Optimizing Quantum Communication through Hybrid Technology

Abdul R Mirza

22 November 2012

To baby Safiya

who brought us eternal joy during her short stay with us.

Submitted in fulfillment of the academic requirements for the PhD degree at the School of Chemistry and Physics, Westville Campus, University of KwaZulu-Natal.

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

Name: Francesco Petruccione

Signed:

Date: 30 November 2012

ABSTRACT

Quantum Key Distribution (QKD) is a symmetric key sharing protocol. The theoretical process exploits the principles of quantum physics to underpin a physical security against any form of eavesdropping. QKD not only ensures an information theoretically secure key exchange but also provides an active *real-time* means of intrusion detection at a physical level. QKD is therefore considered the encryption technology for the next generation of nano-technology powered ICT solutions.

The fundamental science at the basis of QKD has been researched and developed into workable solutions with the current focus on the engineering of *quantum technology enabled* products. The feasibility of integrating QKD systems into conventional communication solutions remains an active field of research. The implementation of QKD across a conventional communication network requires high levels of resources in terms of the network's reliability, transparency, delay and bandwidth. This limits the maintainable Quality of Service of the network. Investigations towards overcoming these constraints will promote the uptake of QKD as a mainstream technology.

There are two classes of technology that focus on the integration of QKD into conventional architecture. The first, and most immediate, development is the adaptation of conventional systems to handle the additional requirements of quantum technology enabled products. In the case of communication networks, *all-optical* solutions provide the ideal platform for this expansion. This ensures that the quantum data carriers remain in the quantum regime and are manipulated by only the authenticated end users or trusted nodes. The second, quantum technology enabled products, render techniques to manipulate quantum information in an untrusted environment within the network. This involves the development of quantum memories, repeaters and data collision control. The combination of both these classes as a hybrid solution will ensure an optimal Quality of Service for quantum communication networks.

The long-term reasearch into quantum networking solutions is presented as the QuantumCity project. The project investigated the long-term stability of a quantum communication network within a live environment. The network is implemented through the adaptation of conventional switched networks. It has provided positive results with various future opportunities available to expand this initiative.

The successful operation of the overall solution is of course dependent of the efficiency of the QKD systems themselves. While the European Telecommunication Standards Institute (ETSI) currently drives the standardisation (ETSI ISG-QKD) of QKD, there is a need for the development of supporting technologies. This thesis aims to understand the current gaps in QKD systems and touch on various technologies that will be essential towards the development of a hybrid QKD solution. This will allow the integration of various established QKD technologies in order to optimally utilise conventional communications networks. The technologies focused on include true random number generators, polarisation-encoded QKD in fibre systems and polarisation tracking in free space units. A study and implementation of each technology is presented in this thesis.

PREFACE

The work described in this PhD thesis was carried out at the School of Chemistry and Physics, University of KwaZulu-Natal, Westville Campus, from the period commencing February 2009 to November 2012, under the supervision of Professor Francesco Petruccione.

These studies represent original work by the author and have not otherwise been submitted by the author 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.

DECLARATION

I Abdul Rahim Mirza declare that

(i) The research reported in this dissertation, except where otherwise indicated, is my original work.

(ii) This dissertation has not been submitted for any degree or examination at any other university.

(iii) This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

  a) their words have been re-written but the general information attributed to them has been referenced;

  b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

(vi) This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the References sections.

Name: _____

Signed: _____

DETAILS OF CONTRIBUTION TO PUBLICATIONS

Publication 1 - Published:

Abdul Mirza and Francesco Petruccione, *Realizing long-term quantum cryptography*, Journal of the Optical Society of America B, Vol. 27, Issue 6, pp. A185-A188 (2010).
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 2 - Published:

Abdul Mirza and Francesco Petruccione, *Quantum-secured Communication*, Quest Science, Vol. 6, Issue 2 (2010): p. 50-53.
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 3 - Published:

Abdul Mirza and Francesco Petruccione, Gaby Lenhart and Gregoiré Ribordy, *Quantum Key Distribution - A World First for Durban*, Quantum Journal, 2010 **10**(5): p. 11-12.
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.
Gaby Lenhart edited the publication.
Gregoiré Ribordy edited the publication.

Publication 4 - Published:

Abdul Mirza and Francesco Petruccione, *QuantumCity gets QuantumStadium*, Physics Comment, Vol. 2 Iss. 2 (2010): p. 2-3.
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 5 - Published:

Abdul Mirza and Francesco Petruccione, *Recent Findings from the Quantum Network in Durban*. In *AIP Conference Proceedings QCMC 2010*, T. Ralph and P.K. Lam, Editors. 2010, American Institute of Physics: Brisbane, Australia. **1362**, p. 35-38.
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 6 - Published:

Sharmini Pillay, Abdul Mirza and Francesco Petruccione, *Polarisation encoded quantum key distribution in fibre*, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria, 2011), pp. 426 - 431. ISBN: 978-1-86888-688-3. Available online at http:\\www.saip.org.za
Sharmini Pillay was the principal researcher, conducted the experimental work and authored the paper.
Abdul Mirza was a co-researcher and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 7 - Published:

Marco Mariola, Abdul Mirza and Francesco Petruccione, *Quantum Cryptography for Satellite Communication*, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria, 2011), pp. 403 - 408. ISBN: 978-1-86888-688-3. Available online at http:\\www.saip.org.za
Marco Mariola was the principal researcher, conducted the experimental work and authored the paper.
Abdul Mirza was a co-researcher and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 8 – In Press:

Abdul Mirza and Francesco Petruccione. *Quantum Technology: A next generation solution for secure communication*. In *Military Information and Communication Symposium of South Africa 2011*. 2011. Pretoria, South Africa.
Available online from: http://micssa.co.za/1.%20Papers%20-%20Day%201%2019%20July%202011/1-02B-3%20MICSSA%20Abdul%20Mirza%20paper.PDF
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 9 – Published:

Abdul Mirza and Francesco Petruccione, *Industrial application for global quantum communication*, In AIP Conference Proceedings, Quantum Africa 2010. Ed. E. Bruning, T. Konrad, F. Petruccione, Vol. 1469, pp. 58-62 (2012).
Abdul Mirza was the principal researcher, conducted the fieldwork and authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 10 – Submitted:

Sharmini Pillay, Abdul Mirza, Timothy B Gibbon and Francesco Petruccione. *Compensating Birefringence Effects in Optical Fibre for Polarisation Encoded QKD.* In Proceedings of SAIP2012, the 57th Annual Conference of the South African Institute of Physics (2012).
Sharmini Pillay was the principal researcher, conducted the experimental work and authored the paper.
Abdul Mirza was a co-researcher and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 11 – Submitted:

Makhamisa Senekane, Abdul Mirza, Mhlambululi Mafu and Francesco Petruccione. *Realization of B92 QKD protocol using id3100 Clavis2 system*. In Proceedings of SAIP2012, the 57th Annual Conference of the South African Institute of Physics (2012).
Makhamisa Senekane was the principal researcher, conducted the experimental work and authored the paper.
Abdul Mirza was a co-researcher and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 12 – In Preparation:

Marco Mariola, Abdul Mirza and Francesco Petruccione. *Influence of the motion of aerospace systems on the polarization angle of qubits for free space QKD*.
Marco Mariola was the principal researcher.
Abdul Mirza is the co-researcher.
Francesco Petruccione supervised the research.

Presentations

The follow is a list of presentations given during the period of this research.

1. Towards Quantum-secured communication, 54th Annual Conference of the South African Institute of Physics, Durban, 2009 (Talk)
2. Quantum Technology, National Science Week, Durban, South Africa, 2009 (Talk)
3. Quantum Technology, NICLE Entrepreneurial Business Workshop, Durban, South Africa, 2009 (Talk)
4. Progress Report on the Durban QuantumCity Project, Quantumcomm, Naples, Italy, 2009 (Poster)

5. QKD in Practice, IDQ Workshop on Practical QKD, Les Diablerets, Switzerland, 2010 (Talk)
6. Centre for Quantum Technology, IST Africa Conference and Expo, Durban, South Africa, 2010 (Exhibition Stand)
7. QuantumStadium, WCIT, Amsterdam, The Netherlands, 2010 (Exhibition Stand)
8. Quantum Cryptography – In Principle and Practice, ISG Durban, Durban, South Africa, 2010 (Talk – Invited)
9. Finding from the recent quantum cryptography applications in Durban, QCMC, Queensland, Australia, 2010 (Poster)
10. Quantum Technology, National Science Week, Durban, South Africa, 2010 (Talk)
11. South Africa has talent, Eskom Science Expo, Port Shepstone, South Africa, 2010 (Guest Speaker)
12. The QuantumStadium - A World First for Durban, QuantumAfrica 2010, Umhlanga, South Africa, 2010 (Talk)
13. Recent Developments in Quantum Secured Communication in Durban, SAIP, Pretoria, 2010 (Talk)
14. Recent Finding from the QKD Applications in Durban, UQCC, Tokyo, Japan, 2010 (Poster)
15. Industrial Application for a Global Quantum Communication Network, SAIP, Pretoria, 2011 (Talk)
16. A Next Generation Solution for Secure Communication, Military Information and Communications Symposium of South Africa (MICSSA), Pretoria, 2011 (Talk)
17. Recent Finding in QKD at UKZN, Quantum Africa 2, Drakensberg, South Africa, 2012 (Talk)

Name: _____

Signed: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADC Analog-digital converters

APD Avalanche Photodiodes

CQT Centre for Quantum Technology

DFB Distributed Feedback

ETSI European Telecommunication Standards Institute

GAN Global Area Network

HWP Half Wave Plate

ICT Information and Communication Technology

JOC Joint Operations Centre

LAN Local Area Network

LEO Low Earth Orbiting

MAN Metropolitan Area Network

OAM Orbital Angular Momentum

OLT Optical Line Terminal

ONU Optical Network Units

OSI Open System Interconnection

OTP One Time Pad

PMD Polarisation Mode Dispersion

QBB Quantum Backbone

QBER Quantum Bit Error Rate

QIPC Quantum Information Processing and Communication

QKD Quantum Key Distribution

QoS Quality of Service

RKR Raw Key Rate

RNG Random Number Generator

SKR Secure Key Rate

SoP State of Polarization

SPD Single Photon Detector

VOC Venue Operations Centre

WAN Wide Area Network

ACKNOWLEDGEMENTS

This work is based upon the research supported by the South African Research Chair Initiative of the Department of Science and Technology and the National Research Foundation.

I thank all those that have assisted in making this research possible, in particular the eThekwini Municipality for funding a major portion of the research into the QuantumCity initiative. I further thank the National Research Foundation, Innovation Fund, Technology Innovation Agency and the UKZN Innovation Company for the various other funding during the course of this research.

I acknowledge the work of Sharmini Pillay who has been the principal researcher in the development of the Polarisation-encoded, fibre-based QKD system presented in Section 3.1.

I acknowledge the work of Marco Mariola who has been the principal researcher in the development of the Polarisation tracking presented in Section 3.2.1.

Finally, I thank my supervisor, Professor Francesco Petruccione, for his immense support during this project.

To my parents, Abdul Hafiz and Nafisa Mirza, my siblings, Mubina and Abdul Rahman, and in particular my fiancé, Aadila Turkey, I thank you for all the encouragement and continuous belief in me.

1. INTRODUCTION

"*It is a maxim of cryptology that what one man can devise, another can unravel.*"

Walter Bigelow Wriston
Risk and Other Four-Letter Words

Cryptography is the practice of techniques of obscuring information such that only authorised parties may derive intelligible data. This form of obscurity may be considered as old as communication itself. Beyond the protection of data, the study of cryptography has lead to the development of protocols in information integrity, privacy and secrecy [1]. The converse is known as cryptanalysis [2], this is the study and practice of breaking cryptographic techniques. The ongoing tousle between cryptography and cryptanalysis provides the propulsion for improvements in information security [1].

1.1 Setting the Scene

The sender, commonly (and hence forth) known as Alice, would like to transmit a message to the receiver, commonly (and hence forth) known as Bob, with the commitment that such a transfer of information remains confidential between Alice and Bob. An eavesdropper, commonly (and hence forth) known as Eve, in particular is interested in obtaining and/or manipulating this information without consent and detection. Eve is assumed to possess unlimited and future technologies bound only by the laws of physics [3]. This scenario may be extended to access controlled storage of data, a primary function of *cloud* services today.

Alice and Bob use a set of protocols, known as a cryptosystem, to convert between the original data, the plaintext, to its obscured or encrypted form, known as ciphertext. The process by

which data is converted from plaintext to ciphertext is referred to as encryption, while the inverse protocol is known as decryption [4].

In the nineteenth century A. Kirchhoff's 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 memorise, implement and change.
- The ciphertext should be transferable by telegraph.
- The apparatus should be portable.
- The system should be user-friendly.

The above implies that cryptographic protocols are assumed to be public knowledge specifically to Eve. The uniqueness, and hence security, of the ciphertext is completely dependent on the input parameters of the algorithm, known as the cryptographic key.

The initial cryptographic methods that were developed are collectively known as *symmetric key cryptography* [5]. This form of encryption uses similar keys for both the encryption and decryption process. The evident constraint is the logistics around distributing the key securely to the intended players prior to any secure communication. Methods of key exchange and expansion have been widely developed over the many years and some applications still use this method of secure communication.

One of the first examples of cryptographic protocols is that of the Ancient Greeks' Scytale which was used to store and communicate information to army generals [6]. A long strip of writing material was coiled around a rod of particular radius at a specific angle such that there was no overlapping of the material. The key, in this case was the radius of the rod and the angle of the coil, was delivered personally to them prior to their dispatch. Subsequently *substitution ciphers* were introduced as a modular addition to the alphabets with a set value, the value/key was refreshed regularly. This method was proven flawed by Al-Khindi [4] as any intelligible plaintext possesses a character frequency signature of the language. Thus with the substitution cipher described above, one may be able to derive the plaintext through a character frequency analysis.

The most important of symmetric key cryptography protocols in terms of security is the One Time Pad (OTP) [1]. The OTP was introduced in 1926 as an extension of the substitution cipher. The modular addition is conducted for each character of the plaintext with a varied key value rather than a constant. This implies that the length of the key is equal to that of the plaintext and that each bit of the key was used only once to encrypt one bit of data [5]. In the transition to

digital media and binary logic, modular addition is replaced with a bitwise XOR of the key and plaintext.

The OTP cryptosystem is therefore characterised by the following [2]:

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

CE Shannon illustrated in his paper, *Communication Theory of Secrecy Systems* [7], that OTP was a secure method of data encryption. It was further noted in this paper that all secure cryptosystems must necessarily comply with the above criteria. Information secured with cryptosystems that comply with these conditions is not susceptible to future advancements in computational power and mathematics. A bit-wise modular addition of the plaintext, P, to a random key will result in an equally random ciphertext, C. Thus a uniform probability exists for the ciphertext to be any permutation of bits that are the length of the plaintext. The probability of deciphering the plaintext from the ciphertext, Prob(P, C), is then equal to the probability of acquiring the original plaintext directly, Prob(P) [8],

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

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 a solution to the key distribution bottleneck, cryptographers developed *public-key cryptography*, also known as *asymmetric cryptography* [5]. These cryptosystems allow for a pair of correlated keys to facilitate the cryptographic procedure. Each pair consists of a public key, used to encrypt data, and a corresponding private key, used in decryption. The computational security of such a system is based on the mathematical complexities such as one-way functions. These functions ensure computational infeasibility in deriving the private key from a given public key. Provided that one does not have access to the private key, it is guaranteed that the deciphering the plaintext will be computationally infeasible (in polynomial time) and hence the cryptanalysis will be more costly than the value of the information.

Public key cryptography is a method of secured one-way communication. The pair of public and private keys ensures the polarity of the communication while providing verification techniques for both the sender and receiver. This gives rise to digital signatures that are uniquely created by the private keys but verifiable through the public key. Public key cryptography is used extensively in the current digital age in the following aspects [4]:

- **Data integrity**
  Verification that the information was not altered during transmission. Hash functions and parity checks appropriate functionality. Truncation, inclusion or manipulation of data is prevented through such techniques.
- **Sender authentication**
  Verifies the identity of the sender. Digital certificates play a central role in this. Such authentication prevents man in the middle attacks.
- **Non-repudiation of origin**
  The trace of data flow ensures that the identity of the sender of a message is coupled with the data. This serves as an electronic receipt. Electronic 'paper trails' are rigorously used by forensics.

Quantum cryptography has provided another paradigm shift in communication security. Quantum-powered security, first proposed by S Wiesner [9] as a means of secure money, exploited the fundamental concepts of quantum mechanics to prevent the fraudulent production of bank notes. CH Bennett and G Brassard extended the concept of these mutually excusive measurements as an application to Quantum Key Distribution (QKD) for cryptographic protocols in 1984 [10]. QKD uses the fundamental properties of quantum particles as cryptographic encoding for data, thus shifting the security bases away from algorithmic procedures to physical properties. Only the laws of physics, rather than mathematical complexities then inform the security bounds.

1.2 Problem Statement

QKD has been in development since 1984 [10]. A number of milestones have been achieved through product development with a fair quality of service and limited commercial value. The developmental field may be considered as a two-pronged task: The development of robust systems and the maturity of communication techniques in terms of the Quality of Service (QoS) rendered to the end-user.

With the current uptake of ICT and the integral platform that it shares in the operations of industries, the promotion and uptake of QKD as a mainstream technology requires the integration of QKD systems into mainstream communication technology. The quantum-powered solutions available today provide point-to-point security. This implies a highly restricted QoS in particular limited spatial coverage. The final envisaged solution for quantum communication is a global network corresponding to the current conventional networks. In order to achieve global coverage the quantum communication networks require the use of various types of communication channels to optimise the QoS. A schematic of a global QKD link is presented in Figure 1.1.

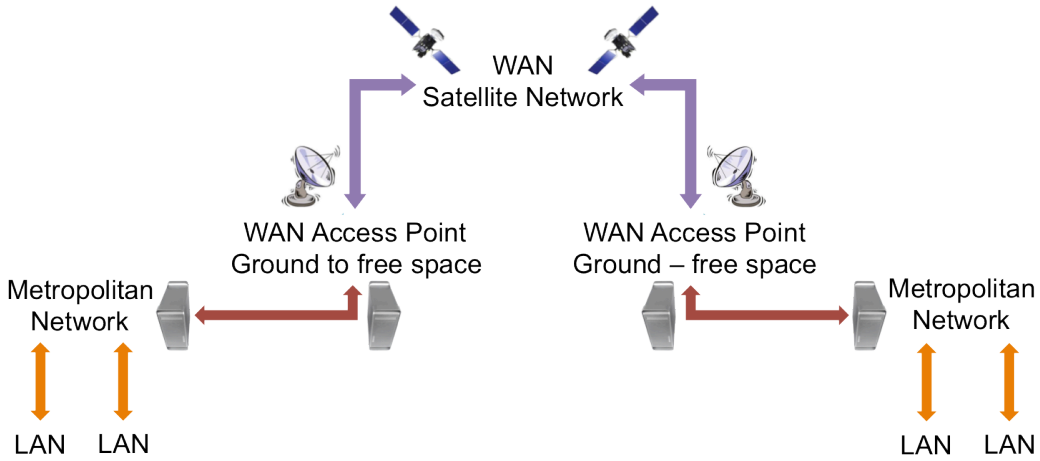

Figure 1.1: A global QKD network requires a variety of communication links suitable in terms of functionality and deployment. Each layer of the network will require a unique channel topology and specific technological advancements. A combination of trusted nodes, free-space and fibre links provide the envisaged solution. Fibre links and mainly used within a LAN and MAN while the WAN and its access points will require free space technology.

The global network will include three types of communication channels:

- Fibre channels,
- Ground (Stationary) to free-space channels,
- Motion variable free-space channels.

These channels require independent optimisation and integration techniques between themselves and the conventional networks. Such techniques currently stand as the foremost barrier to market acceptance of this system.

The European Telecommunications Standards Institute currently drives the standardisation process for QKD (ETSI ISG-QKD) [11]. The initiative aims to understand the current gaps in QKD systems and addresses the standardisation of such issues.

1.3 Motivation and Scope

Quantum Information Processing and Communication (QIPC) is an emerging technology with the potential of reshaping everyday life. The marriage of information science and quantum physics opens up new avenues that are inconceivable with conventional Information and Communication Technology (ICT) technologies. With QIPC, only the laws of physics limit the manipulation of information. Data can be characterised, quantified and processed using the basic rules of quantum mechanics. Exploiting some of the fundamental features of the quantum world, i.e. the superposition principle and the Heisenberg uncertainty relation, QIPC enables new exciting possibilities, a revolutionary new ICT paradigm that will allow us to build computers capable of solving problems that cannot be solved today.

