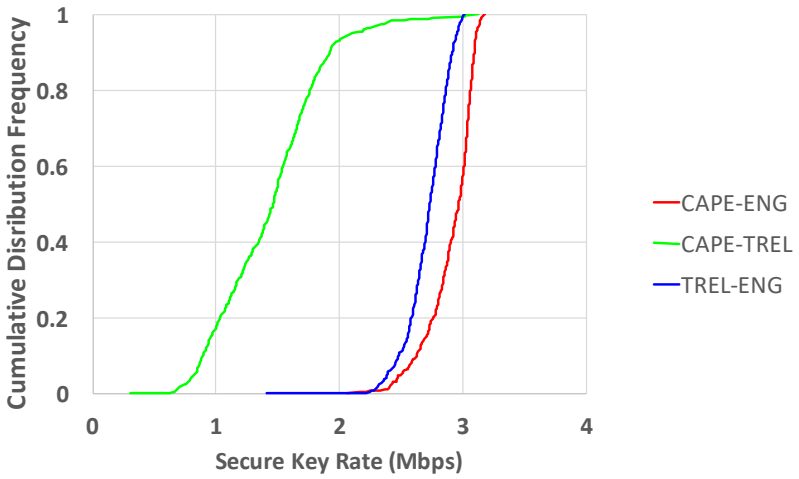


Figure 4.4 (e) Secure key rate in terms of Cumulative Distribution Function

The 33km and 66km fibre link are shown in Figure 4.4(f). For the 33km route, only quantum data enters from TREL unidirectional along the TREL-Dux route through CAPE, then arrives at Dux and re-enters a reverse independent channel to reach CAPE. The Alice was put at TREL and Bob was at CAPE. The quantum power level at TREL is 8.9 dB higher than that at Dux end to compensate the optic loss between TREL and Dux ends. As a consequence, the quantum signal injected at Dux end would be at the target power level ($P_{quantum}$) and then transmitted through a 33km link to CAPE.

And for the 66km link, The one-way length of CAPE and Dux is 33km, so a 66km transmission route directly inputs light from the CAPE end along one optical fibre to reach Dux and then to another reverse optical fibre to return to CAPE. Additionally, there has been sent a 100 gigabits classical channels down that, as well as running the QKD on it. And the power of the classical data is set to be -10 dBm at which it will always remain error free.

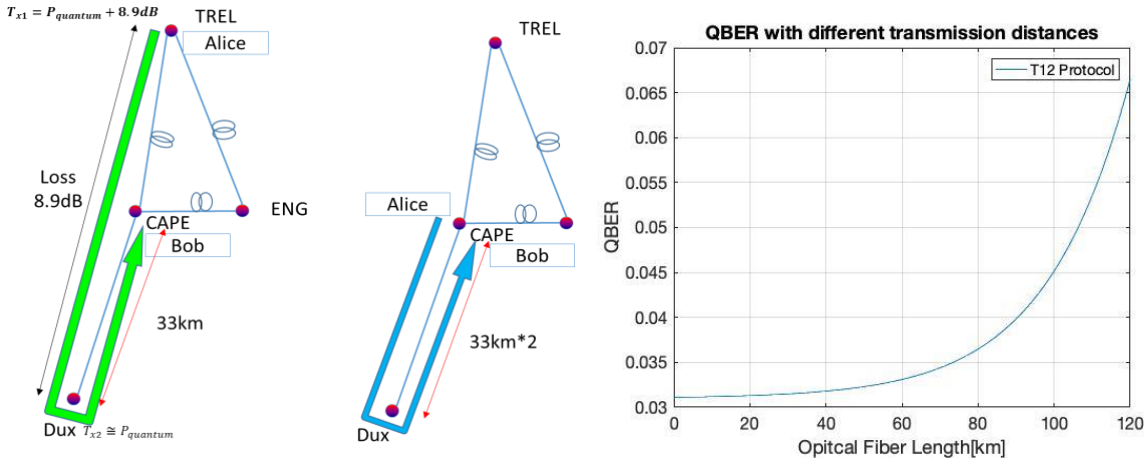


Figure 4.4 (f) 66km-long link structure and T12 protocol of QBER simulation

Experimental QBER results from the longer QKD system are illustrated in Figure 4.4 (g). The 66km link experimental QBER results greatly differ from simulation results (i.e. below 3.5% shown in Figure 4.4(f)). This is because the 66-kilometre-link operates with quite significant input classical powers, there exists a finite amount of coupling from the Raman scatter from the classical channels into the quantum channel. And also, QBER goes up to 6.5% from 3.3% due to 15dBs fibre loss.

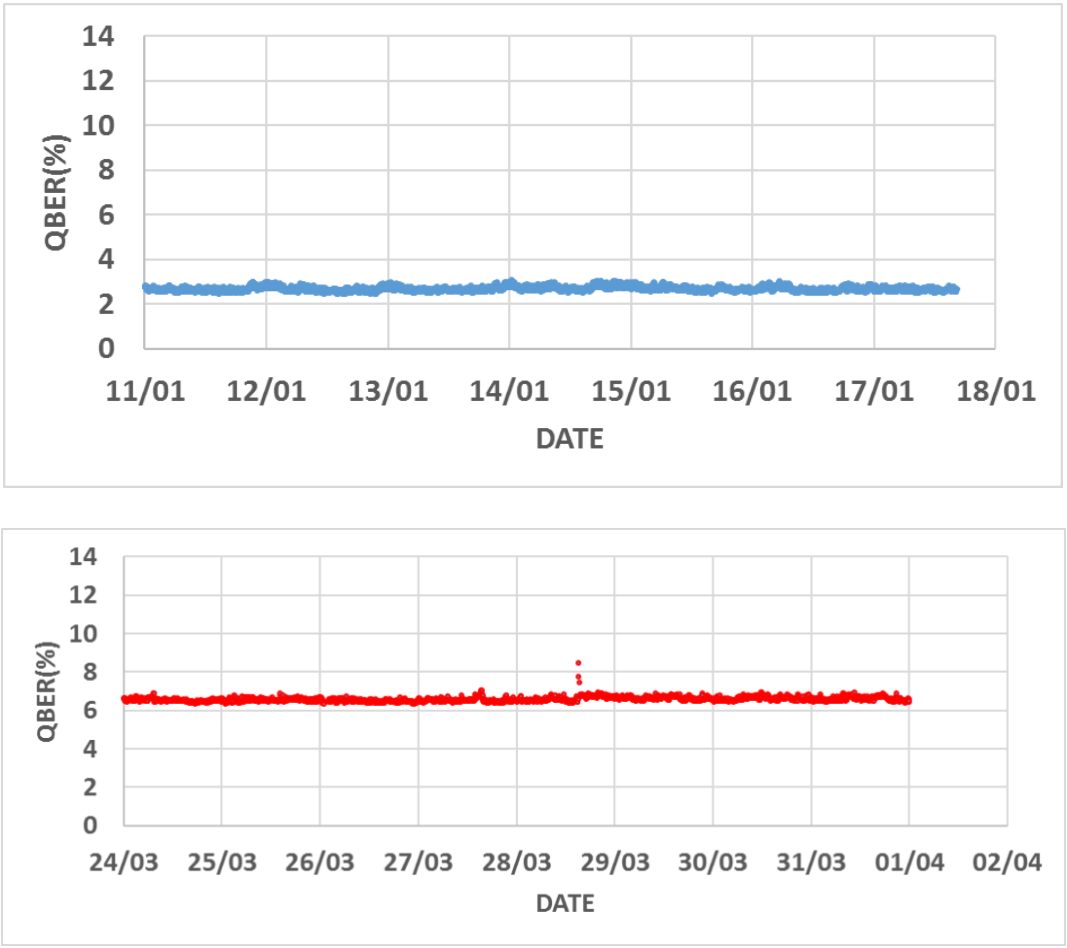


Figure 4.4(g) Trial QBER results for 33km(up) and 66km(down) link

4.5 Discussion

4.5.1 Hybrid quantum network

The Cambridge quantum network has been fully functional quantum network running on optical fibres result in a secure key rate of Mbps. These high key rates are compatible with metropolitan architectures of dozens of nodes. For AES encryption, users can expect 100Gbps of data bandwidth and ~1Hz of AES quantum key refresh rate -- working in the same fibre as QKD. The quantum key rate reported here is enough to support thousands of users, which is enough for most major cities. For example, in the overall three-tier network model, we might expect each node in the Cambridge quantum network to support several quantum access networks (QAN) [159] [93] to serve the area of the city around the node. QANs has been proven to handle converged bandwidth of up to hundreds of kbps [160], so a few QANs on each metro node are ideal for this metropolitan network. Consider a situation where each QAN user communicates with another QAN user only through the Cambridge quantum network. Then, the average bandwidth per user is

$$B \sim 2R/n$$

Where n is the total number of users of each node. For each user's actual bandwidth (or bit rate) (which can support AES key exchange) > 100 bps . The Cambridge quantum metro network, showing QKD links to 2.5Mbps speeds that can support about 100,000 users, which is related to the population of Cambridge. Therefore, the results show that this quantum link can work in most metropolitan environments.

4.5.2 Comparison between theoretical and experimental results

Figure 4.6.1(a) demonstrate the sifted and secure bit rate as a function of fibre length simulated by ***Matlab***. The sifted key rate drops down exponentially with the fibre length, and the attenuation rate is about 0.2 dB/km, which is the characteristic loss of the single mode fibre. For short fibre distances (less than 50 km), the security key rate decreases at the same rate. Figure 4.6.1 (b) shows the experimental results of QBER(symbol) as a function of the fibre reel length. Short fibre length, usually smaller than 50 km results in little changes in QBER. When the length of the fibre is greater than 50km, the QBER gradually increases, because the dark count and Raman contribution are no longer insignificant compared to the signal count. To make it clearer of the contribution of Raman noise, a simulation diagram of QBER without data laser (dotted line) in figure 4.6.1(b) is shown.

Using only the parameters measured experimentally, the simulated the security key rate and QBER are shown in the solid lines in figure below. Both forward and backward Raman scattering have been taken into account. In addition, additional losses due to optical fibre connectors and optical fibre dispersion have been considered. At 90 km, the connector makes up for an additional 0.6 dB loss, while fibre dispersion adds 1 dB penalty to the data channel. The simulation results are in good agreement with the experimental results.

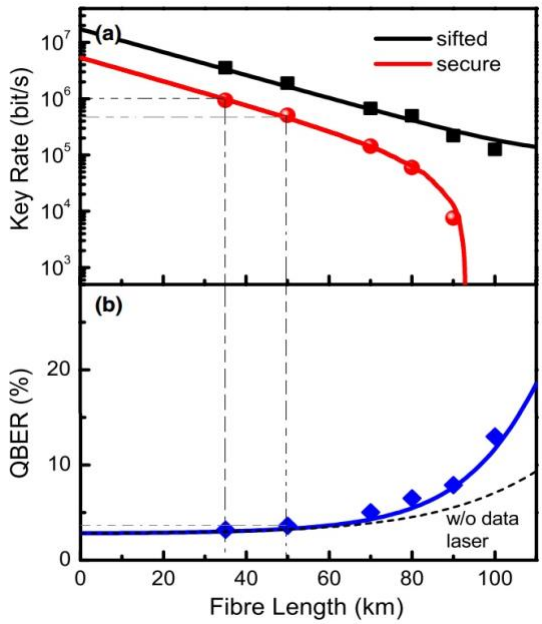


Figure 4.5.1 Secure key rate (up) and QBER (down) versus fibre length [116]

The plot above could be utilized as a roughly calculation for the relationship between secure key rate and QBER for short transmission length. Here two sets of points are taken, that is, secure key rate and QBER at length of 35km 50km.

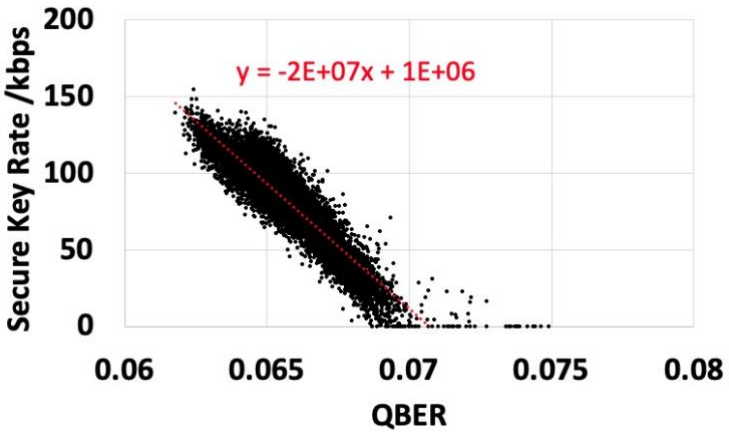


Figure 4.5.2 secure key rate versus QBER

$$\text{Gradient}\left(\text{Secure key}\frac{\text{Rate}}{\text{QBER}}\right) \cong \frac{10^6 - 6\times 10^5}{4\% - 2.5\%} = 2.6\times 10^7$$

Where the gradient is very close to the value 2×10^7 in Figure 4.6.2 which shows the data from Cambridge network.

In the Toshiba system, the number of pulses containing a single photon is a random variable, and the generation and measurement of photons is a random process. At the same time, the Toshiba system, after generating and storing keys, will evaluate a large cluster of keys and eventually calculates an quantum bit error rate. When we do a lot of replications on a lot of random variables, the distributions of these variables add up to very close to a Gaussian distribution. Therefore, based on the random generation of photons, the random process of light pulse contains a single photon, the QBER that measures the photon phase randomly and estimate the QBER based upon thousands of randomized process, the QBER then should obey a Gaussian distribution. During the trial duration, the statistics of the QBER have been found to be Gaussian distributed with a standard deviation of 0.5. The results of the field trial suggest that the system works stably and has considerable potential for applications in metropolitan networks.

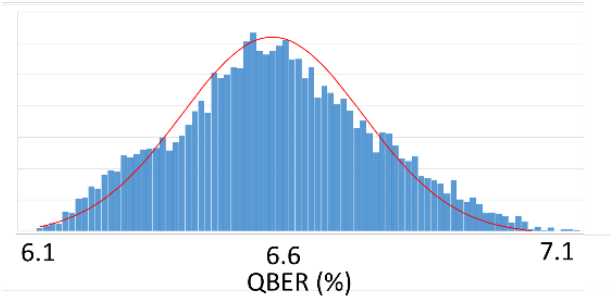


Figure 4.5.3 Trial results of QBER distribution

4.6 Summary

Chapter 4 estimates the theoretical limitation of QKD system in terms of both transmission distance and key generated rate. Laboratory experiments on the Gbps data link secured by QKD have been then conducted through fibre reels and compared with long-term field trials within Cambridge quantum network.

These long-term results from the quantum layer of the Cambridge metro network are comparable to recent long-term network demonstration, which is the Swiss quantum network [5] introduced in previous chapter. The network consists of three metropolitan length links, with an operating time of about 2 years. Cambridge quantum network produced 129 terabits of key materials, so it is about three orders of magnitude larger than Swiss quantum network. The security key material of the three links amounts to 360 Terabit. In conclusion, this Chapter puts forward the view that the system can run stably in the laboratory and report application of the three-node urban network.

Chapter 5. Investigation on system operation temperature effect

Having compared the experimental and trial QKD network system performance in ***Chapter 4***, it is worth nothing that the trial results indicate a relationship between temperature and secure key rate. Hence in this chapter, the cause of the transmission and detection performance of the QKD network is discussed. Theoretical and experimental studies are also discussed in this chapter.

5.1 Motivation

Quantum key distribution allows the distribution of secret digital keys through optical fibres, and its security depends on the laws of quantum physics [2, 44] [25, 32, 98]. The measurement of the quantum state used by third parties to carry the key bit can lead to state coding errors, allowing legitimate users to detect any eavesdropping attempt. QKD has been proven to achieve Mbit/s security key rates (such as Dixon[42, 112]) and communication distances of up to hundreds of kilometres. In Chapter 4, a QKD network is reported, which proves the practicability of QKD by multiplexing with traditional data signals. Recent research has also focused on multi-user access networks, or the development of advanced protocols to improve security and efficiency [43, 45].

One of the key components of a QKD system is a single-photon detector, usually a single-photon avalanche detector. Of course, the passive quenching operation of the InGaAs/InP single-photon avalanche diode detector at low excess bias, including post-pulse analysis, has been discussed in the previous section. Although in the traditional DV-QKD system, the original BB84 encoding scheme [32]was designed to take advantage of the quantum properties of the single-photon polarization state [52], the experimental equipment relies on the measurement of the phase encoding state. These encoding schemes, including the T12 protocol [42] used in this study, rely on interferometers, and encoding is achieved by changing the relative optical path length or phase between the arms of the interferometer. Of course, in a real transmission environment, temperature or polarization changes may occur unpredictably and affect performance [56, 161].

Gigabits/s high speed classical communication systems encrypted by quantum key distribution are sensitive to crosstalk due to signal photons arriving at the detector end which weaken systematic security level causing low secure key rate and a large of quantum bit error rate.

Therefore, it is important to determine the reasons and factors that the affect system performance described in Chapter 4 and find out methods to minimise errors and optimise system performance for future high speed hybrid metropolitan QKD network applications. In the following sections, experimental tests are carried out to explore the influence of temperature on different parts of the whole network equipment. And from the theoretical analysis, the simulation results and experimental results are compared and summarized.

5.2 Analysis of the effect of temperature changes on system

5.2.1 Temperature logger

The DS18B20 temperature sensor meets the requirements for applications in weather stations and home automation systems, and can easily controlled by Raspberry Pi. They are the same size as a transistor and use only one wire for the data signal. The sensor has a sensitivity of plus or minus 0.5 degrees Celsius and can measure temperatures ranging from -55 degrees Celsius to 125 degrees Celsius (-67 to 257 degrees Fahrenheit). In addition, the sensor measure the temperature and store it once for less than a second, which is much faster than the speed of the keys generated and stored in a hybrid network (>5km) using Toshiba equipment in this study.

The sensor connected to a Raspberry Pi forms the temperature logger which is used in this project and shown in Figure 5.2.1.1(***See Appendix 1 for the coding and wiring details of this set up***).

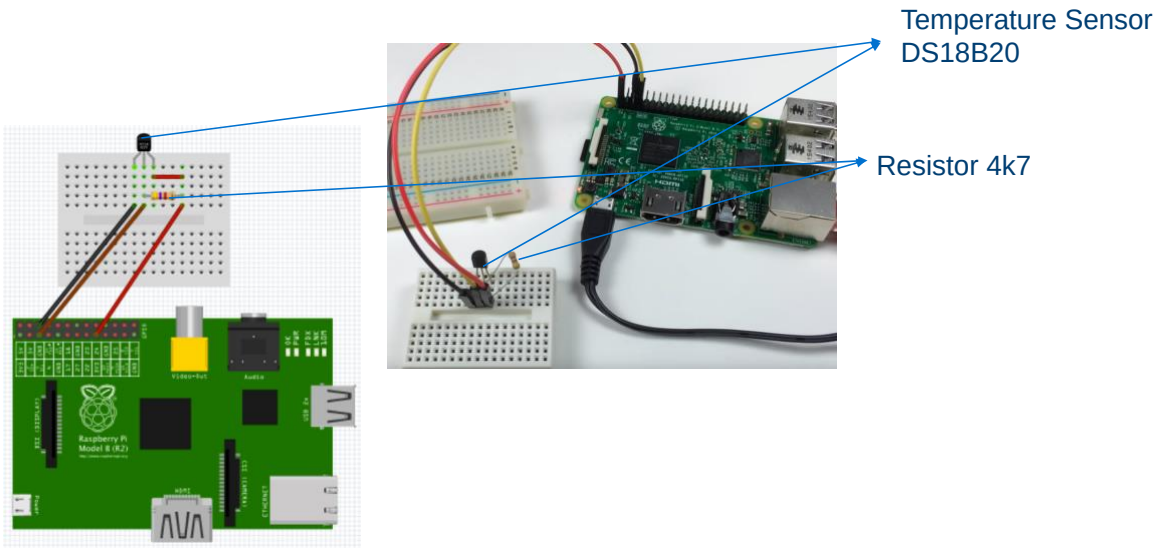


Figure 5.2.1.1 Temperature logger circuit diagram

5.2.2 Long-term QKD system fluctuation trend

Temperature measurements are carried out on two sets of QKD system without classical data systems, which are installed and compatible within a metropolitan area telecom network. Here two transmitters are located in a server room in the Cambridge University electrical division building with one receiver at Cambridge Central Network Facilities (CNF) and the other receiver at the Engineering department main site. The QKD systems from TREL use a decoyed-BB84 type protocol, termed "T12" with efficient basis selection to elevate the key rate, at a clock rate of 1GHz. The systems run at 1GHz clock rate. The effect of finite key size is mitigated with a resulting key failure probability, $\varepsilon = 10^{-10}$ decoy [42]. The locations are linked by two fibre pairs both approximately length of 5 km with a loss of 1.2 dB (0.24 dB/km), slightly higher than the standard spool fibre loss of 0.2 dB/km due to the presence of splices and other joints. More than 90% of the fibre is under ground and often the fibre is reported not susceptible to environmental factors affecting the transmission characteristics which are the received quantum states. The rest of the fibre above ground or in the lab may be affected by the surrounding environment. These factors can include temperature changes, both from ambient air temperature and direct solar radiation, causing expansion and contraction of the fibre length. The result is constantly changing conditions for the photon transmission, with the most important factors for QKD including transit time and birefringence changes.

