Towards Practical Quantum Cryptography

Abdul Mirza

Towards Practical Quantum Cryptography

Towards Practical Quantum Cryptography

Abdul Mirza

January 27, 2009

Submitted in fulfilment of the academic
requirements for the degree of
Master of Science in the
School of Physics,
University of KwaZulu-Natal,
Westville.

As the candidate's supervisor I have/have not approved this thesis/dissertation for submission.

Signed_____
Name_____
Date_____

ABSTRACT

The information society that presides today is dependent on the communication industry to facilitate unintelligible data transfers between authenticated parties. Such requirements have, to date, taken advantage of security based on the mathematical complexities of certain algorithms. However, the advancement of computing power and the advent of the quantum computer together with the vulnerability of this scheme to mathematical progress have prompted the introduction of quantum cryptography. This process, through the laws of quantum physics, ensures provably secure data communication.

Quantum cryptography provides physical protection to individual bits of information thus providing a hardware implemented solution. The implementation of this theoretical concept requires much practical innovation for transparent deployment into current cryptographic solutions.

This thesis introduces the concept of quantum cryptography in a practical perspective. It raises a few core concerns with the present quantum cryptographic technology and provides some solutions towards the practical deployment of commercially feasible quantum cryptographic systems.

The thesis commences with an introduction to classical cryptography focussing on key management protocols. This is followed by the presentation of the basic concepts of Quantum Key Distribution (QKD) together with an explanation of some QKD protocols and parameter required to classify such protocols. Chapter 2 discusses the theoretical and practical aspects of quantum channels in particular optical fibre. The primary challenges of transferring classical and quantum data along these channels are mentioned together with some solutions.

A description of experimental usage with present QKD solutions is presented in Chapter 3. An investigation into highly efficient QKD protocols follows illustrating effective post-distribution processing for increasing the efficiency of the BB84 protocol.

Chapter 4 begins with the limitations of present day QKD systems and explicates Quantum Networks as a possible solution. An introduction to classical networking theory is first presented after which some quantum network architectures based on passive optical networks are illustrated. Finally the proposed *Quantum City* project in conjunction with the eThekwini Municipality is explained. The realization of this project is intended to be complete by the third quarter of 2008 effectively making Durban into the first Quantum City in the world.

PREFACE

The work described in this Masters thesis was carried out at the School of Physics, University of KwaZulu-Natal, Westville Campus, from the period commencing February 2007 to June 2008, under the supervision of Professor Francesco Petruccione.

These studies represent original work by the author and have not otherwise been submitted in any form for any other degree or diploma to any other tertiary institution. Where use has been made of the work of others it is duly acknowledged in this text.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Throughout time information has been gathered, stored and communicated in various forms. The earliest means of information was visual, through diagrams and pictures. Languages were then developed and text became the major means of information management. This continued until the information revolution in the early 20th century with the advent of the digital age. Electronic media propelled our society into an information driven society, however this has come with many complications, one being that of data integrity, privacy and secrecy [2].
Prior to the 20th century, physical security was sufficient to protect sensitive information. A classical example is that of the Ancient Greeks' *Scytale* which was used to store and communicate information to army generals [3]. A long strip of writing material was coiled around rod of particular radius at a specific angle such that there was no overlapping of the material. The information was then written on it and uncoiled. Only those with a rod of the same radii would be able to retrieve intelligible information from the script. However these security schemes required radical improvements as data exchange increased exponentially with the advent of the information age.

1.1 The Need for Cryptography

We currently live in a society that is inherently dependent on information. It is a vital resource in the political, commercial, private and academic sectors. The advent of digital communication has brought with it a plethora of initiatives in the field of information science. Electronic banking via an ATM or a cellphone, emails, intranets and the internet now form the pivotal basis of commerce and industry. Information processing devices provide automated services, serve as data analysis tools and information storage devices while also facilitating the communication of information. However, in such activities information privacy and communication secrecy are of core concern. With electronic information processing and data storage, physical security at storage facilities cannot imply total security, and hence privacy, of the information [4].
Physically protecting information as in storing information in a secret volt or transporting documents in a highly armored entourage is an obscurity and deterrent to accessing the information. Thus once an adversary has infiltrated or bypassed such measures, they have total control over the information. However, information security requires that even if an adversary possess complete knowledge of the protection measures they would not be able to retrieve any information [4]. For such security, methods beyond the classical domain must be explored.

This thesis intends to expound on present cryptographic methods highlighting the limitations therein. An introduction to quantum cryptography follows with a explanation of various implementations of quantum cryptographic protocols. The workings of practical quantum cryptographic systems is then presented together with recent experiments data. Further improvements in the sifting efficiency of currently used quantum protocols is suggested. The increase in efficiency is realized through post-distribution processing. A second generation of quantum cryptographic solutions involving quantum networks are is presented in order to overcome some of the limitations of presently available quantum security solutions. Finally the implementation of a Quantum network implemented over the eThekwini Municipality optical fibre infrastructure is presented.

1.2 Classical Cryptography

1.2.1 The Problem Statement

Sensitive data is generally required to be communicated between spatially separated regions or stored for extended periods of time such that any individual who infiltrates the external protection measures acquires unintelligible, and hence useless, data. Such protection can be realized through *cryptography*. This is the art of rendering one's messages unintelligible to any adversary. The converse is known as *cryptanalysis* [2] which is the study and practice of breaking cryptographic techniques. The ongoing tousle between cryptography and cryptanalysis provides the propulsion for improvements in information security [2].
Suppose the sender, commonly known as Alice, would like to transmit a message to the receiver, known as Bob, securely from any onlooker. Alice and Bob will use an algorithm, known as a *cryptosystem*, to convert the original information, the *plaintext*, to its disguised form, known as *ciphertext*. This procedure is illustrated in Figure 1.1. The process by which information is converted from plaintext to ciphertext is called *encryption*, while the reverse procedure is named *decryption*. The total looped process may be mathematically represented as [4]:

$$P = D(E(P)) \tag{1.1}$$

where P is the plaintext, E is your encryption algorithm and D is your decryption algorithm.
Together with protecting the information content of the message, cryptography also assists in [4]:

Data integrity
This permits the receiver to verify that the content of the message was not altered during transmission. Altering the information would permit the adversary to forward false information to the receiver thereby controlling the knowledge flow between the users.

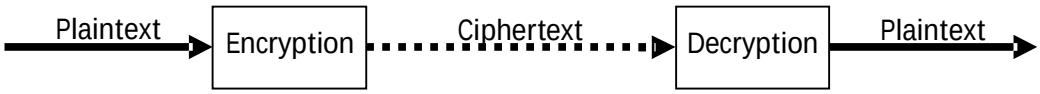

Fig. 1.1: The process through which information is transferred securely over public channels is known as cryptography. A sender encrypts the data such that it is unintelligible to onlookers while the intended recipient decrypts the message to reconstruct an intelligible message.

Sender authentication
The receiver is able to confirm that the message was truly sent from the stated sender. An adversary tapping into the communication channel between the users and posing as the sender or receiver to Bob and Alice respectively would again have full control of the information flow.

Non-repudiation of origin
At some future time the sender should not be able to falsely deny having sent information to the receiver. This serves as an electronic receipt should there be any future discrepancies.

A cryptographic scheme utilizes an algorithm to encrypt and decrypt information. These algorithms form a family T of transformations T_k. Each transformation may be uniquely defined through the choice of parameters known as the *key*. The *keyspace* K is the set of all possible keys for a particular family of algorithms [4], thus

$$T = \{T_{\mathrm{k}} : k \in K\}, \tag{1.2}$$

and

$$E_{\mathrm{k}}, D_{\mathrm{k}} \in T. \tag{1.3}$$

Therefore we have for a specific cryptosystem session

$$P = D_{\mathrm{k}}(E_{\mathrm{k}}(P)). \tag{1.4}$$

Equation (1.4) is illustrated in Figure 1.2. The key selects a particular transformation from the family T to be used in the cryptosystem. Thus even if the general algorithm is known to the adversary, the information will not be compromised until the key, or a portion thereof, is acquired. The eavsdropper may however acquire some knowledge of the information through side information or by an inappropriate choice of a cryptosystem.

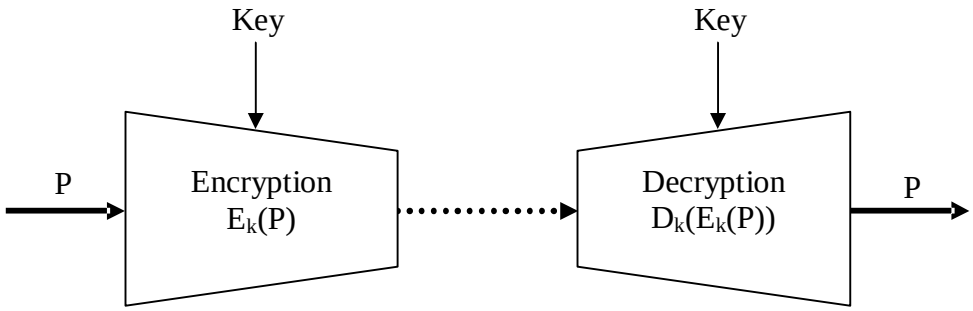

Fig. 1.2: During a cryptographic session, the encryption and decryption algorithms are selected through the choice of a key. The plaintext, P, is then encrypted and decrypted at the entry and exit points of the channel respectively. Prior to the actual cryptographic session, a key is required to be exchanged between the parties. Eve would require the key in order to know which particular transformation was used.

In the nineteenth century Dutchman A Kerckhoffs postulated that any cryptographic system must implement the following [2]:

- The system should be unbreakable in practice.
- Compromising the algorithm should not compromise the system, hence the total secrecy should be embedded within the key.
- The algorithm should be easy to memorize, implement and change.
- The ciphertext should be transferable by telegraph.
- The apparatus should be portable.
- The system should be user-friendly.

Cryptographic systems that are unbreakable in practice are referred to as *Computationally Secure* [5]. In such cases the information is regarded secure if the cost and time of cryptanalysis is greater than the value and validity of the information respectively. Such systems are bound by technological and academic advancements.
A compromise in the algorithm refers to the leakage of the transformation set T used in the cryptosystem to unauthorized individuals. For a robust cryptosystem, the leak will not compromise the system as the security is provided by the key and this, in turn, is chosen randomly and secretly. As each transformation T_k is rendered unique through the choice of a key, the algorithm will also be a random selection of the set T. Thus key distribution plays an integral role in the security of cryptographic process. Cryptographic systems that require the algorithms to remain secret are referred to as

Restricted Algorithms [6]. These are not practical for use in the public domain.
The ciphertext is required to be such that transfer over public media and communication lines is possible. As this will permit the interception of the ciphertext, this point illudes to the imperative requisite of cryptography that requires information to be secured rather than obscured. This is as obscurity provides a deterrent from eavesdropping on the data while security provides protection to the data.

1.2.2 Substitutional Cipher

One of the earliest cryptographic systems involves the modular addition of the alphabets. A classic example of such a cipher is the Caesar Cipher used by Julius Ceaser in 100BC to communicate with his generals [3]. Each alphabet was given a value from 0 to 25. A pre-distributed key, consisting of a single value, was then used to perform a letter-wise modular addition with the alphabets of the plaintext to create the ciphertext. An example of this scheme is illustrated in Table 1.1:

Tab. 1.1: An example of a substitutional cipher. The session key is added in a letter-wise modular fashion to the plaintext to create the final ciphertext. A character frequency analysis can be executed to retrieve the key and hence the plaintext.

Plaintext:	C	r	y	p	t	o	g	r	a	p	h	y
ASCII:	02	17	24	15	19	14	06	17	00	15	07	24
Session key:	65											
ASCII:	17	07	14	05	09	04	21	07	15	05	22	14
Ciphertext:	R	h	o	f	j	e	v	h	p	f	w	o

This method was however shown to be flawed by Al-Khindi [2]. Any intelligible plaintext possesses a character frequency signature. Thus with the substitution method described above, one may be able to derive the plaintext through a character frequency analysis. This method is, however, dependent on side-information regarding the output probability of the plaintext source in order to determine the character frequency signature.
By calculating the character frequency and mapping it onto a model of the plaintext source, the key may be deduced. This may easily be done on a PC today.
To remove the frequency characteristics of the plaintext, it was split into smaller segments of a fixed predetermined size. A unique session key was then allocated to each block. This method was termed the *block cipher* algorithm [5]. The trade-off for greater security in this method came at the expense of utilizing larger keys. The key length required increased linearly with the message size and inversely with the block size.

1.2.3 One Time Pad

The block cipher was modified in 1586 to remove the dependance of the key length

on the plaintext size, this was known as the *Vigenére cipher* [5]. In this scheme the plaintext was again split into fixed size blocks. A key of length equal to the block size was used to conduct a character-wise modular addition within the block. The same key was then reapplied in a similar fashion to encrypt the remaining blocks of the plaintext. Thus the key length was merely a function of the block size. However, the reuse of the key for each block creates a security breach as, with additional side information, the key may be determined [7].
To increase the security of such a system, the block size is increased. This reduces the number of times the key is reused and increases the number of permutations of the key. Joseph O Mauborgne and Gilbert Vernam in 1926 developed the limiting case of such a block cipher where the block size, and hence the key, was as large as the plaintext itself. This cryptosystem is known as the *One Time Pad* (OTP) [4]. This method is referred to as a *stream cipher* where each character of the plaintext is encrypted with a unique key bit. For implementation into the digital media modular addition, central to this encryption scheme, is extended to a bitwise XOR of the key and plaintext. A illustration of the OTP cryptosystem is presented in Table 1.2.

Tab. 1.2: This table demonstrates the digital OTP cyptosystem. The plaintext is encrypted through a bitwise XOR function with the key while decryption is again conducted by an XOR between the ciphertext and key. It should be noted that the key length is required to be at least as long as the plaintext as this is a stream cipher. As the key is a random sequence of bits, the ciphertext produced is also a random sequence.

Plaintext:	0	1	0	1	0	1	0	1	0	1	0	1
OTP key:	0	1	1	0	1	0	0	0	1	1	0	1
Ciphertext:	0	0	1	1	1	1	0	1	1	0	0	0

The OTP cryptosystem is characterized by the following [2]:

- The sequence of key bits is generated in a truly random manner.
- The key size is as long as the plaintext.
- The key is used exactly once.

Truly random numbers are generated through random processes as opposed to pseudo-random numbers that are generated through a deterministic algorithm and environment specific seed variables [8]. Due to their deterministic nature, pseudorandom numbers exhibit patterns as each number is dependent on the former and hence the key may be reverse engineered through the use of sufficient computing power.
Two sets of plaintext codes, P_1 and P_2, encrypted with a common key in a Vigenére cryptosystem produce the ciphertext C_1 and C_2 through the binary modular addition operator $\oplus$. However this set of ciphertexts are prone to cryptanalysis as

$$C_1 \oplus C_2 = (P_1 \oplus k) \oplus (P_2 \oplus k) = (P_1 \oplus P_2) \oplus (k \oplus k) = P_1 \oplus P_2, \tag{1.5}$$

where the commutative property of the XOR funtion has been used.
With further side information about the plaintext, an eavesdropper may be able to decipher the text. Thus the key is required to be as long as the plaintext and used only once. Any successful attack on the OTP cryptosystem would involve an attack on the key. Thus to preserve long-term secrecy, the key bits are also required to be stored or destroyed in a safe manner.
It was shown in 1948 by CE Shannon in his paper *Communication Theory of Secrecy Systems* [9] that OTP was a provably secure method of data encryption. He further stated that any provably secure scheme must necessarily comply with the above criteria. Such cryptosystems are independent of an adversary's computational power and mathematical advancements.
As a random key renders any sequence again random and every key sequence is be equally probable, the ciphertext has equal probability of being any permutation of bits to the length of the plaintext. As an example, the ciphertext corresponding to '*Quantum*' could equally be '*Jpanmwi*' or '*Physics*'. Thus the probability of cryptanalysis of the ciphertext is equal to the probability of acquiring the original plaintext directly [7],

$$Prob(P, C) = Prob(P). \tag{1.6}$$

The only cryptanalysis technique that can be employed to break such a system is a brute force attack where every possible permutation of the key is required to be tested [4].
As one may note, the secure distribution of the key will imply a secure encryption. Thus key distribution and management is integral to the success of this scheme.