Quantum communication is the most advanced QIPC technology. It is driven by quantum encryption or, more correctly, QKD as will be referred to in this thesis. This method of encryption differs from conventional methods in that it encodes data within quantum particles. The data is encoded within a physical parameter of a quantum particle and therefore one is required to physically measure the quantum particle in order to retrieve any data. As the measurement of a quantum particle creates a perturbation in the system, an eavesdropper will necessarily need to break the established laws of quantum mechanics to decipher the data while remaining unnoticed [10]. Many physicists have mathematically proven that QKD is completely secure even if an insecure communication channel is used. This security is further independent of the adversary's technological advantage [12]. The direct application of this technology is secure communication requiring long-term confidentiality.

Quantum-enabled systems however require numerous technological refinements to the currently deployed infrastructure to achieve complete market acceptance.

The quantum-based devices developed as components for use in QKD systems, may also service independent markets such as the medical, military and research sectors by enhancing the resolution and sensitivity of equipment. This thesis, however, concentrates on the advancement of networking techniques while elements of the system development are also considered.

The research conducted is primarily experimental. This thesis considers the current status of QKD both in terms of the QKD units and roll out of QKD network solutions. We propose various solutions and upgrades to current QKD technology as a coupled effort to find sufficient traction for the market acceptance of this technology. The focus, however, is on the long-term implementation of quantum networks in a live environment.

The formulation of the research initiatives was chosen to allow the Centre for Quantum Technology [13] to develop the in-house skills of fundamental QKD systems in parallel to the topical subjects that the global QKD community addressed. The successful adoption of this

strategy has matured the group and given it the opportunity to imprint its position within the global research community.

1.4 Contributions

This thesis is based on the investigations conducted during the four years of research. While all the fundamental work was carried out at the Centre for Quantum Technology (CQT), various experimentations were implemented within the City of Durban. The thesis subject is based around various publications and conference proceedings authored and co-authored during the course of this PhD. These papers are outlined on pages xiii-xv. The main results are collated together in the following subsections.

1.4.1 *Quantum Network Realisations*

Two major projects were implemented as part of the quantum networking aspect of QKD. The *QuantumCity project* was developed, in partnership with the eThekwini Municipality, to showcase the feasibility of quantum cryptography in a commercial environment for extended periods of time and the development of a test-bed quantum network for future experimentation. The initiative saw the deployment of a four-node quantum-secured communication network linking strategic buildings within the eThekwini Municipality. The network is deployed in the suburbs of Westville and Pinetown. It runs through the fibre infrastructure of the eThekwini Municipality. The initiative was first installed in 2008 and has been running since then. The initiative intends to expand its coverage, converting Durban from a Smart City to the first Quantum City in Africa.

The *QuantumStadium project* followed from the QuantumCity initiative, the City of Durban and the CQT again partnered together to provide unprecedented communication security to Durban's 2010 FIFA World Cup™ operations. The CQT secured the communication link between the Venue Operations Centre at the Moses Mabhida Stadium in Durban with the off-site Join Operations Centre for the eThekwini Municipality that housed the South African Police Force, Emergency Services and National Intelligence. The secure communication link was launched by the Minister of Science and Technology and ran for the duration of the 2010 FIFA World Cup™. Both the aforementioned projects encrypted all data, including telephone, internet, video, data and e-mail, through a quantum-secured link.

The Institute of Physics (UK) [14], European Telecommunications Standards Institute [15] and the Scientific American [16] have all recognised this project as a major milestone towards the market readiness of quantum information processing solutions.

1.4.2 *Hybridisation of Network Channels*

Historically QKD has been encoded via two methods: polarisation-encoding through a line-of-site free-space link [17] and phase-encoding through a fibre channel [3]. The method of encoding in either channel was dictated by the limitations around the supporting communication technology. With the advancements in the ICT, lasers and optics, other means of encoding methodologies are now possible to implement on these channels. Of prominence is encoding through Orbital Angular Momentum through free-space links [18] and polarisation encoded QKD in fibre links.

The various links of a communication network are suited for particular encoding methods and communication mediums. This can be due to the accessibility, climate, data volumes, financial implications or terrain. In order to develop the most optimal solution, networks are generally designed with multiple types of transmission channels and a standardised encoding. This removes the bottlenecks associated with the uniform deployment of networks.

In the case of an *all-optical network*, as required for successful quantum communication, the bridge between the various communication channels and mediums is required to remain transparent to the data flow. We have investigated the prospect of deploying polarisation-encoding QKD into fibre with sufficient compensation techniques. This will allow for the interchange of quantum signals between free-space and fibre channels without the need for a trusted node within the network. The apparatus that has been used in our implementation has been simplified with respect to other attempts, making it a more feasible solution.

1.4.3 *System Development*

The development of the QKD units and the key exchange process is, of course, fundamental to the realisation of a quantum-secured communication network. While some units are available, there are many systems currently under active research, both in terms of protocol development and deployment, and as an engineering solution to enhance the output of the systems.

The development of quantum-enabled Random Number Generators (RNG) is core to every implementation of QKD as well as various other gaming and security applications. We developed a quantum-enabled RNG powered with a Zener noise and the opportunity to couple to an optical random source for further enhancements. Various randomisation tests are performed to ensure the quality of the sequence and a further developmental plan is proposed.

Mobile free-space QKD units require a sophisticated tracking system in order to keep a suitable uplink. We propose and demonstrate elementary designs of orientation/birefringence compensation technique. A step motor is driven by orthogonal measurements from a reference signal to implement the compensation. This scheme will be coupled with various other tracking systems to provide a complete solution.

2. BACKGROUND

In this chapter we introduce the background theory to the research and applications that form the body of this thesis. A review of the current state of the respective technology is presented as well as a critical analysis to each.

A detailed introduction of quantum cryptography is followed by the technical specifications of the primitives required for the construction of such a system. The theory of networks is then introduced and parameters constituting the Quality of Service (QoS) are mentioned. An introduction and review of quantum networks is lastly presented.

2.1 Cryptography

Cryptography provides a means to obscure information in plain sight. While an adversary may have access to the raw data, the encoded information, the ciphertext, is unintelligible. This information security, within the data transmission itself permits communication over public, and potentially compromised, channels. The obvious advantage of such a scheme is the free flow of information.

Physically monitoring and protecting information that is in transit or being stored is cost ineffective and at most a mere deterrent to accessing the information. Once an adversary has breached the security measures, he/she will have total control over the information and its flow.

Information security assumes the adversary to have complete knowledge of the security protocols and access to the ciphertext itself. The information is therefore hashed uniquely by the parameters of the protocol, namely the key [4]. Provided the keys are managed securely, the ciphertext may safely flow through any channel without any compromise.

2.1.1 *The Need for Communication Security*

In the knowledge-based economies and the information-centric communities that preside today, the access to information provides a critical vantage point. The need for secure communication and storage of data is therefore fairly obvious. The means and level of security may vary due the secrecy of the information and the timescale to which it requires to remain confidential. A successful cryptanalysis exercise should decipher the information within its critical timeframe and using resources that are less than the value of the information itself.

The FBI's Annual Report of Cybercrime reported a doubling in the value of cybercrime between 2008 and 2009 [19]. It is interesting to note the exponential growth in cybercrime mirrors a similar growth in computing technology as predicted by Moore's Law. Further to this, in HP's *2011 Top Cyber Security Risks Report* states that 87.74 percent of applications are susceptible to insecure cryptographic storage [20].

Conventional cryptography provides only computational security. This ensures that the deciphering algorithm is infeasible (in polynomial time) with the technological and mathematical resources available. However with the growth of technological power and the advancements of mathematics, various cryptosystems have been compromised and decommissioned. A list of such cryptosystems are listed below:

- **DES:** Standardised in 1976, broken by Rocke Verser, Matt Curtin, and Justin Dolske in 1997
- **RSA 100:** Invented in 1977, broken in 1991 by Arjen Klaas Lenstra. Subsequent iterations of RSA have also shown to be vulnerable to decipherment.
- **SHA-1:** Developed 1995, broken by Wang Xiaoyun in 2005
- **AES 256:** Developed in 2001, broken by Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger as published in 2011 [21]
- **KASUMI:** Adopted as a GSM standard in 2002. It was broken by Orr Dunkelman, Nathan Keller, and Adi Shamir in 2010 [22]

2.1.2 *The Concept*

Conventional encryption is a mathematical algorithm that performs a transformative action on the plaintext resulting in a pseudo random sequence. This ciphertext is correlated to the plain text through a confidential key. The basic mathematical structure of the cryptography process is outlined below.

The alphabet of definition, $\mathcal{A}$, is the set of all characters that may be used in sending messages, both in plaintext and ciphertext. In terms of digital communication, $\mathcal{A} = \{0,1\}$. The message space, $\mathcal{M}$, is the set of characters used in a plaintext message. The ciphertext space, C, is the set

of characters used in a ciphertext message. Finally the key space, $\mathcal{K}$, is the set of all possible cipher parameters known as the key.

Mathematically the most general form of an encryption algorithm, E_e, may be denoted as

$$E_e : \mathcal{M} \mapsto C ,$$

where the key $e \in \mathcal{K}$ uniquely determines the E_e that acts upon the units m $\in \mathcal{M}$ such that

$$E_e(m) : c \in C .$$

The decryption algorithm, D_d, is given by

$$D_d : C \mapsto \mathcal{M} ,$$

where the key $d \in \mathcal{K}$ uniquely determines the D_d that acts upon the units c $\in C$ such that

$$D_d(c) : m \in \mathcal{M} .$$

A cryptosystem consists of a set of encryption transformations,

$$E_e : e \in \mathcal{K} ,$$

coupled together with the corresponding set of decryption algorithms,

$$\left\{ E_e^{-1} : e \in \mathcal{K} \right\} = \left\{ D_d \ : d \in \mathcal{K} \right\} .$$

The above implies that there is a unique one-to-one correlation between e $\in \mathcal{K}$ and d $\in \mathcal{K}$ such that $D_d = E_e^{-1}$ and $D_d\left(E_e\left(m\right)\right) = m$ for all m $\in \mathcal{M}$. The keys used for the encryption and decryption of the information can either be symmetric or asymmetric depending on the type of cryptosystem used.

A symmetric cryptosystem uses keys that are easily inferred given the corresponding key. In most cases the encryption and decryption keys are identical. The *substitution cipher* was one of the most widely used cryptosystems [1]. A single element of the key space, $h \in \mathcal{K}$, is used in modulo addition within $\mathcal{A}$. Thus the encryption algorithm is given by

$$E_h\left(m_i\right) = m_i + h\left(\mathrm{mod}\, n\right) = c_i ,$$

where n is the length of the alphabet and $i < n$. As the inverse of modular addition is the modular addition of the negative key, -h, the decryption algorithm is simply

$$D_h\left(c_i\right) = c_i - h\left(\mathrm{mod}\, n\right) = m_i .$$

As may be noted a simple brute force attack would be sufficient to run a successful cryptanalysis in time $O(n)$. A frequency analysis and further *side-channel attacks* may also be employed to resolve the key and the plaintext. Various other mathematical and computational exploits are used in cryptanalysis for the more complex symmetric cryptosystems (e.g. AES) [5]. These cryptanalysis tools are beyond the scope of this thesis.

The One Time Pad (OTP) encryption algorithm is a mere expansion of the substitution cipher where

$$E_h\left(m_i\right) = m_i + h_i\left(\mathrm{mod}\, n\right) = c_i$$

implies that the key is of the same length as the plaintext. Such cryptosystems are known as *stream ciphers*. An identical key is used in the decryption algorithm by subtracting it from the ciphertext,

$$D_h\left(c_i\right) = c_i - h_i\left(\mathrm{mod}\, n\right) = m_i .$$

If the key, *h*, is chosen randomly, then only a brute force attack may be implemented as a cryptanalysis tool. The probability of deciphering the plaintext through a brute force is $O(n^x)$, where *x* is the length of the plaintext [1].

A summary of symmetric cryptosystems is presented in Figure 2.1.

The restrictive nature of the key distribution process in symmetric cryptosystems gave rise to the concept of *public-key cryptography*, or asymmetric cryptosystems [23]. These systems exploit certain mathematical constructs such as *one-way functions* and *trapdoor functions* [2]. A one-way function allows efficient transformations in one direction, while it is computationally taxing to compute its inverse [23]. Computationally efficient is construed as computable in polynomial time while inefficient computations increase with exponential growth.

In an asymmetric cryptosystem, two correlated keys are created. The first is a public key, used only for encryption, the second is a private key used to decipher the ciphertext [23]. Although correlated, the private key is derived in such a way that it in computationally infeasible (with current technology) to generate it from the public key. This form of cryptography overcomes the key exchange bottleneck by making public the encryption key. However the deciphering key remains a secret with Bob. One such key exchange protocol is the Diffie-Hellman key exchange protocol [24]. Although useful in many aspects of current communication, these systems have not been proven unconditionally secure.

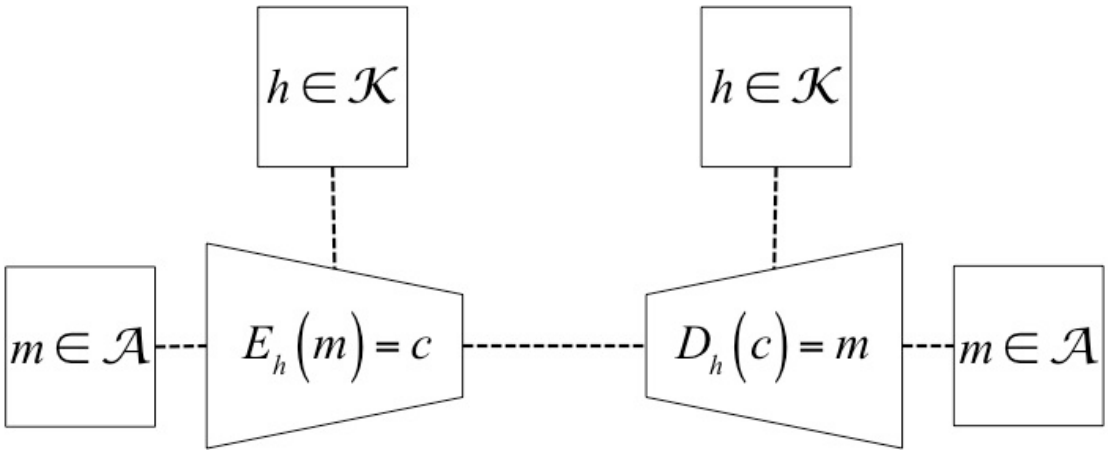

Figure 2.1: A unique set of transformations from the set of algorithms in the cryptosystem by mean of the key, *h*. This key is required to be possessed or inferable by the recipient. The plaintext, *m*, is encrypted into ciphertext, *c*, at the point of entry of the public channel. Decryption occurs at the exit point of the channel. A computationally secure cryptosystem will ensure that it is infeasible (in polynomial time) to apply a successful cryptanalysis without the key.

2.2 *Quantum Physics*

Quantum mechanics deals with the physical phenomena that occur to systems that exist in the scale of Planck's constant [25]. Quantum physical theory departs from the classical Newtonian understanding of physics through the quantisation of classically continuous variables such as motion and energy.

The *Hilbert space* is a multi-dimensional space that can map the interactions of the quantised systems to their respective quantum mechanical environments. This provides a platform for the evolution of the systems and the measurement of observables of the quantum systems. Quantum mechanics accounts for various phenomena due to the quantised nature of the systems. These principles are discussed in the next sub sections.

2.2.1 *Basic Concepts*

Duality

The principle of duality occurs with quantum systems allowing them to demonstrate both particle-like and wave-like properties [26]. Neither the classical particle understanding nor the classical wave understanding fully explains the evolution of quantum particles. Energy carrying waves may act as a stream of quantised energy packets while particles, such as electrons, may exhibit the properties of waves if unobserved. The evolution of the quantum systems is bound by the Schrödinger equation. A prime example of the duality of quantum particles is

demonstrated in the famous double slit experiment [27]. QKD exploits the duality principle allowing the quantum state to evolve in its wave-nature through its preparation, transmission and decoding, while the particle-nature of the system permits the creation and detection.

Superposition

Superposition is a wave-like property [26]. As a quantum system evolves with time, it has the ability to be in all its valid theoretical states with a certain probability. The sum of these probabilities is unitary. Mathematically it is represented by the solutions to the Schrödinger equation [28]. The solutions to the Schrödinger equation are linear and therefore any linear combination is again a solution. Choosing the Eigen states as the basis set for the solutions implies that there is no overlap in the expectations of the each observable state. Upon measurement, however, the superposition of the quantum system from all possible solutions collapses into one observable with its respective expectation values. The superposition principle is at the core of some security proofs of QKD [12]. Upon measurement, Eve creates superposition states causing perturbations within the key stream.

Uncertainty

The uncertainty principle arises due to the intrinsic quantisation of nature [29]. The simultaneous measurements of conjugate parameters of a quantum system instill an uncertainty in the measurements. Measurements are limited in precision in the order of Planck's constant, h. The de Broglie hypothesis states that every particle in this universe may be construed as a wave. Thus, using the wave properties of nature, one may derive the corresponding observables and their respective uncertainties. The superposition of various possible states increases the accuracy of one observable while inducing uncertainties in other properties. Together with the principle of superposition, the uncertainty principle provides the security basis for QKD [30].

Entanglement

When two quantum particles physically interact with each other or produce indistinguishable pairs of particles, there exists a correlation between such particles at a future time even when they are spatially separated [25]. One of the most common methods of producing entangled pairs is through the process of parametric down conversion. With the correct setup to overlap the emission rings and aligned catchment-points, one is able to create indistinguishable photon pairs entangled in polarisation. The shared state remains ambiguous until the measurement of one of the particles from the entangled pair, upon which the state of the corresponding particle is known with certainty even without measurement. Entanglement-based QKD allows for a powerful new standard of device-independent QKD. This implies that the source of quantum particles need not be trusted as a series of tests establish the quality of entanglement, and hence the security of the communication, by the receiving parties [25].

Bell's Theorems

The theorem addresses non-locality and realism in reference to quantum mechanics. Essentially the theorem tests for the presence of entanglement. Classical mechanics embeds local realism as it does not allow distance measurements or manipulations to effect local experiments. However, through entanglement, quantum mechanics permits the non-local realism. Through a set of Bell's inequalities [31] one is able to measure the quality of this phenomenon. These inequalities form a measure of the security for entanglement-based QKD cryptosystems.

No-cloning Theorem

The no-cloning theorem is an intuitive extension of the uncertainty principle. It states that it is impossible to reproduce an identical copy of an unknown quantum system without changing the initial system [32]. The no-cloning theorem prevents Eve from reproducing multiple copies of a quantum system and performing unambiguous measurements. Such measurements would result, with certainty, in the knowledge of conjugate properties of the system violating the uncertainty principle. Some security proofs for QKD make use of this theorem for certain attacks.

2.3 Quantum Cryptography

The fundamental shift from conventional cryptography to quantum-based information security is the move from mathematical encapsulation to physical encoding. This methodology ensures physical protection of the key bits and active detection of a breach. Only the laws of physics, and not computational limitations, bind the security proofs of quantum cryptography. This means that in all proofs the eavesdropper is assigned the upper bound of mutual information in information theoretic terms. Such proofs make QKD secure independent of any future computational advancements [12].

Quantum cryptography exploits the laws of quantum mechanics to expose eavesdropping during the key exchange process. Thus a successful QKD session will ensure secure communication over an untrusted public channel. On the contrary, if a breach is detected during the QKD process, the key generated during the session is only compromised and a new QKD session may be started.

2.3.1 *The Concept*

S Wiesner developed the idea of quantum-based security in 1970 as a means to prevent the forgery of banknotes [9]. The method incorporated a series of quantum systems into the banknotes to verify the serial numbers. The non-orthogonal bases that encoded the quantum verification code ensured that an adversary was unable to reconstruct the code with certainty. CH Bennett and G Brassard expanded the concept in 1984 as a means of symmetric key exchange [10]. Bennett and Brassard showed that QKD was an effective scheme to share symmetric keys and that it was theoretically secure [10]. This form of security analysis sets the

theoretical bounds on the mutual information between Alice and Eve independent of the implementation of the protocol.

The key distribution occurs through the encoding of key bits into the physical properties of the data carrier. In the case of digital communication, the quantum-enabled data carrier is selected to be a quantum two-level system, known as a *qubit* [28]. The qubit has two pure states $|0\rangle$ and $|1\rangle$ upon which it may evolve into any linear combination of these states,

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2$ and $|\beta|^2$ are the probability distributions of the binary states [28] and

$$|\alpha^2| + |\beta^2| = 1.$$

The basis set, $|0\rangle$ and $|1\rangle$, are orthogonal vectors spanning a 2D Hilbert Space and are collectively known as the *computational basis* [28]. As noted earlier, the qubit may evolve to any mixed state; in particular QKD exploits the use of another orthogonal set

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right),$$

where $|+\rangle$ and $|-\rangle$ are assigned the bit values 0 and 1 respectively. The states of a qubit may be represented on the Bloch sphere as in Figure 2.2.