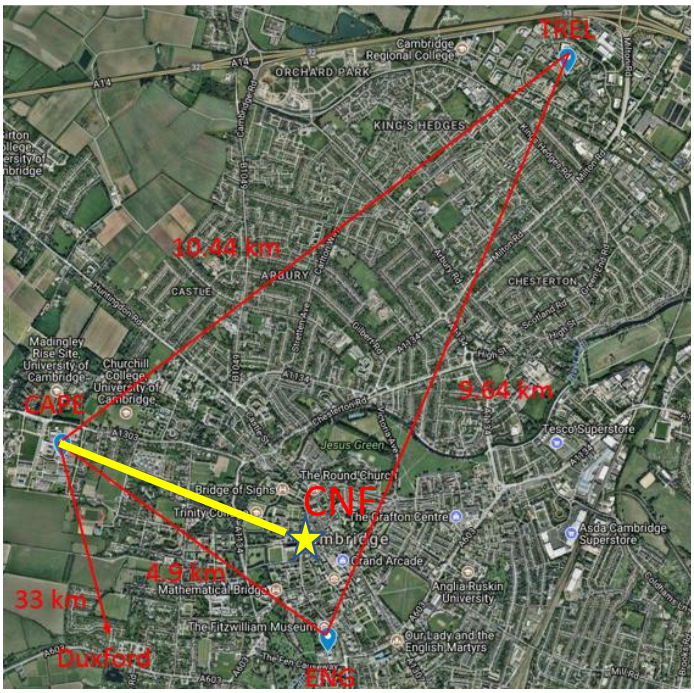


Figure 5.2.2 Temperature measurements map within Cambridge Quantum Network

Note: the image shows that the scale is deviated from the actual, and the straight lines do not represent the actual fibre

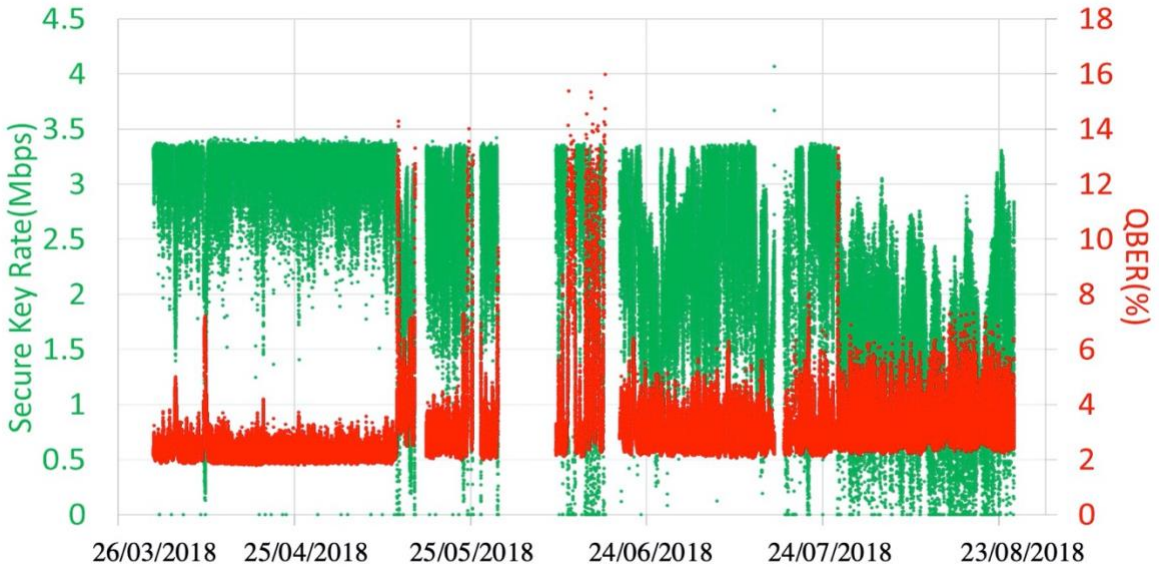


Figure 5.2.2(a). Trial results for the link between Electrical Department and Cambridge CNF

Figure 5.2.2(a) illustrates one of the QKD link between Electrical department and Cambridge University CNF running without high speed classical data in order. The system then resultants in a 2.84 Mbps secure key rate with a 0.84 Mbps standard deviation. And QBER is (2.9 $\pm$ 1.0)% over five months continuous operations.

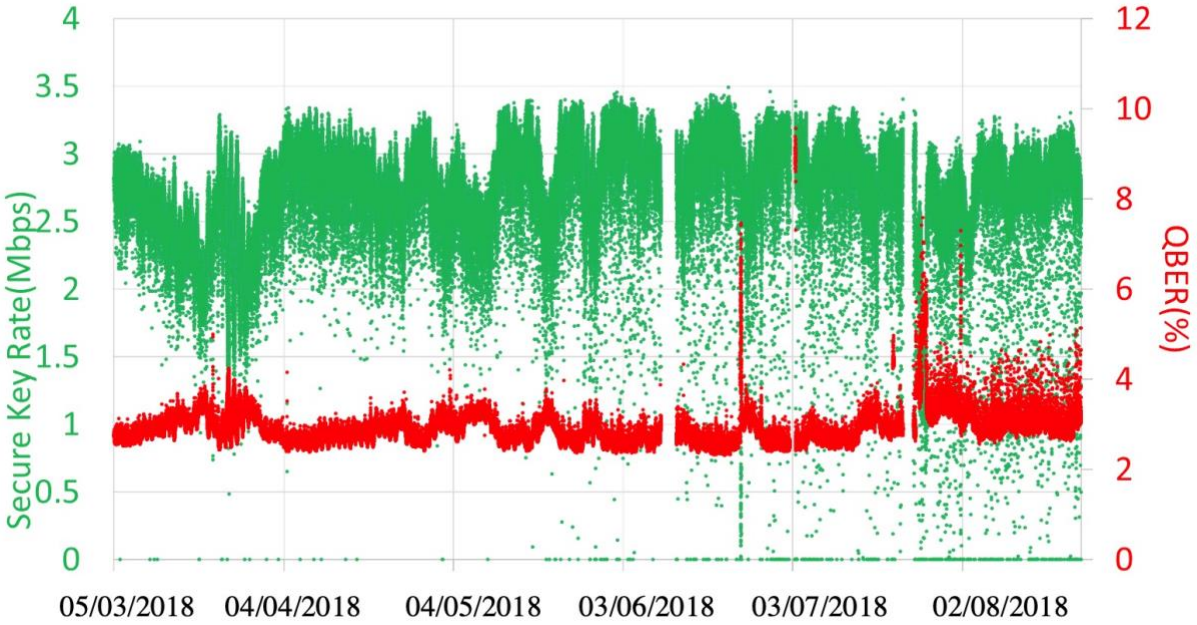


Figure 5.2.2(b). Trial results for the link between Electrical Dept and Engineering main site

Similarly, figure 5.2.2(b) shows another five months system operating results between two nodes connected via optical fibres with a length of 4.9 km within the Cambridge quantum network. This link with a total loss of 1.1dB leads to a mean QBER of 2.89% and standard

deviation of 0.3%. The secure key rate on the QKD link, with a mean of 2.75 Mbps and standard deviation of 0.36 Mbps.

In both of the two figures above, it is worth to be noted that there exist sudden jumps on QBER and zero secure key rate which are both unwanted in real communication system. Spikes on QBER plots means values of QBER increases sharply and this can be caused by system power abruptly shut down, looseness of contact port of optical fibre and possibly system operating temperature which will be discussed in the following. The default settings of Toshiba equipment is that zero secure key rate is determined when the QBER is higher than specific threshold, that is approximately 7% (This value is also found and proved in Chapter 4 in this project, and there will be no secure information in this time.

In addition, both of the figures indicate tendencies for the secure key rate and QBER to increase and decrease periodically to some extent. For any QKD system, especially for future high speed networks encrypted by QKD, it is very important to predict how system perform and those factors which may affect the system security. Hence, the following sections aim to analyse and identify the reasons that leads to such the performance.

5.2.3 Analysis of temperature temporal fluctuation

As mentioned previously, fibre length and detector efficiency affect QBER. Temperature is one of the most important factor that affects the detector's efficiency in term of dark count and also affects fibre operation properties. The temperature history for several weeks in 2017 at Cambridge is plotted with QBER in Figure 5.2.3.1 to observe whether there is any apparently correlation between external temperature and QBER.

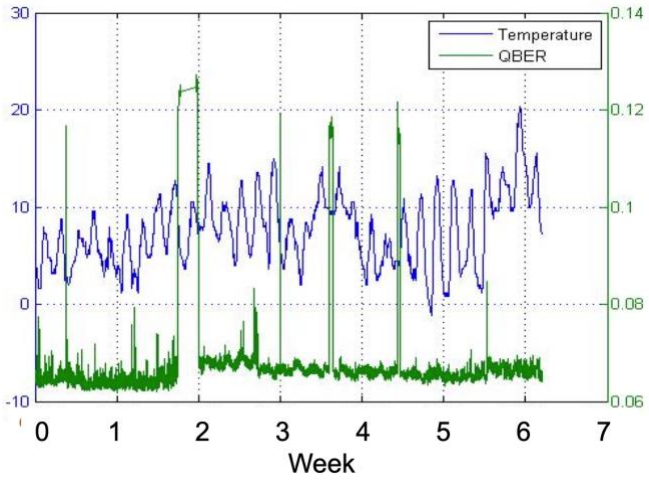
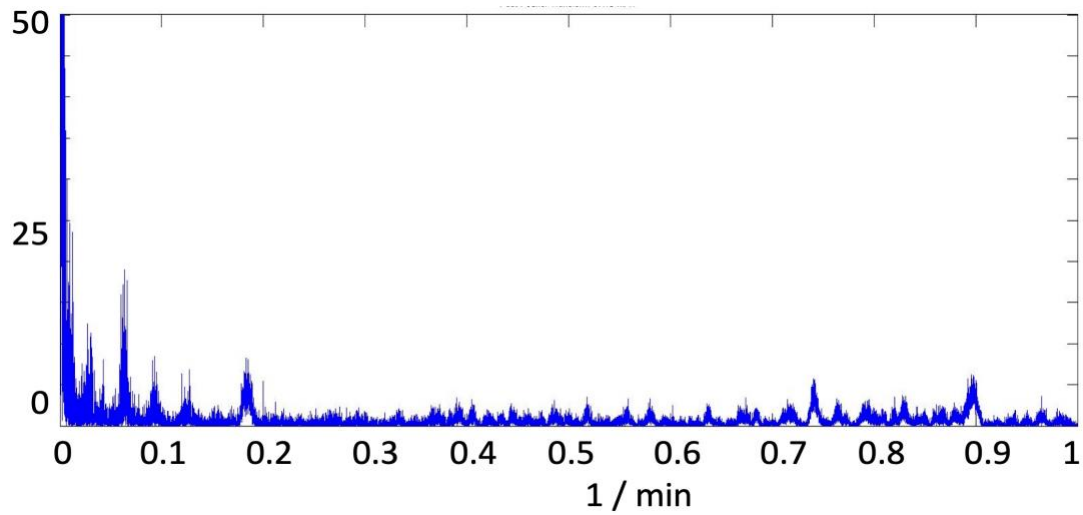


Figure 5.2.3.1 QBER verses Temperature over weeks

From this plot, the value of QBER has an abnormal peak larger than 10% every week and when average temperature was around 10°C. Also, most of the peaks, even smaller peaks (i.e. the peak at ~8% between week 1 and 2, week 2 and week three as well as peak at ~9% between 5 and week 6) all occurred at the trough of the temperature waves. However, QBER did not always jump to such a high peak when temperature approaches 10 °C or peaks at each trough of the wave. Hence it is not very obvious or easy to make any conclusion at this stage. The next stage is to take a more advantage method rather than observations only to analysis these temperature related plot.

Analysing deterministic signals is easy in time domain. However, most of the signals in communication systems are random, for example the noise in the time domain cannot be deterministically. One of way they can be analysed is in frequency domain. The Fourier transform (FT) decomposes a function of time (a signal) into its constituent frequencies. A fast Fourier transform (FFT) is an algorithm that computes the discrete Fourier transform (DFT) of a sequence, or its inverse (IDFT). Fourier analysis converts a signal from its original domain (often time or space) to a representation in the frequency domain and vice versa. The DFT is obtained by decomposing a sequence of values into components of different frequencies.

As the time and QBER are recorded as two set of sequences, i.e. each point in time corresponds to a value of QBER, we compute a fast Fourier transform for the data sets QBER verses Time shown below.



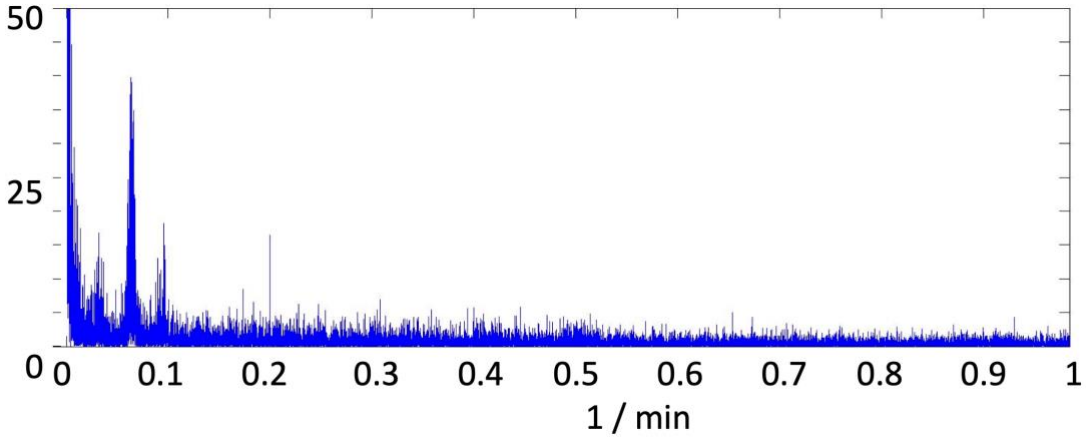


Figure 5.2.3.2 Fast Fourier Transform of QBER

Both of the FFT plots above show peaks at 16.7 min (1 / 0.06), 12.5min (1 / 0.08) or 5min (1 / 0.2). Also, when the x-axis approaches 0.01 and 0, which is hourly and daily in time domain correspondingly, there also are peaks.

The next step is to figure out what factors are consistent with these peaks. Taking a week of the data and plotting them on has shown in Figure 5.2.3.3. This plot clearly show the trend of periodic changes on a daily basis.

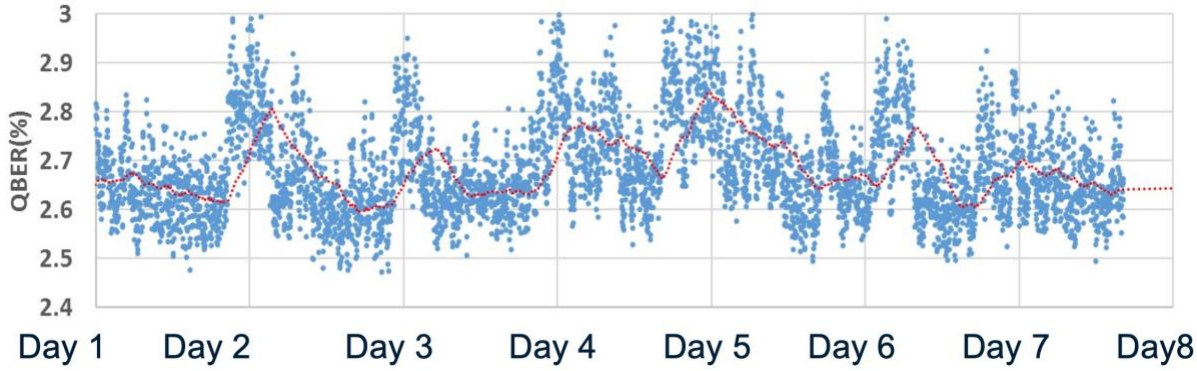


Figure 5.2.3.3 Trial result of QBER daily data with moving average curve

5.3 Performance investigation with temperature logger

It has been discussed that there is no direct relationship between the temperature change of external weather and system abnormal performance. However, fibre and some optical components, such as interferometers, are usually sensitive to operating thermal variations can cause changes in the path and arrival time of the photons and result in changes in QBER and secure key rate.

The temperature loggers, are real-time thermometer shown in figure 5.3.1. These are placed in three different places in the room where the Toshiba QKD equipment is. These three locations were selected based on the location of the equipment‘s build-in cooling fans and the distance between the instrument placement and the air conditioners. The red one is the top of the Toshiba device box and the blue is on the ADVA. The black is in the air between the two systems. These temperature loggers aim to record the temperature at which the system (except for the underground optical fibres) is operating, and then explore whether the temperature is related to the performance of the system.

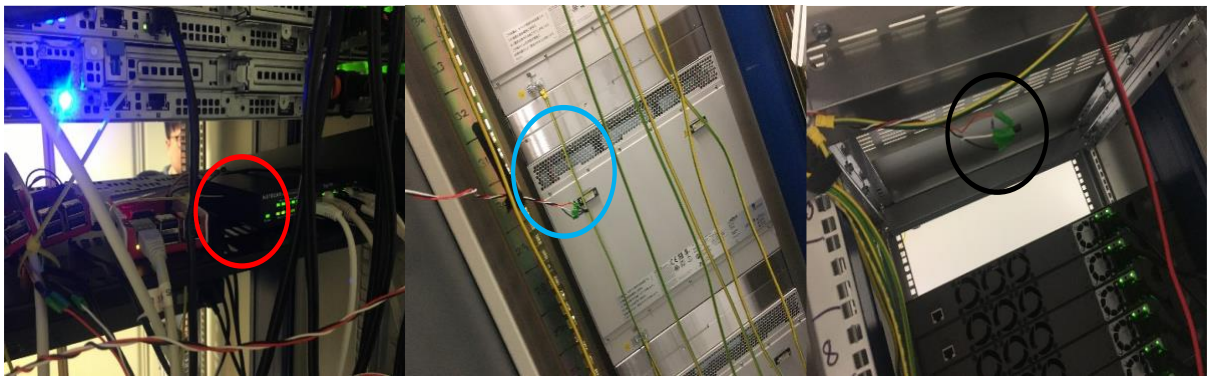


Figure 5.3.1 Room temperature logger placement

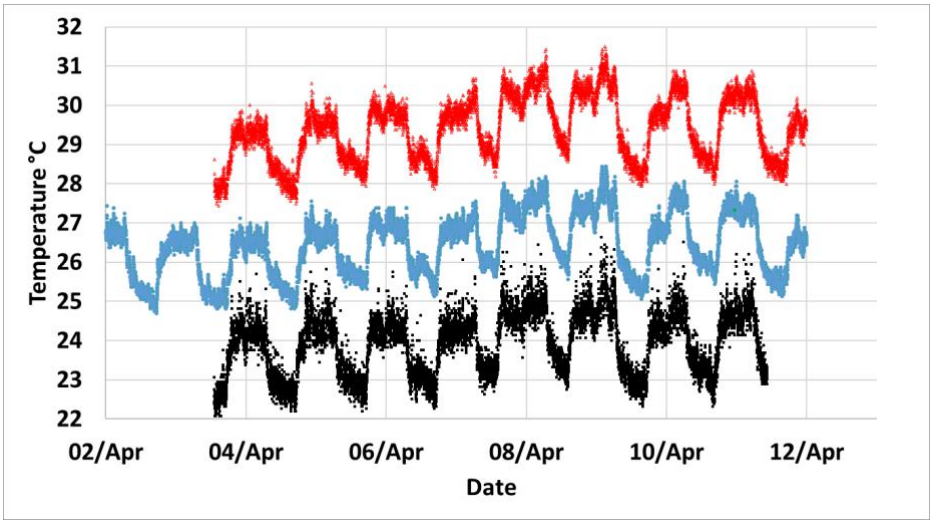


Figure 5.3.2 Room temperature logger over days

(NB: The colour of the curve represents the position of the temperature sensor)

The three scatter plots above show the temperature in different parts of the room over several days. The overall trend in temperature is the same, although the temperature at the three locations differs by around 6 ℃. The temperature difference is mainly due to the high temperature caused by the heating of the equipment housing and the low local temperature

caused by the direct wind direction of the cooling fan. As a result for normal operations, we have chosen a location that is not near either the device housing or the cooling fan to record the operating temperature of the entire system (except for the externally buried underground optical fibres).

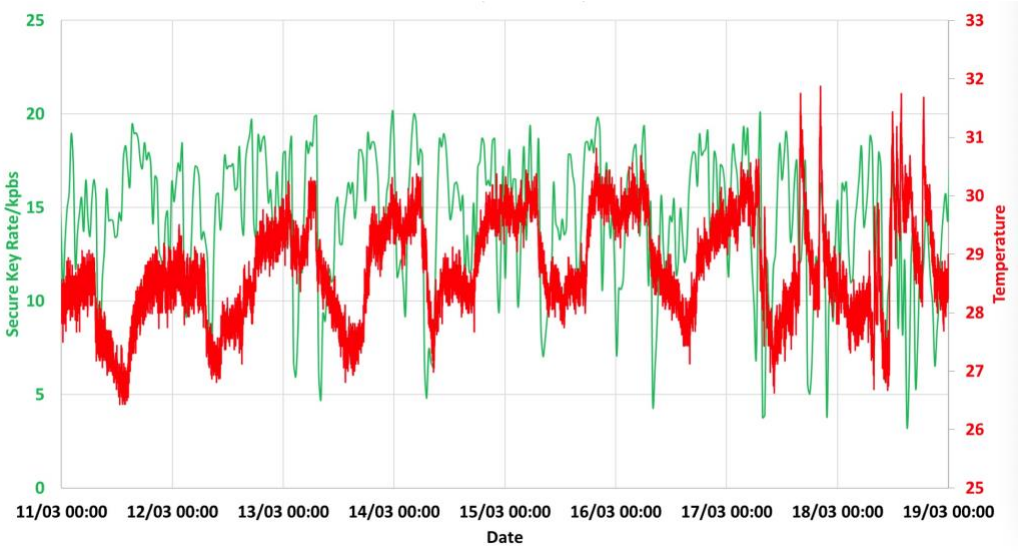


Figure 5.3.3 Experimental result of Secure key rate vs. Room Temperature over a week

Figure 5.3.3 illustrates the relationship between system operating environment temperature and QKD system secure key rate. As you can see, the overall temperature change and the secure key rate change are reversed. When the temperature rises, the secure key rate begins to decline, and when the temperature remains stable, the secure key rate then changes relatively little. The difference between the maximum and minimum temperature is about 3 ℃, while the change interval of the secure key rate is about 10 kbps.

For further comparison, the data of another group of seven days are shown below. It can be seen from Figure 5.3.4 that the change trend of secure key rate and temperature is similar to the figures above.