1.2.4 The Eavesdropper

An eavesdropper, commonly known as Eve, is an unauthorized party that attempts to intercept and extract information from the communications between two legitimate communicating parties. The legitimate parties continuously monitor their physical communication parameters and encryption scheme. The detection of an eavesdropper compromises the session's communication. In the security analysis of key distribution schemes, the eavesdropper is assumed to posses the following resources[10]:

- Unlimited computing power,
- Unlimited technology,
- Unlimited mathematical resources,
- Complete access to the communication channels.

Any scheme that may be securely implemented after having taken the above into consideration is *theoretically secure* and hence *futureproof* against any potential attack [6]. There are six main types of attacks that an eavesdropper may execute:

Ciphertext only
This is an attack in which the eavesdropper has a number of ciphertexts encrypted in one encryption session. Using this information, the eavesdropper tries to determine the plaintext or encryption key.

Known plaintext
The eavesdropper has access to the ciphertext and the corresponding plaintext. The eavesdropper requires the key or algorithm to decrypt future communications.

Chosen plaintext
The eavesdropper again has access to the ciphertext and the corresponding plaintext, however the eavesdropper may choose plaintext to be encrypted. This may be accomplished through an internal accomplice.

Direct key
This type of attack targets the key distribution process directly. The eavesdropper attempts to retrieve the key without detection. This is the only type of attack that is useful against the OTP encryption scheme.

Man-in-the-middle
The eavesdropper falsely identifies herself as the valid reciprocal party to both parties. Eve conducts separate cryptographic communication between either party. The eavesdropper thus has complete control of the information flow between the parties. This type of attack can be prevented through authentication.

Denial of service
The adversary cuts all communication between the two parties disallowing any form of communication. Neither the adversary or respective parties acquire any information. This type of attack would be useful to obstruct an occurrence that relies heavily on pre-communication. The adversary disallows information flow but has no control or knowledge of the information content.

1.2.5 Classical Methods of Key Management

Any successful cryptosystem includes five basic steps [4]:

1. Alice and Bob must agree on a cryptosystem to be used.
2. They must distribute a key securely.
3. Alice should prepare the ciphertext for distribution.
4. Alice must transfer the ciphertext to Bob.

5. Bob should decrypt the ciphertext to regain the plaintext.

An adversary has access to the 1^{st}, 2^{nd} and 4^{th} stages of the cryptosystem. The security of a good cryptosystem for public use should be independent of the secrecy of the algorithm used. While access to the ciphertext permits a ciphertext only attack, some algorithms are known to be secure against such attacks [4]. However, the key distribution stage is critical to the security of the system. Each ciphertext is only as secure as the key(s).
Key distribution and management thus forms an integral part of the security of the cryptosystem. Historically key distribution was implemented manually through a secure courier service or in person. However due to the information overflow and the digital age new methods of key distribution are required that permit cryptography between remote parties on-demand.
Two general key management techniques exist today, namely asymmetric and symmetric key cryptography.

1.2.6 Asymmetric Key Cryptography

This technique may be illustrated as a postbox, anyone may place a message inside the box, however, only those with the key are able to access the information. The key management systems, proposed by Whitfield Diffie and Martin Hellman in 1976 [11], uses *one-way* functions to produce a set of keys. A *one-way* function permits easy computation of a result given the parameters, while the reverse is computationally taxing [12]. *Computationally easy* is construed as computable in a time polynomially dependent on the length of the parameters while exponential growth in computing time is regarded as *computationally taxing* or inefficient.
In asymmetric key cryptography a public and private key is produced through these functions. Given the public key it is computationally intensive to retrieve the private key, however the reverse is possible. This is not the case if sufficient additional information is available as it would permit one to compute in the reverse direction efficiently. This is known as a *trapdoor*. To date there are no known one-way functions without at least one trapdoor [5]. This creates a potential vulnerability in the system.
A public key is made available to all those intending to communicate with a particular party. The plaintext is encrypted using the public key. The ciphertext is then undecipherable by any known efficient algorithm unless one has possession of the private key. The Rivest, Shamir and Adleman (RSA) method is a common asymmetric encryption method used at present [12].
The RSA algorithm is based on the prime factorization of large integers [12]. Given two prime numbers it is easy to find the product, while computationally intensive to find the prime factors of a given product. The complexity is further enhanced by larger prime numbers and a greater amount of prime numbers used to generate the product. However given additional information, such as one of the prime numbers, it becomes relatively easy to reverse the process.

Although solving the key distribution problem, public key cryptography is at most computationally secure. It is known to be prone to chosen plaintext attacks. This is especially the case when the plaintext forms a finite set of inputs [4]. Through trial and error, an eavesdropper may match each ciphertext to its corresponding plaintext. Further the eavesdropper is able to determine what the plaintext is not. This may be valuable in some instances for example, when there are a finite number of input parameters.
Public key cryptography is generally slower than symmetric key cryptography. With the continuous increase in data communication, speed is an essential parameter to note. A greater disadvantage lies in the fact that there are no mathematical proofs for the existence of one-way functions, hence we rely on the assumptions of complexity theory [2] and that no efficient reverse algorithms for these functions have been found to date. Advancements in mathematics may one day produce efficient algorithms for calculating the reverse functions, this will make all such cryptosystems obsolete. Further Peter Shor in 1994, developed an efficient quantum algorithm for such reverse functions [13] and has been experimentally verified on small quantum processors [14]. This further raises the question of a classical counterpart. With the development of quantum computers fast becoming a reality [15], the socio-economic risks of asymmetric cryptosystems cannot be undermined and hence further investigation into alternative key management systems must be considered.

1.2.7 Symmetric Key Cryptography

In this encryption scheme an identical key is distributed between both parties. The scheme may be considered like a safe. The sender locks the information in the safe, only the recipient with an identical key may open the safe and have access to the information. This type of encryption was the earliest type of encryption and has been developed over the years. Ultimately the OTP scheme has been shown to provide provable security while many other variations of symmetric key cryptography have been developed to gain computational security [5].
In such a scheme, both parties distribute and agree on the secrecy of the key before any secure communication is undertaken. A function is then used to combine the information with the key to produce a ciphertext. The function is publicly known while the symmetric key is transferred privately.
It is seen from the above that the entire secrecy of this type of cryptosystem lies is the secrecy of the key [2]. Thus the problems arising within symmetric key cryptography all lie in its key management structure. Firstly the key distribution is required to be secure. This poses a problem in that not only is secure distribution technically challenging, it is also expensive. The storage and disposal of key bits must also be completed in an appropriate fashion to facilitate the long term security of the information. Lastly key throughput is expensive as communication between each set of individuals requires separate and unique keys.
Due to the slow nature of asymmetric keys, public key cryptography is generally used

to distribute a symmetric session key that is in turn expanded using recursive and non-linear algorithms to produce a block key. This is used to encrypt the data. The AES standard [11] is a symmetric cryptoscheme based on the above principle and is again at most computationally secure.
Although the above schemes and standards temporarily solve the key management crisis, we can not rely on these and potentially jeopardize our entire socio-economic system. With the advent of quantum computers, classical key management will be inherently flawed. Quantum key distribution will then be the only perfectly secure method of key exchange.

1.3 Quantum Key Distribution

Quantum Key Distribution (QKD) is a means to symmetric key cryptography. The idea of quantum based security was developed by S Wiesner in 1970 as a means of *secure money* [16]. The concept used quantum principles, in particular the *no-cloning theorem* to develop non-clonable money thus disallowing any fraudulent production of money.
This idea was then taken by CH Bennett and G Brassard in 1984 to developed the first QKD protocol named the BB84 protocol [17]. The protocol was based on the polarization of single photons. A stream of single photons were distributed between the two parties that were in turn used to develop a symmetric key.
Bennett and Brassard also showed QKD to be theoretically secure [17]. The security of this scheme is based on the fundamental laws of quantum physics rather than unproven mathematical assumptions of complexity theory [2]. The scheme utilizes quantum mechanical two-level systems, known as *qubits*, to transfer a symmetric key between two pre-authenticated parties for use in an encryption protocol.
It should be noted at the onset that QKD only provides a platform for secure key distribution. However if this key is used, together with the OTP, one can achieve theoretically secure communication [17]. In this thesis we assume the end-users' stations are secure from hackers etc. and the users are pre-authenticated. Procedures for authentication and checks for data integrity and non-repudiation do presently exist.
Figure 1.3 illustrates the basic setup of a quantum cryptographic system.
Both Alice and Bob are connected to a quantum and classical channel. All authentication, post-distribution processes and encrypted communication is executed over the classical channel while the raw key distribution process is conducted over a quantum channel.
After authentication, Alice begins transmission of a randomly generated stream of qubits to Bob over the quantum channel. Thereafter, the qubits undergo a post-distribution process to form a secure key. If both parties accept the security level of the key, information is encrypted via the OTP scheme and sent over the classical channel. Due to the quantum nature of the particles used in the key distribution process, an eavesdropper would cause discrepancies in the key and hence be detected. The eavesdropper will have access to the ciphertext, but this will be useless as explained earlier. It should be noted that at no point is the data intended for secure communication compromised as

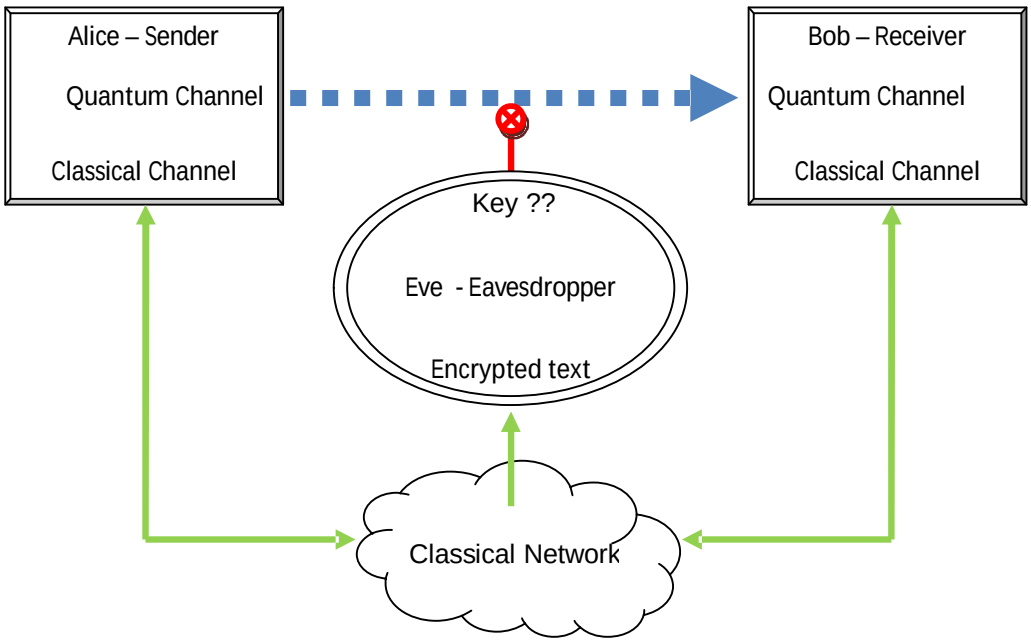

Fig. 1.3: A diagram representing the roles of Alice, Bob and Eve in a quantum cryptographic setup. Due the physical properties of the quantum information, Eve is unable to access the key. As the information is encrypted in through the OTP scheme, the information is provably secure.

infiltration is detected in the key distribution phase.
Some implementations of QKD also use entanglement which refers to the sharing of information between two spatially separated particles that had interacted at some previous time [10]. In the case of qubits implemented through photons, polarization or a phase differential is used to create the two level quantum system [18]. The photon implementations will be explained in further detail in the sections 1.3.4 and 2.5.

1.3.1 The Basis of Security in QKD

The security of this scheme is based on two fundamental laws of quantum mechanics [10]:

- **Heisenberg's uncertainty principle:** The measurement of one quantum observable intrinsically creates an uncertainty in other properties of the system.
- **Principle of superposition:** A qubit may be in a number of states simultaneously until observed at which point the superposition collapses down to a single state.

Any attempt by Eve to extract information from the key will require a measurement. Hence, due to the aforementioned, any observation will intrinsically alter the state of the qubit. Thus the symmetrical nature of the key will change and the presence of an eavesdropper will be detected by the legitimate users.

1.3.2 The Photon as a Qubit

The photon is a quantum of light and hence obeys the duality principle [19]. When unobserved the photon acts as a wave and hence travels as a superposition. Upon observation the photon collapses from a superposition to a particle.
The photon may be encoded as a qubit through a number of procedures. The two qubit states may be represented as $|0\rangle$ and $|1\rangle$ where both are vectors in the Hilbert space [10]. This basis set is known as the *computational basis* [10]. Due to the quantum mechanical nature of the photon, a superposition φ of the computational basis may also occur,

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.7}$$

where $|\alpha|^2$ and $|\beta|^2$ are the probabilities of the measuring states $|0\rangle$ and $|1\rangle$ respectively. In particular we consider the consider the orthogonal set

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{1.8}$$

Note that this set is non-orthoganol to the computational basis set.

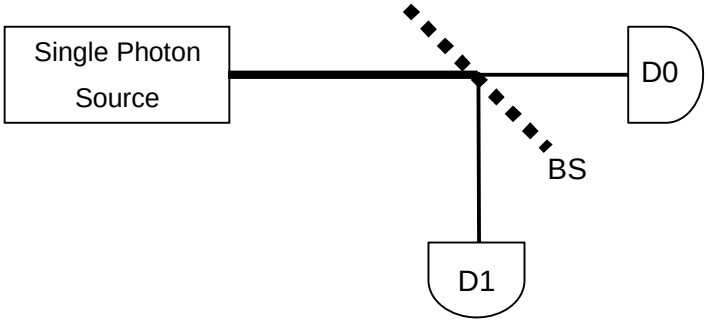

Fig. 1.4: A schematic diagram of a quantum random number generator. Single photons are emitted by the source, these photons then pass through a 50/50 beam-splitter (BS). The photons are randomly routed between the two detectors with an overall probability of 1/2 to each detector. Due to the quantum nature of the photon, the photon can be spilt and routed to both detectors simultaneously but can only be measured at one detector.

CH Bennett and G Brassard identified the polarization of the photon as an implementation of the qubit where the photons are polarized into one of two orthogonal states [20]. A horizontally or vertically polarized photon is an example of a qubit with the polarization axes forming the basis set. This basis set may be represented as $|\rightarrow\rangle$ and $|\uparrow\rangle$ respectively.

1.3.3 Quantum Random Number Generation

Random number generation is imperative to the success of a secure cryptosystem as it is used to create the key bit sequence. Classical random number generators depend on deterministic algorithms [13]. An initial number is randomly selected using current environmental parameters. This number, known as the *seed*, is then fed into the number generation algorithm to produce the next number in the sequence. Likewise all the generated numbers are dependent on the previously generated sequence. This successive routine produces a sequence of pseudo-random numbers. With sufficient computing power or the partial knowledge of the algorithm used, one may reconstruct and predict the upcoming numbers of the sequence. This creates a flaw in the cryptosystem as the eavesdropper has access to the random numbers used in the key generation process.
Quantum Random Number Generators (QRNG) take advantage of the probabilistic nature of quantum mechanics [21]. As the number sequence is dependent on a physical outcome, it cannot be simulated by deterministic methods. The simplest setup for such a generator is illustrated in Figure 1.4. This is an optical generator based on the wave-particle duality of photons.
The setup consists of a single photon source, a beam splitter and two photon detectors, D0 and D1. Detection at D0 or D1 represent a 0 or 1 respectively.

A single photon source emits photons towards a 50/50 beam splitter. At the beam splitter the photons is launched into a superposition and travels towards both detectors simultaneously. The photon state may be represented as

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{1.9}$$

where $|0\rangle$ is the state in which the photon travels towards D0 while $|1\rangle$ is when the photon is routed to D1. The equal probability of both states is due to the 50/50 beam splitter. The detectors measure for the incoming photon simultaneously. Upon measurement, the superposition collapses into its pure states with equal probability.

1.3.4 BB84 Protocol

The first QKD protocol, BB84, was designed by the physicists CH Bennett and G Brassard in 1984 [17] while the first working prototype was developed by IBM at Yorktown Height, New York in 1989 [20]. The BB84 protocol, although the first protocol developed, is still implemented today in commercial QKD systems [22, 23, 24] due to its relatively simple setup and good efficiency. The protocol is described as follows:
Alice has access to a single qubit source, a quantum channel and a public classical channel. She may transmit a qubit in two non-orthogonal basis modes. Each mode has two orthogonal states, viz. 0 and 1. This is summarized in Table 1.3.

Tab. 1.3: Alice may send four different qubit states. These comprise of two non-orthogonal modes, each containing a pair of orthogonal states. The states are assigned binary values such that each mode consists of the complete binary set.