The basic philosophy behind the security of QKD is that if the key bit value is encoded as one of the states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ then no single measurement of the qubit will be sufficient to unambiguously differentiate between all the states [25]. The encoding (bit value) of the qubit is unambiguous and deterministic if and only if the observer knows the correct basis in which the qubit was encoded. Various other QKD protocols exist that use more than four encoding states [33], however the principles of security are similar. A complete analysis of the theoretical security of QKD is beyond the scope of this thesis.

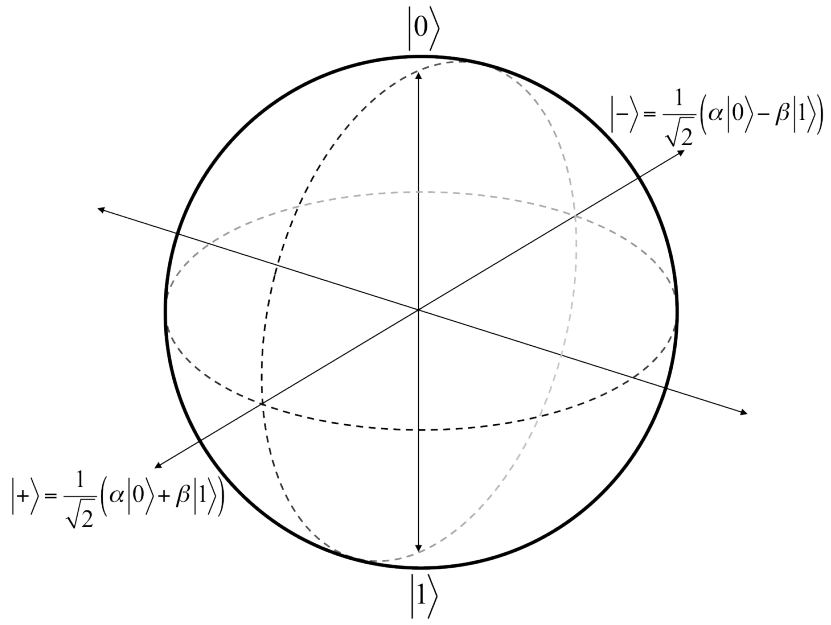

Figure 2.2: A representation of the qubit on a Bloch sphere. The qubit may take the standard values of computational basis or any linear combination of the two. This possibility of superposition of pure states is due to the quantum mechanical properties of the qubit and is significant in the security of QKD.

Most current QKD systems use the photon as an implementation of the qubit [3]. Both polarisation of a photon and the relative phase between pulses of a photon are used to encode a qubit. The polarisation encoding is outlined below.

Assume the computational basis for the state of polarisation is the orthogonal set $|\uparrow\rangle$ and $|\rightarrow\rangle$, representing vertical and horizontal polarisation of the photon respectively. The complementary basis set would then be represented as

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

and

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

These states may be realised as linearly polarised diagonal states as right and left diagonal respectively. It can be easily seen from the above that the complementary (diagonal) basis is non-orthogonal to the computational basis and is illustrated in the *Poincaré sphere* in Figure 2.3.

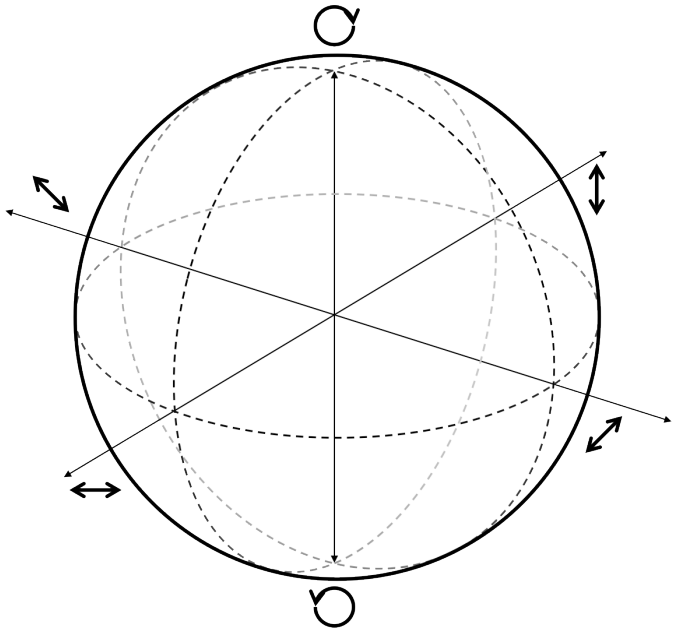

Figure 2.3: The Poincaré sphere represents the State of Polarisation (SOP) of an optical signal. The equatorial plane represents the linear polarisation states of light. Shifting away from this plane represents the presence of elliptical polarisation with pure right and left circularly polarised light at the top and bottom poles respectively.

Two main classes of QKD protocols exist. Both of these classes may be shown equivalent mathematically [12]. These classes are mentioned below:

Prepare and Measure Schemes

In this scheme, Alice is responsible for creating and distribution the qubit. Bob measures the qubits upon arrival and a series of post-distribution communication results in the determination a secret key [3].

Entanglement-based Schemes

The pair of entangled qubits are created and distributed to both Alice and Bob. The originator of the entangled pair may be Alice or any third party. The state of these qubits will be unknown to all parties involved until the measurements are made [3].

2.3.2 *The BB84 Protocol*

The BB84 protocol was the first QKD protocol to be presented [10]. It is still used today as one of the more efficient QKD protocols. The protocol was initially presented in 1984 [10] and IBM implemented this first working prototype in 1989 [17]. The scheme was initially developed as a prepare and measure protocol but was later shown to be equivalent to the Ekert's entangled-based E91 protocol [34].

The scheme was originally realised as a polarisation-encoded scheme. A brief outline of this implementation is given below.

Alice sends a stream of qubits to Bob. Each key bit is independently and randomly encoded in one of the states from the computational or complementary bases. The qubits are transmitted to Bob who measures each qubit through an unambiguous measurement for either the computational or complementary basis. The distribution of qubits and their respective measurements are summarised in Table 2.1. Upon the transfer of the qubit stream, Bob makes public his choice of bases for each qubit and Alice confirms or denies if the qubit was prepared and measured in a common basis. The qubits prepared and measured in varying bases result in ambiguous results and are therefore discarded. Collating the bit values from the qubits prepared and measured in a common basis generates a symmetric key. This process is known as *sifting*. It may easily be shown that the ambiguous measurements in Table 2.1 result in an equal probability of either basis state while deterministic results are obtained when the basis choice is common.

The sifting procedure should theoretically, in a noiseless environment, share symmetric keys between Alice and Bob. However with real implementations of the units, various deficiencies may compromise certain elements of the key. Classical *error correction* and *privacy amplification* techniques are then employed to minimise any information leaked out to third parties [3].

2.3.3 *Primitives for a QKD System*

In this section the required primitives of a practical point-to-point QKD system are introduced. These primitives are the fundamental technologies that are assembled in order to construct the complete QKD solution. Each primitive is discussed in context to the work conducted as part of this thesis.

Qubit Source

The source of qubit in the QKD system is responsible for the raw key distribution rate and the accurate creation of qubits. In the systems that are investigated in this thesis, a photonic implementation of a qubit source is used. Due to the inefficiencies in creating pure photon states, the most common implementation of a single photon source is an attenuated laser [3]. An attenuated laser however does not create pure single photons, rather a Poissonian distribution of a mean number of photons per pulse. This induces the possibility of a compromise of the system through attacks such as the *photon number splitting attack* [35]. Various decoy-state QKD protocols have also been developed to accommodate the lack of pure sources [36].

Table 2.1: In the BB84 Protocol, Alice may send four qubit states from two non-orthogonal bases. The states are assigned binary values. If a common basis is used to prepare and measure a particular qubit a deterministic result is achieved and a symmetric key is shared between the parties.

Alice		**Bob**	**Measurement**	
State	**Basis**	**Basis**	**State**	**Result**
$\|\uparrow\rangle$	+	+	$\|\uparrow\rangle$	Deterministic
$\|\rightarrow\rangle$	+	+	$\|\rightarrow\rangle$	Deterministic
$\|\nearrow\rangle$	×	+	$\|\uparrow\rangle$ or $\|\rightarrow\rangle$	Ambiguous – Discarded
$\|\nwarrow\rangle$	×	+	$\|\uparrow\rangle$ or $\|\rightarrow\rangle$	Ambiguous – Discarded
$\|\uparrow\rangle$	+	×	$\|\nearrow\rangle$ or $\|\nwarrow\rangle$	Ambiguous – Discarded
$\|\rightarrow\rangle$	+	×	$\|\nearrow\rangle$ or $\|\nwarrow\rangle$	Ambiguous – Discarded
$\|\nearrow\rangle$	×	×	$\|\nearrow\rangle$	Deterministic
$\|\nwarrow\rangle$	×	×	$\|\nwarrow\rangle$	Deterministic

Encoder

The qubit is encoded with a binary value prior to its transfer. Two main encoding methods exist for photonic qubits; polarisation and relative phase [3]. The polarisation encoding is achieved by applying standard polarisers to the emerging photons. The orientation of the polariser is adjusted according to the selected state as mentioned Table 2.1. An interferometric setup is used to realise encoding through the relative phase of the photon. In this setup, an asymmetric *Mach-Zehnder interferometer* [37] is used to create a superposition in time of the photon. Thus the photon is released as a superposition of two pulses in differing time buckets. In addition to this, one pulse is given an additional phase shift within the interferometer as the encoded bit value. The method of encoding is selected according to the channel and required Quality of Service.

Random Number Generators

Random numbers are essential to the QKD process and any cryptosystem for that matter. If the choice of the key stream, generated by the Random Number Generator (RNG), is predictable or in any way susceptible to manipulation, the cryptosystem is vulnerable to side channel attacks. Classical RNGs produce pseudo-random sequences through algorithmic procedures. Various conventional RNG use physical information of the environment, such as keystrokes, to randomise the sequence further. However all such sequences generate the stream through

reference to the previously generated numbers and hence susceptible to partial interpretation and compromise of the system.

True random number generators use the probability of nature to construct a random sequence. As the random events in nature are independent of previous such events, a sequence produced through this means is not determinable by an adversary. True, stable and fast RNG are therefore of key interest to cryptography and other security-based applications.

Quantum Channels

The medium through which the qubits are transferred is known as the channel. It is defined as linear, completely positive, trace preserving transformation implying that [8]:

- the channel maps points as a one-to-one relationship,
- positive operators are conserved,
- the channel's transformation should preserve the normalisation of states,
- the channel is able to apply the above transformations from the input space to a space of equal or higher dimensions.

Practical quantum channels used in QKD are classified as *Noisy Memoryless* channels [38]. Memoryless channels are of integral to a QKD system and any channel with a memory would serve as a source of side-channel attacks. Noiseless channels are a theoretical concept that implies perfect communication due to their independence from environmental parameters. Practical channels have a non-trivial environment and thus require compensation techniques to any transformations due to the environment [3].

Compensation Techniques

Compensation techniques are used to offset for noise in the channel as well as the practical aspects of link optimisation. The channel's noise consists of various dispersions and environmental noises. This type of noise can cause decoherence and an increase in the error rates. Spatial, spectral and temporal filters may be used to increase the signal to noise ratio. Link optimisation includes the tracking of the counter unit in order to provide a usable link with high visibility. Tracking generally engages an active feedback loop technology to lock onto the counter unit, both in terms of position and orientation. Each implementation of a quantum channel will require a unique set of compensation techniques.

Decoder

Deciphering the qubits is the inverse operation implemented by the encoder. It measures the relevant observable of the qubit to interpret into a bit value. The decoder is conventionally located in Bob's unit. Considering the photonic implementation, this primitive will consist of polarisation deciphering equipment, such as a polarisation dependent beam splitter, to interpret polarisation-encoded qubits. To decipher the relative phase encoding, the decoder requires an identical asymmetric Mach-Zehnder interferometer with a phase shifter in one arm [3]. As the

photons in a temporal superposition pass through the interferometer a further phase shift is added one of the pulses in order to chose a measurement basis. Upon leaving the interferometer the pulses are recombined and the two pulses interfere with each other causing complete constructive of destructive interference if a common basis between Alice and Bob is chosen. This results in deterministic detector results. Phase-encoded QKD scheme is presented in Table 2.2.

Detector

Single Photon Detectors (SPD) are considered as qubit detectors due to the focus of photonic implementations in this thesis. SPDs form the most intricate unit of the QKD systems. The units are constructed as Avalanche Photodiodes (APD) and are hence very sensitive and various parameters affect the efficiency of the detectors. The low efficiency of the detectors is currently the most fundamental bottleneck in QKD [3].

The APD varies from a PIN diode in that the APD contains a multiplication region where 'loose' electron/hole pairs may be formed upon the absorption of a photon. As a large electric field is applied across the multiplication region, the free electrons induce further electron/hole pairs producing a large current. The APD is disconnected in order to reset the detector and bring it to its ground state.

2.3.4 *Effectiveness of QKD Protocols*

The parameters to assess the Quality of Service of a QKD implementation are presented below. These measure the effectiveness of the system in terms of the key generation rates.

The *Raw Key Rate* (RKR) is the ratio of the number of qubits transmitted between Alice and Bob over the number emitted by Alice. It is a measure of the quality of the overall setup, including the link. This ratio, when adapted for attenuated laser pulses, may be written in the form,

$$R_{raw} = q\mu f \eta_t \eta_d,$$

where q is the transmission efficiency of the theoretical protocol, μ is the average number of photons per pulse, f is the repetition frequency of the photon pulses, η_t is the transmission efficiency of the channel and η_d is the detector efficiency [39].

Table 2.2: The phase-encoded BB84 protocol uses an interferometric technique to encode the key values into the relative phase of a photon. If a common basis is used to prepare and measure a particular photon a constructive or destructive interference results in a deterministic reading of the detectors.

Alice		Bob		Measurement	
Basis	**State**	**Basis**	**Phase Added**	**State**	**Result**
I	0	I	0	0	Constructive Interference
I	π	I	0	π	Destructive Interference
II	$\pi/2$	I	0	$\pi/2$	Ambiguous – Discarded
II	$3\pi/2$	I	0	$3\pi/2$	Ambiguous – Discarded
I	0	II	$\pi/2$	$\pi/2$	Ambiguous – Discarded
I	π	II	$\pi/2$	$\pi/2$	Ambiguous – Discarded
II	$\pi/2$	II	$\pi/2$	0	Constructive Interference
II	$3\pi/2$	II	$\pi/2$	π	Destructive Interference

The *Quantum Bit Error Rate* (QBER) is the percentage of errors contained in the distributed key after the sifting process. It represents the quality of the distributed key and infers information regarding various primitives of the system. The QBER is denoted by [3]

$$\mathrm{QBER} = \frac{\text{False bits}}{\text{Total bits}} = \mathrm{QBER_{opt}} + \mathrm{QBER_{det}} + \mathrm{QBER_{ent}}.$$

The QBER is founded by three error sources, an imperfect optical setup ($QBER_{opt}$), dark counts of the detector ($QBER_{det}$) and inefficient entanglement sources ($QBER_{ent}$) where applicable.

The optical setup consists of equipment and fibre connections that contribute to the decoherence or misalignment of the photon. The $QBER_{opt}$ is a measure of the stability and visibility of this setup. Compensation techniques are often used to rectify this error rate.

Photo detectors are currently the greatest bottleneck in achieving faster QKD rates. The detector inefficiencies may be separated into three broad categories,

$$\mathrm{QBER_{det}} = \mathrm{QBER_{dark}} + \mathrm{QBER_{after}} + \mathrm{QBER_{stray}}.$$

The $QBER_{dark}$ is error related to the dark counts from the detector. Dark counts may occur due to a number of factors including excessive thermal noise and incorrect bias voltages. This error is measured during the active gating time of the detector, it is calculated as the ratio of the probability of dark counts to the detections.

Upon a detection and avalanche, the APD is required to be quenched in order to reset the detector to its stable state. If the detector is not sufficiently quenched after-pulsing may occur. $QBER_{after}$ is the probability of a detector to undergo an avalanche due to after pulsing per active gate.

$QBER_{stray}$ incorporates the false counts of the detector due to stray light from the channel [39]. Rayleigh backscatter is the main cause of these erroneous detections.

The effectiveness of a QKD implementation is measured against the rate of final secret key distillation between the parties,

$$R_{\text{secret}} = R_{\text{raw}}(1 - R_{ER})(1 - R_{PA}).$$

Applying Error Correction and Privacy Amplification algorithms on the sifted key achieves the secret key. The fraction of the sifted key lost due to error correction is

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

while the fraction lost during privacy amplification is [39]

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

The rate of secret key production, R_{secret}, is dependent on both the raw key rate and QBER. A reduction in the quality of the raw key implies greater losses during the sifting, error correction and privacy amplification routines.

2.3.5 *Beyond Unicast Messaging: Global QKD Networks*

Conventional QKD solutions have focused on the point-to-point setup. This is intrinsically limited to unicast messaging with a highly expensive routing table. The current solutions are therefore deployed and used for permanent unicast routes with the deployment of dedicates communication channels. As is inferred, these solutions do not address the network's modern architecture in terms of dynamic routing, multiplexing, multicasting and the overall redundancy within the network. This has a negative impact on the available QoS and limits the application of QKD to a niche market.

Although symmetric key sharing is fundamentally a unicast communication, some degree of flexibility in the key routing and management algorithms are required to overcome the spatial limitation. Conventional QKD is achievable for up to a few hundred kilometers [40, 41] while the optimal length of links for a linear network is known to be 19.7 km [42]. Thus a meshed setup of unicast links for Local Area Network (LAN) and Metropolitan Area Network (MAN) applications. Beyond this span, QKD networks will need to engage with technologies including mobile nodes and further quantum-enabled technologies.

The Figure 2.4 illustrates the sub networks of a global communications system. The conventional QKD setup provided satisfactory coverage within a metropolitan area with various quantum channels active to achieve a hybridised network. Each of these MANs are connected to a wider network through a gateway. The Wide Area Network (WAN) and Global Area Network (GAN) will distribute and manage keys through the respective technologies to ensure uninterrupted communication. Various solutions to the quantum-enabled GAN will be discussed in this thesis. A software implemented key management layer could provide the required routing and redundancy for this solution [43].

The new research focuses on WAN applications. Some preliminary experimentation and tests for the subsystems of a GAN unit is also considered.

2.4 Networking Primitives

The various layers of networking technology are designed to optimise the performance of its core applications. Networks consist of seven layers that provide a systematic stack of interfaces to allow a human user and hardware to communicate with each other and between themselves in a transparent manner. The network layers, illustrated in Figure 2.5 provide an understanding of the operational levels of quantum communication.

The Open System Interconnection (OSI) network model [44] provides a separation of duties within the structure and operation of a network. Each layer within the network provides functionality to the layer directly above it independent of the implementation. This provides a framework for the interfacing and standardisation of networking systems.

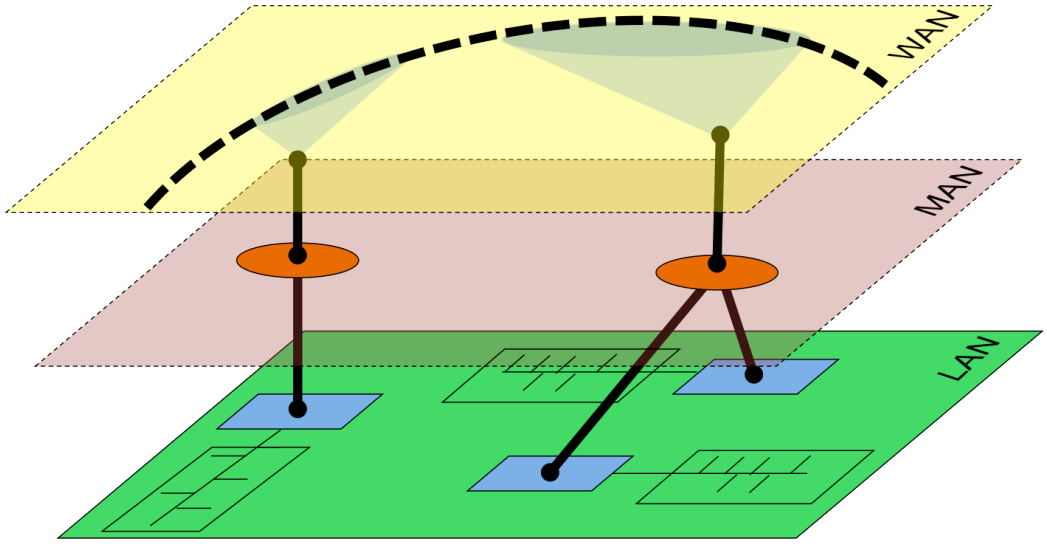

Figure 2.4: The sub networks of a Global Area Network (GAN) the bottom most layer consists of Local Area Networks (LANS) with access points to the Metropolitan Area Networks (MAN). The MANs in turn connect to a satellite network that propagates its global coverage as either a trusted node or a source of entangled qubits.