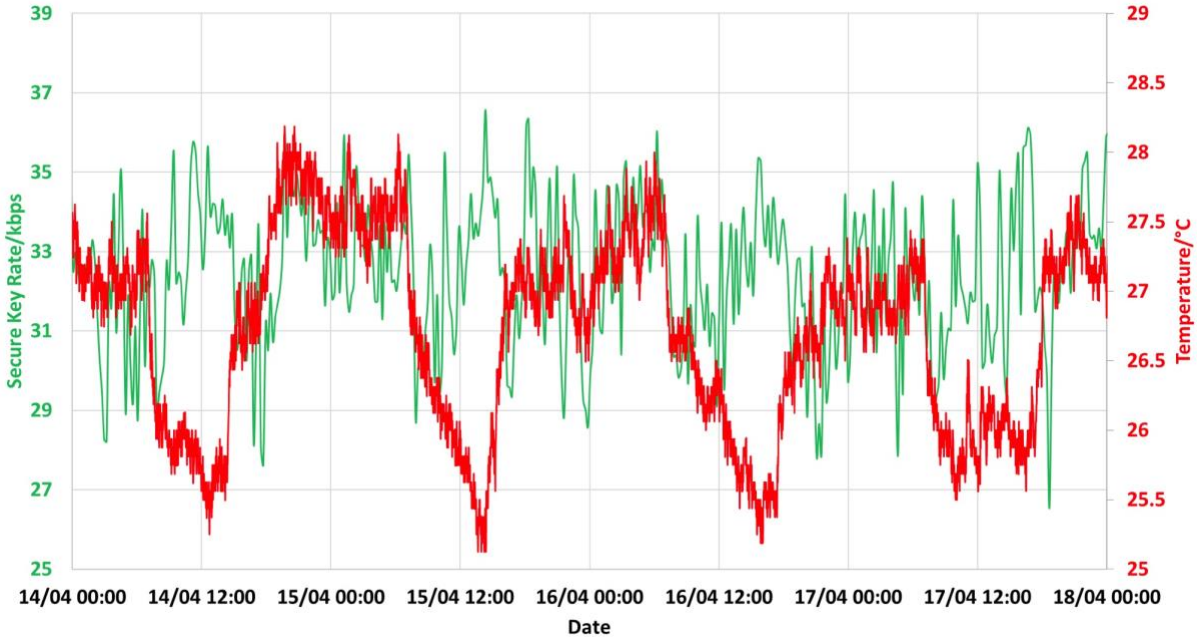


Figure 5.3.4 Contrast experimental results

According to the results of the two graphs, it can be preliminarily concluded that the change of temperature has an impact on the system performance, and low temperature can lead to higher secure key rate which is desirable in practical network.

The next step is to take theoretical analysis and prediction of the effect of temperature changes on the system performance, and verify whether the theory is highly consistent with the previous trial results by using the control variable method.

5.4 Theoretical Analysis

Principles of QKD system set-up have been introduced in Chapter 2 and 3, the following illustration is a reference for further explanation to temperature effect on system performance. Firstly, the time difference between the two red pulses in Figure 5.4 below will affect the result of the system performance. Secondly, the number of photons reaching the last two single photon detectors also affects the value of QBER and then the secure key rate. Therefore, it is necessary to analyse the factors that may affect the pulse time difference and the number of photons in the following.

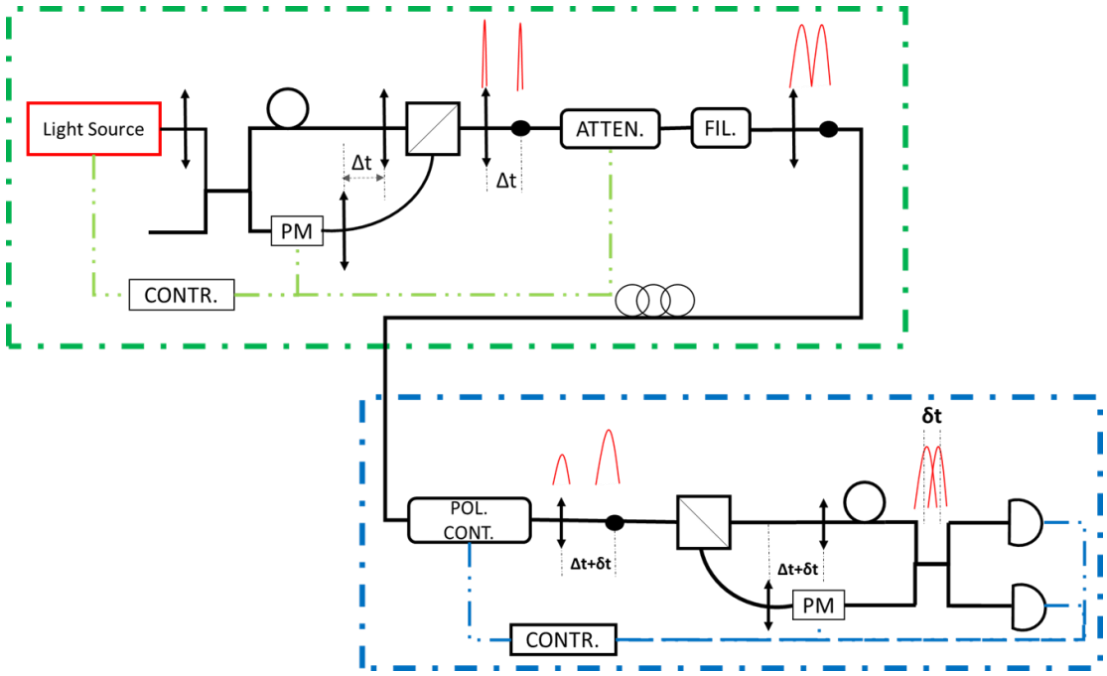


Figure 5.4 Toshiba QKD system structure diagram

Technically, two optical pulses from each arm arrive at the same time on the final beam-splitter. The optical frequency of the light source does not vary in time across the optical pulse and the two optical pulses from each arm arrive at the final beam-splitter with the same intensity. Polarization degradation mechanisms also exist in the optical fibre, and so optical pulse polarization rotation is corrected by polarization controller. Polarization dependent loss (PDL) will causes intensity difference to emerge between orthogonal polarisations of optical pulses. Polarization mode dispersion (PMD) causes time difference to emerge between the orthogonal polarisations of the optical pulses. PMD causes the time difference δt which means the interference at the final beam-splitter is degraded since the light pulses no longer overlap completely. PMD and PDL reduces the visibility V of the system and then QBER increases. However, Intensity issue has been improved by the technique (the T12 protocol [42]) for selecting the optimum intensity for pulses.

Some other Toshiba equipment parameters are as follows,

- Visibility V ~ 99% when δt =0 but drops quickly to < 40% if the light pulse delays δt is greater than 9ps
- A change in visibility of 10% gives a 5% additional contribution to the QBER
- Usually 7% for longer distance (>50km) and 10% QBER for shorter distance (<10km) leads to zero secure key rate

- For short delays of δt ~ 2ps the drop in visibility is negligible and can be regarded as no increase in QBER

The V is the interference fringe visibility defined as

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}$$

Where I_{max} and I_{min} are the average pulse intensities for constructive and destructive interference respective.

5.4.1 Time delay on optical fibre

The propagation time through an optical fibre varies due to environmental changes (temperature, vibrations etc.), which is undesirable in a host of applications, such as precise time and frequency transfers or applications requiring highly accurate time synchronization of (data) signals [162].

As far as the temperature dependence of the refractive index of fused silica is concerned, many experimental investigations have been presented (see for example, Refs [163-165]), and they have shown that the refractive indices of fused silica are directly proportional to the temperature with the temperature coefficients lying in the range of $[5 \times 10^{-6}, 3 \times 10^{-5}]\,(K^{-1})$ when the temperature is in the range from roughly 100 K to 800 K.

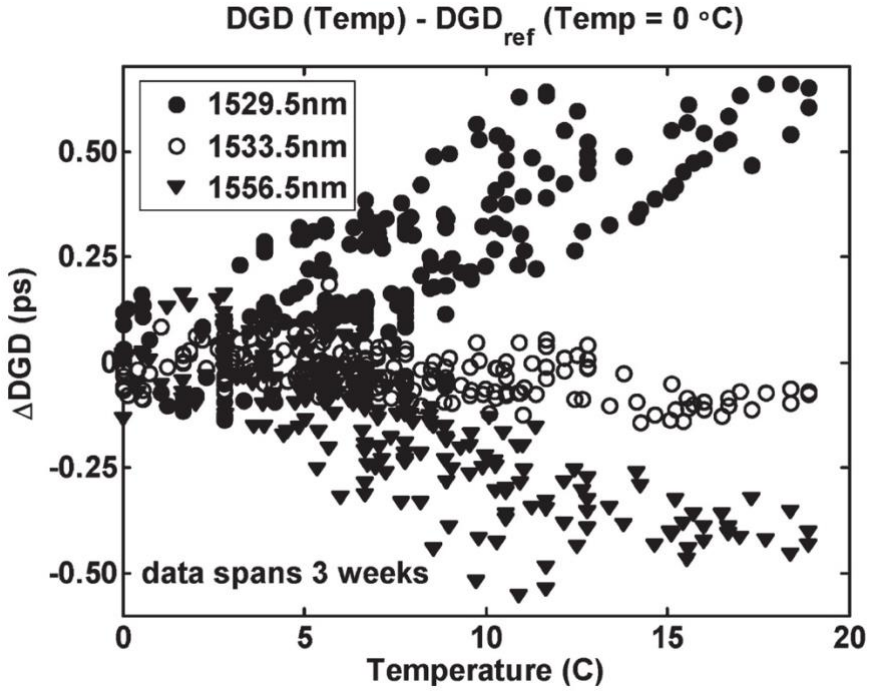


Figure 5.4.1.1 Changes in DGD for three different wavelengths (directly copy from [166])

Studies [166] also report changes in PMD, and hence the differential group delay DGD, are well correlated with changes in the local ambient temperature. As is shown in Figure 5.4.1.1, 48-hour measures shows the DGD is less than 0.5ps for a 150km long Single Mode Fibre.

The temperature in the laboratory where the system operates fluctuates to a maximum of 10 degrees Celsius by non-human factors. Moreover, the total length of the single-mode fibre reel connected to the system during the experiment is no more than 100km (the total fibre loss is usually no more than 25dB).

In summary and theoretically, this value (DGD < 0.5ps) is less than the threshold value($\delta t \sim$ 2ps), so the delay caused by temperature change on the fibre will not affect the system performance.

5.4.2 Dark count at detector

In simple terms, the value of QBER can be simplified as,

$$QBER = \frac{dark\ count}{dark\ count + photon\ output}$$

As the temperature goes up, the number of dark count that reach the detector end is going to rise, so there are more unwanted photons that reach the end and then the value of QBER is going to go up.

In addition, the following figure shows a simplified system performance analysis model for different fibre length.

Figure 5.4.2.1 Basic communication system model

Assume that only dark count is taken into consideration at this stage and the system loss is only caused by fibre attenuation. For a 50km and 100km optical fibre, the photons arrive at single photon detector can be written as,

$$photon_{50km-output} = photon_{input} \times 10\% \text{ (10dB loss)}$$

$$photon_{100km-output} = photon_{input} \times 1\% \text{ (20dB loss)}$$

For light input of the same intensity, when temperature goes up (i.e. dark counts increase) ,the impact of the dark count for a 100km link is more significant than for a shorter 50km fibre link.

5.5 Experimental implementation

It has been seen that temperature changes affect the results of the system performance, and the theoretical analysis predicts that the single-photon detector in the transceiver is susceptible to temperature especially for longer fibre lengths, but the fibre itself is not highly sensitive to temperature. The main purpose of the experiment is to verify the theoretical analysis results and prove that the influence of temperature change on the system mainly comes from Alice and Bob.

The experiment is divided into two parts. The first part is to change the operating environment temperature of the whole equipment (including the transmission fibre) as shown in the Figure 5.5, and the other part is to only change the temperature around the transmission fibre.

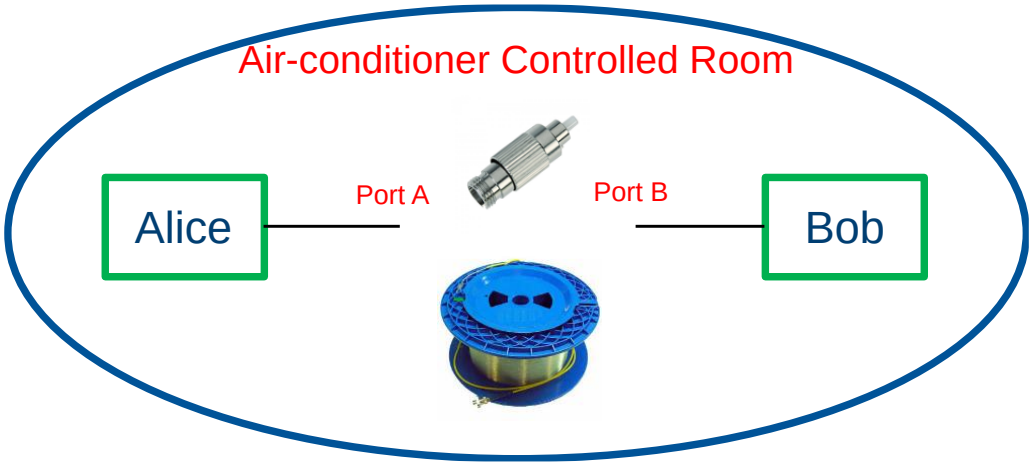


Figure 5.5 Experimental set-up for controlling the room temperature

5.5.1 Room temperature control

First, A pair of Alice and Bob were placed in A temperature-controlled room, with a 90km-long fibre ($\sim 21dB$ loss) optic connection between port A and port B. Do not actively adjust the set temperature of the air conditioning, 24 hours, the system performance is as follows.

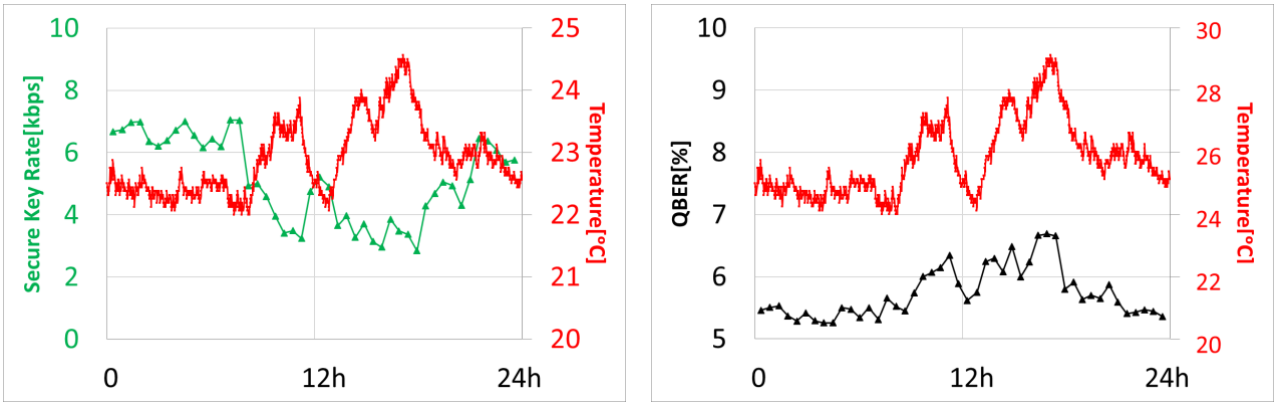


Figure 5.5.1(a) 24h system performance (90km fibre) without adjusting the room temperature

In the absence of any artificial temperature change, the temperature difference in the room over a continuous 24-hour period is approximately 3 ℃. As shown in previous experiments, when the temperature increases, the secure key rate decreases but QBER goes up.

The change of indoor temperature is mainly regulated by the central air-conditioning system according to the external environment. When a specific constant temperature is set actively, the indoor temperature will be relatively stable at the set value.

For a 50km($\sim 11dB\ loss$) optical fibre connected between A and B, secure key rate drops from 100 kbps to 80bps and QBER jumps from 3.5% to 5% when room temperature increase from 21℃ to 25.5 ℃.

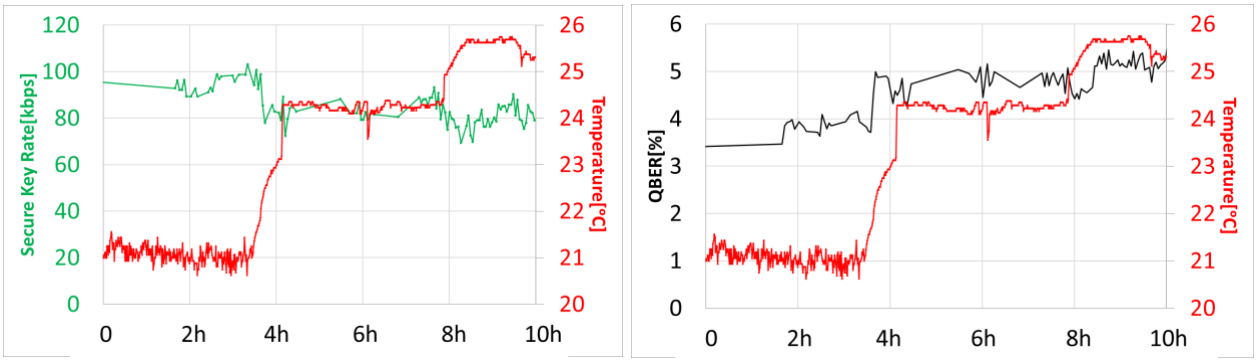


Figure 5.5.1(b) System performance with adjusting the room temperature for 50km fibre

Replacing the connection port A and port B with a 20dB optical attenuator and then setting the room temperature initially to 24℃, and then changing the room temperature in steps after different periods of time, the system performance is shown below. When the temperature is relatively stable at a certain value, such as 24℃ or 25.5℃, the secure key rate remains correspondingly stable. But at higher temperatures, the rate is lower than that at lower temperatures. And QBER has the inverse trend to secure key rate for the whole period.

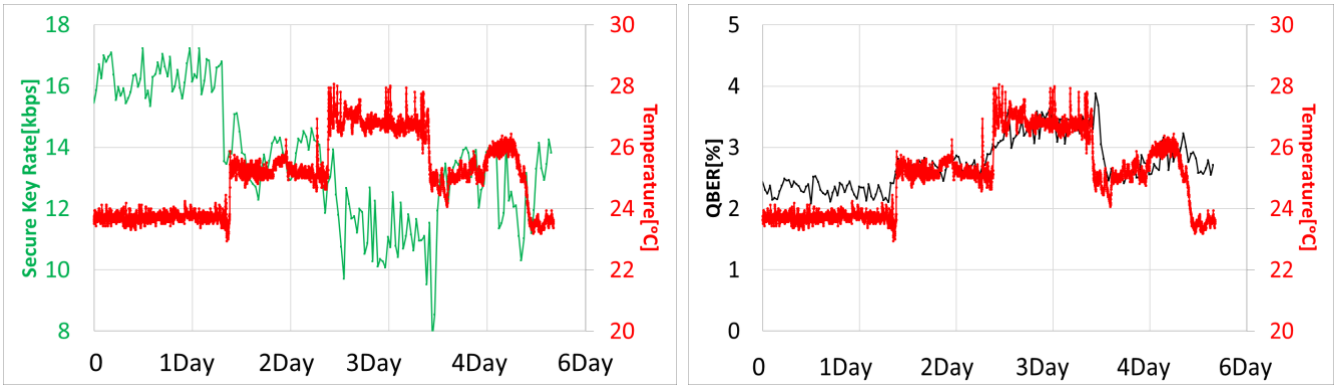


Figure 5.5.1(c) System performance with adjusting room temperature for 20dB Attenuator

Taken together, the preliminary conclusion can be drawn that changing the temperature of the whole system does affect the performance of the system. At the same time, the greater the attenuation of the channel is, the longer the generation time of each key will take. The experimental results here are consistent with the theoretical analysis, and the next step is to control the variables to exclude the influence of temperature on the fibre.

5.5.2 Fibre temperature control

According to the previous results, setting the room temperature to a constant temperature at 21℃. An insulated box is then fitted with the fibre spool, a temperature logger and a Light-House Greenhouse Heater to control the operating temperature of the fibre.

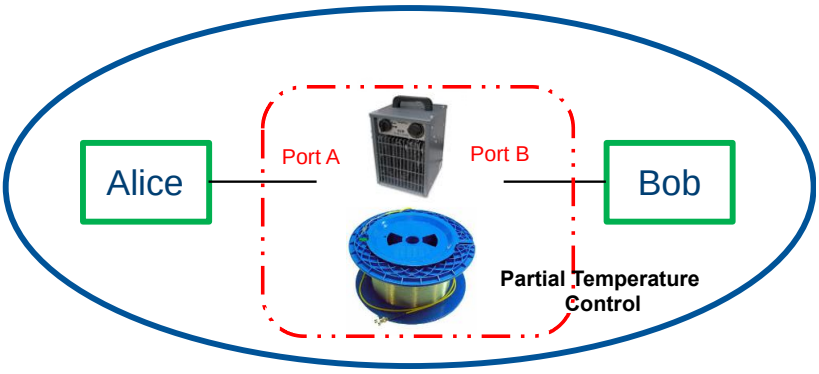


Figure 5.5.2(a) Fibre temperature investigation experimental set-up

For the longest fibre length, 90 km, that the system can withstand, the performance of the system under two different operating temperatures of the fibre is shown in Figure 5.3.2(b).