Mode	**State**	**Ket Representation**
1	0	$\|0\rangle$
1	1	$\|1\rangle$
2	0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
2	1	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$

One implementation of this is through the polarization of single photons [17] as shown in Figure 1.5. The polarization states may be achieved by polarizing classical pulses before attenuating them down to a single photon level [25]. The photons may be polarized in two modes, the vertical-horizontal or the diagonal modes. We may represent the vertical-horizontal mode as

$$|\uparrow\rangle \text{ and } |\rightarrow\rangle,$$

while the diagonal modes may be represented as

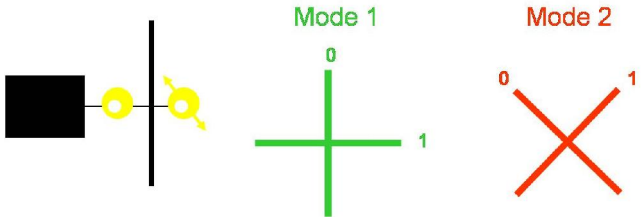

Fig. 1.5: Polarization states that may be sent by Alice in the BB84 protocol. Note that each mode has two orthogonal states corresponding to the key bit values.

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$$

and

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle).$$

It is clear from the above that the modes consist of orthogonal states while the modes themselves are non-orthogonal.
Alice emits a stream of qubits in random modes and states into the quantum channel to Bob. Bob measures the incoming qubits in an independent random sequence of basis modes. Thus there is a probability of 0.5 that Alice and Bob will send and measure in a common basis. Polarization measurements are conducted through the use a polarization dependent beam splitter. The beam splitter causes vertically polarized photons to be routed to detector 0 while horizontally polarized photons to be sent to detector 1. Diagonal mode measurements are first passed through a quarter-wave plate before entering the beam spitter. If a common mode is used in sending and measuring the qubit, a deterministic result will be obtained as shown in Figure 1.6. To illustrate this, assume Alice transmitted a right diagonally polarized photon and Bob measured in the diagonal mode.

At detector 0 we have: $[\frac{1}{\sqrt{2}}(\langle\uparrow| + \langle\rightarrow|)][\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)] = 1$

At detector 1 we have: $[\frac{1}{\sqrt{2}}(\langle\uparrow| - \langle\rightarrow|)][\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)] = 0$

However, assuming differing modes of transmission and measurement, for example a right diagonal photon measured in a vertical-horizontal mode, we have:

At detector 0: $\langle\uparrow|[\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)] = \frac{1}{\sqrt{2}}$.

At detector 1: $\langle\rightarrow|[\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)] = \frac{1}{\sqrt{2}}$.

We note that a probabilistic result with equal probability of detection at each detector. Thus the qubit state remains unknown. This case is illustrated in Figure 1.7.

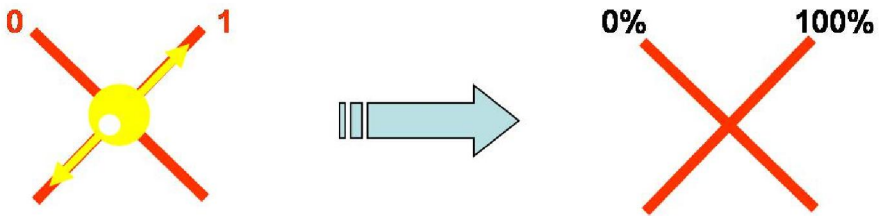

Fig. 1.6: A photon sent and measured in a common basis by Alice and Bob will result in a deterministic measurement. Bob will measure the exact polarization the photon was sent in and thus a key bit may be produced from such a qubit.

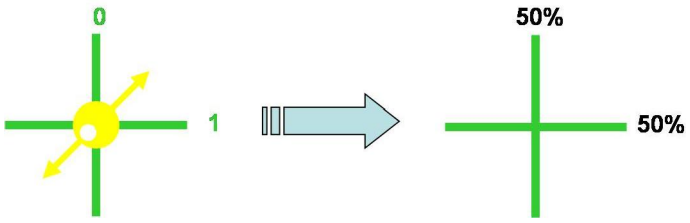

Fig. 1.7: A photon sent and received in unmatched bases will produce a probabilistic result. Bob will measure either a 0 or 1 randomly, thus a key bit can not be produced from such a measurement.

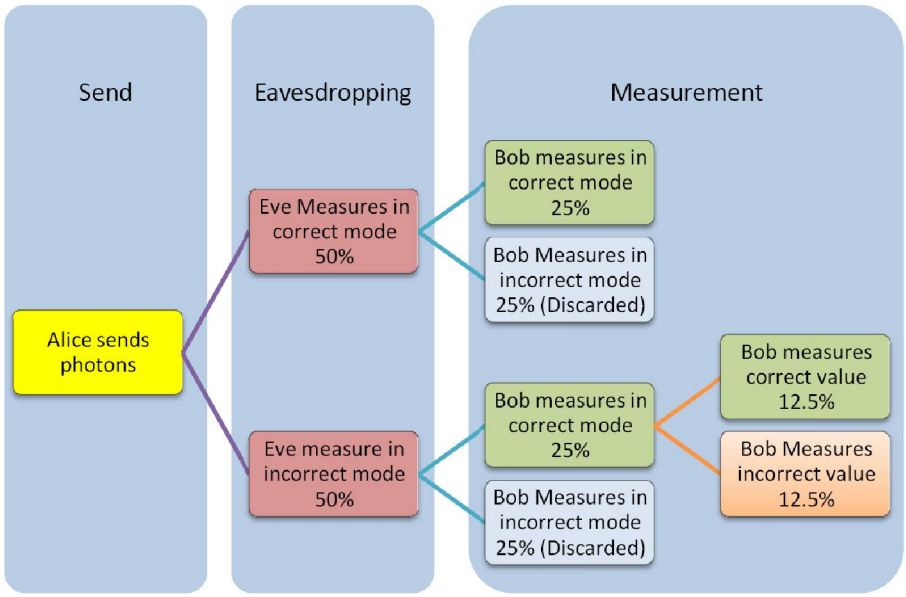

Fig. 1.8: Due to an eavesdropper's interception of qubits during the distribution process, 25% of the qubits measured in the correct basis by Bob contain errors. These qubits constitute 12.5% of the total qubits measured by Bob.

After the qubits have been transferred, Bob informs Alice, via a classical channel, of his sequence of qubit measurement modes. Alice then informs Bob as to which qubits were emitted and received using a common mode, only these qubits are used to form the key, the remaining are discarded. This process is known as *sifting*. We note that in all classical communications, no mention of the sent/measured qubits states is made.
An eavesdropper is unable to measure the value of the qubit without introducing uncertainties. Due to the Heisenberg uncertainty principle, if Eve intercepts the transmission, the qubit is necessarily destroyed or its properties altered. Consider, for simplicity, an *individual attack* attack, Eve can only measure the qubit once while in its original state, this is due to the fact that the qubit undergoes a wave function collapse upon measurement. The original mode is unknown to Eve thus she is forced to guess the mode of polarization. Due to Alice's random choice of modes, Eve does not know the qubit state with certainty and will hence introduce errors in the retransmission of qubits to Bob.
Alice and Bob may easily determine the presence of an eavesdropper by comparing small quantities of their final key. The compared portion of the key is then discarded [22]. The presence of an eavesdropper is confirmed through a statistically significant number of differences in the sifted key. In a noiseless environment, Eve would produce an error of 25% within the sifted key as illustrated in Figure 1.8.

1.3.5 Essential Parameters of QKD

Due to the different regime under which quantum cryptography operates, a special error rate, known as the Quantum Bit Error Rate (QBER), is used together with the raw key rate to quantify usefulness of the implementation [25].
The Raw Key Rate (RKR) is the fraction of qubits that are successfully transmitted between Alice and Bob compared to the total amount of qubits sent by Alice. This, in practice, is less than 1. The equation for RKR is given by

$$R_{\text{raw}} = q\mu\nu\eta_{\text{t}}\eta_{\text{d}}, \tag{1.10}$$

where q is the intrinsic efficiency of the implemented protocol ($\frac{1}{2}$ for BB84), ν is the repetition frequency, μ is the average number of photons per pulse, η_{t} is the transmission efficiency and η_{d} is the detector efficiency [25].
The amount of error present in the sifted key is called the Quantum Bit Error Rate (QBER) [26]. If the QBER is statistically higher than anticipated, the presence of an eavesdropper may be assumed as all errors are assumed to arrive from Eve. The error in the key, and hence Eve's knowledge of the key, may be reduced by use of classical methods of error correction and privacy amplification. The The QBER may be calculated as [18],

$$QBER = \frac{\text{False} \quad \text{counts}}{\text{Total} \quad \text{counts}} = QBER_{\text{opt}} + QBER_{\text{det}} + QBER_{\text{acc}}. \tag{1.11}$$

$QBER_{\text{opt}}$ is a measure of the optical quality and stability of the setup. Quantitavily it is the probability of a photon to propagate to the wrong detector. It is independent of the length of the transmission fibre [25].
The $QBER_{\text{det}}$ comprises of three types of errors originating from detector inefficiencies. It may be written as [26],

$$QBER_{\text{det}} = QBER_{\text{dark}} + QBER_{\text{after}} + QBER_{\text{stray}}. \tag{1.12}$$

The $QBER_{\text{dark}}$ is a measure of the dark count while $QBER_{\text{after}}$ represents the after-pulsing of the detector. Both these error rates are dependent on the type of detectors being used. $QBER_{\text{dark}}$ increases with the length of the transmission line and hence effectively limits the range of QKD [25].
The $QBER_{\text{dark}}$ may be calculated as the ratio of probability of a dark count per gate, p_{dark}, to the probability of a count [18],

$$QBER_{\text{dark}} = \frac{p_{\text{dark}}}{p_{\text{count}}}. \tag{1.13}$$

$QBER_{\text{after}}$ is the probability of each gate to measure an after-pulse. To reduce the effect

of after pulses a dead time is introduced to the detector. During this time, immediately after a detection, no gates are applied. However an increase in dead time decreases the RKR. The optimum dead time varies as a function of distance [25].
Finally, $QBER_{\text{stray}}$ includes the errors caused by stray light within the medium [25]. The largest contribution to this in fibre is that of Rayleigh backscattering. The use of wavelength division multiplexing may also increase this further.
$QBER_{\text{acc}}$ is an error that occurs in entanglement based QKD systems. It occurs due to the fact that uncorrelated photons are produced by imperfect sources [18].

A good system requires not only a high R_{raw} as a high QBER will reduce the length of the final key substantially. The fraction of bits lost in error correction, R_{EC}, routines may be approximated as [25],

$$R_{\text{EC}} = \frac{7}{2} QBER - QBER(\log_2 QBER), \tag{1.14}$$

while the fraction lost to privacy amplification, R_{PA}, is [25],

$$R_{\text{PA}} = 1 + \log_2 \left(\frac{1 + 4QBER - 4QBER^2}{2} \right). \tag{1.15}$$

The final useful key creation rate is given as [25],

$$R_{\text{useful}} = R_{\text{raw}}(1 - R_{\text{EC}})(1 - R_{\text{PA}}). \tag{1.16}$$

Privacy amplification is a classical procedure that removes information that Eve may posses about the distributed key. It is noted that the higher the QBER implies a lower the useful key rate due to the key length reduction in the privacy amplification process. A higher QBER can thus also be interpreted as greater mutual information between Alice and Eve, however a quantitative analysis of such information falls beyond the scope of this thesis.

2. QUANTUM CHANNELS

2.1 Types of Quantum Channels

Together with quantum enabled devices on both Alice and Bob's ends, QKD requires a medium through which such quantum information may be transferred. A quantum channel is a communication channel that can transmit quantum as well as classical information. An example of quantum information is the state of a qubit while that of classical information is the text of this document. Physically, the core difference between the two types of channels is the fact that classical channels encode many information carriers with the same bit of information while quantum channels permit the encoding of exactly one quantum system for a particular bit of information.
Mathematically a channel is defined as a linear, completely positive, trace preserving map [7]. This implies that:

- The channel maps positive operators to positive operators.
- The channel should preserve the normalization of states.
- The above results should apply when the channel maps the input to a sub-space of a higher dimensional space.

Many realizations of quantum channels exist. They vary from natural media, as in 1D magnets used as spin-chain quantum channels [27] to line-of-sight link in free-space through photon communication [28], to fabricated materials such as fibre optic cables. Quantum channels, as in the classical case, are charactorised into various classes according to the chactoristics of the transmission. There are 4 main characteristics of quantum channels [7]:

Channels with memory
The output of a channel is dependent on the corresponding input as well as the previous inputs to the channel.

Memoryless channels
The output of a channel is dependent solely on the corresponding input.

Noiseless channel
The channel is not effected by the environment, thus the output is independent of any environmental parameters. This implies perfect communication.

Noisy channel
The environment of the channel is non-trivial. Thus the output of the channel depends on both the input and the environment.

Memoryless channels are of particular interest to Quantum Key Distribution. This is due to the fact that any channel with memory would become a potential source of side information to the eavesdropper, thus compromising the cryptosystem.
Noiseless channels are only a theoretical concept and are not physically implementable. This is due to the intrinsic environmental background noise and defects within the channel itself.

2.2 Shannon's Coding Theorems

There are two fundamental questions with respect to communication channels. The first is with regards to the amount of resources required to transmit information over a channel. The second question is to the amount of tolerable noise over a channel.
C Shannon wrote two papers in 1948 [29, 9] in which he presented two theorems to answer these questions. These two theorems formed the bases of information theory and are presented below:

Noiseless channel coding theorem
This theorem provides a quantitative measure of the resources required to communicate information over a given channel. It implies that information can not be compressed to a degree more than that corresponding to the total Shannon entropy [29]. Compression exceeding the Shannon entropy will imply a loss of information. This provides the upper bound to the capacity of any channel.

Noisy channel coding theorem
This theorem quantifies the tolerable noise that a channel may contain before information distortion occurs. Shannon illustrated that in the presence of noise, error correcting codes may be used to remove noise from the signal. He further provided an upper bound to the amount of noise that may be removed through error correcting codes.

Corresponding quantum theorems have been explored however only a counterpart to Shannon's Noiseless Channel Coding Theorem was developed by Ben Shumacher in 1995 [30].

2.3 Optical Fibre as a Quantum Channel

Every implementation of a quantum channel is non-ideal due to its physical nature,

however optical fibre has been found to be one of the most practical quantum channels available presently for photonic qubits. Single mode optical fibres act as a memoryless, noisy quantum channels.
The use of fibre as a quantum channel was first considered after CH Bennett presented a phase-encoded photonic implementation of the B92 protocol [31]. Thereafter many QKD protocols were converted to their phase-encoded counterparts for implementation over optical fibres, this includes the original BB84 protocol [31]. Together with this, the fibre optic communication boom of the early 90's saw much research and development of low attenuation fibres and methods of dispersion reduction and compensation. Low attenuation and dispersion rectification are essential as the maximum key distribution distance and the detector gating windows, hence detector efficiency, are dependent on them respectively. Modern fibre is characterized by a low attenuation in the order of 0.2dB/km. Decoherence effects due to polarization and dispersion effects are detailed in sections 2.4.2 and 2.4.3.
Optical fibres further contain high bandwidths through multiplexing techniques permitting high-speed concurrent communication between multiple parties, this will assist the second generation QKD solutions to incorporate networking functionality.
The efficiency of an equivalent free-space system would depend on atmospheric conditions such as humidity, mist and pressure gradients. Beam spreading and ambient light also adversely effect the efficiency of a free-space implementation. However the use of geostationary satellites would facilitate the creation of global QKD networks [32] not achievable with present day optical fibre technology. Free-space channels further have weak dispersion characteristics and almost no birefringence, both which are strongly present in optical fibres.
Presently quantum channels are being developed as free-space satellite links [32], electron spins chains [27] and nuclear magnetic resonance [33].
Each type of quantum channel is suited for a particular terrian. To date two channels have mainly been exploited for QKD deployment, line-of-sight free-space links and optical fibres. Table 2.1 compares these two quantum channels highlighting their benefits and drawbacks.

2.4 Fibre Characteristics

2.4.1 The Propagation of Light in Optical Fibres

The propagation of light through an optical fibre is due to a combination of total internal reflection and waveguide refraction. A varying refractive index profile creates a waveguide within the fibre. The center of the fibre, known as the core, consists of an impurity doped region that has a higher refractive index as compared to the outer cladding. This causes total internal reflection or refraction, depending on the profile of the fibre, thus confining the light pulse within the core. The size of the core varies between the different types of fibre.
Two common types of fibres occur. Multimode fibre has a core diameter in the order

Tab. 2.1: A comparison between two of the most widely used quantum channels for QKD. Each channel is suited for particular usage and as such a global quantum network would require the integration of all such channels to optimize the throughput of the network.