The OSI network model consists to seven network layers. The layers provide systematic functionality to connect the user's human interface to the bit stream in the network channels. The seven layers are detailed below and summarised in Figure 2.5:

- Layer 7: Application Layer
  Responsible for the user interface and the communication with external factors. It consists of common network communication protocols.
- Layer 6: Presentation Layer
  This layer reconstructs data structures in order for compatible transportation over a common network.
- Layer 5: Session Layer
  Defines and manages the protocols of communication sessions between networked nodes.
- Layer 4: Transport Layer
  Reconstructs information to create data packets for data transfer. This provides a hardware independent interface to the software layers above.
- Layer 3: Network Layer
  Controls the optimisation the routing of data through the network. The QoS of the network will determine the routing standards.

- Layer 2: Data Link Layer
  Controls the data flow within the network. It is responsible for error correction, congestion management and conflict resolution.
- Layer 1: Physical layer
  The hardware of the network constitutes this layer. Creates the physical communication channels and defines the standards for data carriers.

QKD operates at the most fundamental layer, Layer 1 of the OSI Network model while conventional encryption runs between layers 2-4 depending on the type of implementation [44]. The optimal network configuration will therefore need to be adapted to ensure the efficiency of the network.

In networking terms, a stream of data from a source to a destination is called a *flow* [44]. Two routing algorithms are standard in flow through the network. *Connectionless* or packet switching algorithms break the data stream into small packets of data, these packets are then switched independently through the network to minimise the congestion on the communication channels. In a *connection-orientated* or circuit switched network, a dedicated path with sufficient QoS is established between the end nodes prior to the data flow.

In connection-orientated networks, which must be used for quantum communication, there are four primary factors that affect the QoS:

- the reliability,
- delay,
- jitter and
- bandwidth.

Quantum communication is demanding with respect to the reliability of the accurate transfer of qubits; the sequence of arrival, ensuring minimal jitter; and the bandwidth usage within the network due to current implementations of QKD and photon isolation. Various primitives of the network can assist in optimizing the above four factors to ensure a seamless integration into a communication network.

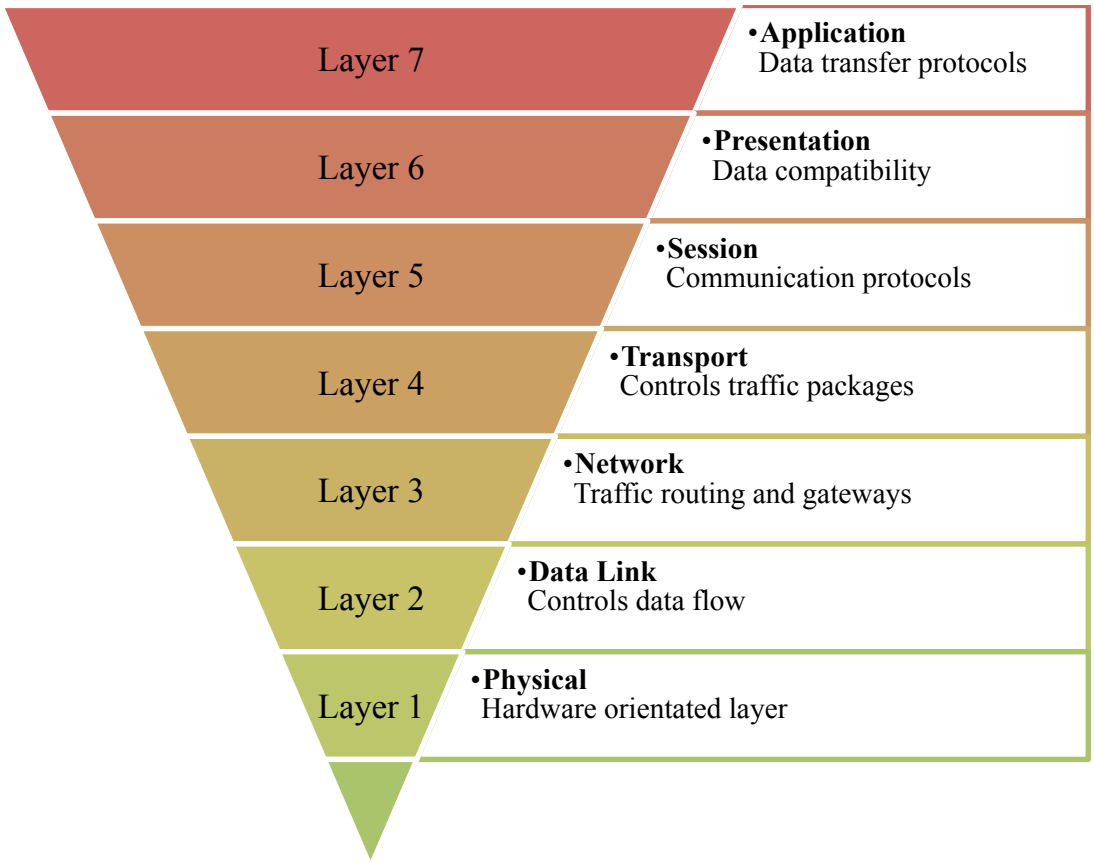

Figure 2.5: The OSI network model is a theoretical configuration of networking responsibilities. The seven layers incorporate a separation of duties in order to provide standards and interfaces for networking devices. Conventional cryptography operates in the layers 2 and 3 while QKD, being a more fundamental and a physical solution, is confined to layer 1.

2.4.1 *Transparency*

The OSI model, as mentioned previously, provides a division of responsibilities with definite and standarised interfaces between the various layers. Transparency is the harmonious integration with these interfaces to ensure the QoS and the functionality of the adjacent layers is not jeopardised. QKD is active in the layers 1 and 2 as it is a physical process. The transparency within the networking equipment and multiplexing of quantum and classical signals is essential to ensure the transparent operation of QKD.

2.4.2 *Network Coverage*

Extending the coverage of a network relies on the infrastructure used to repeat or relay the data flow and is therefore a layer 1 constraint. QKD requires a passive optical solution that is the upcoming standard in high-speed and long haul networks. It further provides a source of redundancy within a network to ensure the reliability of the signal and minimise downtime of any link. Various topologies have been investigated to ensure the integration of QKD systems into deployed infrastructure [45].

2.4.3 *Network Speed*

The speed of the data flow for QKD is limited by the current QKD technology, in particular the single photon detectors. Together with this however, the insertion losses of equipment, compensation techniques, isolation and filtering methods all contribute to lowering the transmission efficiency of the communication channel and hence the raw key rate of the QKD protocol. The jitter and delay of the data flow are affected by the speed of the network. The speed of a network, together with multiplexing, is always under constant scrutiny in order to increase throughput and hence allow a greater bandwidth. The network speed again is an infrastructural constraint to be dealt with at a layer 1 level.

2.4.4 *Key Routing*

The efficient routing of a data flow will minimise network congestion and hence improve the throughput efficiencies of a network. This of course ensures better bandwidth management and shorter latencies. An effective routing table however may be costly due to the infrastructure costs associated with passive optical networks. A completely meshed network would be most ideal as a key routing solution as it introduces maximal redundancy within the network. Various other layer 1 technologies may be introduced to couple the key routing solution to an increase in network coverage. An active routing solution through layer 2 based routing tables to control optical switches offer solutions with comparable QoS.

2.4.5 *Key Management*

In order to reduce latencies and provide a true on-demand encrypted platform, key generation, distribution and usage is to be managed effectively and securely. The implementation of such a solution requires a dedicated platform within layer 3 of the OSI model. The platform is a logic algorithm with a table of rules to ensure the optimised use of the stacked keys. Ensuring that a buffer of keys is always available at each node reduces jitter within the communication resulting in improved QoS.

2.5 Quantum Networks

QKD has traditionally been characterised by a dedicated point-to-point connection-orientated link. This type of QKD setup restricts its application to a niche market due to the following reasons:

1. The point-to-point setup restricts the spatial coverage. At most the network will consist of many disjointed links. Without the ability of regeneration, the channel's absorption and dispersion induces decoherence of the qubit. This limits the transmission distances of the qubit flow. The resulting dark counts increase the QBER and hence effectively limit the transmission distance.
2. While the bandwidth requirement of QKD is high, the secure key rate is lower than its classical counterpart. The QoS of such a network is therefore severely disadvantaged. Detector and multiplexing technologies will address this issue.
3. The reliability of QKD is much lower than its conventional counterpart. The typical QBER is 10^5 larger than the errors found in classical data flow.
4. As the resources to install and operate a QKD system are costly in terms of network operations, niche application of high confidentiality are only worth securing. Increasing the QoS of the solution through improvements in the reliance and bandwidth can reduce the overhead per capita.

The above constraints have catalyzed research initiatives towards the field of Quantum Networks. These networks aim to facilitate routable qubit flows to produce QKD on-demand with a good QoS. The main parameters of the QoS needing improvement are the reliance and bandwidth of the solution.

A quantum network utilises both quantum and conventional technology to streamline the qubit flow in a multi-node environment. Such a network requires the use of a hybrid set of quantum channels to be integrated to form a complete network. As each quantum channel is better suited to particular terrains. This also assists in the reduction of key relation knowledge by any adversary.

3. SYSTEM DEVELOPMENT

There are many QKD solutions that have been realised and deployed over the past few years specifically within test-bed quantum networks. The Durban – QuantumCity [46], DARPA [47] and SECOQC [48] are prominent examples. While the Centre for Quantum Technology at the University of KwaZulu-Natal has concentrated research efforts towards solution deployment, various aspects of system development have also been realised. This chapter presents the research conducted towards the optimisation of QKD units. The aim of these efforts is to integrate these solutions into existing systems to enhance the efficiency of QKD units.

The use of hybrid technology in the implementation of QKD solutions provides an essential flexibility in the deployment of transparent solutions. The integration of both fibre and free space quantum channels into a single network requires both methodologies of phase and polarization encoded photonic qubits to be optimized. While both encoding methods achieve significant advantages in their preferred channels, the use of polarization encoding in both free space and fibre channels excludes the need for a trusted gateway within a hybrid link. This would require the coupling of photons between fibre and free space and the polarization encoding of photon within a fibre. Such hybrid channels can be used in conjunction with standard QKD linkages to optimize the coverage of the network's terrain.

The work on polarisation encoded, fibre-based QKD presented in this chapter has been published in [49].

3.1 Polarisation encoded QKD in Fibre

The deployment of QKD in fibre has mainly been limited to phase encoded qubits due to the birefringent effects associated with fibre transmission. Qubit transmission in fibre is however limited to a few hundred kilometers and is therefore suitable for Metropolitan networks. As

mentioned earlier however, the ability to accommodate hybrid quantum channels within a quantum network provides additional QoS to the network. Various implementations of QKD systems are naturally inclined towards certain terrains. Free space implementations, for example, provide an obvious solution for links involving QKD stations in motion. Free space channels can also support transmission over longer distances allowing for communication with aerial stations [41]. The ability to mesh these channels will ensure flexible network coverage. In a broader view, investigations focussed on coupling fibre to freespace technology creates one of the possibilities for a global QKD network via the use of satellite communication.

One method towards realizing the hybrid networks described above is to ensure a uniformed encoding methodology throughout the network. While both fibre and free space channels use photonic qubits, the encoding within free-space channels has generally been maintained as polarisation while fibre channels have conventionally encoded qubits as a relative phase between qubit pulses. This is due to the inherent birefringence in optical fibre causing a shift in the State of Polarisation (SoP) of the incident photon. The change in the SoP pose challenges to the realisation of polarisation encoding in fibre as both the sender and the reciever are required to make measurements in identically orientated bases relative to the qubit's polarisation. The development of all optical networks and investigations into Polarization Mode Despersion have given rise to various compensation techniques to rectify the birefringent effects prior to measurement of the qubits [74].

In this section we investigate the polarisation encoding of qubits within a fibre channel. The fundamental constraint in quantum communication as opposed to conventional communication is that the data carrier may not be measured except by the intended recipient. All optical technology must therefore be used to ensure the qubit remains within the quantum regime and hence its coherence is upheld.

The encoding of qubits via Orbital Angular Momentum (OAM) is also an active field of research [18] however can not be applied to network integration due to the fact that it requires multimode fibre deployment. Such fibre is not readily deployed in commercial networks due to the effects of modal dispersion.

3.1.1 *Polarisation*

Polarisation of a photon is determined by the orientation of the oscillation of the electric field of an electromagnetic wave. The electric field of the of the photon may be represented as two orthogonal waves [27]

$$\vec{E}_x(z,t) = \hat{\imath}\, E_{0x} \cos\,(kz - \omega t),$$

$$\vec{E}_y(z,t) = \hat{\jmath}\, E_{0y} \cos\,(kz - \omega t + \varepsilon),$$

where k is the wave number and ω is the angular frequency of the electromagnetic wave. The amplitudes of the components are represented by E_{0x} and E_{0y} while z and t are the spatial and temporal parameters of the wave respectively. The symbol ε describes the relative phase difference between the two components and is a measure of the ellipticity of the SoP. Two special cases are noted: In the case of linearly polarised light, $\varepsilon = m\pi,\ m \in \mathbb{Z}$. The photons achieve circular polarisation if the relative phase, ε, between the orthogonal components is described by

$$\varepsilon = -\frac{\pi}{2} + m\pi,\ m \in \mathbb{Z}.$$

Given an arbitrary value of ε, the photon may achieve any state of polarisation within the Poincaré's sphere as illustrated in Figure 2.3 on page 18.

3.1.2 *Jones Calculus*

The SoP of the photon and any optical manipulations thereof can be mathematically represented as a Jones vector and transformation matrices [75] respectively. The elements of the Jones vector consist of the x and y components of the polarisation as represented in Cartesian co-ordinates. The Jones vectors for the six states of polarisation as illustrated in Figure 2.3 on page 18 are presented in Table 3.1. These states of polarisation are commonly used in the application of QKD.

A Jones matrix represents an optical transformation of an initial state of polarisation to another. A 2×2 Jones matrix represents any optical transformation. Jones calculus provides a quantitative manner to simulate or track the evolution of the SoP of a photon through optical apparatus. A general transformation in the SoP may be represented as

$$E_t = A\, E_i,$$

where E_i is the Jones vector for the initial State of Polarisation, E_t is the Jones vector for the final State of Polarisation and A is the Jones matrix for the transformation.

3.1.3 *Birefringence*

Birefringence refers to the property of a material that causes a polarisation dependent refractive index [37]. This implies that light with varying SoP is transmitted through the medium at different speeds. This phenomenon is referred to as the differential group delay [76]. Birefringent material therefore has a natural optical axis with the smallest refractive index. This is known as the *fast axis*. The axis orthogonal to the optical axis is known as the *slow axis*. The interaction between the light traveling in these axes induces a change in the State of Polarisation of the signal.

Table 3.1: The Jones vectors for the State of Polarisation commonly used in QKD applications.

State of Polarisation	Jones vector
Horizontal	$\begin{bmatrix}1\\0\end{bmatrix}$
Vertical	$\begin{bmatrix}0\\1\end{bmatrix}$
Diagonal (+45)	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
Diagonal (-45)	$\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}$
Right Circularly Polarised	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$
Left Circularly Polarised	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$

Birefringence occurs in optical fibre due to asymmetries of the construction and induced stresses on the fibre. The birefringence causes a change in the SoP of the signal as it passes through the fibre. This transformation remains constant provided the stress factors remain constant.

Assume that the optical fibre induces a transformation, A, on the incident photon, a polarisation compensation transformation, A^{-1}, must be applied to the received photon in order to retrieve the original SoP. Both transformations A and A^{-1} must be recalibrated at regular intervals to accommodate the changes in stresses of the fibre [75, 77]. Bends in the fibre, pressure, heating and vibrations cause changes in stress level of the fibre. An active compensation technique is therefore required to ensure that the SoP of the incoming photons is correctly orientated in real time.

3.1.4 *Recent Work towards Birefringence Compensation*

Breguet *et al* first demonstrated an application of QKD with polarisation compensation system in a fibre in 1994 [78]. The initial effort used a pair of Quarter Wave Plates (QWP) to realign the photons' polarisation after birefringent effects experienced within the fibre. While the

ellipticity was corrected with the QWPs, adjusting the angle of the beam splitter rectified the linear disorientation. The error rate of the compensation system was maintained below 0.54%.

Liu *et al* used Time Division Multiplexing (TDM) to insert test pulses within the QKD stream in order to assess and compensate for the birefringent effects on the state of polarisation of the photons [79]. This compensation technique was demonstrated across a 2 km fibre with a sifted key rate of 2 kbps.

Recently a faster compensation technique was realised by replacing the piezoelectric controllers with lithium niobate polarisation controllers [80] [81]. A second lithium niobate polarisation controller was used to switch between the measurement bases. A polarisation scrambler was used prior to the measurement of the photons in order to induce random changes to the SoP and evaluate the efficiency of the lithium niobate controller. With a 0.1 photon count per pulse, channel length of 16 km and total losses of 4.3 dB, the group was able to retrieve a QBER at 1.6% without the use of the polarisation control system. The stabilisation algorithm that forms part of the active compensation in fact increased the QBER by 1.1%. The system however showed that in principle it was possible to control rapid fluctuations in the SoP of photons.

The solution implemented during this work provides a cheaper solution to the solutions presented above. While the dual compensator system may be used to rectify each basis separately by isolation the SoP of photons, the current implementation identifies and isolates the plane of polarisation containing the four possible incident states of polarisation. The system provides an active means of polarisation control prior to basis measurement creating a more generic solution for a wider variety of protocols to be implemented using polarisation encoding in fibre.

3.1.5 *Setup and Results*

The experimental setup demonstrated the recalibration of photons to their original SoP after exposure to a birefringent channel. The birefringence effect of the fibre channel was evaluated as a unitary transformation [74] and the inverse transformation was applied to the photons prior to measurement. The schematic of the general setup is illustrated in Figure 3.1. The setup comprises of preperation apparatus including a laser, attenuators and a state generator; the compensator; and the measurement apparatus consisting of the consisting of basis selection optics and photon detectors. The experiment used an attenuated laser as a source for single photons. The source of the laser light was the Thorlabs PRO8 DWDM DFB Laser Diode Modules housed within a Thorlabs PRO8000 enclosure. The laser was pulsed using an internal trigger of 10 kHz. Various inline attenuators (AT), from Thorlabs, together with a VOA-MI variable optical attenuator from oemarkets were then used to attenuate the laser pulses to a power of 0.1 photons per pulse. A polarisation state generator (PG) was then introduced to encode the photons with a reference SoP. The photons travelled through a temperature and vibration stabalised fibre. The single mode fibre had a length of 1000 m. The fibre remained

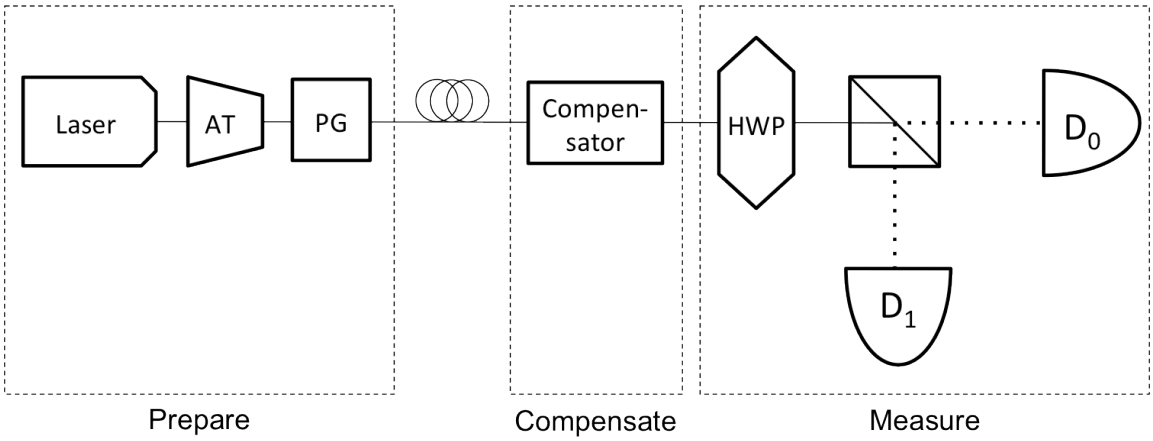

Figure 3.1: The schematic of the implemented State of Polarisation (SoP) compensation technique. The compensation is implemented prior to the measurement apparatus. A modulated laser and attenuators (AT) create a pseudo-single photon source. The polarisation state generator (PG) encodes the photons with a SoP. A compensator applies a reverse transformation to the photon to realign the SoP prior to the measurement of the photons by detectors D_0 and D_1. A half wave plate (HWP) is inserted to induce a choice of basis for the measurement.

vibrationally stable throughout the experimentation while the temperature was allowed to fluctuate with the ambient room temperature as shown in Figure 3.2.