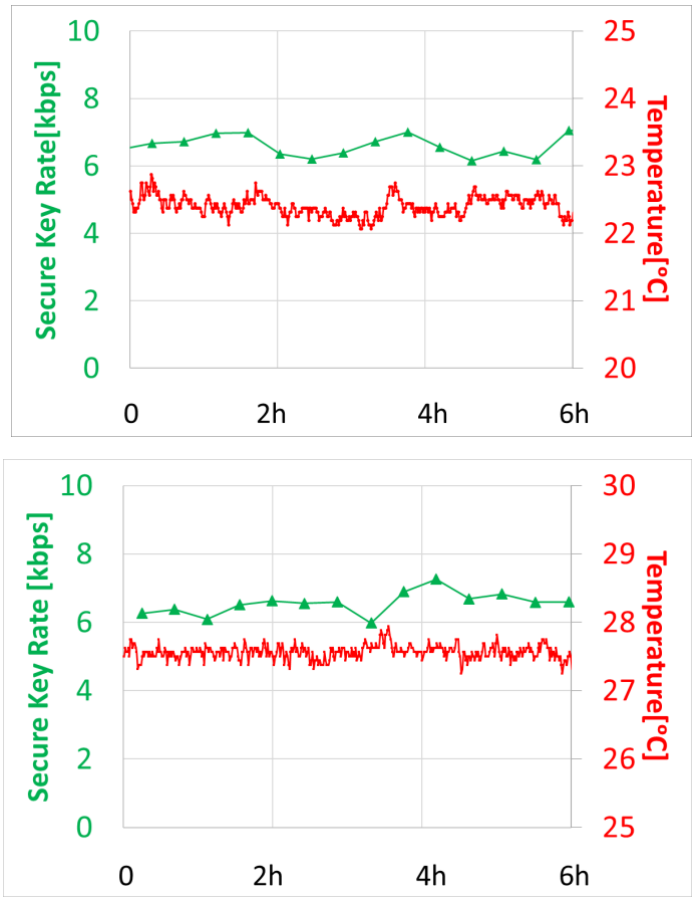


Figure 5.5.2(b) System with 90km fibre connected performance at 22.5℃ and 27.5℃

After the temperature in the box has stabilized for a period of time, record data for six consecutive hours. Secure key rate reaches 6.7 ± 0.4 kbps at 22.5℃ and slightly changes to 6.6 ± 0.3 kbps when temperature goes up to 27.5℃.

5.6 Discussion

The relationship between the number of dark photons and temperature is roughly estimated based upon the research [56], and the ***MATLAB*** simulation results as shown in Figure 5.5.2(c) below are obtained and the parameters are same as previous chapters apart from changing dark current rate as temperature changes (refer to Table 4.2.3). Both simulation and experimental results indicates room temperature increasements will degrade system performance.

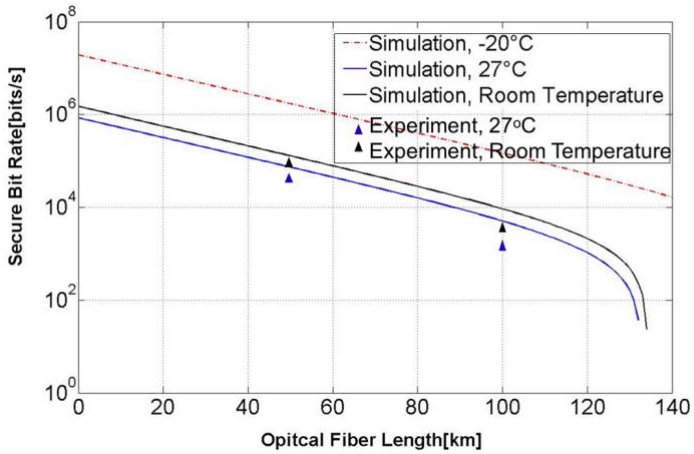


Figure 5.6.1 Matlab simulation for room temperature effect at different fibre length

SKR represents the speed at which the system generates a valid key. Take the average value of a series of temperatures and SKR respectively, and then draw the scatter diagram, as shown in Figure 5.6.2. We find that the value of SKR decreases approximately linearly as the temperature increases. As indicated by Eq (23), dark current noise is proportional to temperature, thus reducing the value of SKR. Since the controlled temperature can only be within the range of 20℃ to 30℃, the trend is approximately linear.

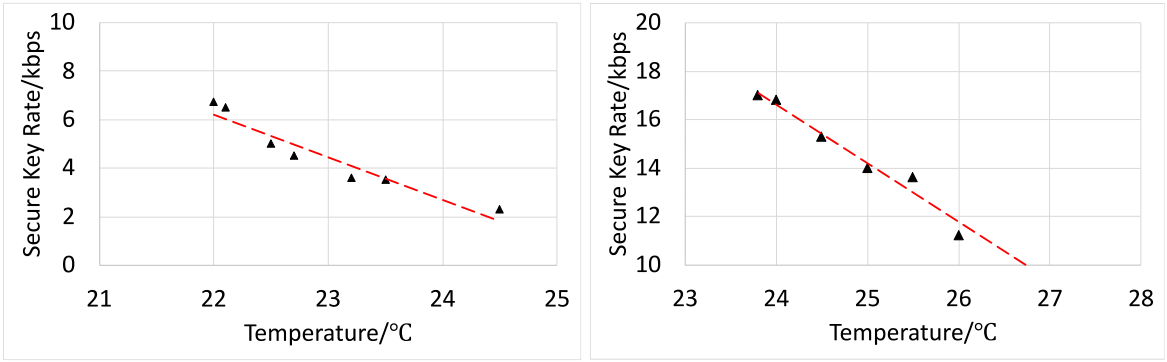


Figure 5.6.2 SKR vs Temperature at 50km(left) and 20dB attenuator(right)

5.7 Summary

Chapter 5 firstly proposed the temperature effect on QKD system performance. Then theoretically analysis and predict the relationship between temperature change and secure key rate as well as quantum bit error rate. It has been proved and verified that time delay effect due to temperature changes around fibre itself can be ignored as it will not lead to any performance degradation. Room temperature changes dominate system performances , that is , the higher temperature environment where system (i.e. Alice and Bob) locate, the lower secure key rate and higher QBER value will be. For both fibre reels, especially long distance(> 50km), and attenuators connected into the system, As the temperature rises from 24 to 28 degrees Celsius, the secure key rate drops from 100 kbps to 80 kbps (appx. 20% performance worse).

Simulations results matches the experimental results as system operation temperatures increases SAPD dark count and will the secure key rate be deducted. Last but not the least, For longer fibres, it is more crucial to keep the operating temperature relatively low and constant.

Chapter 6. Suppression of Raman noise by polarisation control

Chapter 5 has demonstrated some of the factors that will degrade the secure key rate under some circumstances. This chapter report how Raman noise affects the hybrid system and the effect of optical polarization drift on the performance of the system. Finally address these issues corresponding optimal solutions are proposed to.

6.1 Motivation

So far, the design and experimental demonstration of the QKD system have been carried out on dark fibres [4, 90, 94, 97, 113]. This limits the deployable capability of QKD to a limited number of scenarios where the barriers associated with dark fibre availability and price can be overcome. On the other hand, wavelength division multiplexing (WDM) allows sharing a fibre to transmit multiple optical channels using different wavelengths. WDM compatibility between quantum communication and classical communication allows the deployment of QKD on fibre optics. This enhances the compatibility of quantum communications with existing optical infrastructures and leads to significant improvements in QKD in terms of cost effectiveness and addressable markets.

However, the coexistence of QKD with the intense classical channel presents a new challenge to QKD. The optical power of optical classical channel is several orders of magnitude larger than that of quantum channel due to single photon level. Multiplexing classical and quantum signals on a single optical fibre can lead to significant additional noise in quantum communication due to inadequate isolation or optical nonlinearity [167, 168]. Processing this kind of noise is a major problem in quantum key distribution system. Filtering technology is needed to improve the ratio of quantum signal to WDM noise. The realization of this filter will cause additional loss and seriously affect the performance of QKD. This is especially applicable for systems that rely on spectral wideband single-photon detectors [168].

This thesis has introduced the world fastest QKD link and demonstrated a gigabits classical system encrypted by Toshiba QKD system which is stable for long term field trials. Since the transmitter energy level of a traditional data link is proportional to the data rate, it is of great benefit to find the relationship between the appropriate incident energy level and the noise, as well as to find the method that can be optimized for hybrid system performance.

6.2 Raman noise sources in a QKD-WDM system

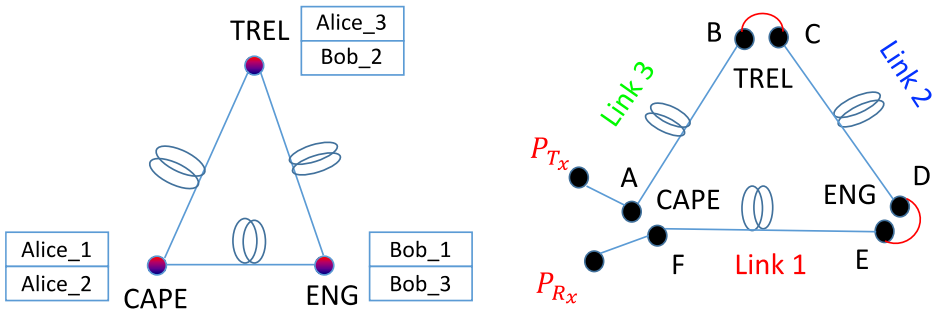


Figure 6.2.1 Hybrid system field trial diagram

In chapter 4, a field trial of a QKD system is introduced, and an experimental design is then carried out as shown in Figure 6.2.1 As shown in the figure above, three traditional optical fibre communication systems are connected in series. Two ends of each fibre have a pair of QKD systems (Alice and Bob) to encrypt the information, and the classical optical signal enters from point A in the figure and passes through a series of nodes (e.g. Node B and C located at TREL) and three segments of fibre and ends at point F.

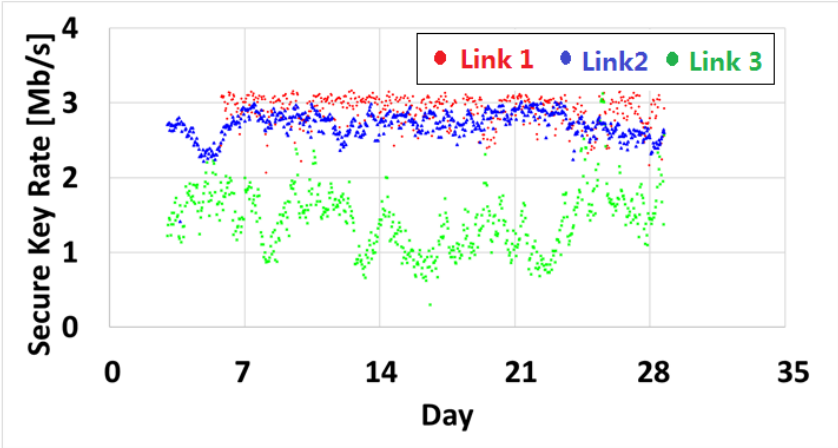


Figure 6.2.2 Hybrid system field trial secure key rate

When the optical signal is input at point A, the signal strength is attenuated by the fiber and the connectors. Hence the light energy input to Link 1 at point E is higher than that of link 3 input at point A and link 2 input at point C. As can be seen from the figure above, the link 3 with the highest power produces the slowest key and the lowest input power into link 1 results in the largest secure key rate. Each pair of Alice and Bob are manufactured to be identical and kept in rooms with a relatively constant and constant temperature. Therefore, the different secure key rates here are mainly due to different classical power level.

Typically the classical and quantum signals are multiplexed using standard wavelength division multiplexing technology (WDM). Two main technical difficulties arise when trying to multiplex the two types of signals in the same optical fiber. The first one is related to the fact that the power level difference between a classical signal and the single-photon level can reach 100 dB. Even small crosstalk can really saturate the single-photon detectors. The other hurdle is noise generated from the classical channels when photons are inelastically scattered due to the spontaneous Raman scattering (SRS) limitation [35, 87, 168] .

Figure 6.2.3 shows how the Toshiba QKD system encrypts high-speed signals through the fibre by multiplexer and de-multiplexer. Ideally there is only a single photon per optical pulse for a quantum channel. And the data channel has much higher power (> 60dB) than the quantum channel. However each pulse contains lots of photons for a Gb/s data link transmission and the majority is lost due to attenuation in the fibre. Although the wavelength of data channel, clock, quantum channel etc. are different, they are all combined and then transmitted in a single optical fiber. If the isolation is insufficient between each channel, expecially the high power signal, it will highly possilbe lead to impairments affect the quantum signals and finnaly degrades the secure key rate.

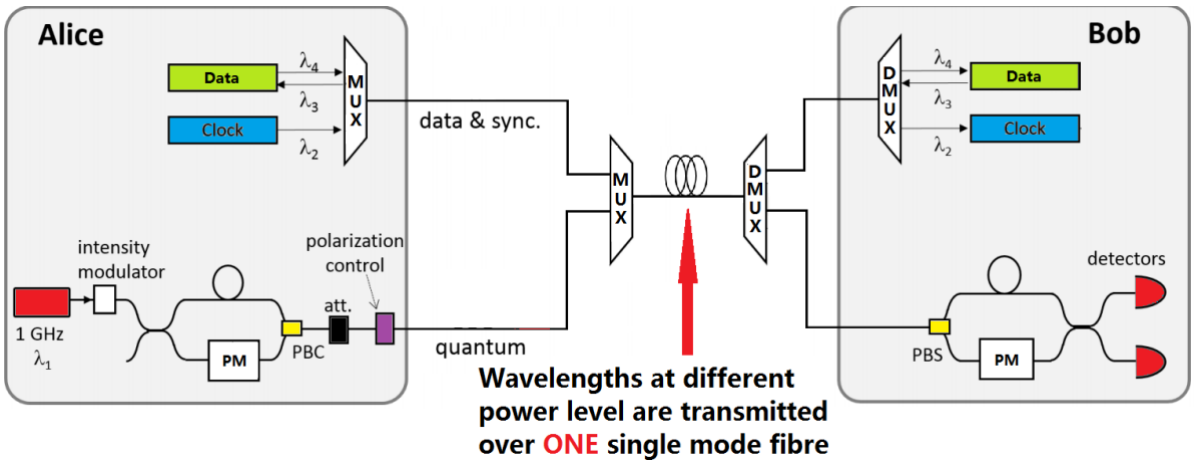


Figure 6.2.3 Hybrid system diagram

The analysis of Raman noise on QKD has been carried out in Chapter 3, In the following, we analyse the impact of the spontaneous Raman scattered noise generated from multiple optical classical channels (all wavelengths produced and transmitted over the system) on a single quantum key distribution channel.

6.3 Experimental implementation of studying Raman scattering on the high-speed QKD-WDM network

Before starting the experiment, it is necessary to identify the wavelengths that the system uses and the measurement appears as shown in Figure 6.3(a). Here connects one Alice and Bob to the Optical Spectrum Analyzer (OSA) in turn, and then measures and records the wavelength data.

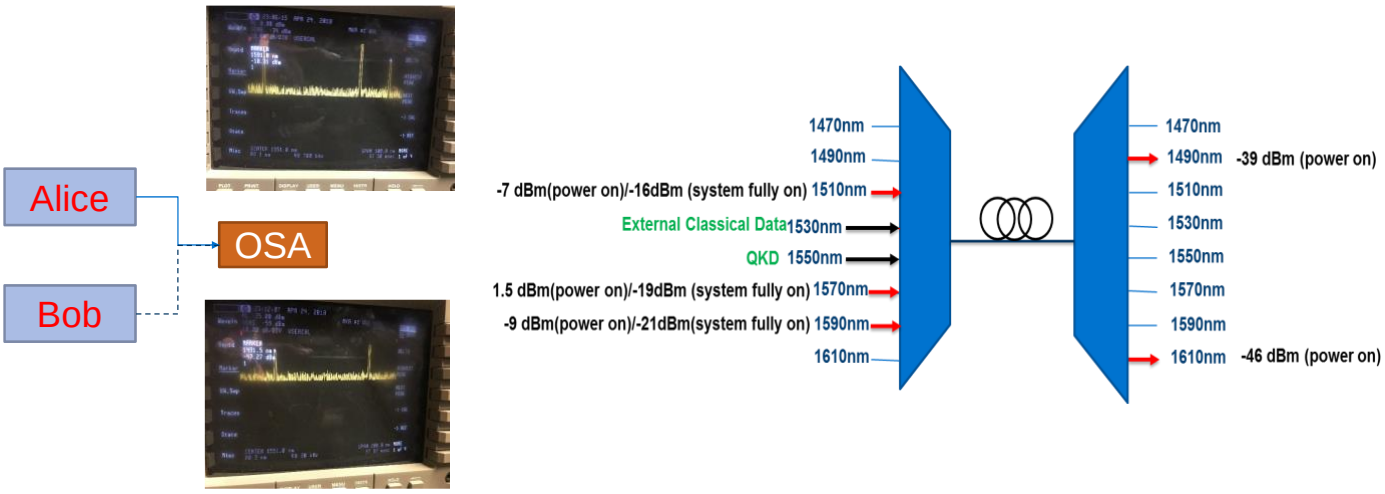


Figure 6.3(a) Alice and Bob wavelength inspections

Each Alice (or Bob) can output (or input/detect) eight different wavelengths of light. The wavelength ranges from 1470nm to 1610nm at intervals of 20nm. Within the detectable range of the OSA, Alice has three different signal outputs when the system is working, with maximum power of -16 dBm at the wavelength of 1510nm. According to the system instructions and practical needs, eight wavelengths are assigned for clock, optical time domain reflectometry (OTDR), phase compensation and reconciliation. 1530nm is allocated for the transmission of external classical high-speed optical signals and 1550nm is used for QKD signal transmissions.

Stimulated Raman scattering (SRS) can occur simultaneously in both forward and backward directions relative to the pump laser propagation. However, due to the different gain coefficients and interaction routes in these two directions, the experimental gain ratio of forward and backward SRS may strongly deviate from unity [169, 170].

In the actual communication process, the light energy at the wavelength of 1530nm will change with the propagation data rate and is much larger than the single photon power at 1550nm, while other wavelengths are set by the system and cannot be changed. Therefore, in the

following experiments, both the forward and backward stimulated Raman scattering effect due to 1530nm light at different power levels acting on the light of 1550nm is mainly focused.

6.3.1 Experimental set-up

The fundamental quantity characterizing spontaneous Raman scattering is the effective Raman scattering cross-section $\rho(\lambda)$, measured as a function of the wavelength λ. The effective Raman scattering cross-section is intimately related to the commonly measured fibre characteristics, Raman gain [169].

The Raman scattered power emerging from the fibre input, $P_{ram,b}$, and fibre output, $P_{ram,f}$, can be calculated as

$$P_{ram,b} = N_b \,.P_{out} \,.\frac{\sinh(\alpha L)}{\alpha} \,.\rho(\lambda) \,.\Delta\lambda$$

$$P_{ram,f} = N_f \,.P_{out} \,.L \,.\rho(\lambda) \,.\, \Delta\lambda$$

where index b stands for "backward" , f for "forward", N_b and N_f denote the number of backward and forward classical channels, $\Delta\lambda$ denotes quantum receiver bandwidth, and the optical power at the fibre output is

$$P_{out} = P_{in} \,.e^{-\alpha L}$$

with $P_{in}$is the power of the optical signal at the fibre input.

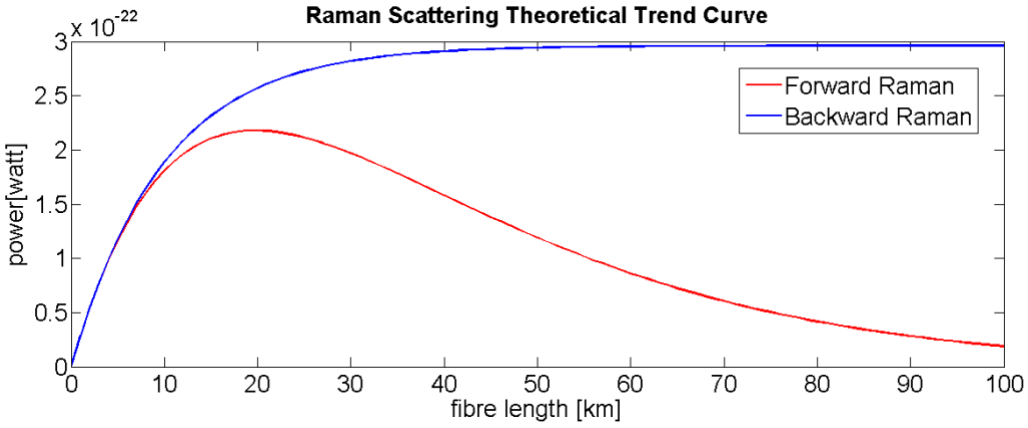


Figure 6.3.1(a) Matlab simulation of Raman noise vs Fibre length

Relationship between the Raman power and the transmission distance are given in figure above. The power of the forward-Raman reaches a peak value at a distance about 25 km in before it starts to decline, while that of the backward-Raman saturates and does not decrease with

distance. In the case of forward-Raman, the accumulation of Raman scattering power along the fibre is eventually outstripped by the increasing fibre attenuation, leading to a reduction of forward-Raman power. In contrast, backward-Raman power travels back to the input of fibre and is not subjected to higher loss with increasing distance. Hence, the power of backward-Raman never decreases but reaches saturation asymptotically.

Raman noise will produce extra photons arriving at Alice and Bob terminals, thus affecting system performance. As for the forward Raman noise, the influence of Raman noise on the system decreases gradually with the increase of fibre transmission length, so it is not a priority concern in the long distance transmission. However, the backward Raman noise is saturated and unchanged in a system over about 10km and increases linearly with the increase of the input optical power. In other words, in the long-distance transmission system, noise photons generated by the reverse Raman noise must be received by Alice, thus the QBER value increases while the system performance gets worse.

Due to the limitations of Toshiba QKD system, the length of the fibre and the classical communication channel power can be modified during the actual operation, apart from the temperature effect mentioned in the previous Chapter. From the equations above, it can be seen that the Raman power is positively correlated with the incident signal power. And the length of the fibre in the system also affects the power.

Considering the limitations of Toshiba's QKD system, the experiment does not use Alice and Bob, but instead, a separate experiment is used to simulate the study which is shown in Figure 6.3.1(b). The main purpose of this experiment is to study how many photons at 1550nm are detected when incident light of different wavelengths is transmitted through a series of components and optical channels.