Free-Space QKD	**Fibre based QKD**
Implements a 'line-of-sight' setup	Implemented over any all-optical fibre link
Weather dependent	Laid fibres weather independent
QKD implemented to a distance of 144km [34]	QKD implemented to a distance of more than 120km [35]
Possibility of the development of global QKD networks through satellites	Ideal for MANs or long haul intercity connections
Cheap efficient detector technology	Expensive inefficient detector technology
Greater susceptibility to beam spreading implying greater transmission loss	Waveguide restricts beam spreading thus energy confined to the core
Greater erroneous detections	Fibre protected from external light sources
Practically non-birefringent	Birefringence causes substantial difficulties
Weakly dispersive	Highly dispersive
Linkage dependant on terrain	Linkage dependant on fibre infrastructure
No commercial QKD systems available	3 commercial suppliers

of 50μm while single mode fibre has a diameter of between 6-10μm. Due to dispersive effects, only single mode fibre is suitable for QKD [18].
Optical fibre has a typical absorption spectrum with three transmission bands. The unique absorption characteristic is due to a superposition of Rayleigh backscattering, infrared absorbtion and certain molecule excitations [36]. The transmission bands are troughs within the absorption spectrum of the fibre. As may be seen in Figure 2.1 the third window at around 1550nm produces the least attenuation and is hence best suited for telecommunication and QKD.

Apart from the attenuation, another factor restricting QKD is the coupling of the photons to the environment. Such coupling causes decoherence and may provide an eavesdropper with sufficient side information to tap the system unnoticed. In this case the environment is regarded as everything beyond the degrees of freedom of the used to encode the photon [18]. Thus if the photon is encoded through phase, the polarization

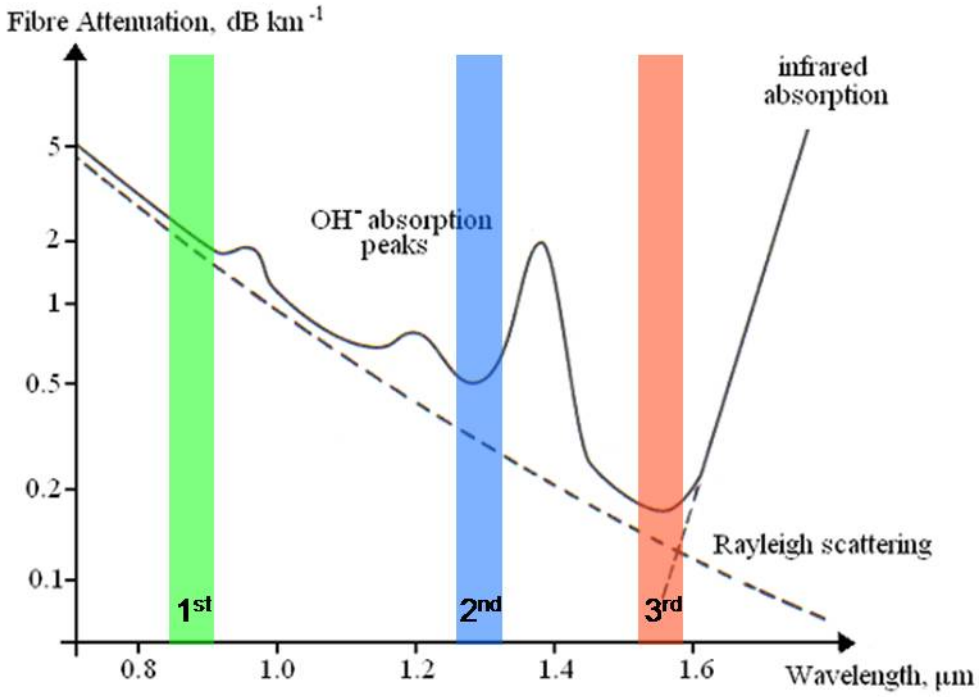

Fig. 2.1: The absorbtion spectrum of optical fibre. Attenuation at smaller wavelengths is due to phonon absorbtion while larger wavelengths are absorbed through infrared absorbtion. This coupled with Rayleigh back scattering and O-H absorbtion producing three attenuation minima known as the transmission bands. *Adapted from [1].*

and wavelength of the photon act as part of the environment. This is significant as if the encoding or measuring instruments have a dependence on any other property of the photon, it would serve as side information to an eavesdropper.
In the following sections we discuss decoherence through polarization and dispersion based effects in fibre.

2.4.2 Polarization Effects

The polarization affected propagation through optical fibres causes many technical challenges towards the implementation of QKD systems. Such effects are inherently a problem for polarization encoded QKD systems, however as the interference visibility is also dependent on the relative polarization of the photons, these effects create complications within phase encoded systems as well. Three major polarization related affects occur as explained below:

Birefringence
Optical fibre consists of two orthogonal transmission axes, the fast and slow axes. All light traveling within the fibre is polarized into these axes. Light traveling in the fast axis travels at a higher group velocity and hence decoupling between the polarization states occur inducing dispersion. The birefringence is caused due to imperfections and stresses within the fibre. Such effects are relatively stable for slow variations in temperature and motion [18].

Geometric phase
This is a quantum mechanical effect based on the *Pancharatnam-Berry* phase. It is a phase shift that is acquired by a quantum state due to a cyclic adiabatic process. The phenomena was discovered in 1956 [37]. The effects of the geometric phase can easily be overcome through periodic calibration of the apparatus and quantum channel. This however may be impractical if the fibre variations occur rapidly as in the case of ariel fibre cables.

Polarization dependent losses
These losses are mainly due to optical components that have polarization dependent effects. Essentially these components act as polarizers blocking off a particular polarization of light [36]. This is a stable effect within the component, however the output intensity of light may be unstable due to the coupling between the component and the input signal that will vary due to the varying birefringence of the fibre.

2.4.3 Dispersive Effects

Dispersion reduces the signal quality through power fading and inter-symbol interference. The former is of greater concern to present QKD solutions as power fading causes a higher temporal variance of the arriving pulse, hence a wider time bin or gating time

is required for the detector. This, as seen earlier, severely degrades the efficiency of the detectors and increases the QBER. Three types of dispersive effects occur:

Modal dispersion
The higher refractive index of the core may be regarded as a potential well. If this well is large, corresponding to multi-mode fibre, then many bounded or guided states may occur [38]. The varying guided modes are produced due to the wavelength dependent refraction of light in the waveguide as well as the acceptance angle of the light into the fibre. As each transmitted pulse consists of multiple modes of light a two fold effect is noticed. Firstly each mode has a high probability of coupling with other modes resulting in the decoherence of the photons. Secondly as the modes travel varying lengths through the fibre, they cause a widening of the received pulse implying a larger window time for detection. This type of dispersion has been largely rectified through the use of single mode fibres. Due to the small core diameter, this type of fibre allows only one mode of propagation. Hence only single mode fibre is suitable for QKD [18].

Chromatic mode dispersion
This type of dispersion is of major concern in phase-encode QKD systems as such systems rely on the localization of the photon in space. Varying group velocities within the different arms an interferometer would cause a drop in visibility. Chromatic mode dispersion is caused due to the dependance of the optical density on the frequency of light [38]. Thus different wavelengths of light travel at varying speeds within the fibre and arrive at the detector with a temporal variance greater than that of the original pulse. As this type of dispersion is a stable effect in that it is a static property of the fibre. The use of Distributed Feedback (DFB) lasers and dispersion shifted fibre may be used to overcome such dispersive properties. DFB lasers emit very narrow bandwidth pulses hence reducing the optical density spread seen by the pulse.

Polarization mode dispersion
This is a birefringence related phenomena. Optical fibre may be viewed as a chain of randomly orientated birefringent segments. These segments are created through stresses and defects within the fibre. The orientation of the transmission axes vary for each of these sections. For a particular segment the birefringence ranges in the order of a few ps per km [38]. The smaller the dispersion between the polarization modes in each segment, the better the polarization mode coupling hence a smaller dispersion effect at the point of defect. The random coupling of the polarization modes may be seen as a random walk and hence the Polarization Mode Dispersion (PMD) is measured in ps per $km^{1/2}$.
PMD has limited effects on phase encoded QKD as the use of a laser with coherence time greater than the largest birefringent section in fibre would readily compensate for this dispersion [18]. Active compensation techniques would be required for the implementation of polarization encoded QKD over optical fibre or photons

produced through parametric down conversion Ḣowever other birefringence related technicalities do pose many complex challenges in the implementation of phase encoded QKD systems.

Due to the quantum based requirements of a single photon stream many of the compensation and regeneration techniques used in classical communication can not be used in QKD. Electro-optical components convert the optical signals to electrical before acting on the signal, this however constitutes a measurement and hence destroys the quantum coherence and superposition of the qubit.
Classical all-optical regeneration techniques rely on the stimulated emission [36]. This process produces relatively high amounts of spontaneous emission. As the probability of stimulation is proportional to the signal power, a single photon would have a negligible stimulation probability. Further this type of regeneration would conflict with the no-cloning theorem.

2.5 Polarization to Phase Encoding

Polarization encoded QKD faces many technological challenges if implemented through optical fibre as noted above. This is mainly due to the presence of transmission axes and the birefringence caused by them. Thus the polarization state undergoes a random walk over the surface of the Poincaré sphere. Such implementations would, in the least, require a complex active compensation system for polarization recovery at Bob's end with a frequent calibration process. The recent developments in all-optical PMD compensation methods for high speed classical communication have however rekindled the interest in fibre based polarization encoded QKD [39].

A convenient fibre-based encoding method was discovered by CH Bennett in 1992 [31]. This uses the relative phase between two photon pulses. The polarization encoding may be directly interpreted into phase encoding through the use of a Mach-Zehnder interferometer as shown in Figure 2.2.
A photon is placed into a superposition through the use of a 2x2 coupler. This serves as a fibre based counterpart to a beam splitter. The two pulses of the photon travel through each arm on which a phase shift is added by Alice and Bob respectively. These combine at the exit point of the interferometer through a coupler that serves, together with the detectors, as the measurement apparatus. The relative phase of the pulses span out the azimuthal angle while the bias in the first coupler adjusts the latitude. Thus any state on the Poincaré sphere may be created by the adjustment of the applied phase and coupler bias.

The orthogonal states measured by a polarization dependent beam splitter is interpreted through the interference of the two pulses upon exit from the interferometer. Constructive or destructive interference leads to the routing of the photons to either detector

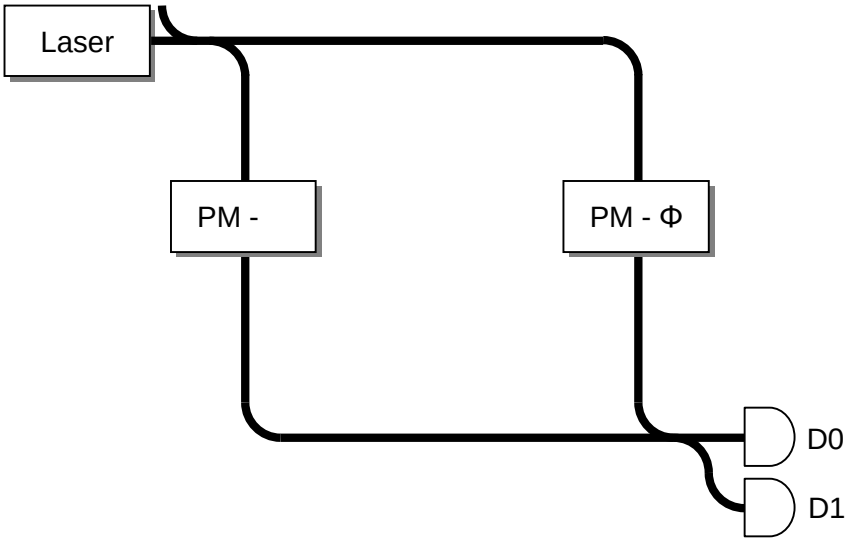

Fig. 2.2: A schematic diagram of a Mach-Zehnder interferometer. The pulse is split at the first coupler and travels through both arms of the interferometer. In each arm a phase differential is added. As the lengths of the arms are identical, the pulses reach the second coupler at the same point in time. Upon recombining interference occurs and the photon is routed to the detectors.

deterministically.
The classical Mach-Zehnder interferometric setup however is impractical to setup in practice. Such a setup would require two fibre based quantum channels, furthermore these fibres are to be equal in length and stable to within a few wavelengths of the photons to ensure good interference visibility. To curb such complications the pulses are sent through a single fibre using a time modulated method. This may be achieved through the use of two asymmetric interferometers, one on each side of a single communication channel separating Alice and Bob. The each arm of the Mach-Zehnder interferometer consists of the common channel, the long arm of one asymmetric interferometer and the short arm of the other. This creates a spatial shift between the two arms of the Mach-Zhender interferometer permitting the pulses to travel in separate time bins within the common quantum channel.
As the lengths of the two arms differ, the pulse emitted by Alice is sent through the quantum channel in two time bins. Upon arrival at Bob's end, the time separated pulses enter a second identical asymmetric interferometer. If the pulses travel through the complementary arms, both will have traveled equal distances. Thus interference will occur at the second coupler [40]. Such a system can be further enhanced by using a '*Plug & Play*' passive auto-compensating system [41] or classical pulse calibration methods [23].

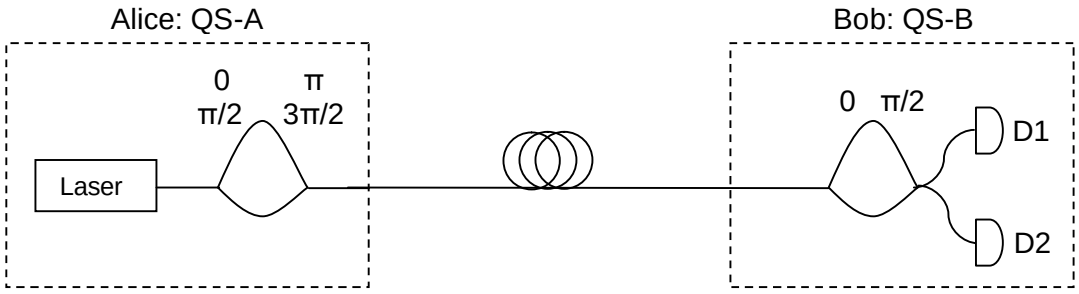

Fig. 2.3: A Schematic diagram of the phase-encoded BB84 protocol setup. Alice may choose 1 of 4 phase shifts corresponding to her mode and state choice while Bob has 2 choices of measurement modes. The nett phase between the pulses routes the photon to a particular detector.

The BB84 protocol may also be implemented using a phase-encoded qubits as illustrated in Figure 2.3.
A photon is emitted by Alice's station; this photon enters a superposition of two time shifted pulses at an asymmetric interferometer. A phase differential is also added to one of the pulses within the interferometer. The phase choice determines the mode and state of Alice's qubit as described in Table 2.2.

Tab. 2.2: Alice may send four different qubit states interpreted as phases. Note again that she has a choice of 2 non-orthogonal modes, each with 2 orthogonal states.

Mode	**State**	**Phase**
1	0	0
1	1	π
2	0	$\pi/2$
2	1	$3\pi/2$

After traveling over the transmission line, the receiver routes the pulses through converse arms of a second identical interferometer such that both pulses will have traveled equal distances upon exiting. Within the interferometer, a phase phase shift of 0 or $\pi/2$ is added to the second pulse corresponding to the mode selection process by Bob. Upon exiting the interferometer, the two pulses of the photon recombine and the photon undergoes constructive or destructive interference due to the nett phase differential added by Alice and Bob [42]. The interference, corresponding to the binary set, is measured through the use of two single photon detectors and used to create the raw key. Table 2.3 demonstrates the permutations that photons may be sent and received in and the corresponding key bit value produced.

Tab. 2.3: Eight emission/measurement permutations occur. For each state sent by Alice, Bob may measure the qubit in the correct or incorrect basis thus giving rise to deterministic or probabilistic results respectively. The '?' below in the table represent probabilistic result from which no key bit can be produced in the BB84 protocol.