A first order compensation technique for a single basis (vertical/horizontal) included a Thorlabs three-paddle fiber polarization controller. The measurement apparatus comprised of a Half Wave Plate (HWP) placed prior to the polarisation dependent beamsplitter (from Thorlabs) on Bob's end. As the initial investigation comprised of just one basis, the HWP remained in a neutral orientation while a polarisation dependent beam splitter was used to differentiate the states. IDQ id201 InGaAs/InP avalanche photo diode detector were used to measure the photons. The detectors were externally triggered from the Thorlabs PRO8000 enclosure. The delay was adjusted to compensate for the trigger delay between the incident trigger and respective optical pulse. A Labview interface was used to analyse the data.

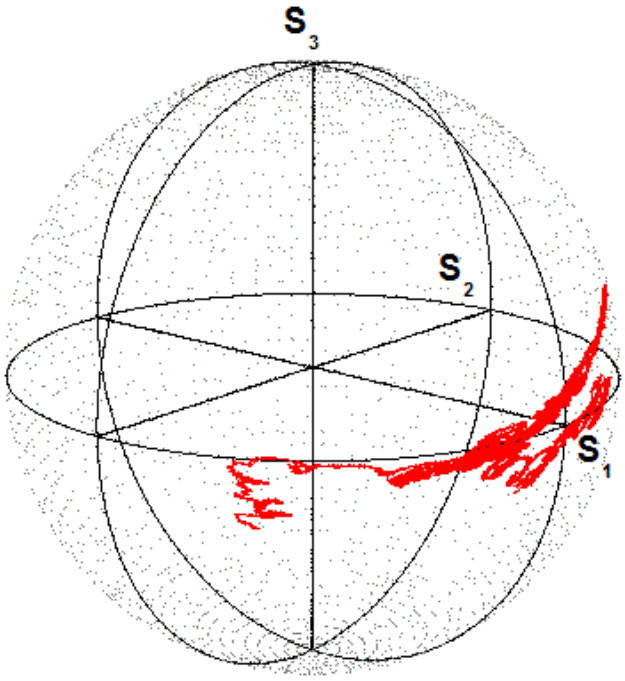

Figure 3.2: A plot of the variation in the SoP of the laser source over 16 hour period. The fluctuations in the SoP are a result of thermal and vibrational changes in the environment. As is seen there is linear and elliptical deviation of the SoP through time. This requires a polarisation compensation technique in order to conduct polarisation encoded QKD over extended times.

The preliminary experiment illustrated the ability to reverse the effects of birefringence for quantum optical communication as illustrated in Figure 3.3 and Figure 3.4. The figures represent the photon count rate for detectors D0 and D1. Initially vertically polarised photons were prepared and transmitted over the fibre channel without the use of the compensator. Due to birefringence present in the fibre, both detectors measured significant count rates. A three-paddle polarization controller was then used reverse the change in polarisation and the the photons were again measured. The three-paddle polarisation controller creates stress induced

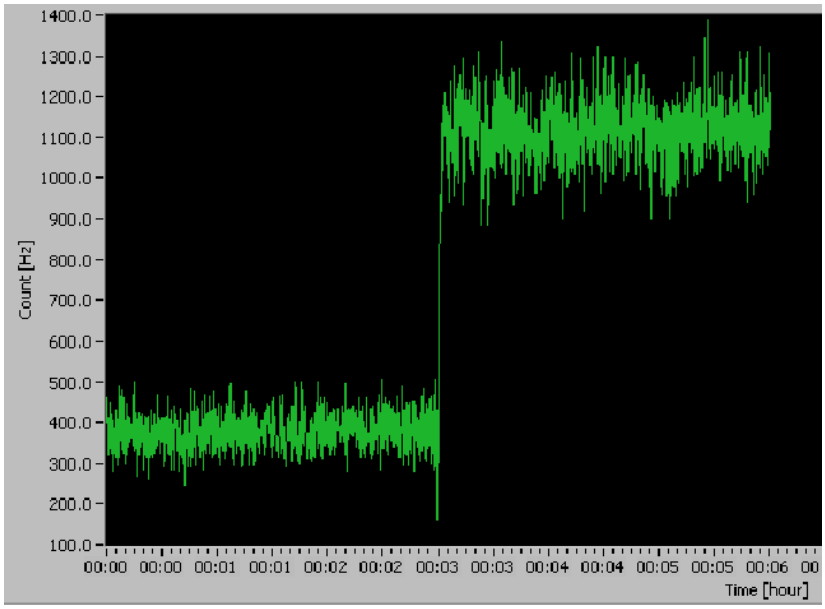

Figure 3.3: The photon detection rates of the detector measuring vertical SoP before and after compensation. A vertically polarised reference beam was transmitted across the fibre, birefringence effects cause a change in SoP and hence reduced detection rates. Upon compensation an increased detection count is noted.

birefringence within the fibre. The manual rotation of the paddles provides a combination of stresses that induce a final change in polarisation. It is noted that a distinct minimization and maximization of the horizontal and vertical count rates occurred respectively after compensation. The HWP was used to flip the states upon which the count rates were reversed.

The birefringence of a communication channel remains stable unless external stresses are applied. In deployed fibre networks a constant flux of stresses are applied to the channel requiring an active compensation technique. While a three-paddle polarization controller was used in the prelimenary investigation, various other devices have the ability to manipulate the SoP of a photon in a controlled and automated manner and were thus investigated as possible polarisation compensators. A polarisation locker with an active feedback system was used for the implemented compensation technique. The equipment used in the final setup is detailed below.

Polarisation State Generator

The PSG-001 polarisation state generator was purchased from General Photonics. The controlling logic circuit was developed in house. The state generator comprises of 6 magneto-optic rotators that can induce any desired SoP. The magneto-optic rotators induce a stress related rotation of the SoP of fibre upon the application of a magnetic field across them. A Transistor–Transistor Logic (TTL) voltage is applied to each magneto-optic rotator causing

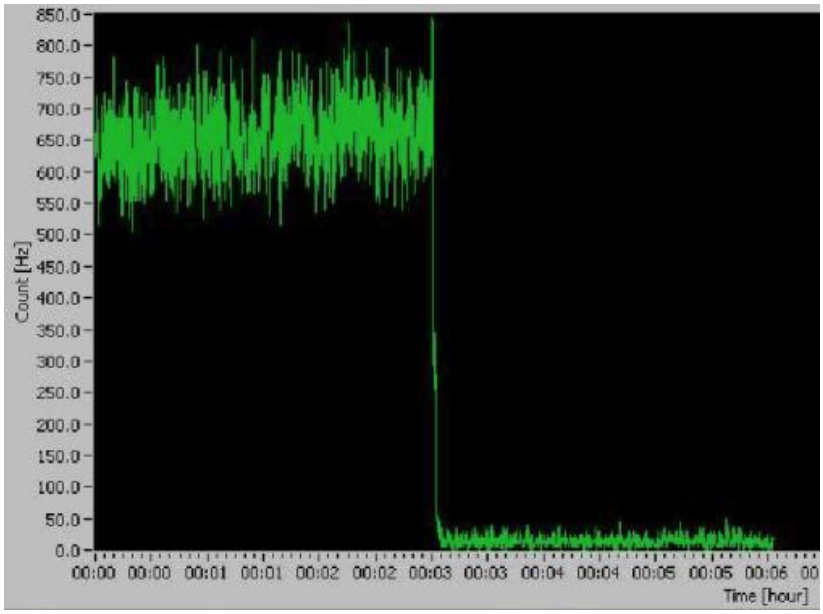

Figure 3.4: The photon detection rates of the detector measuring horizontal SoP before and after compensation. A vertically polarised reference beam was transmitted across the fibre, birefringence effects cause a change in SoP and hence increased detection rates. Upon compensation, a minimised detection count is noted.

a stress and a controlled birefringence. The specific combinations of rotators results in the in 6 states desired states of polarisation required for QKD as illustrated on the Poincaré sphere in Figure 2.3 on page 18.

The polarisation state generator is used to encode the photon a specific bit value by polarizing an incident photon into a one of the predefined states. As the BB84 protocol was implemented, the photons were polarized in a polarisation state from the rectilinear or diagonal bases.

Half wave plate

A OZ Optics HWP was used in the implementation. A HWP retards one of the components of the electric field by half a wavelength along the slow axis of the HWP. This effects the output SoP such that it is flipped across the fast axis of the HWP. In the Jones matrix notation the transformation of a HWP with a vertically orientated fast axis on a right diagonally polarised photon is represented by

$$\frac{1}{\sqrt{2}}\begin{bmatrix}-1\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}-1&0\\0&1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix},$$

illustrating that the SoP has changed to left diagonal.

The HWP is placed prior to the polarisation dependent beam splitter to allow for the choice of a measurement basis.

Polarisation Locker

The polarisation locker used in this experiment was the Thorlabs PL100S. It consists of piezoelectric polarisation controllers managed by varying voltages to the controllers, as with the Polarisation State Generator. Piezoelectric controllers induce stresses on the fibre creating a controlled form of birefringence. The polarisation locker was implemented with a feed back loop developed in house. This provided an active mechanism of polarisation control.

In order to lock the SoP, an in-line polarimeter (Thorlabs IPM5300) and digital signal processor form part of an internal feedback loop to the controller as in Figure 3.5. The external polarimeter measures the plane of polarisation and communicates this to the controller drivers of the polarisation locker. The locker in turn adjusts the controllers to produce the desired shift plane of polarisation. A stepped search approach is used to incrementally rotate the plane of polarisation to the equator of the Poincaré Sphere in order to measure the desired linear modes.

As the intended QKD protocol requires states from two non-orthogonal bases to be transferred across an optical fibre the compensation techniques are non-trivial. This is due to the fact that each qubit is encoded with a random basis that cannot be differentiated by the compensator. In order to compensate for all four states simultaneously, not only does the SoP need to be traced and rectified on the Poincaré Sphere, rather the entire plane of polarisation containing the four states must be manipulated and transformed back to the linear states. Upon passes through the locker, the plane of polarisation around the Poincaré Sphere is traced out by the rotation of a HWP and measured by the external polarimeter. Once the plane is identified by the controlling computer a feedback signal is sent to the locker to incrementally adjusted the plane of polarization over the Poincaré Sphere until the resultant plane coincides with the linear modes along the equatorial plane of the Poincaré Sphere.

3.1.6 *SoP Compensation Techniques*

By applying the Jones matrix for an arbitrary rotation, φ, to two orthogonal states

$$\begin{bmatrix}\cos\varphi\\ \sin\varphi\end{bmatrix} = \begin{bmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix},$$

and

$$\begin{bmatrix}-\sin\varphi\\ \cos\varphi\end{bmatrix} = \begin{bmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix},$$

we notice that the resultant states are again orthogonal. This illustrates that a single rotational transformation can compensate for orthogonal states. Two polarisation controllers may therefore compensate for one basis each in the BB84 protocol [82].

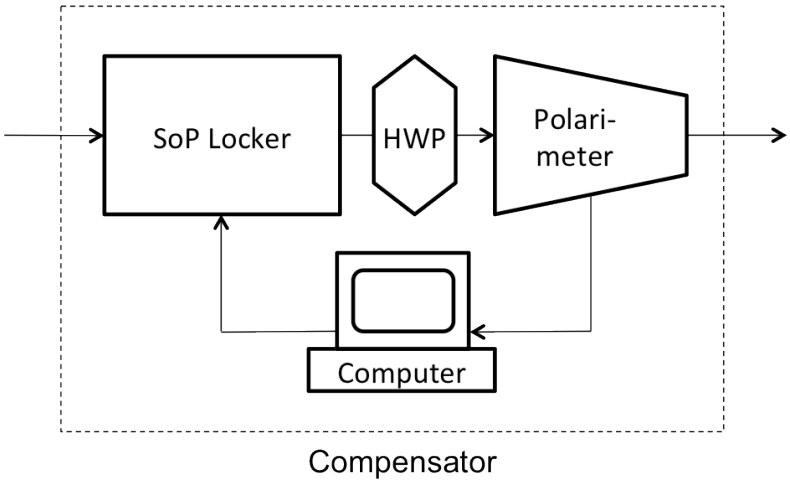

Figure 3.5: The implemented compensator comprises of the State of Polarisation (SoP) Locker that isolates the plane of polarisation and performs an incremental rotation of the plane. The Half Wave Plate (HWP) performs a linear rotation around the Poincaré Sphere to isolate the current plane of polarisation. The external polarimeter measures the plane of polarisation while the computer controls the feedback to the locker. The locker incrementally searches the Poincaré Sphere in order to rotate the incident plane of polarisation to the linear polarisation states.

The scheme implemented in this work uses only one SoP locker that is placed prior to the bases selection apparatus. The final setup is illustrated in Figure 3.6. The SoP locker is programmed to step search with a *plane of polarisation* rather than just the State of Polarisation. The plane of polarisation is defined as the plane on the Poincaré sphere that cuts through the 4 states being used in the QKD protocol. Correcting the plane of polarisation ensures that all four states are compensated with one transformation.

While a SoP locker is traditionally used to transform all incoming light to one fixed SoP on the Poincaré sphere it may also be used to apply a common rotational transformation on all incoming light. If this transformation is adjusted to the inverse of the birefringence of the setup, an accurate correlation will exist between the prepared and measure photons. This inverse transformation may be mathematically calculated or practically found through a step search function with respect to the plane of polarisation. The compensation technique was temporally multiplexed with the quantum signals. The initial compensation time varies due the initial orientation of the plane of polarisation. In a QKD system the duty cycle for the compensation should be implemented as per the fluctuations in the QBER.

In this setup, time division multiplexing is utilised to switch between the qubit stream and the conventional calibration signal. A single source of pulses is used while the attenuation is varied to switch between conventional and quantum signals. While the calibration signal is sent with

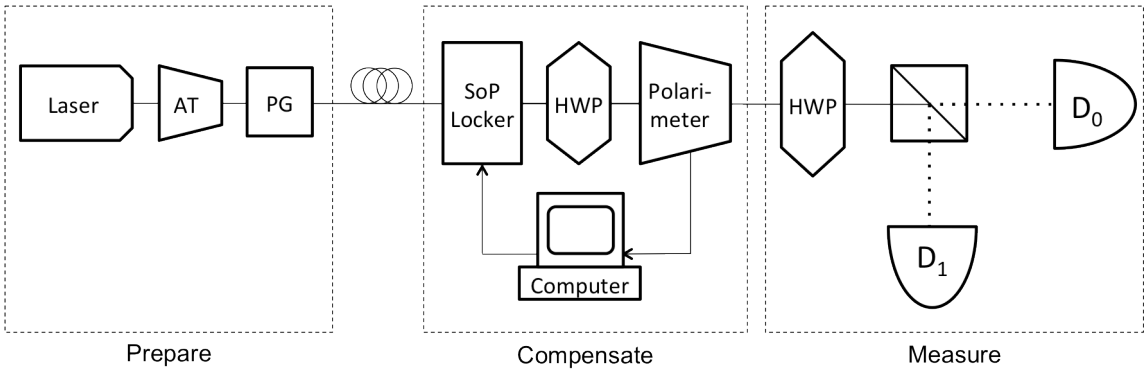

Figure 3.6: The optical setup for the SoP compensation technique is shown above. The setup uses one SoP locker with a feedback loop placed prior to the bases choice of Bob. The feedback loop within the compensator corrects for the *plane of polarisation* rather than just one SoP on the Poincaré sphere. The prepare and measure systems remain unchanged as mentioned before.

only one constant SoP, e.g., vertical, the polarimeter is used in collaboration with the HWP to scan the plane of polarisation and to perform a step search to calibrate the signal to its original preparation states. The result of the compensation technique is demonstrated in Figure 3.7 and Figure 3.8. The plane of polarization is constructed by the polarimeter through the linear rotation by a HWP. Conventional light pulses are used for the compensation technique. In this experiment the HWP was rotated manually and the remaining step search was conducted in person. This system may be automated through regular routines.

The QBER that will arise from the compensation technique described above would result from an inaccurate compensation of the plane of polarisation to the equatorial plane. This will result in an improper distribution of photons at the beam splitter of Bob. Malus' Law [74] predicts that the intensity of light passing a polariser is determined by

$$I = I_0 \cos^2 \delta,$$

where I_0 is the incident intensity of light and δ is angle between the angle of polarisation of the light and polarisation axis of the polariser. Due to the short distances and synchronisation between the beam splitter and detectors, a change in intensity will result only in a change in the number of photons reaching each detector. The intensity is directly proportional to number to photons received by a detector. It is thus possible to estimate the error bars for this compensation technique with regards to a defined QBER.

The change in the intensity of the transmitted light as a function of δ and the corresponding increase of the intensity of the orthogonal state is shown in Figure 3.9. This relationship is used

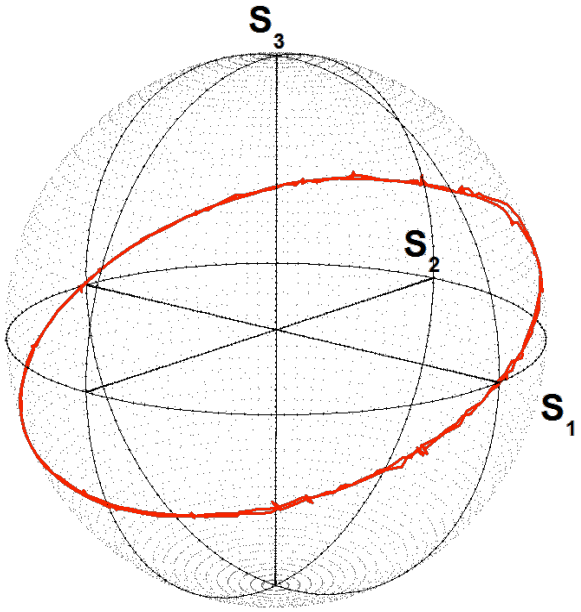

Figure 3.7: The SoP of a signal prior to the compensation technique passes through an arbitrary plane of polarisation as indicated by the red circle. The plane of polarisation is traced out by a linear rotation created by a HWP. The plane of polarisation may be optimised through a step search in order to isolate the intended plane.

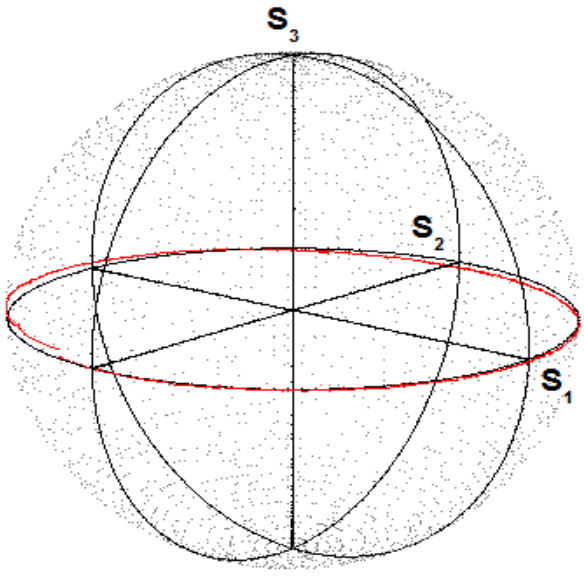

Figure 3.8: After the compensation technique is complete, the plane of polarisation is maintained on the equatorial plane of the Poincaré sphere as indicated in red. The plane of polarisation is traced out by a linear rotation created by a HWP. This ensures the both the computational and complementary bases are compensated for by one transformation.