A Continuous Wave(CW) Laser is used in the experiment to produce the required wavelength of light. Since the wavelength of light produced by the laser is hardly possible to produce a pure wavelength of light, a band pass filter (BPF) selecting corresponding wavelength is connected after the CW laser in order to screen out the specific wavelength of light more accurately. A circulator is a passive, non-reciprocal three- or four-port device, in which an optical signal entering any port is transmitted to the next port in rotation (only). It aims to divert scattered photons from two directions to each detector. The two variable optical attenuators (VOA) are used to change the overall attenuations of the link not only for protecting single photon detector but also find out the system limitations. Once the optical signal passes through

the fibre, it is then divided into two beams by an optical splitter. 10% of the light is used for monitoring and the other 90% goes into a 1550nm band pass filter. Here the filter aims to select 1550nm photons only and lead them to the single photon detector (SPD) at the receiver end. Similarly, the band pass filter and single photon detector on the backward arm work for the same purpose.

The CW laser is tuneable and is able to output different wavelength and power, and VOA#1 can also change the intensity of the light entering the fibre. Hence the next step is to explore how many 1550 nm photons can be produced by the same power at different wavelengths and by the same wavelength at different powers.

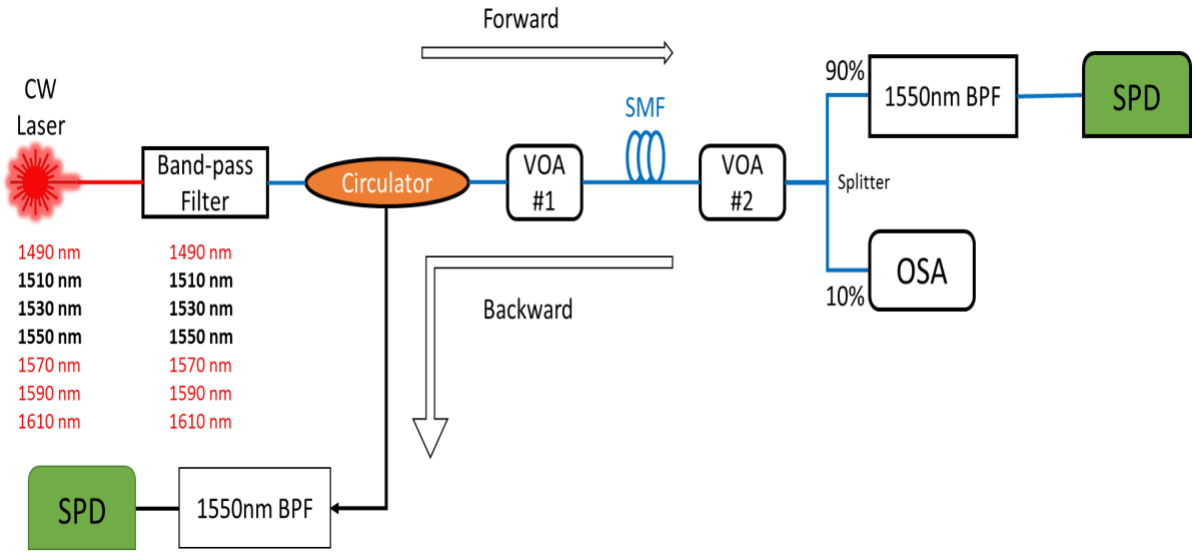


Figure 6.3.1(b)Raman scattering experiment set-up

6.3.2 Analysis of experimental results

a. 1550nm input and BPF + 1550nm photon detection

Firstly, an 8.9km optical fibre reel is connected to the system as shown in Figure 6.3.1(b). When both of the wavelength of incident light and first band-pass filter range is 1550nm, VOA#1 in the figure above is adjusted to change the light power entering the fibre. Gradually the power into the fibre is increased and the corresponding value on the single-photon receiver at the forward end is recorded.

The trigger frequency of the single photon detector, that is the internal clock, is 1MHz and the maximum count per trigger is 500,000. Within the range of the optical power injected into the

fibre being changed from $-105\ dBm$ to $-70\ dBm$, the difference between power input to the fibre and the power at the forward end single photon detector is 15dB due to transmission loss (fibre attenuation, insertion loss, components attenuation etc.) through the link. The single photon detector count saturates when the incident power is larger than -65dBm. So ideally, assuming the single photon detector has no upper limit, the number of photons is proportional to the power of the incident signal.

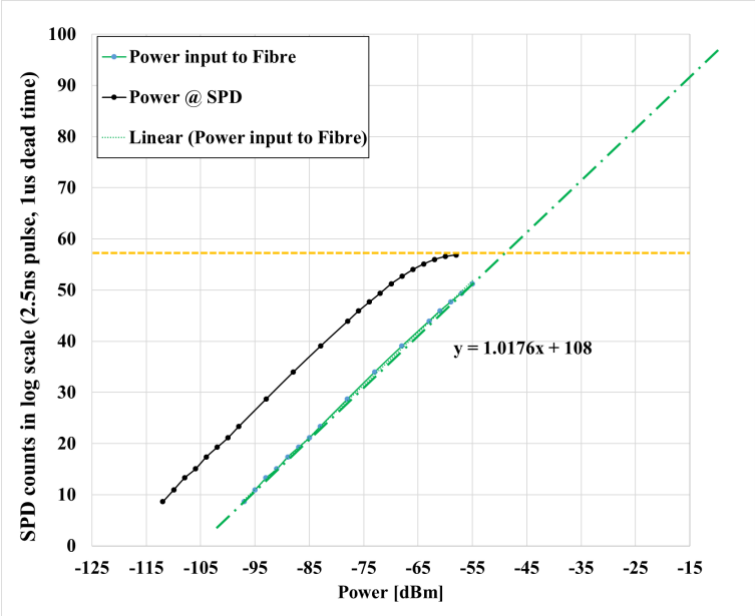


Figure 6.3.2.1 1550nm input and detection plot

b. 1510nm input and BPF + 1550nm photon detection

The input wavelength of the light is set to 1510nm and the filter at the input is replaced with a 1510nm- band-pass filter. Then, 5km of optical fibre is connected to the system and gradually adjusts the value of VOA#1 to change the optical power into the fibre.

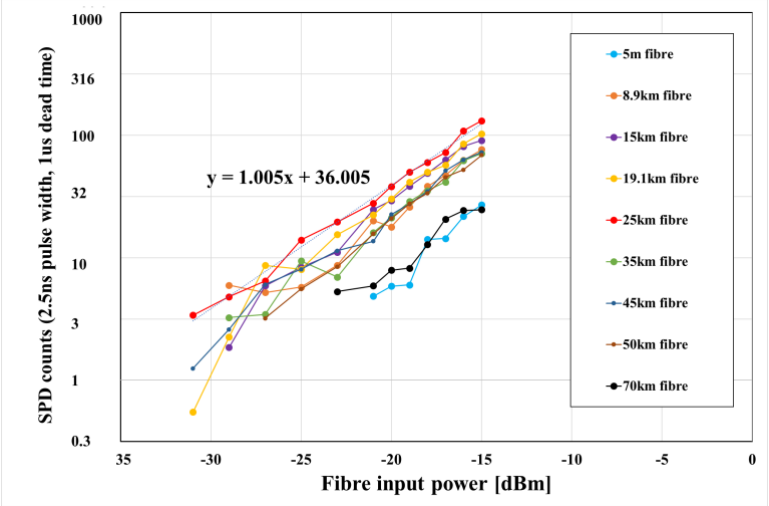


Figure 6.3.2.2(a) 1510nm input and 1550nm detection plot

The corresponding counts shown on single photon detector is recorded for each value of fibre input power. And then replace the fibre with longer length and repeat the steps. The input wavelength is approximately pure 1510 nm due to the 1510nm band-pass filter at input end and therefore should not be any 1550nm photons detected at the end. Any 1550nm photons arriving at the single photon detector are regarded as the forward Raman effect.

The results are plotted in figure 6.3.2.2(a) and in general, for a fixed fibre length, the forward Raman effect is approximately linear to the power launched onto the fibre. As can be seen from the figure above, when the input light power is fixed and the length of the fibre is varied, the forward Raman effect result is different.

Figure 6.3.2.2(b) demonstrates the trend line for forward Raman counts at different fibre lengths when the power into the fibre is -15dBm. For the same input power, the forward Raman counts increase when fibre length gets longer and peaks at 25km. In other words, forward Raman effect becomes less significant for long-haul fibre transmission.

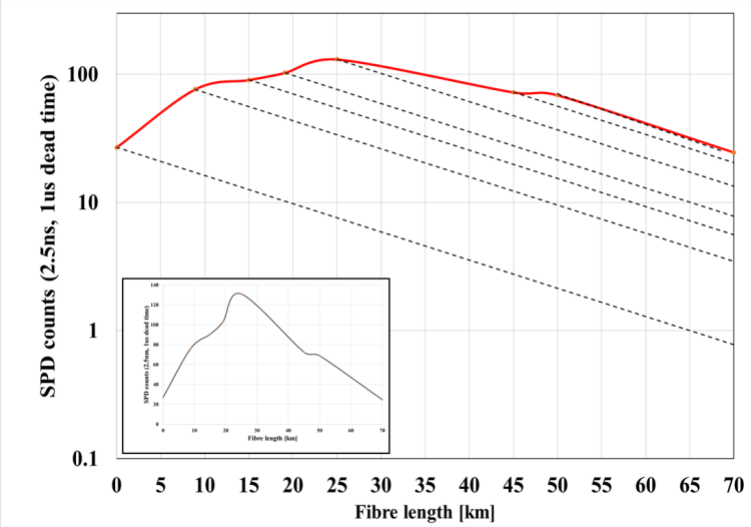


Figure 6.3.2.2(b) SPD vs Fibre length for 1510nm input and 1550nm detection

c. 1530nm input and BPF + 1550nm photon detection

In order to study the forward Raman effect at different wavelengths, especially the designed wavelength 1530nm allocated to Giga-bps classical data channel, one changes the input wavelength of the light to 1530nm and replaces the filter at the input with 1530nm- band-pass filter. Then, 5km fibre is connected to the system and one gradually adjusts the value of VOA#1 to change the optical power launched into the fibre.

The corresponding counts shown on single photon detector are recorded for each value of fibre input power. The fibre is replaced with longer lengths and as the steps repeated. The result of the 1530nm input signal is shown in figure 6.3.2.3 and indicates the same trend as figure 6.3.2.2(a). For each fibre length, the forward Raman effect is proportional to fibre input power. And for any fixed input power, The forward Raman noise first increases and then decreases with increasing fibre length and a 25km fibre length causes maximum noise.

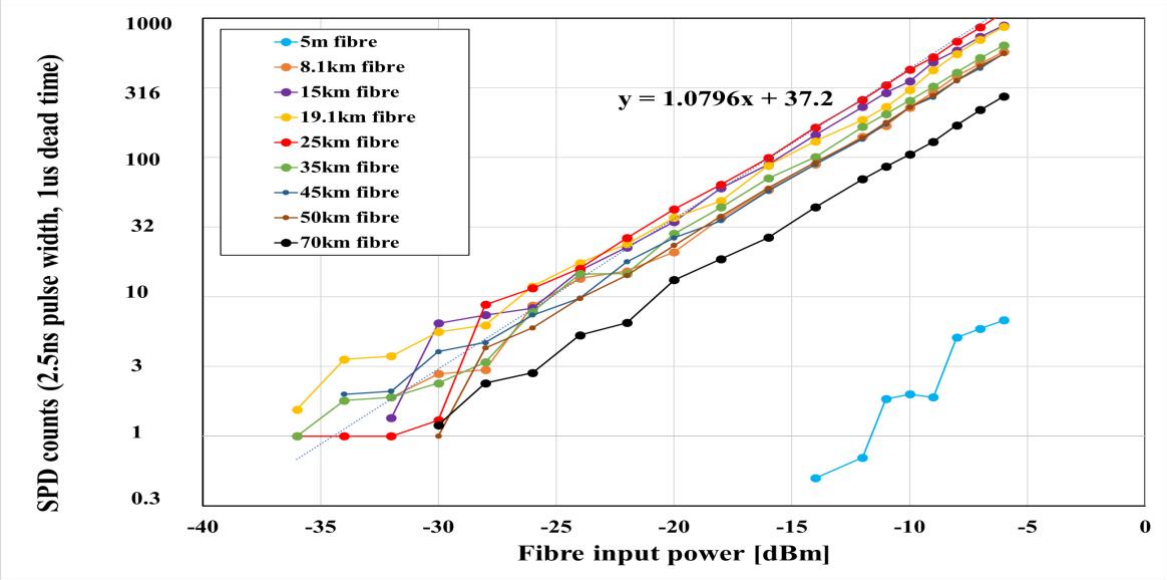


Figure 6.3.2.3 1530nm input and 1550nm detection plot

d. Comparison between forward and backward Raman noise

In addition to forward Raman noise, backward Raman noise, which has been mentioned earlier, also affects the number of photons on the receiving end. Figure 6.3.1(a) compares the relationship between A and B in terms of fibre length based upon theoretical mathematics models via ***Matlab***. As we can see, in the forward scattering direction Raman noise reaches a maximum 20km, and then decreases along with classical channel power. In the backward direction, noise reaches a saturation level as the distance increases. The count number of single photon detector at backward direction end shown in Figure 6.3.1(b). This shows the backward Raman effect on the system. The experimental results of forward and backward Raman scattering are integrated and fitted on the simulation curve shown in Figure 6.3.2.4.

For the 1510nm input and 1550nm detection experiment, measurements are taken at a fixed $-19\ dBm$ input power for each different length of fibre ranging from 8.9km to 98km. The forward Raman scattering starts to decline when fibre length is longer than 26.7km (fibre loss $fibre\ loss \sim 5.8dB$) experimentally and backward Raman begins to saturate at fibre length longer than 31.5km ($ibre\ loss \sim 6.9dB$).

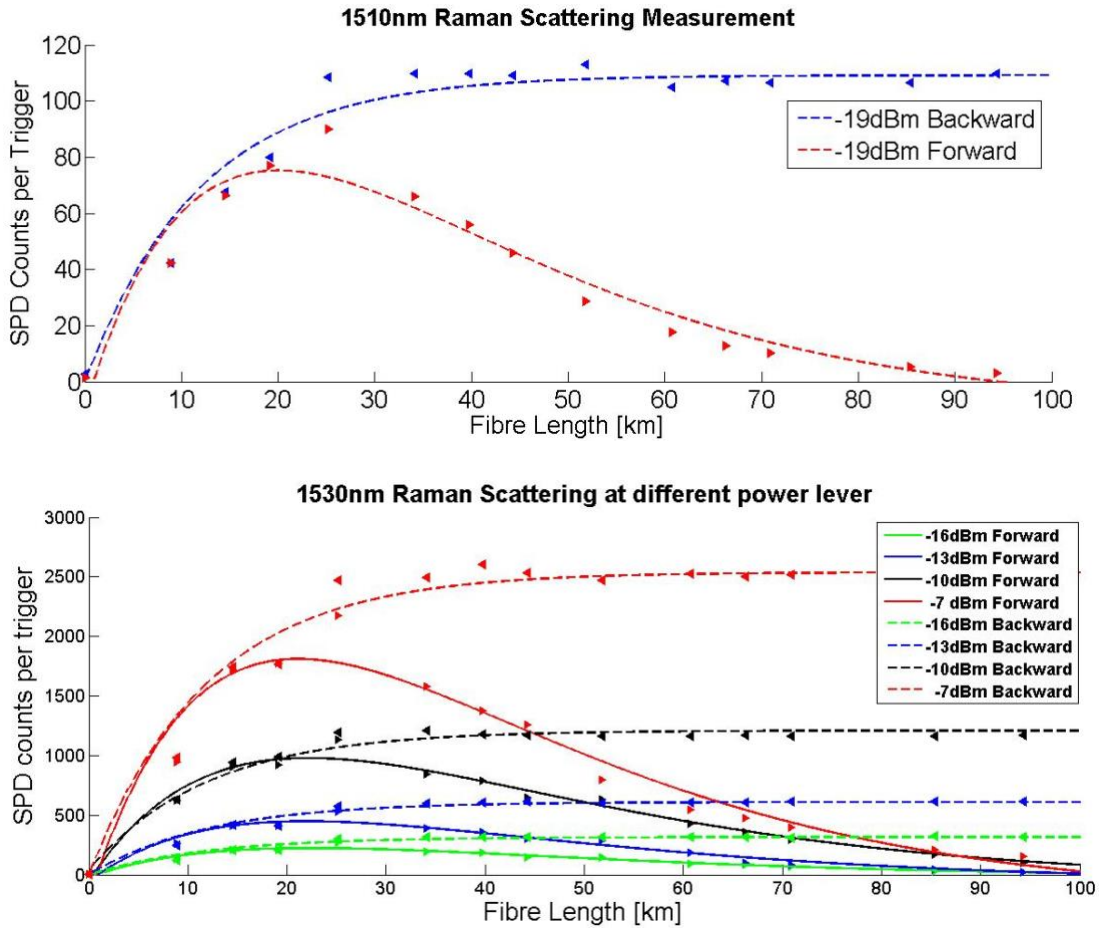


Figure 6.3.2.4 Fitted curve for 1510nm(up) and 1530nm(down) Raman scattering

For the 1530nm input and 1550nm detection experiment, measurements are produced at different input powers for lengths of fibre ranging from 8.9km to 98km. At each different fibre input power, the forward Raman scattering all starts to decline when fibre length is longer than 26.7km (fibre loss $fibre\ loss \sim 5.8dB$) experimentally and the backward Raman scattering begins to saturate at fibre length longer than 31.5km ($ibre\ loss \sim 6.9dB$). In addition, the backward Raman saturations levels (SPD counts) double with a 3dB increase of fibre input power.

e. Wavelength reversal

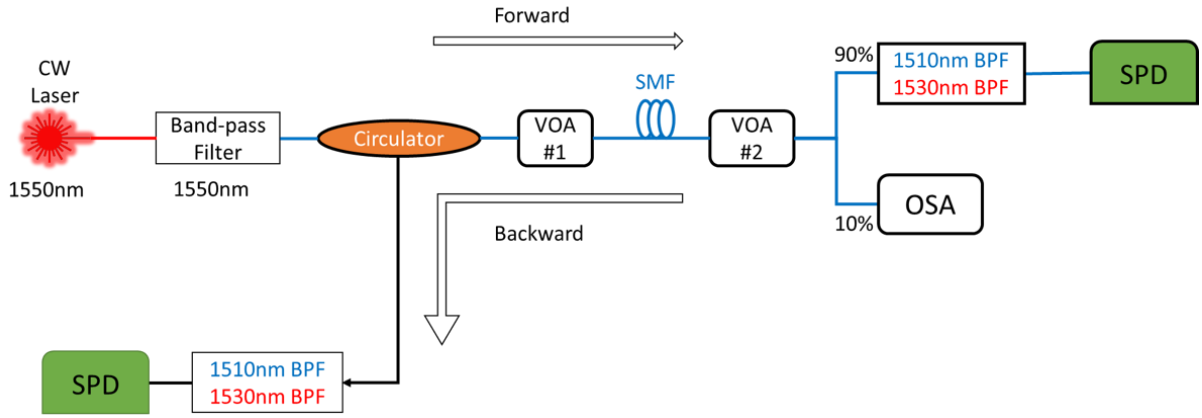
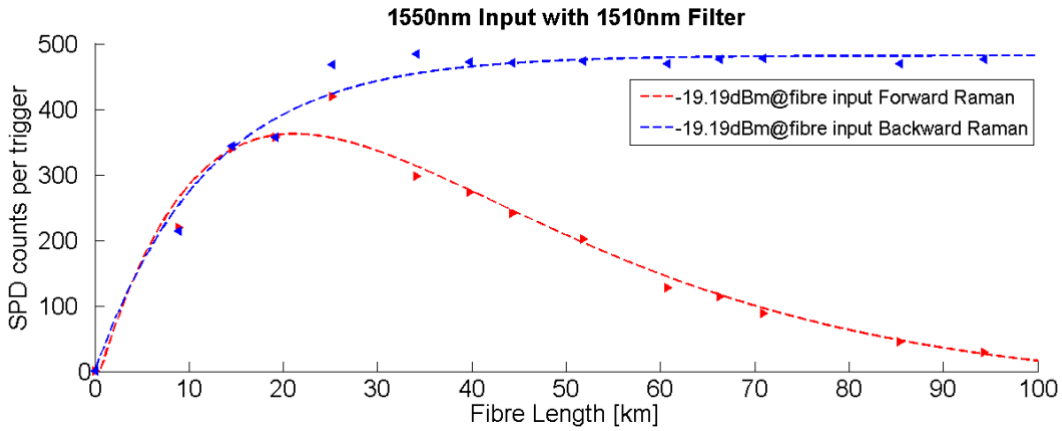


Figure 6.3.2.5(a) Wavelength reversal experiment set-up

The previous sections have studied the effects of relatively short wavelengths on longer wavelengths (i.e. 1510nm and 1530nm Raman effect on 1550nm), and the effects of slightly longer wavelengths on shorter wavelengths (i.e. 1550nm Raman effect on 1510nm or 1530nm) will be discussed here.

Similarly, the experiment is shown in figure 6.3.2.5 (a). The input end is a 1550nm Continuous Wave laser (CW laser) connected with a 1550nm band-pass filter which aims to select and output 1550nm light only onto the later system. The forward and reverse end single photon detectors are each connected to a band-pass filter of a particular wavelength (i.e. 1510nm or 1530nm).