Alice			**Bob**		**Raw Key**	
Mode	**State**	**Phase**	**Mode**	**Phase**	**Phase Differential**	**Key Bit**
1	0	0	1	0	0	0
1	0	0	2	$\pi/2$	$\pi/2$	?
1	1	π	1	0	π	1
1	1	π	2	$\pi/2$	$\pi/2$	?
2	0	$\pi/2$	1	0	$\pi/2$	?
2	0	$\pi/2$	2	$\pi/2$	0	0
2	1	$3\pi/2$	1	0	$3\pi/2$	?
2	1	$3\pi/2$	2	$\pi/2$	π	1

As a key bit may only be created when the photon is sent and measured in a common mode, half of the sent qubits are wasted thus reducing the efficiency of the BB84 protocol.

3. QUANTUM KEY DISTRIBUTION IN PRACTICE

In this section we introduce a practical QKD system through which our initial tests on quantum networks will be performed. We further explain a practical method of increasing the efficiency of QKD protocols through post-processing means.

3.1 id3000 Clavis QKD System

3.1.1 Principle of operation

The id3000 Clavis Quantum Key Distribution System has been developed by id Quantique, Switzerland. This QKD system implements a phase-encoded BB84 '*Plug & Play*' scheme, proposed by H Zbinden *et al* from the University of Geneva [40].
The setup described in section 2.5 requires identical interferometers for good interference visibility and hence low error rates. The coupling ratios and lengths of the corresponding arms of the two interferometers should be equal. Furthermore, phase modulators (PM) are generally polarization dependent; hence polarization rectification must be observed during the transmission. Due to the above, the interferometers need to be frequently aligned and the internal path lengths kept stable to an order of tens of nanometres [43]. The 'Plug & Play' system is based on the above. However it integrates a time-multiplexed auto-compensating procedure using Faraday mirrors [40]. The advantage of such an implementation is that it is stable and polarization independent. Figure 3.1 highlights the differences of the clavis system from the conventional setup.
The system consists of a single interferometer in Bob's apparatus (QS-B). Due to the fact that fluctuation time of the fibre birefringence is longer than the time of flight of the photon, passive compensation of polarization dependent effects are observed [40]. Thus any modifications in the polarization of the photon are compensated on the return trip.

A classical light pulse of high intensity is emitted by QS-B. The pulse is then split through an asymmetric interferometer. The first pulse, P1, moves directly to Alice's station (QS-A) through the short arm of the interferometer, while the second pulse, P2, undergoes a polarization rotation in the long arm. The classical pulses then propagate towards QS-A as shown in Figure 3.2(a). After reflection QS-A attenuates the pulses to single photon levels. Alice's phase shift is also incorporated into P2 with the use of the phase modulator in QS-A. This is illustrated in Figure 3.2(b). Due to the Faraday Mirror, the reflected pulses are in orthogonal polarizations with respect to the incident

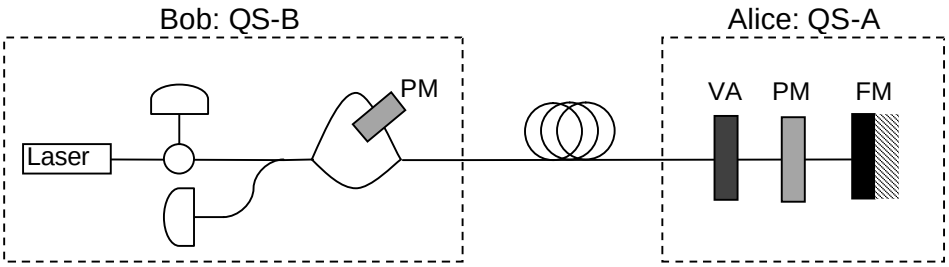

Fig. 3.1: A schematic diagram illustrating the setup for the phase encoded auto-compensating BB84 protocol. This setup is characterized by the use of a single interferometer and a Faraday Mirror (FM). A variable attenuator (VA) reduces the classical pulses to photon levels while the phase modulators (PM) acts to select the modes and states of transmission and measurement.

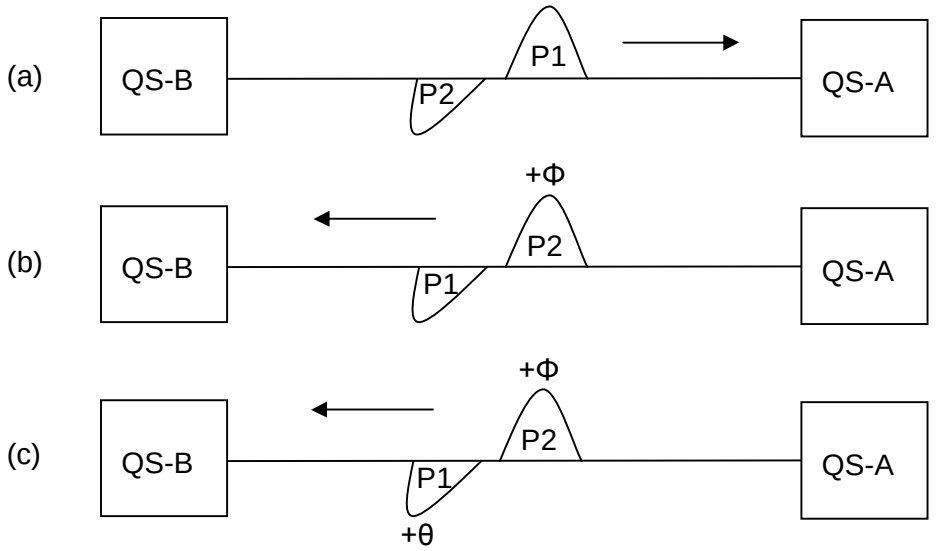

Fig. 3.2: This figure illustrates when phase shifts are added to the pulses in the Plug & Play QKD scheme. Figure 3.2(a) depicts the classical pulses being sent to Alice with no encoded information. In figure 3.2(b) the pulses are attenuated to single photon level, polarization switched to orthogonal state and a phase shift added to P2. While in the interferometer in the return trip, a phase shift is added to P1 in the long arm as depicted in figure 3.2(c).

beam thus on the return trip, P2 propagates through the short arm and P1 through the long arm, hence both pulses travel equal distances. A phase shift is added to P1 corresponding to the measurement choice of Bob, as in Figure 3.2(c). The pulses interfere upon exiting the interferometer as in the original setup.

3.1.2 A Comparison of the Randomness of Numbers Generated through Classical and Quantum Methods

The Clavis system was tested over a dedicated 13km of optical fibre in a laboratory environment. A secure key of 50 Mbits was created and distributed between the two stations. Data was encrypted and transferred at over an ethernet cable.
During the key distribution the avalanche photo-diodes are set to a temperature of -50^{O}C and a dark count probability of 6.41705x10^{-6} and 1.00671x10^{-5} was measured on the two detectors respectively. The maximum interference visibility on each detector was 3.6% and 4.7% respectively. All the above parameters were measured on the Clavis system through software provided with the system.
A total of 52,248,000 qubits were sent while the detectors were gated 11,726,727 times. Thus only 22.4% of the pulses produced were measured due to the dead time of the detectors after a photon measurement. During the distribution 7.29% of detector gates resulted in detections of which 0.06% were double detections and 3.62% were valid measurements (send and received in a common basis). The overall QBER was measured at 0.93%.
Figure 3.3 represents the detector counts for the two detectors according to the phase selection permutations of Alice and Bob given in Table 3.1.

Tab. 3.1: Phase selection permutations in the BB84 Protocol.

Mode Selection	**Phase Added by Alice**		**Phase Added by Bob**	
1	0	Mode 1	0	Mode 1
2	π	Mode 1	0	Mode 1
3	0	Mode 1	$\pi/2$	Mode 2
4	π	Mode 1	$\pi/2$	Mode 2
5	$\pi/2$	Mode 2	0	Mode 1
6	$3\pi/2$	Mode 2	0	Mode 1
7	$\pi/2$	Mode 2	$\pi/2$	Mode 2
8	$3\pi/2$	Mode 2	$\pi/2$	Mode 2

A further key stream of 5 million bits was generated through the QKD system and analysed with the acclaimed 'diehard' tests [8]. In such tests, the randomness of the input is assigned a value between 0.000 and 1.000 indicating the independence of the key stream. A uniform distribution of P-values indicates good independence of the input

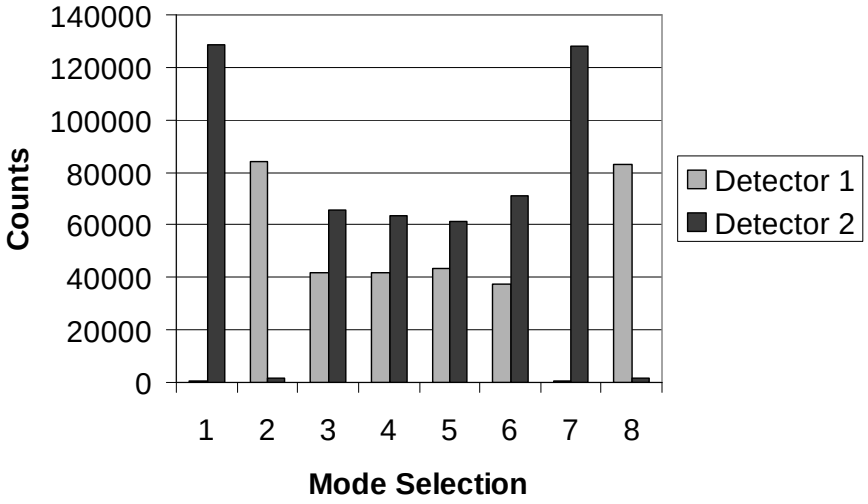

Fig. 3.3: A graph illustrating the detector count summary as per the phase selection permutations given in Table 3.1. It is seen that common mode measurements result in deterministic results. Detector 2 received a greater number of photon detections in the uncorrelated measurements due to a higher interference visibility.

stream. A summary of the results are given in Table 3.2.
It may be calculated that the quantum random number generation process produces a smaller standard deviation amongst the p-values for the 14 tests. As a uniform set of p-values indicate good independence [44], it is noted that the quantum random numbers are better suited for OTP applications.

3.2 An Alternate QKD Protocol for a BB84 Cryptosystem Apparatus

Cryptosystems implementing the BB84 cryptosystem, may be used to implement other protocols such as the SARG [18] and Singapore protocols. Such protocols have various benefits as compared to the BB84 protocol.
The BB84 protocol distributes the raw key through the transfer of qubits in two non-orthogonal basis modes. The distribution and measurement modes are chosen independently and randomly by Alice and Bob while transmitting and receiving the qubits respectively. Thus, as mentioned earlier, the BB84 protocol, although simple to implement, has an intrinsic loss of 50%. The number of key bits created per qubit distributed, or the sifting efficiency, is 1/2.
Further the above protocol verifies the security of the key with a post-sifting process to ensure the correctness of a key sample through two-way communication over a public channel. A statistical analysis is then performed on the results to confirm key's secrecy. The key segment used for this process must then be discarded reducing the key length further.

Tab. 3.2: Test results from the diehard random number tests indicate the a greater uniformity of p-values, hence randomness, of the quantum generated key stream when compared to classically generated random numbers.

Random Test	P-Value	
	Classical Random Numbers	**Quantum Random Key**
Birthday Spacings Test	0.8942	0.2309
Overlapping 5-Permutations Test	0.7897	0.5307
Binary Rank Test (31x31 matrixes)	0.3956	0.3201
Binary Rank Test (32x32 matrixes)	0.4051	0.4197
Binary Rank Test (6x8 matrixes)	0.7907	0.3179
Bitstream Test	0.3567	0.0772
Count the 1s Test	0.3026	0.5114
The Parking Lot Test	0.1898	0.4022
Minimum Test	0.2172	0.3625
3D Spheres Test	0.6625	0.6422
Squeeze Test	0.4966	0.2204
Overlapping Sums Test	0.4387	0.3562
Craps Test (Wins)	0.7984	0.0966
Craps Test (Throws)	0.6181	0.6063

Integrating the tomographic analysis of the Singapore protocol [45] into the BB84 setup can enhance the overall efficiency of the system. The enhanced protocol uses the original physical BB84 setup, however the Iterative Key Exchange (IKE) algorithm [46] is used to process the unmatched qubits of the BB84 protocol. All the experimental verification was conducted on the id3000 Clavis QKD system explained earlier.

3.2.1 Singapore Protocol

The Singapore protocol is a method of QKD devised by BG Englert *et.al.* in 2003. It is known to have a better noise tolerance than the BB84 protocol [45]. This protocol has the potential of achieving a theoretical efficiency of 41.4% for key bits produced per qubit. The minimal qubit tomography used in the Singapore protocol minimizes the the number of redundant parameters measured in the more general six-state tomographic protocols. The Singapore protocol is characterized by [46, 45]:

1. Minimal Qubit Tomography (MQT) for acquisition of raw data.
2. State tomography for security verification.
3. Key generation through an iterative method.

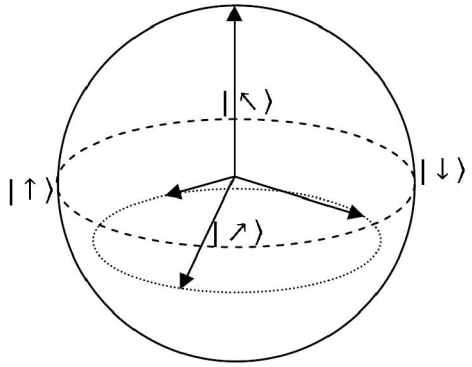

Fig. 3.4: The Poincaré sphere representing the four basis states used in the Singapore protocol. The four states maybe alternatively constructed by taking four vectors from the center of a cube to its non-adjacent corners.

In the Singapore protocol four basis states are used to span the Poincaré sphere and hence characterize all other states. This reduces the redundant tomography in the original six state tomographic protocols. The four state protocol also allows for a higher mutual information as compared to the six state protocol. Details of the implementation may be found in [45]. When seen on the Poincaré sphere, the four basis states, as shown in Figure 3.4, are formed by vectors from the center to non-adjacent corners of a cube resulting in a tetrahedral. These basis vectors will completely characterize any other arbitrary state in the Poincaré sphere.

In essence, the security verification of the Singapore protocol is based on detection statistics. The method of key generation relies on the fact that each phase selection by Alice ensures that Bob has a null detection probability on a unique detector. The remaining three detectors in each case posses equal detections probabilities according to Table 3.3 [46].

Tab. 3.3: The detection probabilities for each detector in the Singapore protocol as per the phase selection of Alice. Each phase selection of Alice disallows a click on unique detector, while the detection probabilities on the remaining detectors are equal.

Alice	**Probabilities of Detector Clicks**			
Phase Options	**A**	**B**	**C**	**D**
A	0	0.083	0.083	0.083
B	0.083	0	0.083	0.083
C	0.083	0.083	0	0.083
D	0.083	0.083	0.083	0

The security verification is confirmed through the correct detection statistics measured by Bob [45]. A recursive algorithm, called the Iterative Key Exchange (IKE), is utilized to form a secret key from the raw qubit exchange. Each of Alice's phase options with its corresponding detector of null detection probability are preassigned a value from A-D. After the qubits have been exchanged, the key bits are produced in the following manner:

1. Bob chooses two position in his sequence that contain a common letter. These positions are communicated to Alice over a classical channel.
2. Alice checks her sequence at the respective positions. She may either have identical or differing letters at these positions.
3. If Alice has different letters, she groups the two letters together and creates another set from the two remaining letters. She knows that Bob received a detection on a detector from the latter group.
   (a) Alice then randomly assigns bit values to both the sets and relays this back to Bob over a public line. She records the value of the latter set as her key bit.
   (b) On receiving the sets and the corresponding values, Bob records the the value of the set that contains the detector on which he measured a detection.
4. If Alice finds a common letter at the positions Bob conveyed she informs Bob. Both then store their respective letters in a secondary sequence. The secondary sequence contains the same statistical distribution as the original sequence [45].
5. After the primary sequence has been exhausted, the above procedure is repeated with the secondary sequence.

The above iterative method can continue indefinitely, however it is only practical to perform the cycle 3-5 times as thereafter the efficiency is not substantially increased. This is due to the exponential growth of the number of distributed qubits required to create a key bit in successive cycles [45].

3.2.2 IKE implemented on the BB84 Setup

The physical setup for the enhanced BB84 protocol is identical to the original phase encode BB84 protocol [31] illustrated in Figure 3.5.