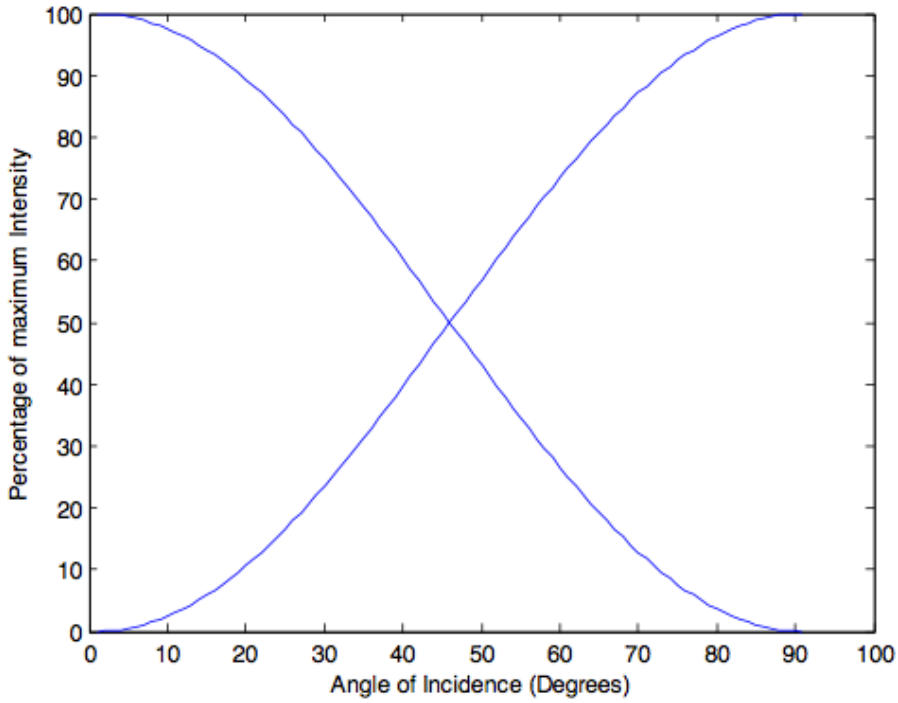

Figure 3.9: The above plot depicts the change in the intensity of the transmitted light relative to the incident beam due to an angular mismatch between the linear SoP of the signal and measurement basis. It is noted that here is a complementary increase in the intensity of the transmitted orthogonal SoP as shown.

to control the QBER at an acceptable minimum by permitting the step search an allowed angle of deviation. As an example, if an error rate of 1% is acceptable from the polarisation compensator, the angle of incident light may deviate by 5.74°.

The results from Figure 3.2 were used to determine the time intervals for the acceptable deviations of the measured photon. The average time interval for the angle of azimuth on the Poincaré Sphere to change by 5.74° was 332.75 s and the corresponding time interval for the angle of inclination was 1057.59 s. Using a TDM technique, the duty cycle for the polarisation compensation for this environment and acceptable QBER is 333 s. Each environment is different and in order to effectively use the TDM method, a SoP stability test must be conducted for a new environment as well as for varying environmental conditions.

3.2 Free space QKD

Free space QKD systems can provide a means of secure communication between remote sites that have a line of sight vision between them. While no commercial free space QKD systems are currently available, these systems play an integral role in defining the market acceptance of QKD as a complete networkable solution. Free space QKD units have already been involved in test bed networks [43].

One of the major advantages of free space communication links is the possibility of quick low-cost rollouts of terrestrial links and the access to mobile stations. Provided a line of sight link is maintained between the two units, QKD will be possible. A global communication network, illustrated in Figure 1.1 on page 5, will consist of three types of free space links:

- Ground station (stationary) to ground station [83]: Typically used as an inter and intra city setup where good visibility and stable conditions are present.
- Ground station to a mobile unit [84]: These links would permit ground to satellite communication. Provided the satellite is *trusted*, this could aide in the construction of a global QKD network.
- Mobile unit to mobile unit [85]: This is the most generalised free space link. It will provide the platform for inter-satellite or inter-aircraft communication. A satellite network would provide a quantum backbone with access points in every participating city as expanded upon in Section 4.4 on page 71. Various feasibility studies have been conducted regarding free space QKD between earth and satellites [84-86].

Free space QKD systems have thus far mainly used polarisation encoding for communication. As free space links are not confined within a waveguide, as in the case of fibre, spatial, temporal and spectral filtering is required for all such links. However, due to the translation and rotation of mobile units, these require secondary optimisation techniques. Polarisation tracking, being one such critical technique, is discussed in this section.

3.2.1 *Polarisation Tracking*

It has been shown that the polarisation of light, as it propagates through the atmosphere, is not significantly altered [84], neither is the SoP affected by the Faraday effect due to the Earth magnetic field.

When communicating with a mobile unit through polarisation encoded QKD, the orientation of each unit with respect to the other is of vital importance. This is due to the fact that an incorrect orientation would imply mismatched bases between the sender and receiver. Such an error would cause a misalignment between the intended and actual measurement of the system and induce an increased QBER.

Polarisation orientation tracking has been considered both mathematically [84] and as a corrective measure to a reference signal [87]. In the latter, Toyoshima uses a series of HWP, beam splitters and polarisors within a feedback loop to rotate the beam such that it receives the greatest power is hence aligned with a reference beam.

3.2.2 *Setup and Results*

The schematic of the implemented system is shown in Figure 3.10. It suggests a method that varies from [87]. In the setup a reference beam, with a predetermined polarisation (e.g. vertical) is transmitted to the receiver. The receiver contains two polaroids orientated at 45° on either side of the incident reference beam (e.g. right and left diagonal). The reference beam is split and directed towards the polaroids. A pair of light sensors is placed past the polaroids to measure the power of the transmitted beams. The digitalised signal is then passed through a comparator to drive a step motor that will rotate the measurement equipment. The solution is mechanical and therefore not suitable for satellites due to the effects of angular momentum. However such a system is a cheaper alternative for terrestrial systems as well as mobile stations such as vehicles, ships and aircrafts.

If the QKD units are perfectly orientated, Malus' Law predicts the intensity of the incident light is equally distributed after the polaroids. The sensors are therefore illuminated with the same intensity of light such that digital signals of equal voltage are passed to the comparator. The step motor will remain inactive.

If there is an orientation mismatch, there will be a variation of power reaching each detector. The voltages from the detectors that reach the comparator will result in a discrepancy and engage the step motor to correct the orientation of the apparatus. As the apparatus corrects its orientation, the voltage induced at the comparator is reduced and the step motor comes to rest.

Figure 3.11 illustrates the current Proof of Concept setup. In order to save further costs the reference beam used is a diagonally orientated beam while the polaroids have been replaced by a single polarisation dependent beam splitter with horizontal-vertical axes. The step motor with its respective electronics is shown in Figure 3.12. Both sub systems have been tested individually and remain to be combined. The quantitative results, such as the associated QBER, can only then be measured.

As a preliminary test for the proof of concept, the expected voltage feed to the comparator was compared to the experimental results. The graphs in Figure 3.13 show that there is a good correlation between the theoretical and experimental results. A constant phase lag in the experimental data is predicted to be a misalignment of the polarizer used to rotate the incident signal.

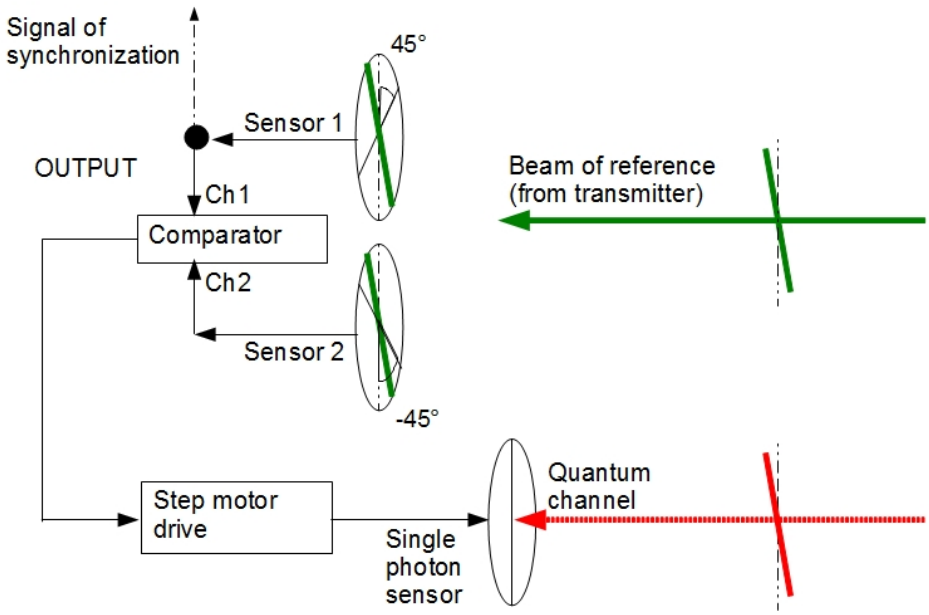

Figure 3.10: Polarisation orientation tracking is implemented by comparing the output of two orthogonal polarisers when illuminated by a reference pulse. If the orientation is mismatched, the comparator induces a step motor to correct the orientation of the unit.

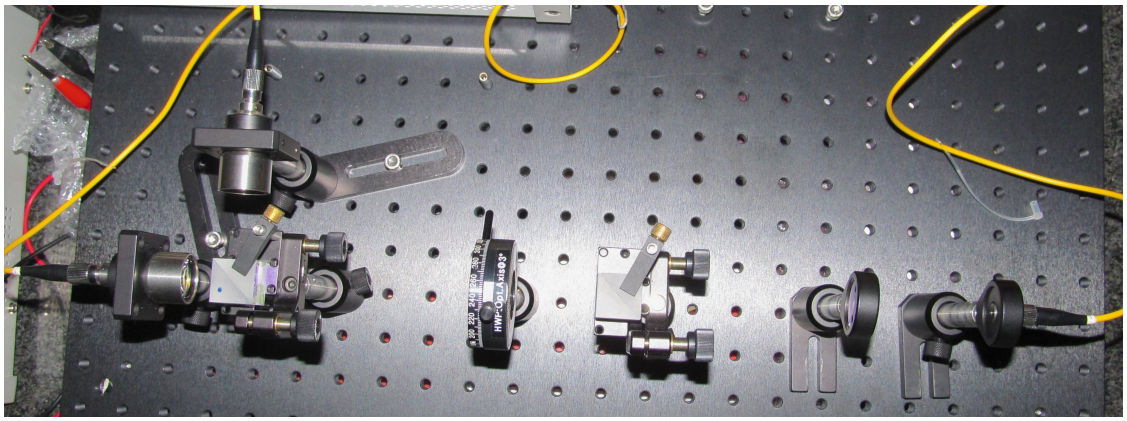

Figure 3.11: The optical implementation of the polarisation tracking system. It can be noticed that a polarisation dependent beam splitter replaces the polaroids while a further polarisation dependent beam splitter and a HWP is used to create the polarisation orientation of the incident beam.

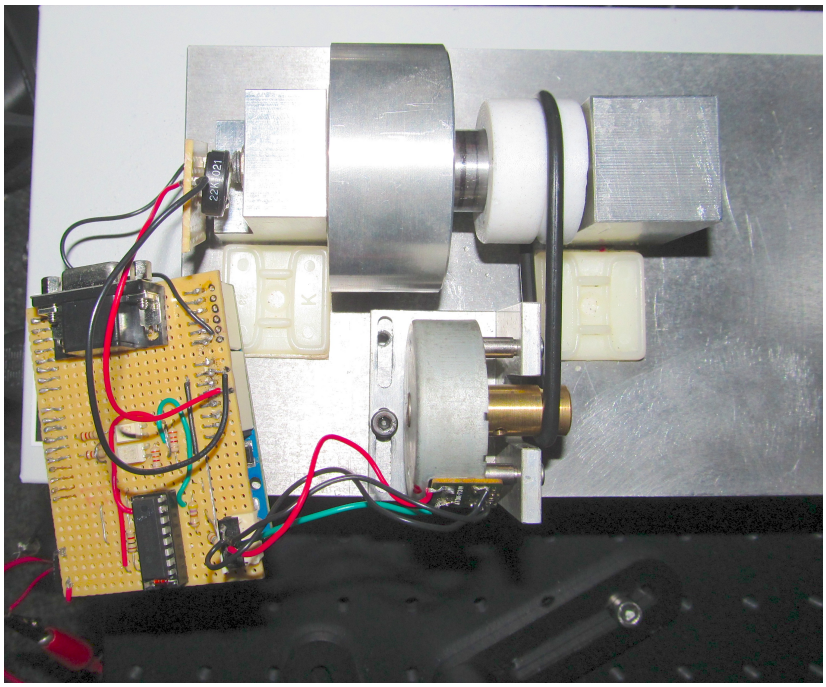

Figure 3.12: The step motor is controlled by the comparator in order to realign the station relative to the incident beam and hence the sending station.

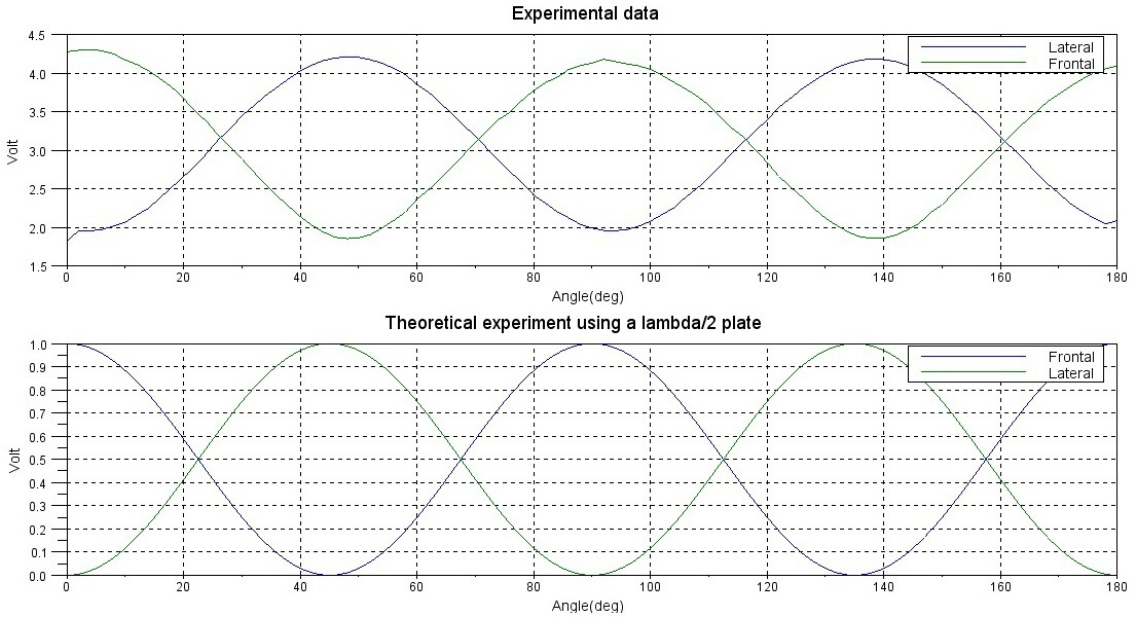

Figure 3.13: A good correlation between the theoretical predictions of the incident voltage to the comparator and the experimental results can be seen. A constant phase lag in the experimental data is predicted to be a misalignment of the polarizer used to rotate the incident signal. The electronics and detector efficiency causes the slight closure of the eye in the experimental results.

4. SOLUTION DEPLOYMENT

The development of a system must be done in conjunction with the knowledge of the environment of deployment. This will provide a substantive advantage in the integration process. The QKD solution driven research at the Centre for Quantum Technology at the University of KwaZulu-Natal has focused on the deployment of QKD in a live networking environment for extended periods of time. The aim of this research was to investigate the feasibility of QKD deployment and integration techniques focused on achieving an acceptable QoS.

Both the implemented projects, the *QuantumCity* and *QuantumStadium*, presented in this chapter have been recognised as major milestones in the realisation of quantum networking solutions by the Scientific American [16].

The work presented in this chapter is based of the publications of the author [15, 46, 88-90].

4.1 Quantum Networks

A quantum network is a quantum-secured platform with an addressable communication infrastructure and multi-node accessibility. The concept of a quantum network is a natural progression from the original point-to-point QKD setup. A quantum network will provide substantial value-adds to the QKD solution in order to achieve market acceptance as a mainstream technology.

The first implementations of quantum cryptography solutions have illustrated the long-term stability of the units through the continuous usage of QKD over extended periods of time. The research and product development have focused largely on the robustness of the point-to-point setup. However the overhead and running costs involved with the deployment of these systems in a multi-node configuration result in infeasibility of networks operations. Due to the dedicated communication channels and the severe limitation on the data flow manipulation of a quantum

signal, the host networks incur a drop in the QoS with inefficient bandwidth usage and communication latencies and jitter.

The evolution of qubits through a quantum channel induces a superposition of states. In order to preserve these quantum characteristics, and hence the security of QKD, the qubits must remain unobserved until reaching the intended recipient. In the case of photonic qubits, the channel must remain within the optical domain forcing the use of *all-optical* networks. In particular, qubits may be switched through a network but cannot be routed, hence conventional *connectionless networks* cannot be used for such the implementation of quantum communication. Amplification and regeneration of qubits will also interfere with the superposition and coherence of the qubit.

To provide cost effective coverage and the required bandwidth for quantum-secured communication, the hybridisation of the network must be considered. Multiplexing classical and quantum signals has been the center of much research interest [91, 92] as dedicated quantum channels increase bandwidth costs across the network and provide side channel information to key sharing relationships.

The optimal coverage of the network relies on the choice of the types of channels used to deploy the network. Channel interoperability with regards to the qubit flow is therefore essential for an effective switching table. The ability of qubits to be switched across various mediums (fibre and free-space), enroute from Alice to Bob, provides an additional degree of freedom with respect to the available redundancy. This will result in an improvement of network congestion and latencies.

There are two parallel efforts towards the improvement of the QoS of quantum networks. The first solution focuses on the development of advanced quantum information processing and communication devices [93]. These include entangled sources, quantum memories and quantum repeaters. The main advantage of the above technologies is the ability to create *untrusted networks*. These networks provide a communication platform that does not compromise the security aspects of QKD and may hence remain publicly accessible infrastructure. The adaptation of conventional networking technology for the propagation of qubits provides a second method of integration. This is realised with an all-optical, connection-orientated network with classical relays. An adapted conventional networking platform serves as a quantum network however must remain *trusted*. This implies that certain key elements of the network must remain in the full control of the authenticated parties or a mutually trusted third party.

In order to optimise the provided QoS of a quantum-secured communication network [43], both the network components and the network operations are to be adapted to accommodate the dynamics of the qubit. These initiatives are presented in the following sections.

4.1.1 *Quantum Enhanced Technology*

In order to fully exploit the quantum nature of the qubit, all manipulations to the qubit must be undertaken in a controlled quantum environment. Quantum-based operations will allow the qubits to undergo computational transformations without compromising the coherence of the state. Various network operations that are unable to be conducted on qubits by conventional networks, e.g., conflict resolutions and signal regeneration, may be introduced with the development of such technology. Provided a suitable efficiency, these quantum processes will introduce a QoS comparable to conventional networks.

Formally, Quantum Information Processing and Communication (QIPC) is a wide and active field of research [28] that is beyond the scope of this thesis. A few critical devices that are relevant to networking protocols are, however, discussed below:

Quantum memories

A quantum memory may be interpreted in several different ways [94]. Effectively a quantum memory, as the name suggests, is a method of storing quantum information while maintaining the quantum nature of the qubit. They are important primitive structures in the development of QIPC devices such as quantum repeaters and quantum computing [95]. Quantum memories are also important in realisation of loophole-free Bell inequality tests, advanced communication network protocols and precision measurements [94]. A quantum memory can be realised as a single particle or an ensemble of particles depending on the application.

Quantum memories can be evaluated by the following parameters [96]:

- Fidelity: In the case of *store and emit* quantum memories, this refers to the commonality, or overlap, between the photon sent and retrieved from the memory.
- Efficiency: The probability to recover the exact state of qubit sent into the memory.
- Bandwidth: The amount of information that may be stored and the repetition rate for storage, delivery and resetting.
- Wavelength: The operational wavelength of the quantum memory
- Photon storage capacity: The ability to efficiently store multiple qubit at one time. This increases the bandwidth of the memories.

Quantum repeaters

Quantum repeaters are a special application of quantum memories [96]. These devices are essential for long distance QKD. The type of memory required is a *store and emit* memory, however the storage time may vary upon the application. Quantum signal regenerators will require a high efficiency and short storage time, while quantum routers with collision detection functionality require multi photon storage capacity with long storage times.

4.1.2 *Adapted Conventionally Networking Technology*

The development in high-speed communication technology has prompted the introduction of all-optical networks. These networks exploit the properties of light or implement switching tables to route the data flow towards the intended recipient. Passive optical networks or connection-orientated switched networks achieve this type of connectivity respectively.

Passive Optical Networks

Passive Optical Networks (PON) use devices such as optical couplers, circulators, cross-connects and multiplexers to route particular frequencies of light to various sub networks [74]. The wavelength of light is exploited as a degree of freedom in order to provide addressable packets of light. The devices used to implement this fibre optic access network consist of unpowered devices that distribute light pulses by means of Bragg gratings.

While the PON architecture is point-to-multipoint, QKD is undertaken between just two nodes depending on the chosen wavelength [97]. The keys are distributed between Optical Line Terminals (OLT) and one of the Optical Network Units (ONU) closer to the recipient. It is then assumed that the LAN connecting the end users to the OLT or ONU is trusted or a further QKD procedure is preformed.