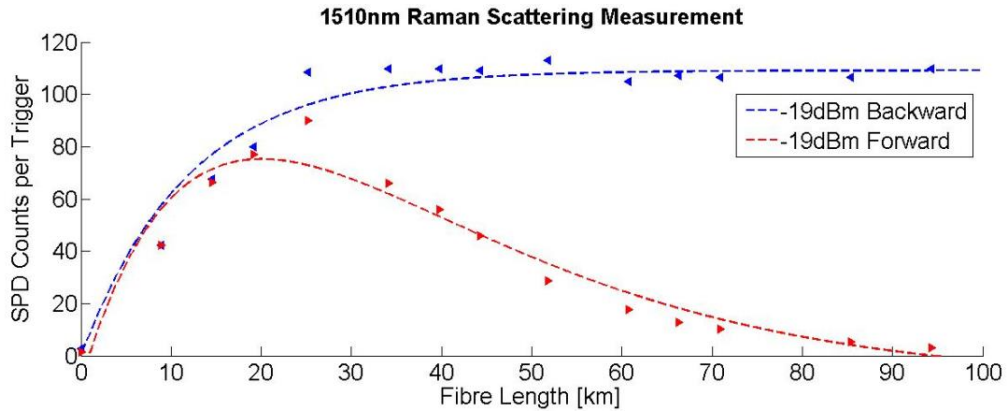


Figure 6.3.2.5(b) Raman effect of 1550nm on 1510nm and 1510nm on 1550nm

Firstly, one sets the two band-pass filters at the end to 1510nm and adjusting both the CW laser power output and VOA#1 to make sure the power input to the fibre is $-19.19\ dBm$. For fibre length ranging from 8.9km to 98km, experimental results fit the simulation curves shown in figure 6.3.2.5(b). The backward saturation level of the Raman effect of 1550nm for 1510nm is larger than that of 1510nm on 1550nm light.

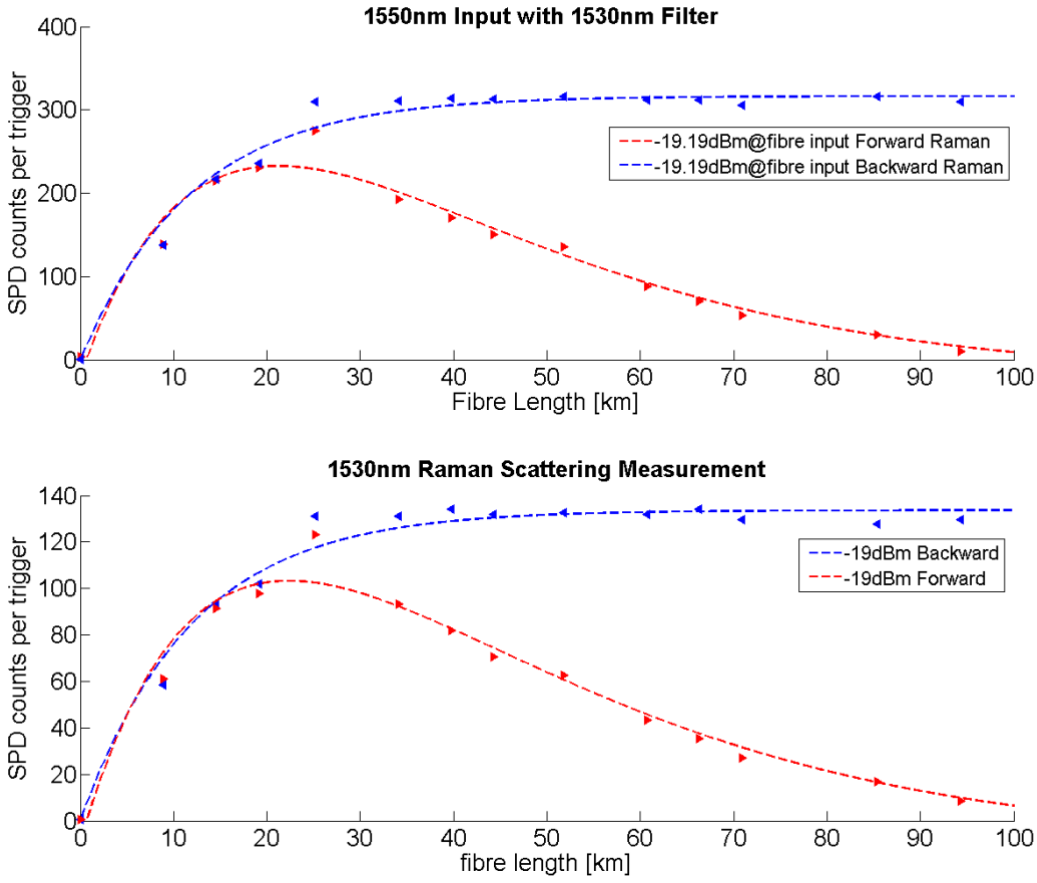


Figure 6.3.2.5(c) Raman effect of 1550nm on 1530nm and 1530nm on 1550nm

Similarly, with the two band-pass filters at the end set to 1530nm, one sets both the CW laser power output and VOA#1 to make sure the power input to the fibre is $-19.19\ dBm$. Figure 6.3.2.5(c) demonstrates both the experimental and simulation results.

6.4 Analysis of an external polarization controller effect on the network

The top half of the Toshiba QKD device is a transmitter that includes a light source that generates short pulses of linearly polarized light, so that light travels along the slow axis of the polarization-maintaining fibre. However, while light travels along the slow axis in the system shown below, in other systems the light source can be coupled to the fibre, allowing light to travel along the fast axis. The light pulse then enters an asymmetric Mach Zehnder interferometer (MZI), which in this case ACTS as a phase encoder encoding random critical information.

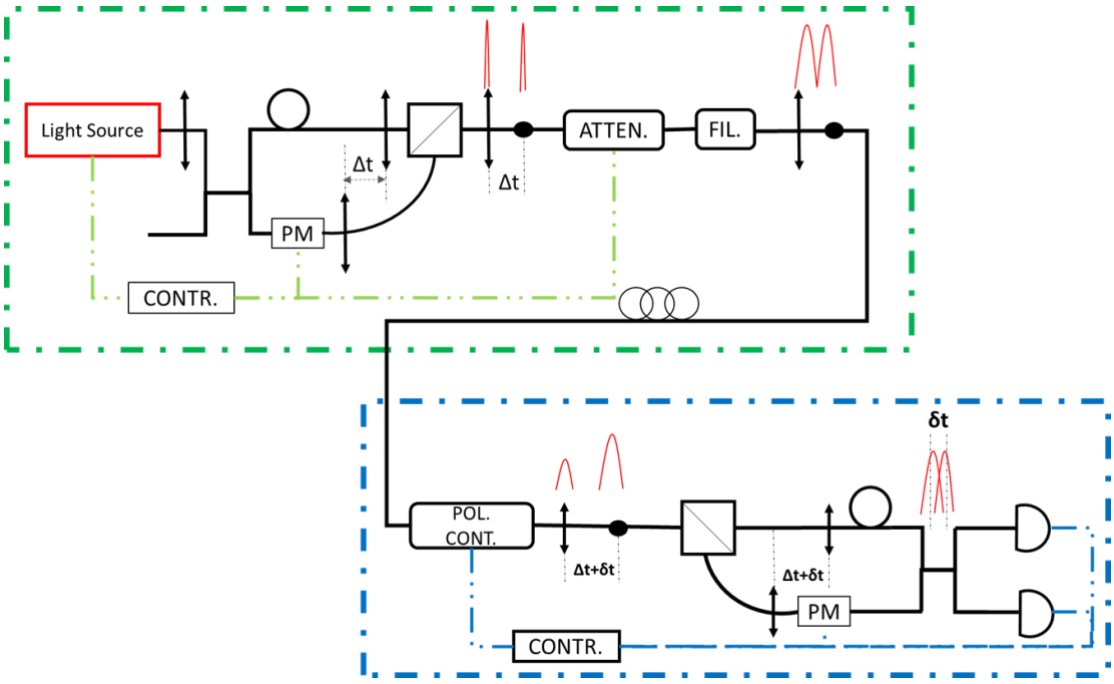


Figure 6.4 schematic of Toshiba QKD system

The Mach-Zehnder Interferometer is constructed using polarization maintaining fibre. First, the light pulses on entering the MZI pass through a coupler that splits the incoming light pulses into two paths. The first path comprises a longer arm (i.e. the upper arm in the diagram) of the interferometer using an optical delay loop. The other shorter path comprises a phase modulator that encodes random key information onto the light pulse. Due to the variation in the length of two arms, light pulses that follow either the short path and the long path suffer a temporal

separation Δt. This temporal separation may be set to $\frac{1}{2}$ the inverse clock rate of the QKD system. The pulses are then combined at a polarizing beam splitter (PBS). The PBS has the property that one of the input arms polarization is rotated by 90 degrees. This results in an output which has a polarization that can be decomposed into two orthogonal polarizations separated by a short time Δt. The pulses are then attenuated to the single photon level using an optical attenuator resulting in single photon pulses and before being emitted from the transmitter into an optical channel which is the optical fibre in this thesis.

The polarization beam splitter directs the light pulse to the long or short arm of the MZI containing the phase modulator based on the input polarization of the light phase. The receiving terminal phase modulator is used to decode the random key information on the optical pulse. In the PBS inside the transmitter, the PBS rotation at the receiver end comes from the polarization of the different arms. Therefore, the two outputs have the same polarization. With the correct input polarization, one of the two light pulses travels along the long arm of the transmitter interferometer and the other along the short arm. Thus, the delay loop cancels out the time difference between the two light pulses Δt, and since the two light pulses completely overlap, the optical interference results in the final beam-splitter.

In the process described above, the most important thing is that the PBS is polarization dependent and also the reference signal and quantum signal will be recombined at the same time at the receiver. If there is a classical light, that is the photon produced due to Raman effect, arrive at the same time of quant signal and orthogonal, it won't affect the detector. Otherwise, the noisy photons induced by classical signal will be wrongly detected and discard according to T12 protocols which will leads to higher QBER and lower secure key rate.

Therefore, changing the polarization of classical signal Raman photons to the detector can reduce the impact of noise on system performance to some extent.

6.4.1 Experiment on changing the photon polarization

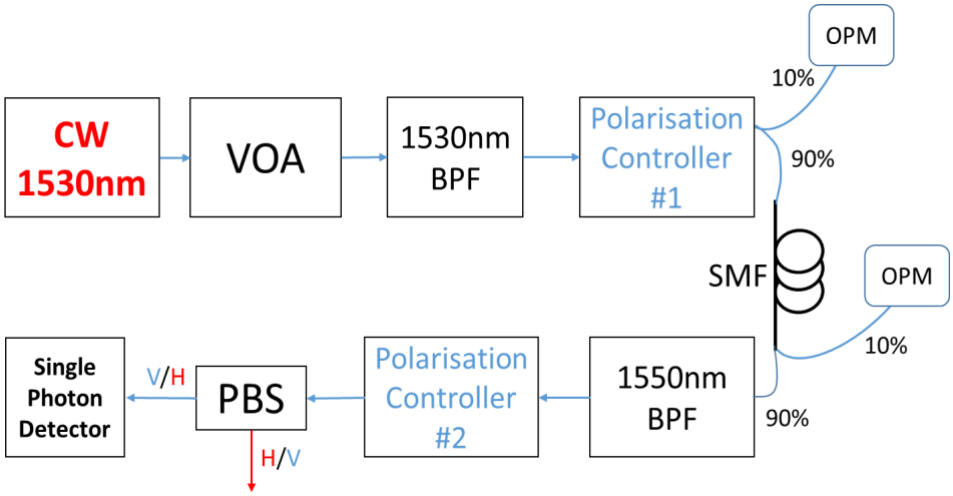


Figure 6.4.1 (a) experiment set-up for changing classical polarization at receiver

Figure 6.4.1(a) illustrates the experimental setup for changing the classical signal Raman noise photon polarization. CW laser is used to output the optical signal with the wavelength of 1530nm. Then a VOA is used to adjust the system attenuation and protection instrument. The band pass filter has a passing frequency of 1530nm to ensure that the signal entering the subsequent optical path is as close as possible to 1530nm, which is the frequency band of the traditional signal in the actual QKD hybrid communication network. The two polarization controllers are then positioned as shown to change the polarization direction of the photons entering the fibre and the final single photon detector. The bandpass filter has a passing frequency of 1550nm to ensure that as many photons as possible enter the single-photon detector at 1550nm, so that the number of photons measured by the single-photon detector can represent the light at 1530nm for the Raman noise at 1550nm.

Firstly, connecting the PBS to the optical path as shown in the figure 6.4.1(a), and then one adjusts the two polarization controllers to record the number of photons shown on SPD. Then the PBS is removed, and the polarization controllers are adjusted separately to record the number of photons and the results are shown in the Figure 6.4.1(b). The number of counts differs when the PBS is connected onto the path and changes either the polarization controller#1 or #2. Also the SPD counts doubled if the source increases the input signal by 3dB.

PC #1	PC #2	PBS	Raman Counts Changes
Y	Y	Y	Changes when PC#1 varies
Y	Y	Y	Changes when PC#2 varies
Y	Y	N	No Changes when PC#1 varies
Y	Y	N	No Changes when PC#2 varies

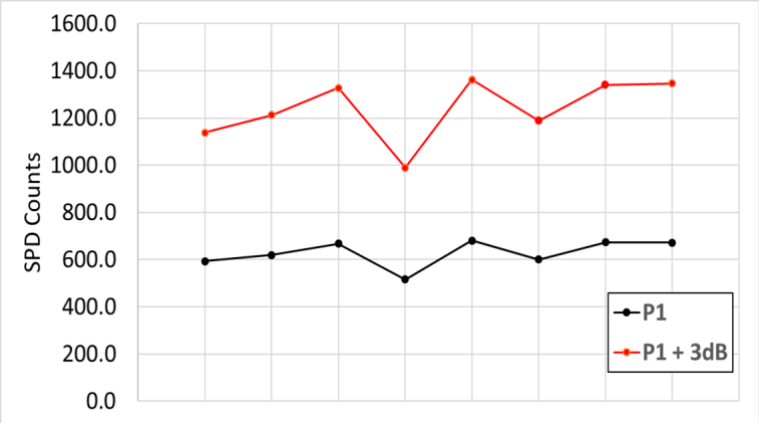


Figure 6.4.1 (b) Experimental results of polarization control

A polarization controller is an optical device which allows one to modify the polarization state of light. Once the polarization controller varies during the transmission, some photon polarizations states are changed to vertical or horizontal so that they can be selected or filtered by the PBS. As shown on the left of figure 6.4.1(b), the SPD counts can be minimised under some circumstance and hence changing the photon states potentially reduces the Raman counts on system performance.

Next, the polarization controller is connected to the hybrid QKD system to explore whether the system performance can be improved in the actual network communication process. But because of the limitations of the Toshiba system's interface (i.e., the system has no manually controlled optical output), the processing of the signal takes place inside the box, and only a polarization controller can be added before the quantum transmitter Alice to change the polarization of the photon through the later optical path.

6.4.2 Experiments on adding external polarization controller

Figure 6.4.2 (a) shows the experiment setup used to add an external optical polarization controller to reduce the effect of the Raman noise of the traditional communication signal on the quantum signal. In the dotted box is the optical path diagram that realizes the high speed traditional communication. The resulting high-speed optical signal at 1531nm is encrypted by the quantum signal produced by Toshiba Alice and transmitted to Bob via optical fibre. At the Bob end, the quantum signal and the traditional optical signal are separated (i.e. de-multiplexed), the quantum signal is then used for encryption and decryption analysis based up T12 protocol, and the traditional signal can be analysed or for further error correction after output from one of Bob's ports.

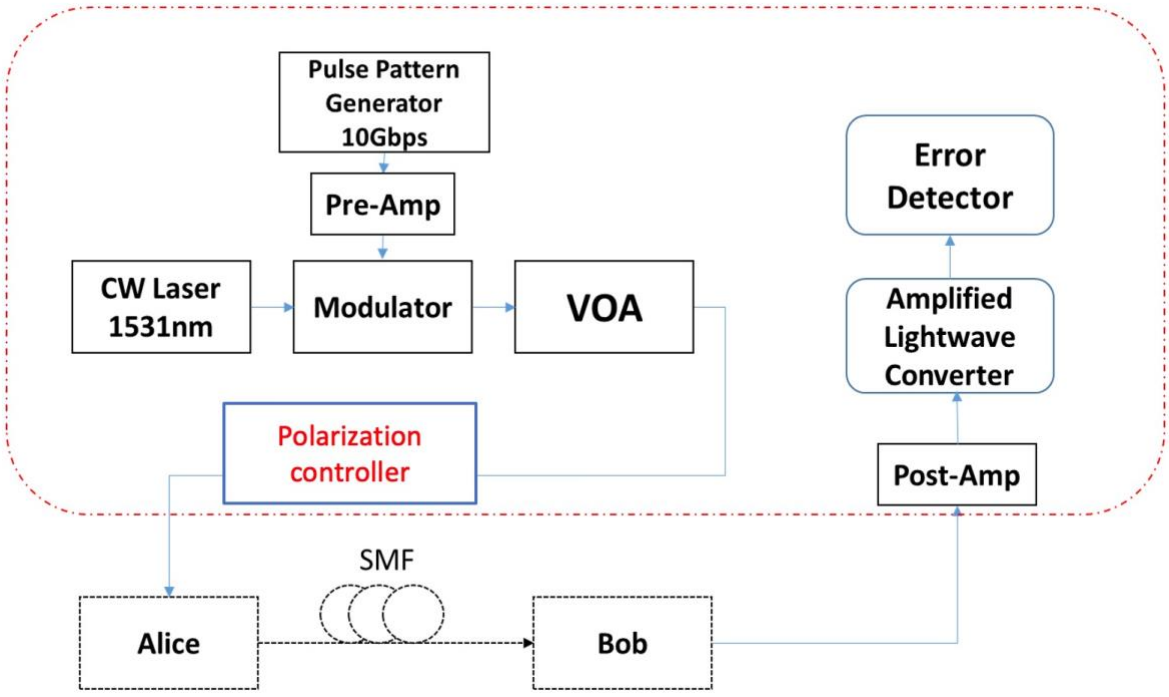


Figure 6.4.2(a) Diagram of adding external polarization controller

In this experimental exploration, the modulation mode of traditional high-speed signal and the performance of the system (i.e., the bit error rate) are not that important, as long as the data rate reaches the required level and other parameters such as the classical data power into Alice port meet the equipment requirements.

The traditional communication signals in the dotted box are pre-tested and calibrated before being fed into the transmitter, Alice. The data rate is set to be 10Gbps and the link is able to operate up to 25km (error free BER $< 10^{-12}$) and the power launches into fibre is up to

$-8\ dBm$. However, since the input signal to Alice should not be greater than $-10\ dBm$, the optical signal is set to attenuate to $-10.2\ dBm$ before being sent to Alice, resulting in the bit error rate rising to 10^{-9}.

First, the QKD system is put into a laboratory with little temperature change (Room temperature ~ 20.0 ± 0.5 ºC) in order to minimise the temperature effect on system performance and run for 24 hours. The result is shown in figure 6.4.2(b) where the QBER value is $4.1\% \pm 0.18\%$.

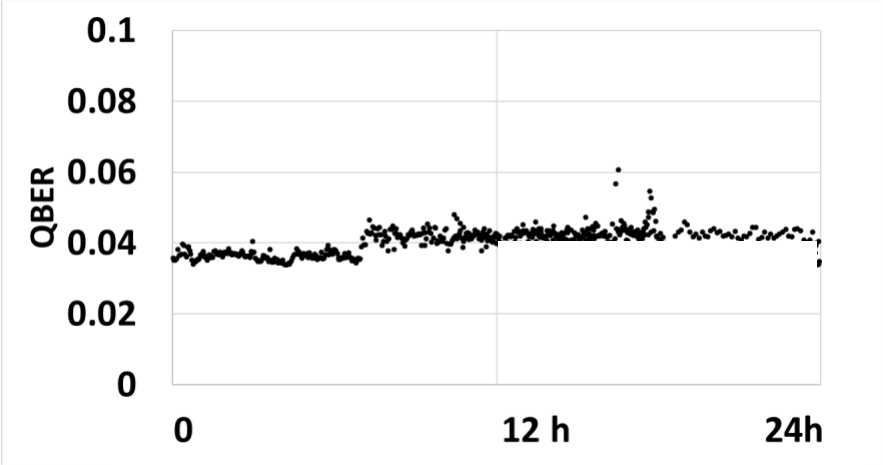


Figure 6.4.2(b) QKD only plot

Next, the modulated 10Gbps traditional signal is fed into Alice to be encrypted and then transmitted through a 19.8km single mode fibre (fibre loss ~ $4.4dB$). The value of QBER increases to $5.7\% \pm 0.44\%$ and fluctuates more than that of QKD signal only shown in figure 6.4.2 (c).

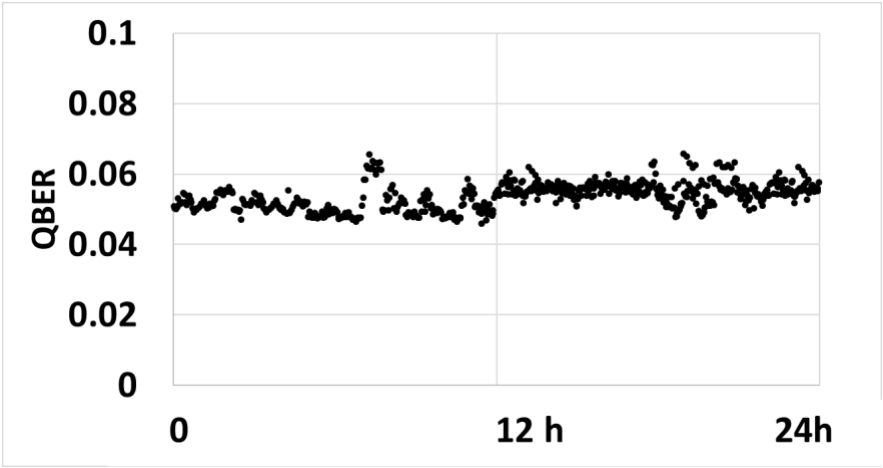


Figure 6.4.2(c) QKD+10Gbps classical plot

Connect a optic polarization controller prior to Alice's classical signal input port. Then slowly one adjusts the angle of the control plate of optic polarization controller to change the polarization angle of the classical signal into the system. Then the whole system is left to run without any changes for an hour and the changes in the value of QBER are recorded. Then one changes the angle of the polarizer a little bit and repeats the previous steps and records the data.

When the optical polarization controller is added and the angle of the polarizer is changed, the power of the output signal measured by the optical power-metre at the Bob end remains unchanged. Therefore, the addition of the polarization controller does not change the optical power of the original traditional signal. As shown in the figure below, changing the angle of the light polarizer does change the value of QBER in some short periods of time (1h-2h and 5h-6h).