The post-distribution analysis, the IKE, requires an alternate interpretation of the apparatus setup. In this technique, the two phase modulations in the receiver's interferometer double each physical detector as two detecting devices. Thus the setup is viewed

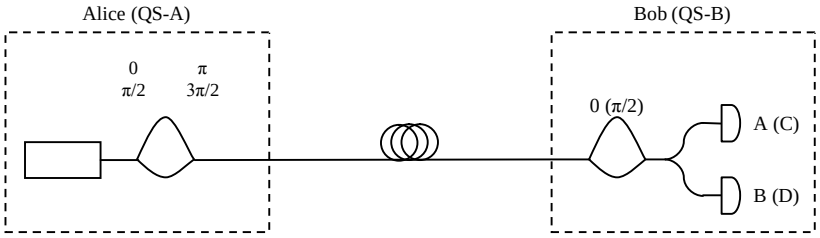

Fig. 3.5: Schematic diagram of the phase encoded enhanced BB84 protocol setup. A laser creates pulses of low intensity light as photonic qubits. These qubits are phase encoded through a set of identical asymmetric interferometers. The physical setup of this protocol is identical to the normal BB84 protocol setup except that each detector is doubled as two virtual detectors depending on the phase shift of Bob's interferometer.

as having 4 virtual detectors. However, only two of these 'detectors' may be evaluated during a given measurement. A random phase shift at the interferometer simulates the random path taken by the photon in the original setup.
Each phase shift of Alice creates a null detection probability on a unique virtual detector. For example a phase shift of π added to the qubit by Alice, Bob may either select a phase shift of 0 or $\pi/2$. With a 0 phase shift detectors A and B are measured while detectors C and D are measured with a phase selection of $\pi/2$. A net phase shift of π would result from a 0 phase shift thus causing destructive interference and hence a deterministic result is produced. Thus, for the aforementioned example, detector B will always click. However a phase selection of $\pi/2$ will result in a probabilistic measurement with each detector clicking 50% of the time.
If the phase shifts are chosen randomly, the resultant detection probability will be as in Table 3.4.

Tab. 3.4: The detection probabilities of the proposed enhanced BB84 protocol has the same core property permitting the IKE process. Each phase selection by Alice induces a zero detection probability on a unique detector. The remaining detectors have a symmetric detection probability although to equal.

Alice	**Probabilities of Detector Clicks**			
Phase Options	**A**	**B**	**C**	**D**
0	0	0.125	0.063	0.063
π	0.125	0	0.083	0.063
$\pi/2$	0.063	0.063	0	0.125
$3\pi/2$	0.063	0.063	0.125	0

The key creation process consists on a number of cycles. The first cycle implements the standard BB84 approach [17], thus creating a key with a sifting efficiency of 50%. The remaining qubits, with an unmatched basis, are used in the following recurring cycles.

The key developed through the IKE process, creates a key with 40% sifting efficiency. There is one scenario in which a possible security breach may occur during the additional IKE cycles. This will occur when both the letters of Alice's selection consists of detectors from one mode of measurement. The security breach is caused as the measured bases will have been broadcast in the previous BB84 sifting cycle. Thus an eavesdropper may infer the key bit through the knowledge of the measured basis. In this situation the sender calls for the abandonment of the particular qubits in question.
The IKE process can be implemented on the without the the first cycle of BB84 sifting. In this case, the sifted key will be produced with 40% efficiency however it will be more noise resistant. This is due to the fact that the IKE process is less susceptible to noise than BB84 sifting [45].

3.2.3 Experimental Verification

Experimental verification of this setup was realized on the id3000 Clavis QKD System. 10 sets of 100 Mbits each were distributed between the stations using a 'Plug & Play' BB84 setup. The detection probability was then calculated. Due to the asymmetric interference visibility of the detectors, the theoretical detection probabilities were recalculated and shown in Table 3.5. It is noted that the visibility did not effect the zero detection probability induced by Alice's phase choices.

Tab. 3.5: Due to technical reasons, the physical detectors have an asymmetric detection visibility. The theoretical detection probabilities of Bob, induced by Alice's phase choices, is thus modified and presented here. It is noted that probabilities still posses the unique property required for IKE.

Alice's	**Probabilities of Detector Clicks**			
Phase	**A**	**B**	**C**	**D**
0	0	$0.160 \pm 8.00 \times 10^{-3}$	$0.045 \pm 2.25 \times 10^{-3}$	$0.080 \pm 4.00 \times 10^{-3}$
π	$0.090 \pm 4.50 \times 10^{-3}$	0	$0.045 \pm 2.25 \times 10^{-3}$	$0.080 \pm 4.00 \times 10^{-3}$
$\pi/2$	$0.045 \pm 2.25 \times 10^{-3}$	$0.080 \pm 4.00 \times 10^{-3}$	0	$0.160 \pm 8 \times 10^{-3}$
$3\pi/2$	$0.045 \pm 2.25 \times 10^{-3}$	$0.080 \pm 4.00 \times 10^{-3}$	$0.090 \pm 4.50 \times 10^{-3}$	0

Each key of 100 Mbits was distributed and analyzed independently. The average result was then calculated and is presented in Table 3.6.

The measured detection probabilities maintained the properties of the theoretical model. In particular, the disallowed states, required for the IKE process in the enhanced BB84 protocol, were maintained. Less than 1% of all detections were measured in the disallowed states. These errors may be due to noise on the line or detector inefficiencies such as dark counts. These errors are sifted out during the IKE process and form part of the

Tab. 3.6: The experimental detection probabilities of the photon detectors correspond closely to the predicted values. In particular the disallowed states, essential for the IKE process in the enhance BB84 protocol, are maintained.

Alice's Phase	**Probabilities of Detector Clicks**			
	A	**B**	**C**	**D**
0	$0.001 \pm 1.85 \times 10^{-5}$	$0.159 \pm 2.93 \times 10^{-3}$	$0.045 \pm 8.30 \times 10^{-4}$	$0.081 \pm 1.49 \times 10^{-3}$
π	$0.092 \pm 1.69 \times 10^{-3}$	$0.002 \pm 3.69 \times 10^{-5}$	$0.041 \pm 7.56 \times 10^{-4}$	$0.081 \pm 1.49 \times 10^{-3}$
$\pi/2$	$0.046 \pm 8.49 \times 10^{-4}$	$0.073 \pm 1.34 \times 10^{-3}$	$0.001 \pm 1.85 \times 10^{-5}$	$0.159 \pm 2.93 \times 10^{-3}$
$3\pi/2$	$0.041 \pm 7.56 \times 10^{-4}$	$0.085 \pm 1.57 \times 10^{-3}$	$0.085 \pm 1.57 \times 10^{-3}$	$0.002 \pm 3.69 \times 10^{-5}$

QBER.
A further 50 Mbits were distributed and the efficiency of the standard and enhanced BB84 protocol compared. The results are shown in Table 3.7.

Tab. 3.7: An analysis of the key sifting cycles in the enhanced BB84 protocol shows that an increase of almost 40% in the efficiency is achieved through five cycles of the IKE as compared to the original BB84 protocol.

Cycle	**Method**	**Total Key Size**	**Efficiency**	**QBER**
1	Standard BB84	413,039	0.508	$0.039 \pm 7.22 \times 10^{-4}$
1	IKE	511,233	0.628	$0.032 \pm 5.81 \times 10^{-4}$
2	IKE	535,610	0.658	$0.030 \pm 5.56 \times 10^{-4}$
3	IKE	541,540	0.665	$0.029 \pm 5.48 \times 10^{-4}$
4	IKE	542,942	0.667	$0.029 \pm 5.48 \times 10^{-4}$
5	IKE	543,195	0.668	$0.029 \pm 5.48 \times 10^{-4}$

It is seen from Table 3.7 that the resultant key size, and hence the sifting efficiency, has increased by 31.51% from the standard BB84 protocol. It is also noted that the IKE algorithm tends to its asymptotic limit after 5 cycles thus further cycles will not be worth the computational time required.

4. QUANTUM NETWORKS

To date, QKD has been characterized by a dedicated two-point connection between end-users. This has served as a bottleneck towards the maturity of this research field into a commercially viable end product. Presently there are 3 companies globally producing such cryptographic devices[1].
A two-node QKD setup has restricted applicative use due to the following reasons:

1. QKD is intrinsically limited in spatial coverage. This is mainly due to the absorption and dispersion of the qubit within the quantum channel as explained earlier. The dark counts increase the QBER and hence effectively limit the distance a key may be distributed securely.

2. The quantum key distribution rate is lower than its classical counterpart. Commercially viable products would require data rates comparable to present today cryptography. This again may be shown to be related to the detector inefficiency and need for a dead time between detections. Free space QKD does however permit faster key distribution rates due to the silicon detectors used.

3. The QBER exceeds the classical error rate by an order of 10^5. This is exceptionally high, however this can be measured as a trade-off for the enhanced security.

4. The two-point QKD setup is prone to Denial of Service (DoS) attacks that isolate the end users. Hence a two-point setup would be considered frail. In order for a robust system, redundant light paths should be available to prevent such attacks.

5. The resources required for QKD far exceeds the product output. Hence the overhead capita is vastly increased when compared to classical cryptography.

6. Due to the dedicated fibre links between parties, mapping of key distribution relations is easily accessible. This may act as possible side information, thus compromising the provable security of the system.

The limitations may be viewed as a trade-off between the security and capita cost of the key. Commercial quantum cryptographic systems are available at present, however many have integrated classical cryptographic schemes to offer enhanced security rather than provable security [47].
To counter the above bottlenecks, much research has been performed in the field of

[1] id Quantique, MagiQ and SmartQuantum

Quantum Networks (QN) in order to facilitate multi-user QKD on-demand with good Quality of Service (QoS).
A QN is a network that utilizes quantum mechanical principles to implement provably secure key transfer in a multi-node system. Such networks permit a hybrid of quantum channels to be integrated to form a complete network. This is essential for the optimization network throughput as some quantum channels are better suited to particular terrains. There is greater robustness against DoS attacks due to redundant lightpaths within a network. This also assists in the reduction of key relation knowledge by any adversary.
Many investigations have been conducted and are currently being executed in an attempt to resolve the present limitations of QKD [48, 49]. Spatially separated entanglement of photons and quantum percolation theory [50] are two such examples. The integration of QKD systems into existing network architecture is of particular interest for developing commercially viable solutions.
The implementation of multi-user QKD over a fibre domain was spurred by the introduction of second-generation *all-optical* fibre networks. Previously fibre networks were opto-electrical, thus while the links between networking components and nodes were in the optical domain, the networking components converted optical signals to electrical pulses in order to manipulate or route the signal. The pulses are then converted back into the optical domain. These types of networks are unsuitable for QKD as the photons would be destroyed upon measurement by the components. All-optical, or second generation, networks use the properties of the light-pulses, eg the wavelength or intensity, to manipulate the pulses within the network. Thus the photon is not converted out of the optical domain and hence is not destroyed.
Present QKD systems also require dark fibre and hence have a highly inefficient channel capacity usage. This increases overhead costs and decreases the practicality of the system. One method of increasing the throughput of data and hence the usage efficiency is through Wavelength Division Multiplexing (WDM). We discuss the above in greater detail in this section.

4.1 Classical Networks

4.1.1 Network Layers

Modern network architecture follows a layered structure derived from a service-orientated approach. Each network layer provides functionality to the layer directly above it independent of the implementation. One such network model is the International Standards Organization's Open System Interconnection (OSI) Model [51]. It was first proposed in 1979 by Day and Zimmermann and was adopted as an international standard in 1983. [51].
The OSI model consists of 7 network layers detailed below:

Layer 7: Application layer

This is the layer that creates the user interface for the network. It consists of the common protocols used in network communication.

Layer 6: Presentation layer
This layer allows for the compatibility and translation of varying data structures to be transported over a common network. This layer also provides a platform for classical encryption of data.

Layer 5: Session layer
Communication sessions between stations may be setup throught this layer. This defines and manages the protocol to be followed by the computers during the session.

Layer 4: Transport layer
This layer defines and creates packets for data transfer. It is responsible to provide a hardware independent interface to the software layers.

Layer 3: Network layer
The optimal routing of data throught the network is controled throught the network layer. Different types of routing standards may be applied according to the Quality of Service of the network.

Layer 2: Data link layer
The software machinery for data transfer is provided by this layer. Error correction and conflict resolution are some of the responsibilities of this layer.

Layer 1: Physical layer
This layer consists of the underlying hardware of the network. It is used to create the physical links between end-users and to define the standards used for bit transfers.

It is interesting to note that general classical encryption is software driven and hence implemented through layer 6 [51] although some encryptors work at lower levels. QKD is hardware implemented and is thus embedded within the bottom two layers. This in itself illustrates the superior security of quantum cryptography as the security is embedded in physical quantum particles as opposed to computer algorithms.
The network layer offers two main types of network services, these are connection-orientated and connectionless links between nodes. In a connectionless (CL) or packet switching service the message is broken into small packets of data that are switched through the network depending on the destination and congestion of lightpaths. A connection orientated (CO) or circuit switched network establishes a dedicated lightpath between the two end-users before any data is transferred. Hybrid services such as Multi Protocol Label Switching (MPLS) are also available. This breaks the message up into small packets, the first packet is switched as in a CL network, however the other packets then follow the same lightpath as the first. This type of switching however does not utilize dedicated lightpaths and hence may be prone to congestion at switches.

CL and MPLS networks are not feasible for QKD at present due to line congestion. This due to the fact that if a packet is required to be switched through a congested line it would require temporary storage. With present technology this would require the photon to undergo conversion from the optical to electrical domain and would hence be destroyed.
Layers four to seven are essentially software orientated, a quantum network requires a new implementation in layers 1-3. Presently pure quantum cryptography has been implemented within layer 1 and 2 as point-to-point links. The focus of the remainder of this chapter will be on creating a layer 3 for the quantum network.

4.1.2 Multiplexing

Multiplexing in terms of networking is the division of channel capacity through some means to allow for concurrent multiple usage of the channel. Many methods of multiplexing have been investigated and are presently deployed in networks. Optical networks have a unique multiplexing technique knows as Wavelength Division Multiplexing (WDM).
WDM permits signals to be sent through a fibre optic cable at varying frequencies. Due to the wave nature of the signals they do not generally interfere with the propagation of each other, further techniques exist for the separation of waves of varying frequencies. This allows signals of such type to be sent through a single fibre simultaneously, hugely increasing the capacity of the channel. As the technique and equipment for frequency separation improves, the capacity will also increase. This however can not continue indefinitely as a build up of light intensity causes non-linear effects to arise. This method in essence creates many virtual lightpaths within a single fibre.
WDM was introduced with the development of second-generation optical networks. This scheme allows one to send non-interfering pulses of different wavelengths carrying independent information through a single optical fibre simultaneously. The process also allows for all-optical ultrafast network switching.
A list of optical networking components relevant to QKD are presented below:

Optical couplers
These devices merge or split two incident light signals into one or more output light signals through fibre fusion. The proportion of coupling may be adjusted to ones specifications. The coupling constant may be wavelength dependent or independent. Such devices are used in many applications such as interferometers.

Isolators and circulators
These are unidirectional devices. Insulators have a low forward attenuation and an extremely high reverse directional attenuation. Circulators are multi-port insulators that only permit pulses from a certain input fiber to be outputted through its adjacent fiber in either a clockwise or anticlockwise direction.

Wavelength filters
Wavelength filters permit only a certain bandwidth of pulses to pass through the

device. The remainder of the wavelengths are outputted through an additional exit fibre. These devices are the basis of Optical Add/Drop Multiplexers (OADM).

Wavelength dependent multiplexers (WM) and demultiplexers (WD)
Multiplexers split a multi-wavelength signal traveling on a single fiber into many single wavelength signals over individual fibres. Demultiplexers are the inverse of multiplexers, thus creating a multi wavelength signal from many single wavelength signals. Such devices are used extensively in WDM.

Optical cross-connects (OXC)
Such devices demultiplex two or more input fibers into their constituent single wavelength signals, then reconstruct a multi-wavelength output signals using a combination of the decoupled single wavelength signals.

Optical add/drop multiplexers (OADM)
The addition or removal of a signal of a certain wavelength into or from a multi-wavelength signal is achieved with the use of such devices. They are a created by a sequence of multiplexers, demultiplexers, circulators and Bragg gratings [38].

Optical switches (OS)
This is an all-optical component to perform the general switching within the network.

In section 4.2.2 we propose the use WDM with the aforementioned components in the realization of passive optical networks (PON) as quantum networks.