Quantum Channel Switching

A connection-orientated switched network identifies the most cost effective route across the network and programmes optical switches to create an all-optical link between the two parties, as demonstrated by the US Defense Advanced Research Projects Agency (DARPA) network [98, 99]. This is accomplished through the use of active switching mechanisms within the hardware layer of the network infrastructure [74].

A switched network operates on the physical layer of the network and is thus opportune to the implementation of QKD in terms of redundancy and hence allows for the use of shared infrastructure. The connection-orientated network provides an all-optical link thereby the security of the communication remains as safe as a point-to-point solution. The network will however require compatible encoding technology across all links in the network while the network coverage is limited as in the case of the traditional point-to-point QKD systems.

Trusted Repeater Networks

A meshed network topology may be realised with the use of active, trusted intermediary nodes within the network [42]. While QKD remains a point-to-point resource, the distribution of keys between nodes is managed through an independent secure platform and modified network layers in the OSI network model. The skeletal network consists of a mesh of point-to-point links creating a quantum backbone (QBB) network [100]. The keys created at the physical layers are filtered up to secure software-based layers where key management protocols share keys between end-users on the network [91]. Such an implementation was realised with the

SECOQC project [43]. The QuantumCity project investigates the long-term stability of a QBB network implementation in a live environment.

Trusted repeater networks offer the possibility to extend the range of QKD beyond point-to-point setup through a robust *hop-by-hop* setup. A meshed network provides ample routing paths and hence redundancy in the network. Trusted repeater networks intuitively offer themselves to the integration of various types of quantum channels, in particular entangled photons. The security of this network, however, depends on the fact that all intermediary nodes must remain trusted at all times.

4.1.3 *Examples of Quantum Networks*

In the recent past various quantum networking projects have been implemented and provided case studies for quantum communication rollouts. These test bed networks have allowed for feasibility studies to be conducted focused on integrating QKD systems into conventional communication solutions. Four prominent projects investigated quantum-networking techniques in metropolitan laid optical fibre.

DARPA Sponsored Quantum Network

The first quantum network was developed as the first metropolitan quantum network for continuous operation [98]. It was established in 2004 with 6 nodes and was expanded to 10 nodes thereafter. The networks coverage is across the region of Cambridge, Massachusetts, USA as shown in Figure 4.1. The network was built in collaboration between BBN Technologies, Harvard University and Boston University and sponsored by DARPA. Four of the nodes operate across a switched telecom fibre network. Any transmitter is able to communicate with any receiver as per the settings of the optical switch. While the units named Alice and Bob where housed at BBN Technologies, Anna is housed at Harvard, with a 10.2 km fibre link, and Boris at Boston University, with a 19.6 km fibre link. A further free space QKD system developed by NIST, Ali and Baba, is combined to this network. Alice and Ali form a trusted node with a secured key-sharing relay between them. The network also implements a polarization-entangled system across a fibre link and a second free space system developed by QinetiQ.

While the DARPA network implements the BB84 protocol, it supports a variety of technologies and incorporates hybrid architecture to achieve an optimal communication network. The network achieves key management, routing and relay through custom protocols developed by BBN Technologies. The secure key generation rate across the network is approximately 1 kbps with a QBER of 3 %.

European FP6 Project Secure Communication using Quantum Cryptography

The Secure Communication using Quantum Cryptography (SECOQC) project has implemented a layered network model achieves a separation of duties with regards to network management

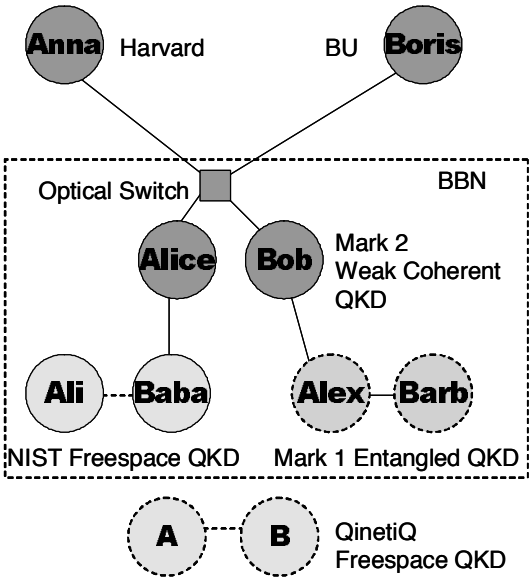

Figure 4.1: DARPA Quantum Network consists of 10 nodes. Four of the nodes run standard phase-encoded BB84 through a switched fibre network. Two free space systems are further connected to the network through a key relay implementing a trusted node. A final polarization-entangled system operates over a fibre channel. (Source [47])

and network security. This is essential to promote accountability and task delegation as per the OSI model.

This hybrid network consisted of five nodes with both fibre and free space systems. It further implemented various QKD protocols including BB84, SARG, COW and BBM92 [100]. These systems operated at the physical layer while being controlled by a single network-wide key management software within the transport layer to realise transparent end-to-end key distribution. The network is implemented as a QBB. The scalability and redundancy of the QBB network provides a high QoS while the seperation of key management from distribution allows the hybridisation of the physical layer. As oppossed to the connection-orientated network of DARPA, the SECOQC mesh continuously generates keys to a stack in the transport layer at each node. The keys are then consumed as per the requirements of the network.

The SECOQC metropolitan wide network was implemented in 2008 across the Siemens' fibre ring in Vienna, Austria. The network topology is shown in Figure 4.2. The QKD links of the QBB operate over dedicated fibres and span beween 6 km and 85 km. The cross connection links used patched fibres within the Siemens' fibre ring. A further link outside of the QBB linked in with a free space connection from a distance of 3 km while the last deployed a handheld QKD device with a distribution distance of under a meter. All devices used in the

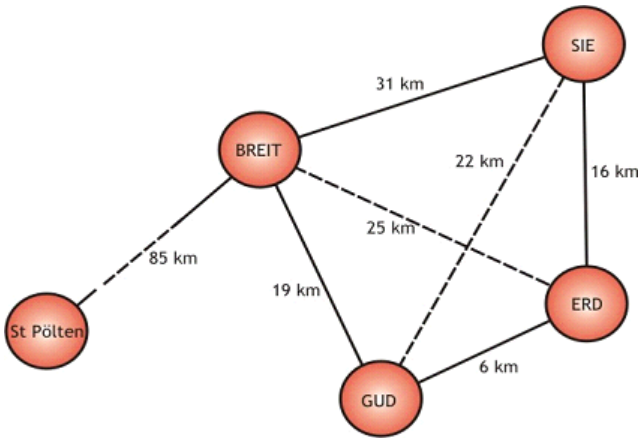

Figure 4.2: SECOQC project of a Quantum Backbone (QBB) network consisted of five nodes. Four of the nodes (GUD, ERD, SIE and BREIT) were located in Vienna while the last was situated at St. Pölten, 85 km out of the city. The QBB continuously produces keys and stacks them in the key management layer for use by nodes in the Quantum Access Network. The QBB comprises of various fibre based QKD links. (Source [101])

QBB were required to produce a secure key rate of 1 kbit/s over 25 km of fibre and downtime of less than a minute after a link failure.

Tokyo Quantum Network

The Tokyo Quantum Network demonstrated the commercial use of quantum networks by streaming an uninterrupted videoconference using keys distributed by the quantum network. The network architecture is similar to SECOQC with the three tier key distribution, management and usage layers [102]. The network, however, does not implement a QBB but rather extrapolates each node vertically between the physical and communication layers.

As shown in Figure 4.3, the Tokyo Quantum Network consists of 6 nodes. All the QKD links are implemented through fibre-based systems. The protocols used in the distribution of keys within the physical network include the BB84, Deferential Phase Shift, BBM92 and SARG04. While there were only four physical nodes, two patched links looped back to the same physical site simulating additional nodes. 50% of the fibre network that was used was aerial fibre creating lossy links and susceptibility to environmental factors. The fibres therefore experienced high levels of attenuation in the links, between 0.3 – 0.5 dB/km. The average QBER ranged from 2.3 – 3.8 % while the final secure key rate ranged from 0.25 – 304 kbps. The large variation in the secure key rate generation is due to both the link stability and the raw key rate of the individual systems [102]. These variations in rates should be compensated with sufficient redundancy when designing the network architecture. This will ease network congestion.

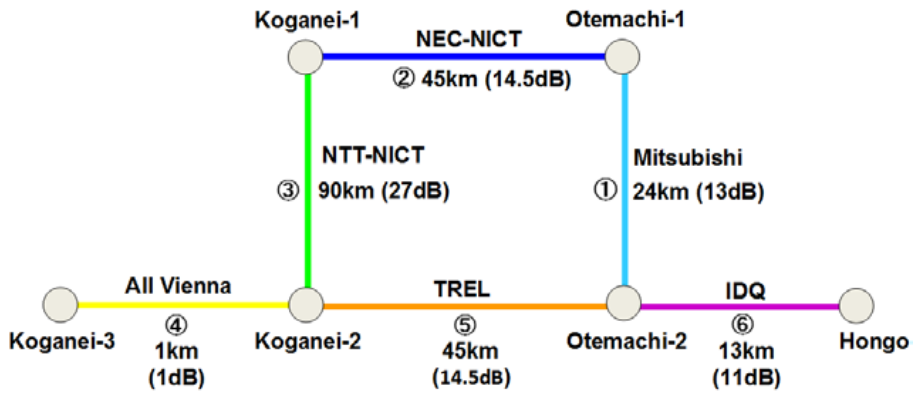

Figure 4.3: The Tokyo Quantum Network consists of a pure fibre network connecting various technologies into a hybrid communication solution. The network implements a layered approach as with the SECOQC project. It consists of 6 nodes that are extrapolated vertically from the physical layer to the communication layer to provide a transparent QKD solution. (Source: [102])

SwissQuantum Network

The SwissQuantum network is a realisation of a 3-node ring network focusing on the long-term stability of the QKD systems and supporting software. The project was run for 21 months across the Geneva Metropolitan network [103]. The systems used in the network were the plug and play units developed by id Quantique. The links varied between 3.7 and 17.1 km with losses of 2.5 – 5.3 dB, respectively.

The network deployed a layered approach with key management layers connected to a 10 Gbps high-speed conventional encryptor. The network was able to achieve high stability during the operational time of the quantum network [103].

4.2 QuantumCity Project

This section draws extracts from [15, 46, 88, 90, 104] that represents original work by the author.

The Durban–QuantumCity project seeks to test the long-term performance of QKD devices in a commercial environment. The City of Durban possesses optical fiber infrastructure that is primarily used to link some of the vital services of the Municipality [105]. The QuantumCity project uses this fiber infrastructure to provide QKD-secured communication between nodes on the network. This was the first QKD network to have been deployed in a commercial environment for extended periods of time.

4.2.1 *Network Architecture*

The QuantumCity project was a collaboration of the Centre for Quantum Technology (a Research Group at the University of KwaZulu-Natal), eThekwini Municipality, the Innovation Fund, and the Innovation Company of the University of KwaZulu-Natal. The network is required to operate at the physical and link layer of the network. In order for this to be implemented the eThekwini Municipality provided dedicated dark fibre pairs for use on the network. The fibres were required to be dark in order to facilitate the quantum communication. The quantum systems used in the deployment of the network was the IDQ Cerberis systems.

The physical layer of the quantum network consists of three point-to-point QKD links connected together in a star-configuration as shown in Figure 4.4. The transmitters (Station A) are housed within the trusted server while the receivers (Stations B) are installed in the peripheral nodes. This is due to the fact that the Station B consumes high amounts of electrical power in order to cool the detectors. A concentration of Stations B creates strain on the electrical grid. As the point-to-point links of the network accumulated at the central node, this link was assumed to be secure. The assumption is required as the communication is converted to plaintext within this node.

The network coverage extends through the suburbs of Pinetown and Westville in the eThekwini district. The quantum channels vary between 2.6 km to 27 km as illustrated in Figure 4.5 and Figure 4.6. The test-bed network connects the Pinetown Civic Centre to the eThekwini Architecture Office, Pinetown Clinic, and Westville Civic Centre. All the links were deployed within high traffic regions. The network is used as a platform to test the long-term stability of QKD systems in a commercial environment. The systems run and encrypt live data between the nodes. The data consists of data records, telephones, and internet traffic.

Each link is connected to the respective nodes through four fiber strands as shown in Figure 4.7. One fiber pair is used for the QKD process and data transfer while the second pair provides redundancy for system recovery should the quantum systems fail. The quantum-encrypted fiber pair utilises one core for the raw QKD process, while the other core is frequency modulated providing duplex communication between nodes at up to 1 Gbps. This fiber strand is used for both QKD post-processing communication, as well as the transfer of the encrypted data through Coarse WDM. The primary objective of the recovery pair is to provide uninterrupted communication through the links as the nodes serve the vital services of the Municipality. Any errors or failures of the equipment are reported through the Simple Network Management Protocol (SNMP). Each LAN within the premises is assumed secure while the server room at the Pinetown Civic Center, serving as the central node, is assumed trusted.

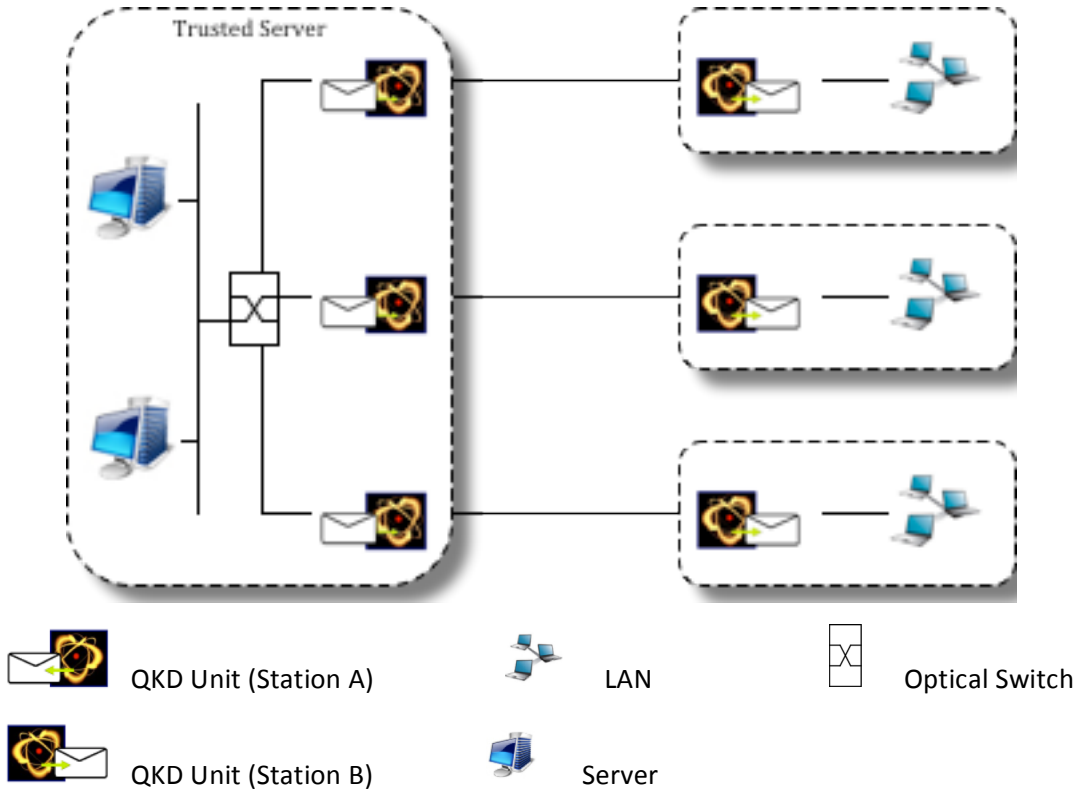

Figure 4.4: A schematic representation of the physical layer of the QuantumCity network. The quantum systems provide a gateway between the quantum MAN and their respective LANs. A single trusted node houses the Stations A of each link pair while each of the spokes contain a Station B.

Single-mode fiber is used throughout the network. The fibre was required to be dark due to the current restrains on multiplexing quantum communication. Further only all-optical links were used in the network as a further constraint due to the layer 1 nature of quantum communication. As the network uses laid fiber, the systems are ensured of good stability. Angled polished connectors (APC) were also used to ensure minimal reflective losses at fiber interconnections. The quantum signals operate at a wavelength of 1550 nm while the conventional communication is multiplexed at various other transmission windows such as 1310 nm and 1490 nm. The encryptors and QKD units were installed at the gateway of each building and the public network.

Figure 4.5: The layout of the test bed network for the QuantumCity project consists of a four-node star topology. All the links are connected via underground single-mode optical fibre. The lengths of the links vary between 2.6 km to 27 km.

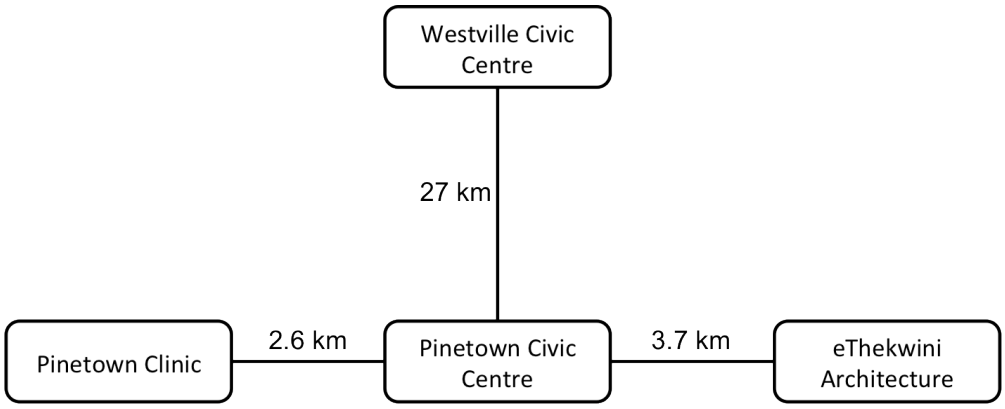

Figure 4.6: The Durban-QuantumCity network consists of a pure fibre network connected by three plug and play QKD systems. The network implements a layered approach. The physical layer is used for key exchange while the key is then stacked in high-speed layer 2 encryptors in order to accommodate the information flow. The Pinetown Civic Centre was used as the central node while the peripheral nodes consisted on the Pinetown Clinic, eThekwini Architectural Office and the Westville Civic Centre.

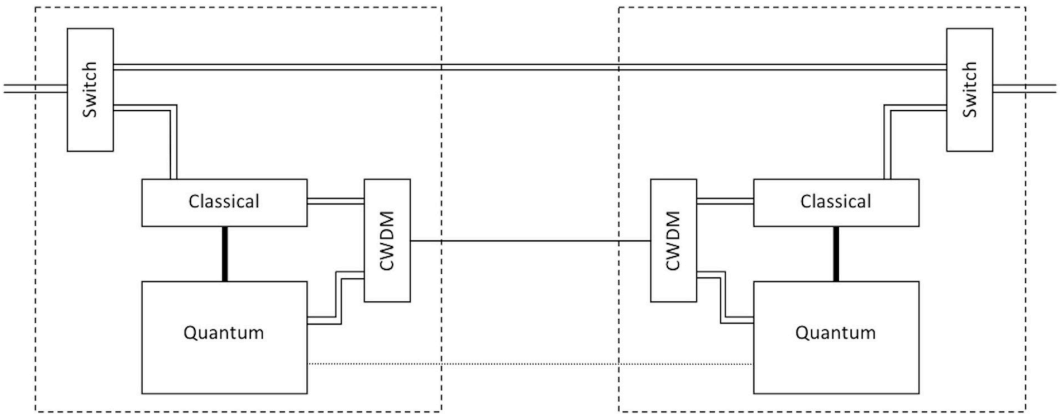

Figure 4.7: A schematic of the physical fibre connections used for each of the links in the QuantumCity project. Two fibre pairs at utilised within each link. One pair of fibres is used for the quantum key exchange process and classical encryption while the other remaining fibres serves as a redundant pair. A switch provides the *failsafe* mechanism. The primary pair uses Coarse Wavelength Division Multiplexing (CWDM) for duplex communication over one strand and a dedicated strand for the quantum key exchange.

The QKD systems implement the BB84 protocol [10] with error correction and privacy amplification. The BB84 protocol is realised through an auto-compensating *plug-and-play* system [39]. The plug-and-play system is a phase encoded QKD system based on a prepare and measure scheme. The plug-and-play technique makes use of a Faraday mirror and one bidirectional interferometer. The pulses travel through a closed loop reversing the birefringence effects of the fiber on the photon. The Faraday mirror, together with polarisation dependent beam splitters at the interferometer, provides enhanced visibility to the system. The secure keys generated by the QKD systems are passed up to the conventional encryptor and stacked for future use.