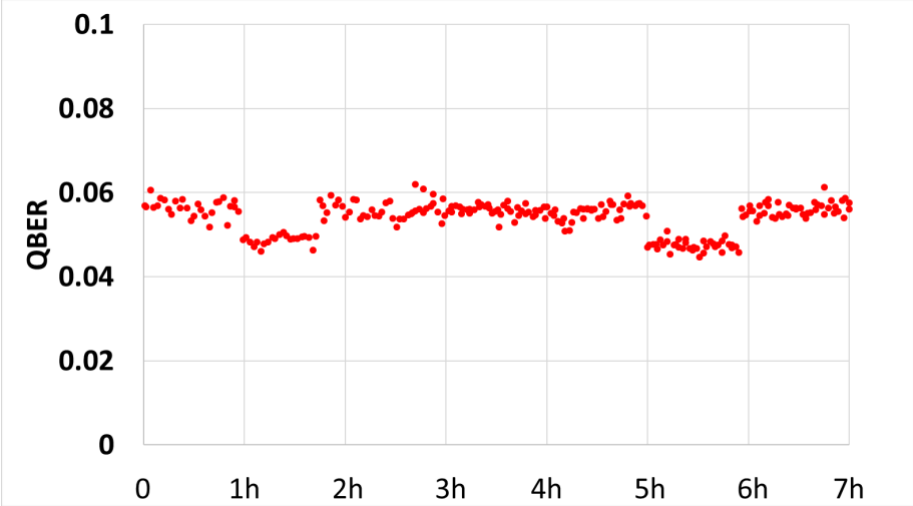


Figure 6.4.2(d) QKD+10Gbps classical plot with external polarization controller

$$\boldsymbol{QBER_{1h-2h} = 4.7\% \pm 0.13\%}$$

$$\boldsymbol{QBER_{5h-6h} = 4.6\% \pm 0.21\%}$$

$$\boldsymbol{QBER_{rest} = 5.7\% \pm 0.31\%}$$

$$\boldsymbol{QBER_{diff} = \frac{\left(\frac{(4.7 + 4.6)}{2}\right) - 5.7}{5.7} = -18\%}$$

During the time period of the two abnormal results, the value of QBER decreased by about 1% due to the change of polarization controller's angle.

6.5 Discussion and summary

In this chapter, it is firstly concluded from the previous field trial results that the input of traditional communication signals weakens the quantum signals to a certain extent. For the Toshiba QKD system pair that can be considered as identical, the input of a higher traditional signal will lead to a lower secure key rate, and the results show that the input signal increases by 3dB, and the secure key rate decreases from about 2.7 Mbps to 1.3 Mbps. Then it is pointed out theoretically that the traditional optical signal input simultaneously produces Raman noise to the quantum signal and degrades the secure key rate as well as increasing the value of QBER as a consequence. Then, the experiment confirmed that the signals of 1530nm and 1510nm wavelength would produce Raman noise for the quantum signals of 1550nm in the single-photon level, which would affect the performance of the system. Although the Toshiba system in practical applications generate signals in other bands except 1510nm and 1530nm, for instance 1490nm and 1570nm, since the Raman noise is proportional to the light power input demonstrated from this experiment, the Raman noise generated by the relatively small signal input power of other bands need not be considered.

At the same time, high wavelength on low wavelength and low wavelength on high wavelength Raman noises are explored, and it is proved that 1510nm and 1530nm can be selected as the wavelength of traditional communication channels. However, in this research, Toshiba equipment also pre-limits the wavelength of traditional signal to 1530nm.

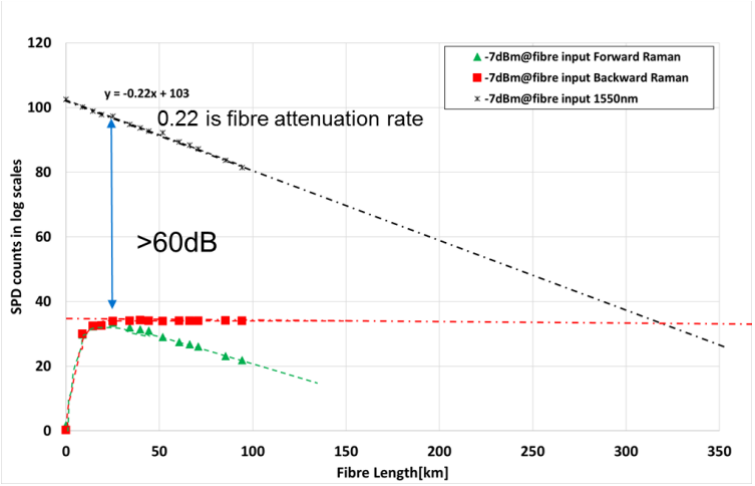


Figure 6.5.1 Raman noise limitation to transmission distance

As for Raman noise, the greater the power of the traditional signal is, the greater the number of photons will be produced. For each 3dB of input power, the number of photons doubles. For

optical fibres of different lengths, positive Raman noise first increases and then decreases with the increase of length, and reaches its peak at about 20km. The inverse Raman noise increases with the length of the fibre and becomes saturated after about 30km. That is to say, for a long-distance (usually greater than 30km) quantum cryptographic communication system, the reverse Raman is an important reason to limit the communication distance. The system requires that the signal to noise ratio should be greater than 10dB. Therefore, if only the long-distance optical fibre is considered to be affected by the reverse Raman noise, as shown in Figure 6.4.1, the communication distance of the system is up to about 280km. However, the actual communication system is subject to other influences such as attenuation, dispersion and channel cross talk, so the communication distance is much less than 280km.

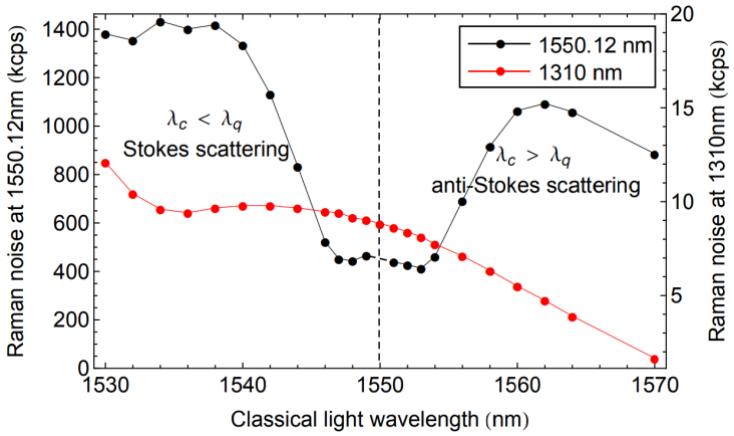


Figure 6.4.2 1550nm Raman scattering from different wavelength (directly copy from [171])

Due to the limitation of the main operating band of the laboratory laser and the filter in the C band, the influence of the wavelength signal greater than 1560nm on the quantum signal (1550nm) in the system has not been explored. However, since the power of signals in these bands is far less than that of traditional communication signals (the difference is more than 10dB), and anti-stoke scattering is smaller than stoke scattering as shown in the figure, only 1530nm signal's influence on 1550nm Raman noise should be considered in actual communication.

Finally, through the analysis of Toshiba system, it is found that adding a light polarization controller can improve the performance of the system, that is, QBER can improve about 18%. However, since the optical polarization controller changes the angle randomly, one cannot accurately measure and determine the relationship between the angle of the photon and the wave plate. Therefore, in the future, quantitative analysis can be carried out to further improve the impact of Raman noise on Hybrid QKD system in terms of polarization control.

Chapter 7 Conclusion and future work

Quantum key distribution is changing and revolutionizing the distribution of secret keys for securing the data information. Different from traditional cryptography, QKD makes the security of information transmission ensured by quantifiable security and detection of eavesdroppers become possible. In additional, QKD is able to potentially protect corporate and individual data and protect critical information infrastructure. Since the establishment of the initial fundamental protocol of QKD in 1984, huge progress in many aspects has been archived in this communication and encryption field. Not only QKD protocols have been improved to eliminate vulnerabilities caused by imperfect practical QKD equipment, but also breaking through the transmission distance of QKD on dark fibres in both laboratory and the field trials.

Developing the security for the current network infrastructure reliably and facing the coming quantum computing level decryption have never been a more pressing issue. Accounts in which personal and business data have been hacked are often reported, and the resulting consequences can cause significant damage and loss to the parties involved. Therefore, strengthening the security of networks that transmit sensitive data is critical to mitigate the threat of data theft. Using quantum cryptography to protect network data channel is a robust data communication security protection method, whose security comes from the quantum mechanics law. However, this security comes at a cost: quantum states often have to be used to transmit information, and these carriers are extremely fragile. As a result, previous approaches to building quantum networks have allocated extra dark fibres to quantum communications, unlike traditional data transmission fibres.

This thesis introduces the realisation and identifies difficulties of a three node hybrid quantum network, Cambridge Quantum Network. Firstly, a secure and high speed QKD encrypted link needs to be established both in laboratory using fundamental electrical devices and field with commercial advanced equipment. In addition to this advanced commercial QKD system, there have been secure key rate analysis comparisons between laboratory fibre coils and practical field trials demonstrating the practical QKD link performance. Comparisons based upon the highest QKD links help to identify factors that limit future QKD network scale and performance.

Secondly, systematic differences in performance indicates that the secure key rate is temperature dependence and then further studies have been done to determine the ambient

temperature effect on both transmission optic fibre and the devices. It has been then investigated how the polarization mode dispersion, which is supposed to create additional time difference between signal and reference pulses, leads to secure key rate changes. The ambient temperature changes on optic fibre can incur PMD but it has been proved in this thesis that it plays a trivial role in the system. On the other hand, changing of the ambient temperature on QKD devices in the lab plays a notably important role in performance of system for the dark count rises when temperature goes up.

Thirdly, for the QKD-WDM system, several classical channels are assigned for system clock, reconciliation and classical data and the power level can be 70dB higher than the quantum channel. Hence the Raman scattering from any of the classical channels onto quantum channel is remarkable. In order to confirm the significance of Raman scattering, the lab scale experiments have been conducted and concludes Raman scattering can be the dominant source of impairments to secure key rate in long distance QKD – WDM systems. And this type of noise can be mitigated by optimisation of the launch power of the classical optical channels, subject to maintaining adequate optical signal to noise ratio. In addition, a field trial within Cambridge quantum network has been performed and demonstrate the Raman scattering effect in real metropolitan QKD links. Last but not the least, an external polarisation controller aims to change the state of Raman photon comes from classical channel to be orthogonal to the reference signal so that the noise photons could be distinguished at the detector end on account of the delay line and hence system performance is optimised potentially.

7.1 Quantum network with 10/100 Gbps data encrypted by QKD

In this thesis, it has performed a comparison between laboratory experiment through fibre reels and field trial around the Cambridge Quantum network, with long term QKD transmission around a triangle between The University's Electrical Engineering building (CAPE), the main Engineering Dept. (ENG) and Toshiba Research (TREL). These links operated continuously for several months, with an average QBER around 3.0% and secure key rate reaches up to 3.2 Mb/s achieved for point-to-point link trial.

A field trial of QKD transmission has been performed from Duxford to CAPE, a distance of 33km with a loss of 7.5dB. This achieved a QBER of 3.4% and secure key rate of 1.4Mb/s. In addition, another extended duration field trial has been in operation from the Electrical Engineering building to the first node of the NDFIS network at Duxford and back. The total

transmission distance is 66km over a loss of 16dB. Here QKD traffic has co-existed with 2 x 100Gb/s classical traffic, all within the ITU C band for compatibility with telecoms networks.

The time evolution of QBER in the co-propagating QKD system archived a mean QBER of 6.62% with a standard deviation of 0.51%. This QBER value should occur at a loss of 16.4dB, in excellent agreement with the measured 16dB. And the secure key rate on the QKD link, with a mean of 80.2kb/s and standard deviation of 28.4kb/s. The results of this extended trial with co-existing classical and QKD signals are in excellent agreement with the previous trial, with the QBER increasing from 3.4% to 6.6% with a doubling of transmission distance.

Field trial results demonstrates the highest long-term secure key rates ever achieved within a hybrid quantum network. Based on the analysis of the results, the impact on performance caused by the addition of the classical signal and environmental temperature fluctuations have been figured out. And also the trial results matches theoretical and predicted results.

7.2 Factors affect the hybrid quantum network

In this thesis, system operating temperature and classical channel power level have been identified and quantified its corresponding impact on hybrid quantum network performance.

Firstly, the influence of temperature on the performance of QKD system is summarised from field trial performance. Then the relationship between temperature changes and security key rate and quantum error rate is analysed and predicted theoretically. It has been proved that the time delay effect caused by the change of temperature around the fibre is negligible and will not cause abrupt change of performance. The performance of the system is dominated by indoor temperature variation. The system is in a high temperature environment will lead to poorer performance than that in a lower temperature environment. When the temperature rises from 24℃ to 28℃, the security key rate drops from 100kbps to 80kbps (appx 20% decreases) and it will be even worse for longer fibre reel connected to the system (> 50km) or link attenuation/loss is greater than 10dB.

Besides, the simulation results are in agreement with the experimental results. When the operating temperature of the system increases, the SAPD dark count increases and the security key rate decreases. Last but not least, for longer fibres, it is more important to keep the operating temperature relatively low and constant.

It is also concluded from the field test that the input of traditional communication signal weakens the quantum signal to some extent. The higher the traditional input signal will lead to the lower safe key rate, and the results show that the input signal increases by 3 dB and the secure key rate drops from 2.7 Mbps to 1.3 Mbps. Then, it is theoretically pointed out that the conventional optical signal input generates Raman noise to the quantum signal when they two are transmitted through the same fibre, which reduces the security key rate and increases the value of QBER. Then, the experiment confirmed and quantitated that the 1530nm and 1510nm wavelength signals will produce Raman noise to the 1550nm single-photon quantum signal, which would affect the performance of the system. Although the Toshiba system in practical use generates signals in other bands other than 1510 nm and 1530 nm, such as 1490 nm and 1570 nm, and Raman noise is proportional to that from other wavelengths, the Raman noise from relatively small input power generated by other bands need not be considered.

At the same time, the short-wavelength and short-wavelength Raman noise are explored, and it is proved that 1510nm and 1530nm can be used as the wavelength of traditional communication channel. However, in this study, the Toshiba device also pre-limited the wavelength of the conventional signal to 1530nm.

Finally, through the analysis of Toshiba system, it is found that adding the optical polarization controller can improve the performance of the system, that is, QBER can improve about 18%. However, due to the random angle change of the optical polarization controller, the relationship between the photon and the wave plate angle cannot be accurately measured and determined quantitatively. Therefore, quantitative analysis can be carried out in the future to further improve the impact of Raman noise on the mixed QKD system from the aspect of polarization control.

7.3 Future work

There are a number of possibilities where the research studies can be taken onto further steps.

In this thesis, 10 Gb/s and 100 Gb/s modulated data channels have been used in the experiment. However, higher or different data rates systems such as 40 and 200 Gb/s have started to become available. Incorporating QKD with these systems will be required to be compliant with the next generation high speed data systems such as 5G.

The work described in this thesis mainly addresses point-to-point QKD links for both experiments and field trials. Perhaps the next step would be the implementation of QKD signal manoeuvring and routing in the presence of network elements such as routers, network switches, and Erbium doped fibre amplifiers. Dynamically switched and reconfigurable quantum networks using add drop multiplexers need to be developed to be compatible with the existing data communication infrastructure. Using WDM, preliminary theoretical proposals in this direction, around the form of link budget calculations for QKD, have been made [86].

Both QKD and classical data generation equipment are commercial devices and hence very limited parameters can be changed during the research. For example, it is not possible to experimentally identify what chip or electronic elements in the boxes are significantly thermal sensitive. Therefore, there can be a research associated with Toshiba to improve internal infrastructure such as adding dynamic and thermostatic compensation part. Also the polarisation controller can be embedded onto commercial classical data generation devices.

In terms of future large scale quantum network, I hope to further address three issues: the first is to develop an efficient key management technique that allows multi-point network configurations and multicast applications. The Cambridge QKD network is currently only available for point-to-point running. Therefore, the job of key management is to monitor the link and switch to other secure links. Complex node processing is also not used in this study. A multicast application consumes a large number of keys. In order to reduce the security key consumptions, a new method of node processing in the users' data communication layer based on network coding may also be helpful.

The second is to integrate the QKD network technology into an emerging optical communication infrastructure, known as photonic network. The optical signal is processed in the optical domain and does not need to be converted into an electronic form. The quantum network should be realized in the wavelength division multiplexing infrastructure of optical network, which corresponds to the lowest layer of photonic network. According to the user's request, the efficient QKD link can be directly realized through optical cross-connection and reconfigurable optical external multiplexer. With the expansion of quantum transparency range, the control signals in the control plane can be tightly encrypted with security keys. In fact, new control technologies, such as generalized multi-protocol label switching, make the control plane more open to the upper layers of other operators and end users. Malicious hackers may also have the opportunity to easily access the control plane, seriously endangering the security

of the entire network. QKD will play a key role in the development of secure photonic networks. Therefore, it is necessary to further integrate the coexistence of quantum signals and classical signals in existing WDM networks and explore more factors that limit the network performance.

The last is to broaden the QKD application to not only protect data confidentiality from being hacked, but also provide internet services, which are the basic functions of current security systems, such as identity recognition, authorized certification and digital signature. While QKD "unconditionally secure" support still needs further research, it may be achieved using existing QKD hardware and different attack models to assume that the enemy is subject to limited quantum memory or additional constraints on quantum resources of legitimate parties such as quantum processing and quantum memory. In any case, if QKD performance improves further and costs are reduced, then the expected QKD network can become the basic infrastructure for generating security keys for various cryptographic targets. This may be the main impetus to promote the development of QKD technology and the future research of QKD network.

Bibliography

1. Gisin, N., et al., *Quantum cryptography.* Reviews of modern physics, 2002. **74**(1): p. 145.
2. Scarani, V., et al., *The security of practical quantum key distribution.* Reviews of modern physics, 2009. **81**(3): p. 1301.
3. Gottesman, D., et al. *Security of quantum key distribution with imperfect devices*. in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* 2004. IEEE.
4. Jouguet, P., et al., *Field test of classical symmetric encryption with continuous variables quantum key distribution.* Optics Express, 2012. **20**(13): p. 14030-14041.
5. Stucki, D., et al., *Long-term performance of the SwissQuantum quantum key distribution network in a field environment.* New Journal of Physics, 2011. **13**(12): p. 123001.
6. Wang, S., et al., *2 GHz clock quantum key distribution over 260 km of standard telecom fiber.* Optics letters, 2012. **37**(6): p. 1008-1010.
7. Dixon, A., et al., *High speed prototype quantum key distribution system and long term field trial.* Optics express, 2015. **23**(6): p. 7583-7592.
8. Elliott, C., *Building the quantum network.* New Journal of Physics, 2002. **4**(1): p. 46.
9. Yoshino, K.-i., et al., *Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days.* Optics express, 2013. **21**(25): p. 31395-31401.
10. Qi, B., L. Qian, and H.-K. Lo, *A brief introduction of quantum cryptography for engineers.* arXiv preprint arXiv:1002.1237, 2010.
11. Vernam, G.S., *Cipher printing telegraph systems: For secret wire and radio telegraphic communications.* Journal of the AIEE, 1926. **45**(2): p. 109-115.
12. Pierce, J., *The early days of information theory.* IEEE Transactions on Information Theory, 1973. **19**(1): p. 3-8.
13. Van Meter, R., *Quantum networking*. 2014: John Wiley & Sons.
14. Biggs, N.L., *Coding natural languages*, in *Codes: An Introduction to Information Communication and Cryptography*. 2008, Springer. p. 1-16.
15. Lando, S.K. and V. I͡Ashchenko, *Cryptography: An Introduction: An Introduction*. 2002: American Mathematical Soc.
16. Stinson, D.R., *Cryptography: theory and practice*. 2005: Chapman and Hall/CRC.
17. Stallings, W., *Cryptography and Network Security, 4/E*. 2006: Pearson Education India.
18. Rivest, R.L., A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, 1978. **21**(2): p. 120-126.
19. Shor, P.W., *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM review, 1999. **41**(2): p. 303-332.
20. Coppersmith, D., D.B. Johnson, and S.M. Matyas, *A proposed mode for triple-DES encryption.* IBM Journal of Research and Development, 1996. **40**(2): p. 253-262.
21. Daemen, J. and V. Rijmen, *Rijndael, the advanced encryption standard.* Dr. Dobb's journal, 2001. **26**(3): p. 137-139.
22. Thakur, J. and N. Kumar, *DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis.* International journal of emerging technology and advanced engineering, 2011. **1**(2): p. 6-12.
23. Massa, N., *Fiber optic telecommunication.* Fundamentals of photonics, 2000: p. 298.
24. Giamarchi, T., *Quantum physics in one dimension*. Vol. 121. 2003: Clarendon press.
25. Bennett, C.H., *Quantum cryptography using any two nonorthogonal states.* Physical review letters, 1992. **68**(21): p. 3121.
26. Ma, H.-X., et al., *Continuous-variable measurement-device-independent quantum key distribution with photon subtraction.* Physical Review A, 2018. **97**(4): p. 042329.
27. Zhang, L., C. Silberhorn, and I.A. Walmsley, *Secure quantum key distribution using continuous variables of single photons.* Physical review letters, 2008. **100**(11): p. 110504.