4.2 Quantum Network Architectures

4.2.1 Classification

Quantum networks maybe divided into trusted or untrusted networks. Trusted networks utilize relays to increase spatial coverage of the network. This is implemented through nodes acting as trusted servers or through a hop-by-hop process where a series of nodes operate as relays. Such a service introduces redundant lightpaths between nodes, thus increasing the robustness against DoS attacks and decreasing the information about key distribution relations. The use of relays facilitates heterogeneous quantum channels within a network. The relays used in this type of environment are assumed to be trusted, however this has great implications on the security of the network.
Untrusted networks consist of all-optical lightpaths linking nodes solely through optical networking components. The qubits are neither amplified nor converted between varying domains. The QKD distance between nodes is limited as in the two-node QKD setup, however the network coverage may be large. The distribution limit may in fact reduce due to the insertion losses by routing components within the network. In such a system,

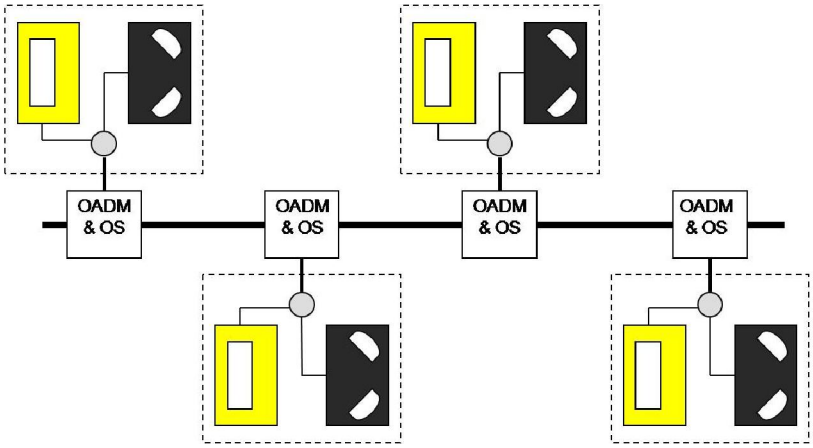

Fig. 4.1: A block diagram of a Bus network topology. Each node is connected to the backbone fibre via an OADM and an optical switch (OS). Each node is assigned wavelength as an address.

one is not required to assume security for any part of the network and is thus ideal for ultra security.

4.2.2 Different architectures and topologies

Quantum networks may be realised as a number of classical network architectures. This decstationc focuses on wavelength routed passive optical networks (WRPON). The significance of developing QNs around classical architectures is for the transparency of these backbone networks in present day communication. Quantum implementations of some of the most common classical architectures are presented in the following pages.

Bus topology

This topology implements full-duplex communication and is an example of a Quantum WRPON. Each node is a transceiver and are connected to the bus line via an OADM and circulator as shown in Figure 4.1.

Each node is assigned a specific wavelength. The OADM filters out any pulses received at the node's allocated wavelength. These pulses are directed to the detectors via a circulator. If the node would like to distribute a secure key between another node, the tunable laser is set to the specific wavelength and routed through the bus line via OADM and OS. The latter is used to ensure the photons are routed in the correct direction along the bus line.
The major advantage of such network architecture is that in is easy scalability of the

network. Adding a new user amounts to the allocation of wavelengths to the new nodes. This type of network would use minimal fiber lines and hence would be cost effective. The coverage of the network would be limited to the 'quantum limit' (≅100km) between the users of either end of the bus line. The use of nodes as trusted relays will enhance the coverage of the network. The bus topology is venerable to DoS attacks, such attacks would create two sub-networks, denying service between nodes in the different sub networks.
The use of a tunable laser and one set of detectors disallows for one node to perform independent QKD with a number of nodes simultaneously. To overcome such a bottleneck, a dedicated laser and photodetectors for each wavelength would be needed. However these would imply a lack of scalability thus increasing costs and maintenance complexity. The bus topology may be realized as a trusted or untrusted network. This architecture has been experimentally realized [52].

Ring topology

The ring topology is constructed as in the case of the bus topology with the 'ends' of the bus line linked, thus forming a ring. The hardware implementation is as that of the bus topology. The ring topology provides two routes between nodes due to the circular architecture. Thus it has better resistance to a DoS attack. A break in the ring line would render the network a bus topology. The topology allows for a wider coverage than the bus topology, although the maximum distance between two nodes without trusted relays would be in the region of the 'quantum limit'. The installation costs, maintenance complexity and QoS are all similar to that of the bus topology.

Mesh topology

In the mesh network topology the nodes are considerably inter-connected. A four node mesh topology is illustrated in Figure 4.2. Each node again consists of a tunable laser and a set of photodetectors connected via a circulator. Each node is connected to the network through a WM. An OS is placed at the interconnection of the diagonal fibers to facilitate rerouting if a fiber link is down. A mesh topology is generally used as a backbone network on which a complex classical network is built. For example, the nodes shown in Figure 4.2 may be gateways to secure LANs.
This type of network utilizes CO routing. Each lightpath is allocated a unique wavelength. In order to distribute a key between two nodes, the laser is tuned to the respective wavelength, the photons are then routed through the optical components to the receiver. The meshed architecture creates a great number of redundant lightpaths ensuring such a topology is robust to a DoS attack. However the mesh architecture results in an increase of optical components, hence increases the insertion losses of the system, reducing the spatial coverage. The meshed topology also requires many route miles of fibre-optics. This firstly accelerates the cost of installation and also reduces the

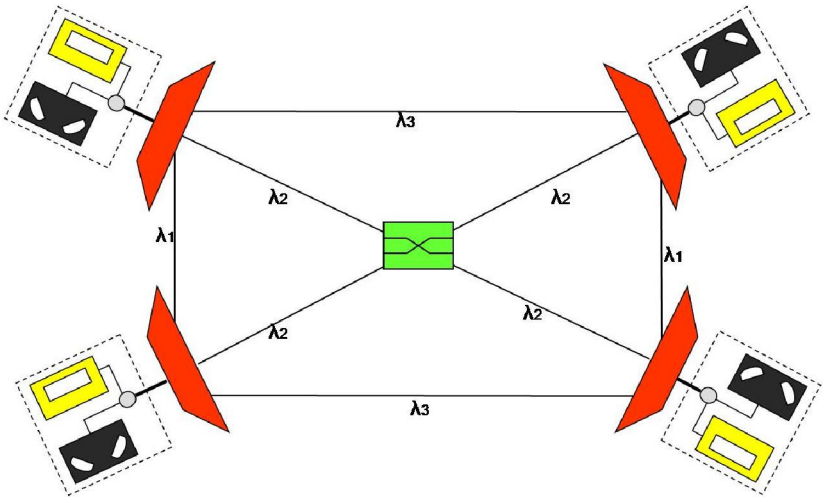

Fig. 4.2: A block diagram of a mesh network topology. In such an architecture the nodes are considerably interconnected creating many redundant light paths between nodes.

efficiency of fiber utilization.
Additional nodes may compel extra cabling and the reassignment of lightpath wavelengths. Mesh topology networks may be used as trusted networks, with the nodes acting as active relays, or as an untrusted network.

Star topology

The star topology with a trusted server is shown in Figure 4.3. This type of architecture is the simpliest quantum network to realize [53]. Its architecture implements simplex key exchange between the server and peripheral nodes and is again based on WRPON architecture. The server consists of a tunable laser while the nodes each contain a set of photodetectors. Each node is assigned a wavelength. The photons for the respective wavelengths are routed through a WM.
The two nodes that require a distribution of a secure key between them first request for a distribution of a secure key with the trusted server. The server would then, in turn, encrypt the first key with the second and send the encrypted file to the second user. The second node would decrypt the file and a secure key would be effectively distributed between the two nodes.
Such a topology is prone to DoS attacks as a node is completely isolated if the connection to the server is severed. The server, as mentioned previously, is assumed secure, as any type of mole within the server would lead to a compromise in the entire network's security.
The effective RKR in such a topology would be reduced by a factor of two. This is due to the fact that each QKD between two nodes is the resultant of two key distributions

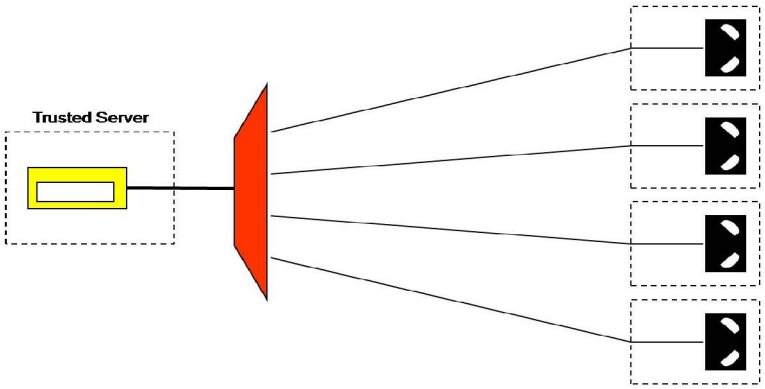

Fig. 4.3: A block diagram of the trusted star topology. All key distribution is implemented through the server. Thus the server must be assumed secure. A compromise in the server will result in a compromise in all communication.

that may not be performed simultaneously due to the tunable laser in the server. This may be overcome with the replacement of the tunable laser with DFB lasers at specific wavelengths for each user.
Such a substitution is feasible as inserting additional nodes into the network would require a hardware adaptation of the server only. Thus the addition would be transparent to all other users. Network maintenance of this architecture would be centralized to the server as all end users would contain only passive equipment. Installation costs would be less than other protocols due to fewer technologies embedded within each node.
The network coverage without additional trusted relays would encompass an area of diameter twice the quantum limit. This is because the trusted server acts as a relay between nodes.
If the server is installed with DFB lasers, continuous simultaneous QKD may be performed between the server and all nodes. The keys then stored in a secure key storage. Thus when two nodes require a secure key, the server may instantaneously encrypt and distribute the key as described above. Thus providing a means of *key-on-demand* communication.

Untrusted star topology

A star topology may also be realized without the use of a trusted server. In this case the server is replaced by an OXC and each node is assigned a wavelength. The OXC acts as a router to direct the photons to the correct nodes as per the wavelength. A schematic representation of the setup is shown in Figure 4.4.

Due to the star topology, this setup is again extremely vulnerable to DoS attacks as

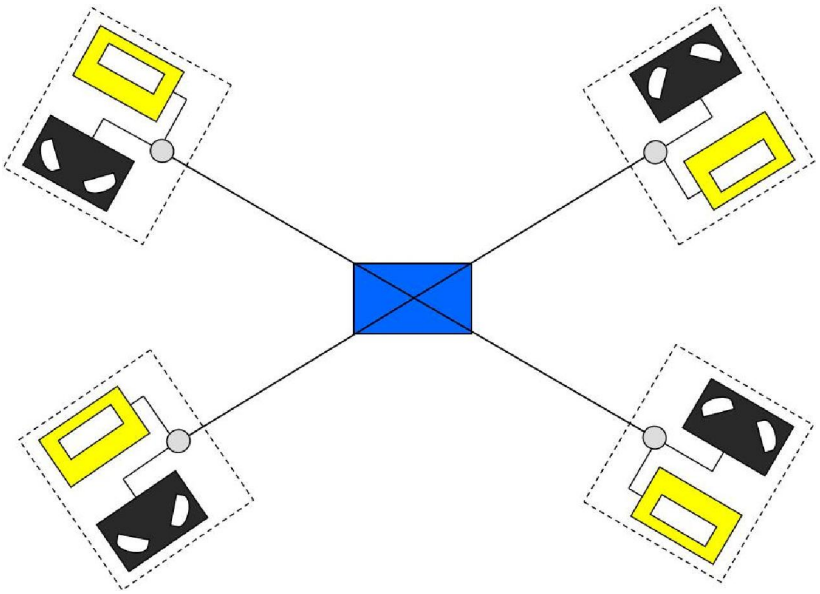

Fig. 4.4: A block diagram of a untrusted star network topology. A quantum WRPON is achieved in this architecture through optical cross-connects. Such an architecture can also be realized with optical switches and a classical control layer. However this may provide vital key relation information to the eavesdropper.

explained previously and has limited spatial coverage. The addition of a new node into the network requires a fibre connection to the OXC and a wavelength assignment to the node.

A layered QN would allow for for a classical layer to control the routing techniques through electronically controlled optical switches (MEMS). Such routing would again have to remain as CO. However this type of routing technique would expose the key distribution relations.

4.2.3 Plug & Play Architecture

While the QKD systems implementing the auto-compensating system have advantages in a 2 point QKD setup, they introduce limitations in QNs. These limitations arise as the laser and detectors are both placed in one unit (Bob) and the photons are required to return from Alice along the same lightpath as Bob sent them. Network components may not reverse polarization effects on the return trip, thus causing an error in the interferometeric readings.
These systems can only be used with a CO network due to the common lightpath required for transmission during QKD. Modifications to node hardware are specific to the implemented topology.

4.2.4 eThekwini Municipal Quantum Network

As a subsiquent development to the *Durban - Smart City* project, the eThekwini Municipality funded the Quantum Research Group (QRG) for the development of the first municipal quantum network in the world. The network will initially consist of a 3-4 node setup to form the backbone infrastructure linking the municipal switching offices to internal and other commercial customers. Two network architectures have been researched as part of the *Quantum City* project. Both the proposed networks will be implemented as trusted architectures.
The intial network hardware will consist of the Cerberis QKD solution [47] for id Quantique. This is a phase-encoded photonic Plug & Play QKD system implementing the BB84 and SARG protocols. The QRG will be adding other systems to the network in future layouts.
The primary objective of this research is to develop quantum networks to a commercially viable option and further the development of communication standards for QKD.

The first quantum network envisaged is a four-node star architecture as shown in Figure 4.5. The central node of the star topology is assumed to be safe and hence trusted.
The central node will be a municipal switching office from which the spokes of the network will link the peripheral nodes. Each peripheral node consists of a *station A* of the cerberis solution while the complementary stations are to be housed in the the server.
Network adaptability and scalability are the main advantages of this architecture. Network expansion will be transparent to all client nodes. Network maintenance will be centralized to the server node as all end users would contain mostly passive equipment.

A 3-node mesh architecture is also being researched as illustrated in Figure 4.6. This would inter-connect and secure communication links between the municipal switching stations. A mesh network creates direct links between each node with the network. Each node contains both stations of the cerberis system. A pair of optical switches facilitates the routing between the two stations.
This network may be regarded as an untrusted network as no intermediary node is required for communication between end-users under normal circumstances.

The implementation of this network is intended to be realised during the third quarter of 2008. The intention is to create a basic setup and expand the network in the future to offer its services to other interested parties in the corporate sector.
After the implementation of the quantum network and general encryption of the network traffic other pronounced applications will be investigated. The enhancement of QKD through networking techniques will also be pursued. The integration of other QKD solutions will further allow us to create standards and models for quantum communications.

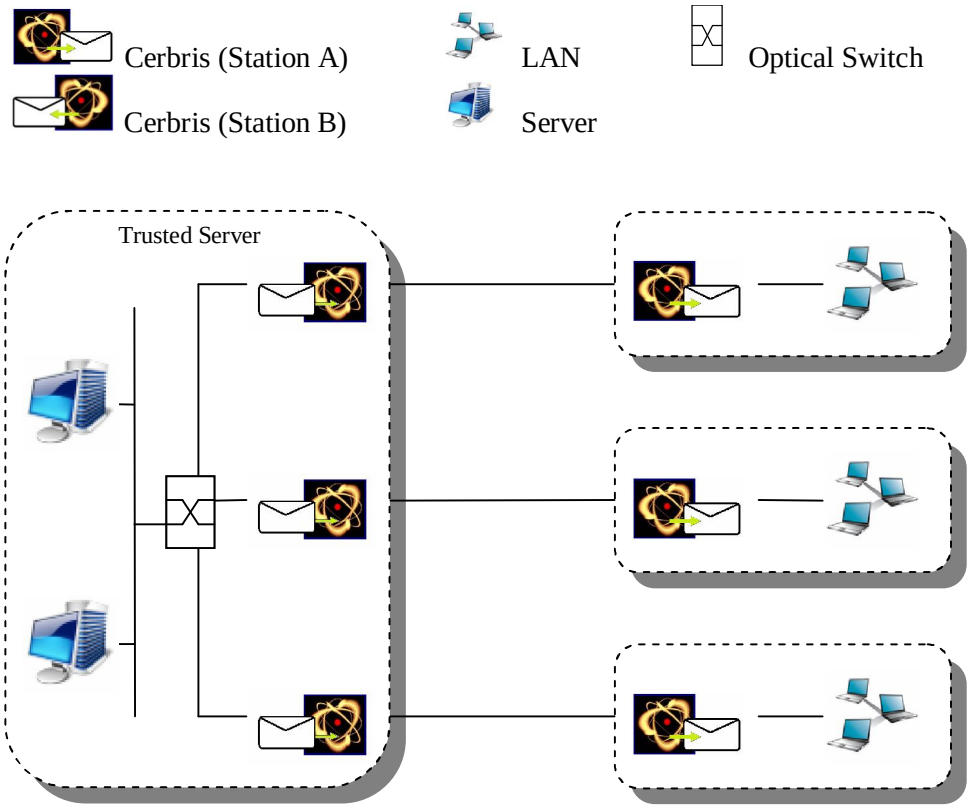

Fig. 4.5: Schematic diagram of the trusted star network topology envisaged to be implemented into the eThekwini Municipal optical network in the third quarter of 2008. The network will use the Cerberis QKD solution.

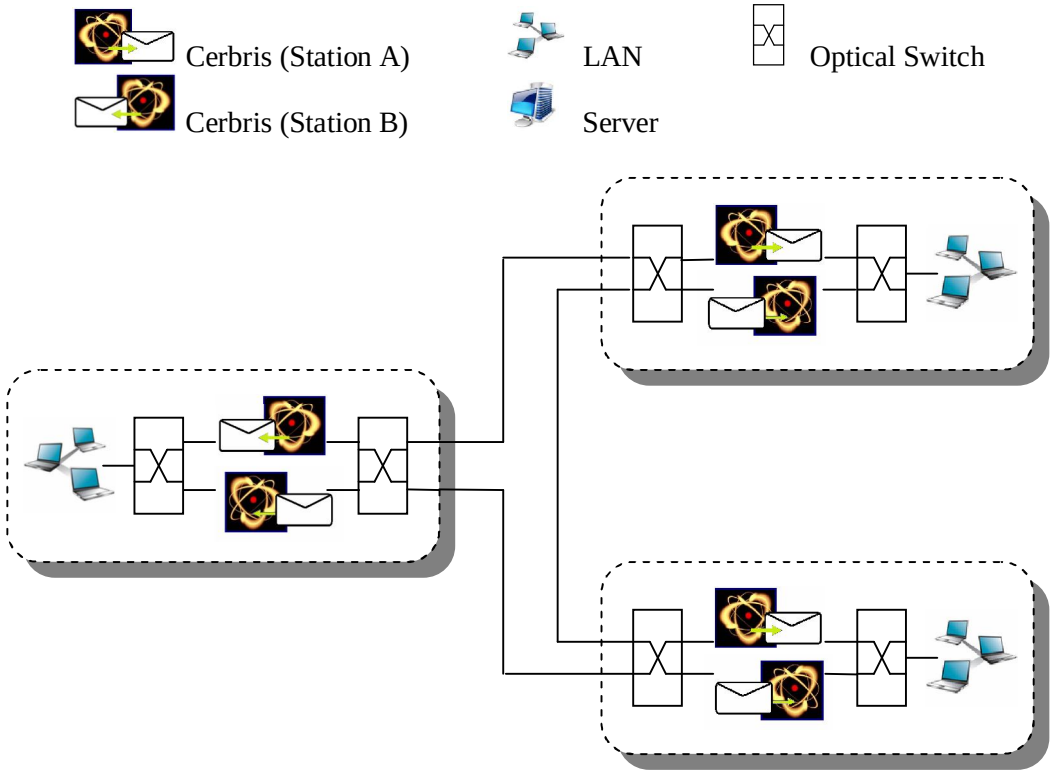

Fig. 4.6: Schematic diagram of the Mesh Network Topology.

5. INTENDED RESEARCH ON QUANTUM NETWORKS

The networking procedure outlined in the previous sections essentially facilitates network enabled QKD through a layer 3 implementation, however this still lacks some essential properties required for full commercial use. These, amongst others, include the financial viability for such implementations. In this section we present a few issues presently limiting quantum networks and enumerate on research we intend to undertake on the municipal quantum network.

As has been noted previously the quantum nature of the key distribution has intrinsic and technical limitations. Through wavelength division multiplexed quantum networks many of the obstacles are overcome. However besides the technical complications of such an implementation further research is required in the following aspects:

1. Presently dark fibre is required for all available QKD systems. This is highly inefficient. A dark fibre used solely for classical cryptography could also enhance the security considerably through numerous parallel key exchanges and a complex function to derive a final key from the raw exchanged keys, this would provide for a much higher key production rate. The optimization of fibre capacity usage in QKD is dependent on the quality of the fibre as well as the networking components. The fibre limitations are concentrated around non-linear effects occurring through a buildup of component waves within the fibre. These effects are limited in QKD as an accumulation of single photon pulses in every frequency of the ITU grid will not create an intensity that will pass the threshold required for the creation of non-linear effects. The insertion loss due to WMD equipment does however play a significant role in limiting the number of concurrent QKD signals in a particular fibre. The first and more obvious reasoning for this is the increased attenuation resulting in a shorter spacial coverage. Further WDM devices have a finite crosstalk suppression and hence leakage may occur between channels creating false detections and increasing QBER. This problem is enhanced if a common fibre is used for both quantum and classical communications.

2. PONs are the center of current research in the realization of quantum networks as discussed earlier. This method however does not efficiently utilize the potential throughput of the network. An actively routed quantum network could be realized through an array of optical switches or crossconnects interconnecting the quantum layer of the network overlayed by a classical control network to facilitate

Multi-Protocol Label Switching. This, coupled with the aforementioned could potentially create commercially feasible quantum networks for the medium to large enterprize sector.

3. The quantum networks present today rely on trusted nodes to for the enhancement of spatial coverage. This however creates additional security vulnerabilities. Some theoretical solutions to this problem have been investigated with entanglement-based QKD and Quantum Percolation Theory [50]. In essence the proposals state that if the nodes of a network are sufficiently linked through entangled pairs, entanglement can be extended between any two nodes through unitary operations [50]. This however posses great technological challenges and has not as yet been realized.

4. A secure key management layer is also required to overlay the quantum layer [54]. This layer will be used for increasing key distribution rates is through classical postprocessing. After a secure key has been distributed through a quantum backbone network, the keys are passed onto an overlaying classical network layer.
This network layer expands, manages and stores primary distributed keys through other quantum phenomena. This has the potential of producing key distribution rates comparable with classical key distribution. Presently some QKD solutions, such as the Cerberis solution [47], has partially implemented this layer. The key expansion and management is conducted through classical means such as the AES expansion. This however produces computationally secure keys.

We intend to pursue many of the aforementioned through the eThekwini Municipal Quantum Network. Quantum networks based on percolation theory require entanglement based QKD and is hence beyond the scope of the presently implemented network.

6. SUMMARY AND CONCLUSION

Quantum cryptography has developed an entire field of research around itself merging together quantum mechanics and information theory to form Quantum Information Science. Its development has further been propelled by the rapid enhancement of quantum optics and fibre optic technology.

Present technological challenges mainly revolve around detection efficiencies and fibre attenuation. These factors limit the rate and distance of quantum key distribution. The recent interest into the deployment of quantum networks have been to address factors that are hindering the mass commercialization of quantum cryptography.

This thesis has presented a brief outline of classical cryptography and an introduction to quantum cryptography. It has also expounded on present day quantum cryptographic systems, some improvements to quantum cryptographic protocols, possible architectures for Quantum Passive Optical Networks and intended research into the commercially feasible quantum networks.

Classical cryptography, due to its deterministic nature and dependency on assumed complexity, renders it at most computationally secure. Technologically independent secure communication may be realized through quantum cryptography. The security of this cryptosystem lies in the physical properties of the quantum information carriers.

Some commercially produced quantum cryptographic solutions are available presently. These, although offering future-proof secure key distribution, fall short of the data capacity requirements of present data communication and standards. To fulfill such requirements both the quantum protocols and the physical implementation needs improvements.

Most Quantum Key Distribution (QKD) protocols have a relatively low sifting efficiency, hence many successfully distributed qubits are left unused. The enhanced BB84 protocol proposed in this thesis is a minimally computer intensive, post-distribution algorithm that permits the recycling of qubits to enhance the efficiency of the original protocol. The key advantage of such a system is that no physical alterations are required to the system. Further any implementation of the BB84 protocol can be enhanced in the manner described.

It is shown that through an IKE algorithm and a modified interpretation of the BB84 setup, the sifting efficiency is increased by 40% from the standard BB84 protocol. In general the recycling of unwanted qubits through various analytical means will permit highly efficient QKD algorithms with relatively simple setups.

Quantum networks are the second-generation quantum cryptographic solutions. These

provide further Quality of Service to the end-users by enhancing the distribution process and increasing the efficiency of the infrastructure usage thus lowering the implementation cost of QKD.
Simple Wavelength Routed Passive Optical Networks as a first order implementation of quantum networks. However multi layered quantum networks with quantum communication standards are required to be appended to their classical counterparts to facilitate practical quantum cryptography.

7. APPENDICES

7.1 Appendix A - List of Abbreviations

Acronym	**Abbreviation**
AES	Advanced Encryption Standard
ATM	Automated Teller Machine
CL	Connectionless
CO	Connection orientated
DFB	Distributed Feedback
DoS	Denial of Service
IKE	Iterative Key Exchange
ITU	International Telecommunication Union
MAN	Municipal Area Network
MEMS	Micro-Electro-Mechanical Systems
MPLS	Multi Protocol Label Switching
MQT	Minimal Qubit Tomography
OADM	Optical Add/Drop Multiplexers
QRG	Quantum Research Group
OSI	Open System Interconnection
OTP	One Time Pad
OXC	Optical Crossconnect
PMD	Polarization Mode Dispersion
PON	Passive Optical Network
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QN	Quantum Networks
QoS	Quality of Service
QPON	Quantum Passive Optical Network
QRNG	Quantum Random Number Generator
QS-A	Quantum Station Alice
QS-B	Quantum Station Bob
RKR	Raw Key Rate
WD	Wavelength Division Demultiplexers
WDM	Wavelength Division Multiplexing
WM	Wavelength Division Multiplexers
WRPON	Wavelength Routed Passive Optical Network

8. ACKNOWLEDGEMENTS

I thank Professor Francesco Petruccione for his immense support during this project. I also thank the **National Research Foundation**, **Innovation Fund** and **eThekwini Municipality** for providing financial support in this project.

BIBLIOGRAPHY

[1] "Transmission bands of optical fibre." [Online] www.kingfisher.com.au.

[2] A. Konheim, *Cryptography: A Primer*. John Wiley & Sons Inc, 1981.

[3] D. Kahn, *The Code-breakers*. Macmillian Pub. Co., 1967.

[4] B. Schneier, *Applied Cryptography*. John Wiley & Sons, 2007.

[5] N. Ferguson and B. Schneier, *Practical Cryptography*. John Wiley & Sons Inc, 2003.

[6] M. J. Fischer, "Cryptography and computer security." Yale University, 2006.

[7] R. Blahut, *Principles and Practice of Information Theory*. Addison-Wesley, 1987.

[8] G. Marsaglia, "Diehard tests." [Online] http://www.stat.fsu.edu/pub/diehard.

[9] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[10] M. Nielsen, *Quantum Computation and Quantum Information*. Cambridge University Press, 2004.

[11] W. Shay, *Understanding Communications and Networks*. Thomson, 2004.

[12] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaing digital signatures and public-key cryptosystems," *The Communications of the ACM*, vol. 21, pp. 120–126, 1977.

[13] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J.SCI.STATIST.COMPUT.*, vol. 26, p. 1484, 1997.

[14] L. Vandersypen, "Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature Physics*, vol. 414, pp. 883–887, 2001.

[15] M. Nielsen, "Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state," *Phys. Lett. A.*, vol. 308, pp. 2–3, 2003.

[16] S. Wiesner, "Conjugate coding," *SIGNAT News*, 1983.

[17] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," (New York), p. 175, IEEE Press, 1984.

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Review of Modern Physics*, vol. 74, p. 145, 8 March 2002.

[19] K. Krane, *Modern Physics*. John Wiley & Sons Inc, 1996.

[20] C. Bennett, "The dawn of a new era for quantum cryptography: The experimental prototype is working!," *Sigact News*, pp. 78–82, 1989.

[21] idQuantique, "Quantis." [Online] http://www.idquantique.com/products/quantis.

[22] idQuantique, "A quantum leap for cryptography." [Online] http://www.idquantique.com/products/files/clavis-white.pdf.

[23] "Toshiba qkd system." [Online] http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html.

[24] "Magiq qpn security gateway." [Online] www.magiqtech.com.

[25] G. Ribordy, "Fast and user friendly quantum key distribution," *Journal of Modern Optics*, pp. 517–531, 2000.

[26] D. Stucki, "Fast and simple one-way quantum key distribution," *quant-ph*, no. 0506097, 2006.

[27] S. Bose, "Quantum communication through unmodulated spin chain," *Quant. Phy.*, 2003.

[28] B. Jacobs and J. Franson, "Quantum cryptography in freespace," *Opt. Lett.*, vol. 21, p. 1845, 1996.

[29] C. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, pp. 656–715, 1948.

[30] B. Schumacher, "Quantumm coding," *Phys. Rev. A.*, vol. 51, p. 2738, 1995.

[31] C. Bennet, "Quantum cryptography using two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, 1992.

[32] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurther, G. Gorman, P. Tapster, and J. Rarity, "A step towards global key distribution," *Nature Physics*, vol. 3, p. 419, 2002.

[33] M. Nielson, E. Knill, and R. Laflamme, "Complete quantum teleportation using nuclear magnetic resonance," *Nature Physics*, vol. 395, pp. 52–55, 1998.

[34] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Free-space distribution of entanglement and single photons over 144 km," *Nature Physics*, vol. 3, pp. 481 – 486, 2007.

[35] C. Gobby, Z. Yuan, and A. Shields, "Quantum key distribution over 122km standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, pp. 3762–3764, 2004.

[36] R. Ramaswami and K. Sivarajan, *Optical Networks*. Morgan Kaufmann Publishers, second edition ed., 2002.

[37] J. Anandan, J. Christian, and K. Wanelik, "Geometric phases in physics," *Am. Journal of Physics*, vol. 65, p. 180, 1997.

[38] J. Hecht, *Understanding Fibre Optics*. Prentice-Hall, 2002.

[39] X. Tang, L. Ma, A. Mink, A. Nakassis, B. Hershman, J. Bienfang, R. Boisvert, C. Clark, and C. Williams, "High speed fiber-based quantum key distribution using polarization encoding," *Proc. of SPIE*, vol. 5893, 2005.

[40] H. Zbinden, "Plug and play systems for quantum cryptography," *Applied Physics Letters*, pp. 793–795, 1997.

[41] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug and play system," *New Journal of Physics*, vol. 4, pp. 1–41, 2002.

[42] K. Zetie, S. Adams, and R. Tocknell, "How does a mach-zehder interferometer work?," *Phys. Educ.*, vol. 35, 2000.

[43] X. Ma, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, pp. 230–235, 2005.

[44] "Diehard random tests." [Online] www.stat.fsu.edu/pub/diehard/cdrom/source/tests.txt.

[45] J. Rehácek, B.-G. Englert, and D. Kaszlikowski, "Minimal qubit tomography," *Physical Review A*, vol. 70, no. 052321, 2004.

[46] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, and J. Anders, "Highly efficient quantum key distribution with minimal state tomography," *quant-ph*, no. 0412075, 2006.

[47] id Quantique, "Cerberis." [Online] www.idquantique.com/products/files/Cerbiris-specs.pdf.

[48] C. Elliott, "Building the quantum network," *New Journal of Physics*, vol. 4, no. 46.1, 2002.

[49] C. Elliott, "The darpa quantum network," *quant-ph*, no. 0412029v1, 2004.

[50] A. Acín, I. Cirac, and M. Lewenstein, "Entanglement perocolation in quantum networks," *Nature Physics*, vol. 3, pp. 256–259, 2007.

[51] A. Tanenbaum, *Computer Networks*. Prentice-Hall Inc., fourth edition ed., 2003.

[52] P. Kumarvor, A. Beal, E. Donkor, and B. Wang, "Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture," *Journal of Lightwave Technology*, vol. 24, no. 8, pp. 3103–3106, 2006.

[53] W. Chen, Z. Han, T. Zhang, H. Wen, Z. Yin, F. Xu, Q. Wu, L. Yun, Y. Zhang, X. Mo, Y. Gui, G. Wei, and G. Guo, "Field experimental "star type" metropolitan quantum key distribution network," *quant-ph*, no. 0708.3546, 2007.

[54] R. Alleaume, F. Roueff, O. Maurhart, and N. Lutkenhaus, "Architecture, security and topology of a global qkd network," *LOES Summer Topical Meetings*, 2006.