28. Ivonovic, I., *Geometrical description of quantal state determination.* Journal of Physics A: Mathematical and General, 1981. **14**(12): p. 3241.
29. Brassard, G., *Modern cryptology: A tutorial*. Vol. 325. 1988: Springer.
30. García-Patrón, R. and N.J. Cerf, *Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution.* Physical review letters, 2006. **97**(19): p. 190503.
31. Shor, P.W. and J. Preskill, *Simple proof of security of the BB84 quantum key distribution protocol.* Physical review letters, 2000. **85**(2): p. 441.
32. Bennett, C.H., et al., *Experimental quantum cryptography.* Journal of cryptology, 1992. **5**(1): p. 3-28.
33. Mauerer, W. and C. Silberhorn, *Quantum key distribution with passive decoy state selection.* Physical Review A, 2007. **75**(5): p. 050305.
34. Chong, S.-K. and T. Hwang, *Quantum key agreement protocol based on BB84.* Optics Communications, 2010. **283**(6): p. 1192-1195.
35. Brassard, G., et al., *Limitations on practical quantum cryptography.* Physical Review Letters, 2000. **85**(6): p. 1330.
36. Wang, X.-B., *Beating the photon-number-splitting attack in practical quantum cryptography.* Physical review letters, 2005. **94**(23): p. 230503.
37. Lo, H.-K. and H.F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances.* science, 1999. **283**(5410): p. 2050-2056.
38. Liu, Y., et al., *Decoy-state quantum key distribution with polarized photons over 200 km.* Optics express, 2010. **18**(8): p. 8587-8594.
39. Lo, H.-K., X. Ma, and K. Chen, *Decoy state quantum key distribution.* Physical review letters, 2005. **94**(23): p. 230504.
40. Lim, C.C.W., et al., *Concise security bounds for practical decoy-state quantum key distribution.* Physical Review A, 2014. **89**(2): p. 022307.
41. Ma, X., et al., *Practical decoy state for quantum key distribution.* Physical Review A, 2005. **72**(1): p. 012326.
42. Lucamarini, M., et al., *Efficient decoy-state quantum key distribution with quantified security.* Optics express, 2013. **21**(21): p. 24550-24565.
43. Scarani, V. and R. Renner, *Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing.* Physical review letters, 2008. **100**(20): p. 200501.
44. Scarani, V. and R. Renner. *Security bounds for quantum cryptography with finite resources*. in *Workshop on Quantum Computation, Communication, and Cryptography*. 2008. Springer.
45. Cai, R.Y. and V. Scarani, *Finite-key analysis for practical implementations of quantum key distribution.* New Journal of Physics, 2009. **11**(4): p. 045024.
46. Renner, R., N. Gisin, and B. Kraus, *Information-theoretic security proof for quantum-key-distribution protocols.* Physical Review A, 2005. **72**(1): p. 012332.
47. Kraus, B., N. Gisin, and R. Renner, *Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication.* Physical review letters, 2005. **95**(8): p. 080501.
48. Koashi, M. and J. Preskill, *Secure quantum key distribution with an uncharacterized source.* Physical review letters, 2003. **90**(5): p. 057902.
49. Hasegawa, J., et al., *Security analysis of decoy state quantum key distribution incorporating finite statistics.* arXiv preprint arXiv:0707.3541, 2007.
50. Singh, H., D. Gupta, and A. Singh, *Quantum key distribution protocols: a review.* Journal of Computer Engineering, 2014. **16**(2): p. 1-9.
51. Krawec, W.O. *Asymptotic analysis of a three state quantum cryptographic protocol*. in *2016 IEEE International Symposium on Information Theory (ISIT)*. 2016. IEEE.

52. Kim, Y.-S., Y.-C. Jeong, and Y.-H. Kim, *Implementation of polarization-coded free-space BB84 quantum key distribution.* Laser Physics, 2008. **18**(6): p. 810.
53. Nikolopoulos, G.M. and G. Alber, *Robustness of the BB84 quantum key distribution protocol against general coherent attacks.* arXiv preprint quant-ph/0403148, 2004.
54. Lütkenhaus, N., *Security against individual attacks for realistic quantum key distribution.* Physical Review A, 2000. **61**(5): p. 052304.
55. Eriksson, T.A., et al. *Coexistence of continuous variable quantum key distribution and 7× 12.5 Gbit/s classical channels*. in *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*. 2018. IEEE.
56. Comandar, L., et al., *Room temperature single-photon detectors for high bit rate quantum key distribution.* Applied Physics Letters, 2014. **104**(2): p. 021101.
57. LaGasse, M., *Temperature compensation for QKD systems*. 2006, Google Patents.
58. Bennett, C.H., G. Brassard, and N.D. Mermin, *Quantum cryptography without Bell's theorem.* Physical Review Letters, 1992. **68**(5): p. 557.
59. Marand, C. and P.D. Townsend, *Quantum key distribution over distances as long as 30 km.* Optics Letters, 1995. **20**(16): p. 1695-1697.
60. Hughes, R.J., et al., *Practical free-space quantum key distribution over 10 km in daylight and at night.* New journal of physics, 2002. **4**(1): p. 43.
61. Ursin, R., et al., *Entanglement-based quantum communication over 144 km.* Nature physics, 2007. **3**(7): p. 481.
62. Buttler, W., et al., *Practical free-space quantum key distribution over 1 km.* Physical Review Letters, 1998. **81**(15): p. 3283.
63. Townsend, P., et al., *Design of quantum cryptography systems for passive optical networks.* Electronics Letters, 1994. **30**(22): p. 1875-1877.
64. Aleksic, S., et al. *Impairment evaluation toward QKD integration in a conventional 20-channel metro network*. in *2015 Optical Fiber Communications Conference and Exhibition (OFC)*. 2015. IEEE.
65. Wang, Q., et al., *Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source.* Physical review letters, 2008. **100**(9): p. 090501.
66. Zhang, Y., et al., *Practical non-Poissonian light source for passive decoy state quantum key distribution.* Optics letters, 2010. **35**(20): p. 3393-3395.
67. Jiang, M.-S., et al., *Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states.* Physical Review A, 2012. **86**(3): p. 032310.
68. Schmitt-Manderbach, T., et al., *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km.* Physical Review Letters, 2007. **98**(1): p. 010504.
69. Rau, M., et al., *Spatial mode side channels in free-space QKD implementations.* IEEE Journal of Selected Topics in Quantum Electronics, 2014. **21**(3): p. 187-191.
70. Lee, M.S., et al., *Free-space QKD system hacking by wavelength control using an external laser.* Optics express, 2017. **25**(10): p. 11124-11131.
71. Pfennigbauer, M., et al., *Free-space optical quantum key distribution using intersatellite links*. 2003: na.
72. Nauerth, S., et al., *Air-to-ground quantum communication.* Nature Photonics, 2013. **7**(5): p. 382.
73. Wang, J.-Y., et al., *Direct and full-scale experimental verifications towards ground–satellite quantum key distribution.* Nature Photonics, 2013. **7**(5): p. 387.
74. Miki, T. and H. Ishio, *Viabilities of the wavelength-division-multiplexing transmission system over an optical fiber cable.* IEEE Transactions on Communications, 1978. **26**(7): p. 1082-1087.
75. Miya, T., et al., *Ultimate low-loss single-mode fibre at 1.55 μm.* Electronics Letters, 1979. **15**(4): p. 106-108.

76. Stucki, D., et al., *Quantum key distribution over 67 km with a plug&play system.* New Journal of Physics, 2002. **4**(1): p. 41.
77. Ribordy, G., et al., *Automated'plug and play'quantum key distribution.* Electronics letters, 1998. **34**(22): p. 2116-2117.
78. Kanapin, A., et al., *Urban QKD test for phase and polarization encoding devices.* International Journal of Quantum Information, 2017. **15**(08): p. 1740018.
79. Brackett, C.A., *Dense wavelength division multiplexing networks: Principles and applications.* IEEE Journal on Selected Areas in Communications, 1990. **8**(6): p. 948-964.
80. Park, S.-J., et al., *Fiber-to-the-home services based on wavelength-division-multiplexing passive optical network.* Journal of lightwave technology, 2004. **22**(11): p. 2582.
81. Ishio, H., J. Minowa, and K. Nosu, *Review and status of wavelength-division-multiplexing technology and its application.* Journal of Lightwave Technology, 1984. **2**(4): p. 448-463.
82. Grobe, K., *Optical Wavelength-Division Multiplexing for Data Communication Networks*, in *Handbook of Fiber Optic Data Communication*. 2013, Elsevier. p. 85-122.
83. Lee, J.H., et al., *First commercial deployment of a colorless gigabit WDM/TDM hybrid PON system using remote protocol terminator.* Journal of Lightwave Technology, 2009. **28**(4): p. 344-351.
84. Basak, A., M.Z. Talukder, and M.R. Islam, *Performance analysis and comparison between coarse WDM and dense WDM.* Global Journal of Research In Engineering, 2013.
85. Kartalopoulos, S.V., *DWDM: networks, devices, and technology*. 2003: IEEE Press Wiley.
86. Ciurana, A., et al., *Quantum metropolitan optical network based on wavelength division multiplexing.* Optics express, 2014. **22**(2): p. 1576-1593.
87. Chapuran, T., et al., *Optical networking for quantum key distribution and quantum communications.* New Journal of Physics, 2009. **11**(10): p. 105001.
88. Lo, H.-K., M. Curty, and K. Tamaki, *Secure quantum key distribution.* Nature Photonics, 2014. **8**(8): p. 595.
89. Shibata, H., T. Honjo, and K. Shimizu. *Quantum key distribution over a 60-dB channel loss using SSPD with ultralow dark count rate*. in *2013 Conference on Lasers and Electro-Optics Pacific Rim (CLEOPR)*. 2013. IEEE.
90. Peev, M., et al., *The SECOQC quantum key distribution network in Vienna.* New Journal of Physics, 2009. **11**(7): p. 075001.
91. Fujiwara, M., et al. *Field demonstration of quantum key distribution in the Tokyo QKD Network*. in *International Quantum Electronics Conference*. 2011. Optical Society of America.
92. Yin, J., et al., *Satellite-to-ground entanglement-based quantum key distribution.* Physical review letters, 2017. **119**(20): p. 200501.
93. Fröhlich, B., et al., *A quantum access network.* Nature, 2013. **501**(7465): p. 69.
94. Sasaki, M., et al., *Field test of quantum key distribution in the Tokyo QKD Network.* Optics express, 2011. **19**(11): p. 10387-10409.
95. Vakhitov, A., V. Makarov, and D.R. Hjelme, *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography.* journal of modern optics, 2001. **48**(13): p. 2023-2038.
96. Makarov, V., A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems.* Physical Review A, 2006. **74**(2): p. 022313.
97. Elliott, C., et al. *Current status of the DARPA quantum network*. in *Quantum Information and computation III*. 2005. International Society for Optics and Photonics.
98. Bennett, C.H., et al. *Quantum cryptography, or unforgeable subway tokens*. in *Advances in Cryptology*. 1983. Springer.
99. Elkouss, D., et al. *Efficient reconciliation protocol for discrete-variable quantum key distribution*. in *2009 IEEE International Symposium on Information Theory*. 2009. IEEE.

100. Braun, R.-P., et al. *Tbit/s 1000 Km field trial, achieving increased spectral efficiency, SDN enabled application traffic, and passive wavelength switching*. in *2015 Opto-Electronics and Communications Conference (OECC)*. 2015. IEEE.
101. Agrawal, G.P., *Fiber-optic communication systems*. Vol. 222. 2012: John Wiley & Sons.
102. Midwinter, J., *A study of intersymbol interference and transmission medium instability for an optical fibre system.* Optical and Quantum Electronics, 1977. **9**(4): p. 299-304.
103. Townsend, P.D., *Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing.* Electronics Letters, 1997. **33**(3): p. 188-190.
104. Xia, T.J., et al. *In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels*. in *Optical Fiber Communication Conference*. 2006. Optical Society of America.
105. Xavier, G., et al. *Scattering Effects on QKD Employing Simultaneous Classical and Quantum Channels in Telecom Optical Fibers in the C-band*. in *AIP Conference Proceedings*. 2009. AIP.
106. Peters, N., et al., *Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments.* New Journal of physics, 2009. **11**(4): p. 045012.
107. Eraerds, P., et al., *Quantum key distribution and 1 Gbps data encryption over a single fibre.* New Journal of Physics, 2010. **12**(6): p. 063027.
108. da Silva, T.F., et al., *Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems.* Journal of lightwave technology, 2014. **32**(13): p. 2332-2339.
109. Caves, C.M., *Quantum limits on noise in linear amplifiers.* Physical Review D, 1982. **26**(8): p. 1817.
110. Desurvire, E. and E.-D.F. Amplifiers, *John Wiley & Sons.* New York, 1994.
111. Gobby, C., Z. Yuan, and A. Shields, *Quantum key distribution over 122 km of standard telecom fiber.* Applied Physics Letters, 2004. **84**(19): p. 3762-3764.
112. Dixon, A., et al., *Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate.* Optics express, 2008. **16**(23): p. 18790-18797.
113. Zhang, Q., et al., *Megabits secure key rate quantum key distribution.* New Journal of Physics, 2009. **11**(4): p. 045010.
114. Shimizu, K., et al., *Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area.* Journal of Lightwave Technology, 2013. **32**(1): p. 141-151.
115. Stucki, D., et al., *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres.* New Journal of Physics, 2009. **11**(7): p. 075003.
116. Choi, I., et al., *Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber.* Optics express, 2014. **22**(19): p. 23121-23128.
117. Lo, H.-K., *Getting something out of nothing.* arXiv preprint quant-ph/0503004, 2005.
118. Koashi, M., *Simple security proof of quantum key distribution via uncertainty principle.* arXiv preprint quant-ph/0505108, 2005.
119. Pfister, C., et al., *Sifting attacks in finite-size quantum key distribution.* New Journal of Physics, 2016. **18**(5): p. 053001.
120. Welsh, D., *Codes and cryptography*. 1988: Oxford University Press.
121. Yamamura, A. and H. Ishizuka. *Error detection and authentication in quantum key distribution*. in *Australasian Conference on Information Security and Privacy*. 2001. Springer.
122. Brassard, G. and L. Salvail. *Secret-key reconciliation by public discussion*. in *Workshop on the Theory and Application of of Cryptographic Techniques*. 1993. Springer.
123. Lütkenhaus, N., *Estimates for practical quantum cryptography.* Physical Review A, 1999. **59**(5): p. 3301.

124. Bennett, C.H., G. Brassard, and J.-M. Robert, *Privacy amplification by public discussion.* SIAM journal on Computing, 1988. **17**(2): p. 210-229.
125. Watanabe, Y., *Privacy amplification for quantum key distribution.* Journal of physics A: Mathematical and theoretical, 2006. **40**(3): p. F99.
126. Fung, C.-H.F., et al., *Quantum key distribution with delayed privacy amplification and its application to the security proof of a two-way deterministic protocol.* Physical Review A, 2012. **85**(3): p. 032308.
127. Yuan, Z., J. Dynes, and A. Shields, *Avoiding the blinding attack in QKD.* Nature Photonics, 2010. **4**(12): p. 800.
128. Ekert, A.K., et al., *Eavesdropping on quantum-cryptographical systems.* Physical Review A, 1994. **50**(2): p. 1047.
129. Huttner, B. and A.K. Ekert, *Information gain in quantum eavesdropping.* Journal of Modern Optics, 1994. **41**(12): p. 2455-2466.
130. Fuchs, C.A., et al., *Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy.* Physical Review A, 1997. **56**(2): p. 1163.
131. Slutsky, B.A., et al., *Security of quantum cryptography against individual attacks.* Physical Review A, 1998. **57**(4): p. 2383.
132. Biham, E. and T. Mor, *Security of quantum cryptography against collective attacks.* Physical Review Letters, 1997. **78**(11): p. 2256.
133. Inamori, H., N. Lütkenhaus, and D. Mayers, *Unconditional security of practical quantum key distribution.* The European Physical Journal D, 2007. **41**(3): p. 599.
134. Mayers, D. and A. Yao. *Quantum cryptography with imperfect apparatus*. in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*. 1998. IEEE.
135. Inamori, H., L. Rallan, and V. Vedral, *Security of EPR-based quantum cryptography against incoherent symmetric attacks.* Journal of Physics A: Mathematical and General, 2001. **34**(35): p. 6913.
136. Tamaki, K., M. Koashi, and N. Imoto, *Unconditionally secure key distribution based on two nonorthogonal states.* Physical review letters, 2003. **90**(16): p. 167904.
137. Bennett, C.H., et al., *Generalized privacy amplification.* IEEE Transactions on Information Theory, 1995. **41**(6): p. 1915-1923.
138. Yuan, Z., et al., *High speed single photon detection in the near infrared.* Applied Physics Letters, 2007. **91**(4): p. 041114.
139. Tosi, A., et al., *Low-noise, low-jitter, high detection efficiency InGaAs/InP single-photon avalanche diode.* IEEE Journal of selected topics in quantum electronics, 2014. **20**(6): p. 192-197.
140. Li, H., et al., *Statistical-fluctuation analysis for quantum key distribution with consideration of after-pulse contributions.* Physical Review A, 2015. **92**(6): p. 062344.
141. Zhang, J., et al., *Comprehensive characterization of InGaAs–InP avalanche photodiodes at 1550 nm with an active quenching ASIC.* IEEE Journal of Quantum Electronics, 2009. **45**(7): p. 792-799.
142. Liu, M., et al., *High-performance InGaAs/InP single-photon avalanche photodiode.* IEEE Journal of selected topics in quantum electronics, 2007. **13**(4): p. 887-894.
143. Stucki, D., et al., *Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs.* Journal of modern optics, 2001. **48**(13): p. 1967-1981.
144. Fan-Yuan, G.-J., et al., *Afterpulse analysis for quantum key distribution.* Physical Review Applied, 2018. **10**(6): p. 064032.
145. Ben-Michael, R., M.A. Itzler, and B. Nyman. *Afterpulsing effects in 1.5 μm single photon avalanche photodetectors*. in *LEOS 2006-19th Annual Meeting of the IEEE Lasers and Electro-Optics Society*. 2006. IEEE.

146. Collins, R.J., et al., *Low timing jitter detector for gigahertz quantum key distribution.* Electronics Letters, 2007. **43**(3): p. 180-182.
147. Liang, Y., et al., *Low-timing-jitter single-photon detection using 1-GHz sinusoidally gated InGaAs/InP avalanche photodiode.* IEEE Photonics Technology Letters, 2011. **23**(13): p. 887-889.
148. Rogers, D.J., et al., *Detector dead-time effects and paralyzability in high-speed quantum key distribution.* New Journal of Physics, 2007. **9**(9): p. 319.
149. Williams, G.M. and A.S. Huntington. *Probabilistic analysis of linear mode vs. Geiger mode APD FPAs for advanced LADAR enabled interceptors*. in *Spaceborne Sensors III*. 2006. International Society for Optics and Photonics.
150. Khalique, A., G.M. Nikolopoulos, and G. Alber, *Postponement of dark-count effects in practical quantum key-distribution by two-way post-processing.* The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics, 2006. **40**(3): p. 453.
151. Kurochkin, V.L., et al. *Effect of crosstalk on QBER in QKD in urban telecommunication fiber lines*. in *International Conference on Micro-and Nano-Electronics 2016*. 2016. International Society for Optics and Photonics.
152. Namekata, N., Y. Makino, and S. Inoue, *Single-photon detector for long-distance fiber-optic quantum key distribution.* Optics letters, 2002. **27**(11): p. 954-956.
153. Bourennane, M., et al., *Experiments on long wavelength (1550nm)"plug and play" quantum cryptography systems.* Optics Express, 1999. **4**(10): p. 383-387.
154. Goodman, M., et al. *Quantum cryptography for optical networks: a systems perspective*. in *The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society, 2003. LEOS 2003.* 2003. IEEE.
155. Tanizawa, Y., R. Takahashi, and A.R. Dixon. *A routing method designed for a Quantum Key Distribution network*. in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*. 2016. IEEE.
156. Ma, X., *Quantum cryptography: theory and practice.* arXiv preprint arXiv:0808.1385, 2008.
157. Takahashi, T., et al., *Modelling of intersymbol interference effect on signal to noise ratio measurement in long haul optical amplifier systems.* Electronics Letters, 1995. **31**(25): p. 2195-2197.
158. Tzimpragos, G., et al., *A survey on FEC codes for 100 G and beyond optical networks.* IEEE Communications Surveys & Tutorials, 2014. **18**(1): p. 209-221.
159. Townsend, P.D., *Quantum cryptography on multiuser optical fibre networks.* Nature, 1997. **385**(6611): p. 47-49.
160. Fröhlich, B., et al., *Quantum secured gigabit optical access networks.* Scientific reports, 2015. **5**(1): p. 1-7.
161. Peng, C.-Z., et al., *Experimental long-distance decoy-state quantum key distribution based on polarization encoding.* Physical review letters, 2007. **98**(1): p. 010505.
162. Fokoua, E.N., et al., *How to make the propagation time through an optical fiber fully insensitive to temperature variations.* Optica, 2017. **4**(6): p. 659-668.
163. Frey, B.J., D.B. Leviton, and T.J. Madison. *Temperature-dependent refractive index of silicon and germanium*. in *Optomechanical technologies for Astronomy*. 2006. International Society for Optics and Photonics.
164. Malitson, I.H., *Interspecimen comparison of the refractive index of fused silica.* Josa, 1965. **55**(10): p. 1205-1209.
165. Gupta, R., et al., *Absolute refractive indices and thermal coefficients of fused silica and calcium fluoride near 193 nm.* Applied Optics, 1998. **37**(25): p. 5964-5968.
166. Brodsky, M., et al., *Polarization mode dispersion of installed fibers.* Journal of Lightwave Technology, 2006. **24**(12): p. 4584-4599.
167. Chraplyvy, A.R., *Limitations on lightwave communications imposed by optical-fiber nonlinearities.* Journal of Lightwave Technology, 1990. **8**(10): p. 1548-1557.

168. Subacius, D., A. Zavriyev, and A. Trifonov, *Backscattering limitation for fiber-optic quantum key distribution systems.* Applied Physics Letters, 2005. **86**(1): p. 011103.
169. Choi, Y.S., *Asymmetry of the forward and backward Raman gain coefficient at 1.54 μm in methane.* Applied optics, 2001. **40**(12): p. 1925-1930.
170. Sentrayan, K., A. Michael, and V. Kushawaha, *Intense backward Raman lasers in CH 4 and H 2.* Applied optics, 1993. **32**(6): p. 930-934.
171. Wang, L.-J., et al., *Long-distance copropagation of quantum key distribution and terabit classical optical data channels.* Physical Review A, 2017. **95**(1): p. 012301.