The systems used in the QuantumCity network operate at multiple layers. The QKD process is validated, undertaken and processed at the physical layer through dedicated fibres as illustrated in Figure 4.7. The secure keys are then stacked at a Data Link Layer where they are used by a classical encryptor for use as primary session encryption keys. In these systems, the QKD replaces the conventional public key distribution process for the sharing of the primary key. An AES key expansion mechanism [4] is then used to expand the primary key to provide suitable key rates. The complete solution provides a transparent layer-2 encryption to all passing data.

The trusted server is the hub of the network. While it routes information between peripheral nodes, it does not store this information. However the information is decrypted and re-encrypted using a new key previously shared with the recipient of the message. The presence of plaintext within the node is the primary reason the node must remain trusted. A number of physical measures including access control and surveillance can be used to enhance the security of the

trusted node. The successfully distributed quantum keys are stacked in the layer 2 encryptor and operate on a First In First Out (FIFO) basis. The stacks are secured through a RSA 2048 bit key. The systems provide an SNMP notification on failures. A fail-safe mechanism through a convention key distribution and encryption ensures a secure uplink in the case where the quantum systems go down.

4.2.2 *Results*

The visibility of the fiber is defined as the ratio of the intensities of the interfered wave and the sum of the original waves. The visibility is measured to track the stability of the fiber due to environmental factors. These factors include temperature fluctuations and mechanical stress. Fluctuations in these parameters would cause the signal coherence to decrease, thus increasing the error rate. The temperature fluctuation alters the properties of fiber thus creating additional stresses and birefringence within the fiber thereby desynchronizing the system.

The Raw Key Rate (RKR) does not, however, provide a complete and feasible assessment of the apparatus. The quantum bit error rate (QBER) is the ratio of the incorrectly distributed qubit as compared to the total distributed qubits [39]. The QBER comprises errors caused by the transmission line and detector imperfections. Dispersion and scattering along the fiber are the major cause of QBER in the transmission line. As the system operates on telecommunication wavelengths, InGaAs detectors create substantial dark-counts and after-pulses that are non-negligible when calculating the QBER. Due to a finite QBER, it is assumed that some information regarding the key would have been leaked to an eavesdropper. The potential information of the eavesdropper is minimised through the use of conventional error correction and privacy amplification routines [2]. The resultant key string is reduced in length and hence the final secure key rate (SKR) together with the secrecy level of the key ultimate characterise the QKD system. The QKD parameters presented in Figure 4.10 and Figure 4.11 were plotted at intervals of 20 min.

The QuantumCity links were commissioned in a staggered approach as shown in Figure 4.8. This was due to the availability of the links as the eThekweni was undergoing an active roll out of their network. Further the two of the links were decommissioned in 2010 to accommodate the QuantumStadium project as presented in Section 4.3.

The first link of the QuantumCity project was installed between the Pinetown Civic Centre and the Pinetown Clinic on February 17, 2009. A picture of the installed units in the trusted node (Pinetown Civic Centre) is shown in Figure 4.9. The link has been encrypting all the live data between the two buildings since September 2009. The fiber link is 2.6 km in length and completely consists of underground laid fiber. The system's overall performance has been stable during its operational period. The system achieved a QBER of 1.7% with an average final secure key rate of 981 bits/s during the 3 month session.

The visibility of the system was calculated at 99.5% and has remained stable. The stability of the system was assisted by the fact that the fiber was laid underground thus minimizing mechanical stresses in the form of vibrations, compressions, and extensions. Furthermore, as the fluctuation times for both temperature and external stresses was greater than the time of flight of the photon in the auto-compensating setup, the stability of the system was optimised.

The RKR fluctuated between 10000 bits/s and 13000 bits/s with a standard deviation of 452.63. Figure 4.10 shows the QBER for the three links of the QuantumCity network. The corresponding SKR for the links is presented in Figure 4.11. The Pinetown Civic Centre–Clinic link averaged a QBER of 1.7% and has a standard deviation of 8.57×10^{-4}. Various periods within the sketched timeframe have substantially higher QBER. This is due to the fact that road works were being conducted for the installation of new water pipes in the area during that period.

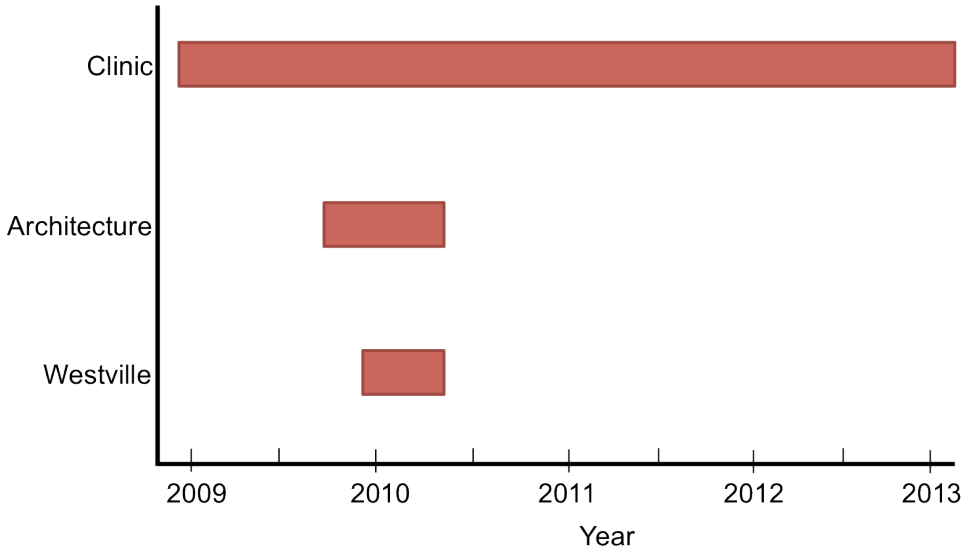

Figure 4.8: Deployment of the QKD links during the QuantumCity project was implemented in a staggered approach. This was due to the active roll out of the eThekweni fibre during this time. Two links were later decommissioned to accommodate the QuantumStadium project. Currently one link is still active.

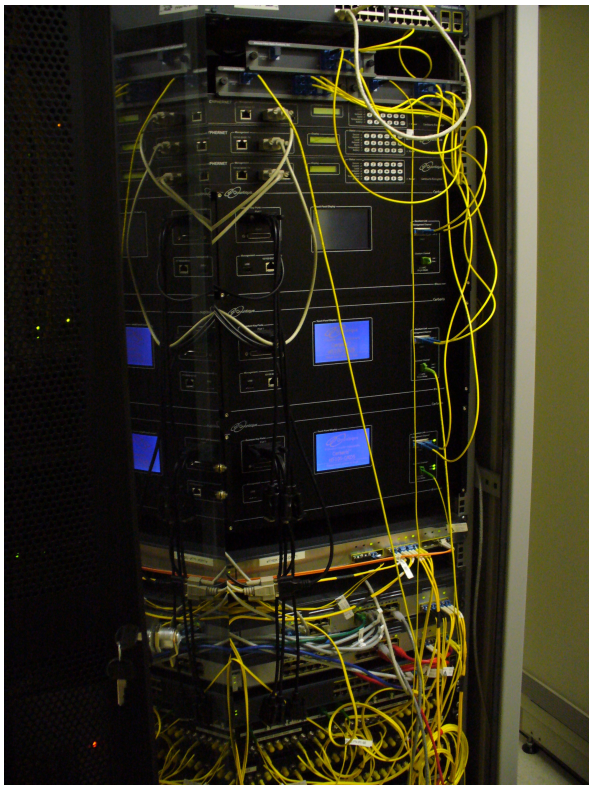

Figure 4.9: The installed equipment for the central node (Pinetown Civic Centre) of the QuantumCity project consists of 3 sets of layer 1 QKD systems and layer 2 encryptors.

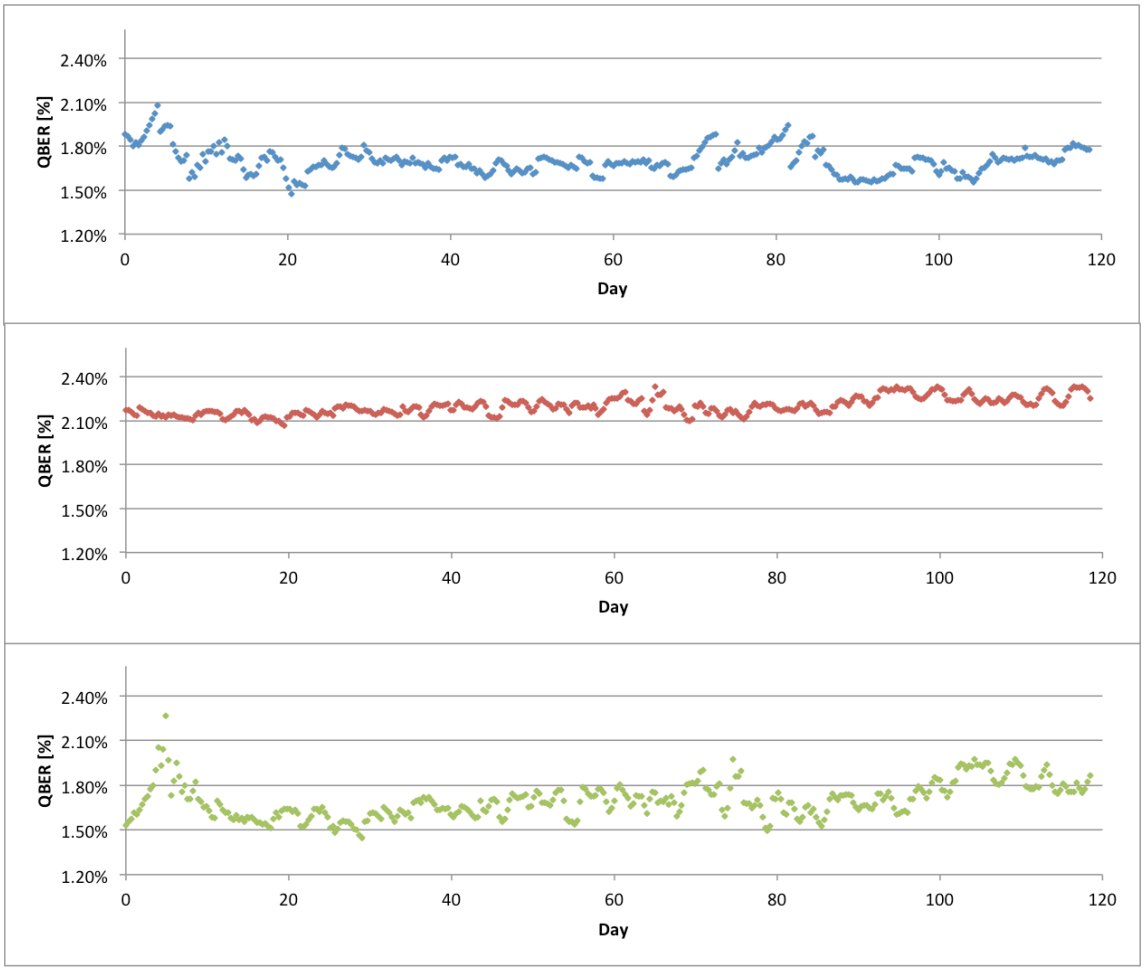

Figure 4.10: The Quantum Bit Error Rate (QBER) for the three links of the QuantumCity network maintained a relatively stable state. The data is represented above was collated over 118 days between January 2010 to March 2010. The blue data indicates the measurements of the link to the Pinetown Clinic, the red data indicates the measurements of the link to the eThekweni Architectural Office and the green data points indicate the measurements of the link to the Westville Civic Centre.

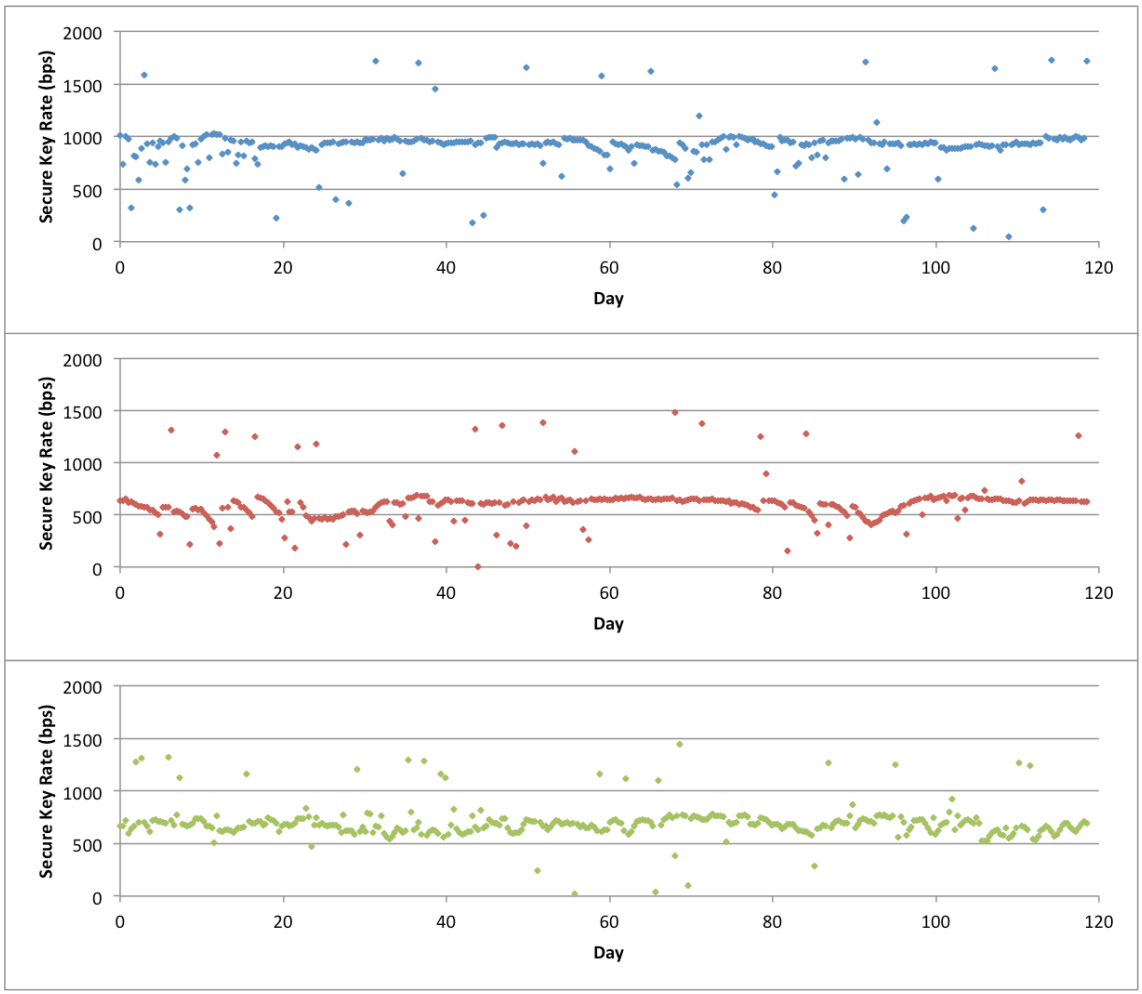

Figure 4.11: The Secure Key Rate (SKR) for the three links of the QuantumCity network maintained a relatively stable state. It is noted that the systems recalibrated when the SKR dropped below a threshold. The data is represented above was collated over 118 days between January 2010 to March 2010. The blue data indicates the measurements of the link to the Pinetown Clinic, the red data indicates the measurements of the link to the eThekweni Architectural Office and the green data points indicate the measurements of the link to the Westville Civic Centre.

The link between the Pinetown Civic Centre and the Pinetown Clinic has run continuously running since 2009. The SKR for this duration is averaged at 977 bits/s and is presented in Figure 4.12. The graph depicts the average SKR over 2 hour intervals. It is noted that the link has remained stable since installation.

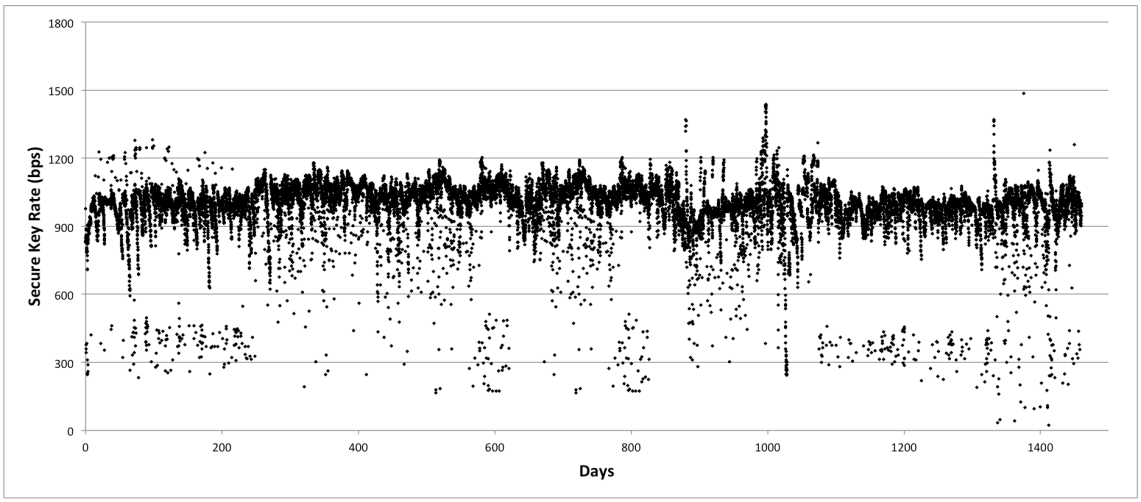

Figure 4.12: The QKD link between the Pinetown Civic Centre and the Pinetown Clinic has been running since 2009. The secure key rate for this link has remained stable at an average of 977 bits/s throughout this period. The link is still live and operates to secure the transfer of patient records and all communication to and from the Clinic.

It is noted that the graph illustrates that the QKD system has been operating at 450 bps fairly often however rarely at 600 bps. This plot depicts such behavior due to the averaging algorithms used to reduce the number of data points. As noted each point depicts the average rate over 2 hours. Due to the unsuccessful distribution of keys during some periods, the average rate will decrease, hence the reduced key rate.

The commercial implementation of the system was met with various challenges. The foremost challenge was the commissioning of dedicated dark fiber. This is a major drawback to widespread use of quantum secured communication systems as it severely restricts the bandwidth and the versatility of the networking infrastructure. However, there are many groups currently investigating techniques to overcome this bottleneck. Most work in this field is focused around the use of WDM techniques [74]. The physical, layer 1, implementation of the system requires an all-optical link that further restricts the deployment of quantum key distribution systems as most sites connect through an exchange. This will be partially addressed through the next generation of all-optical networking techniques that operate at a layer-1 level providing all-optical linkages thus improving networking speeds. QKD engineers will still, however, have to overcome issues of cross-talk and attenuation at these exchanges. The supporting software technology around QKD also requires much attention towards the development of multiplatform key exchange servers. This would require standardisation of QKD technology that is currently being undertaken by the Quantum Group at the European Telecommunication Standards Institute.

The second link of the QuantumCity project connects the Pinetown Civic Centre and the eThekweni Architecture Offices. The effective fiber distance is 3.7 km. The link was installed in November 2009. The data transferred through the network include telephone, internet, email, and data retrieval. This link was lossy due to the patches and interconnects. The total loss of the link was 1.6 dB. The systems produced an average secure key rate of 573 kbps with a QBER of 2.2%. The QBER and SKR for this link during a 118-day duration are presented in Figure 4.10 and Figure 4.11, respectively.

The Pinetown Civic Centre to Westville Civic Centre link services critical data and high network traffic as both sites are disaster recovery stations for the eThekweni network. This link was commissioned in December 2009 for 3 months. As the equipment used in this link was required for the installation of the QuantumStadium project, the link was decommissioned in March 2010. The effective fiber distance of this link is 27 km with an attenuation of 6.8 dB. The visibility remained constant at 98%. The systems produced an average secure key rate of 519 kbps with a QBER of 1.7%. The QBER and SKR for this link during a 118-day duration are presented in Figure 4.10 and Figure 4.11, respectively.

4.3 QuantumStadium Project

This section draws extracts from [46, 89, 104] that represents original work by the author.

The QuantumStadium project is an extension of the QuantumCity initiative that provided the quantum-based encryption during the 2010 FIFA World Cup™. The purpose of the project was to employ QKD-based security in a live environment with real time data of various types. The QuantumStadium project was the first implementation of a QKD platform during a globally relevant event. The network carried voice, email and data traffic between the two buildings. It was installed in April 2010 and was decommissioned the end of the 2010 FIFA World Cup™.

As this project was an extension of the QuantumCity initiative it shared a similar network architecture. A single layer 1 QKD solution underpinned the communication security. The distributed keys were stacked in two layer 2 encryptors with a second encryptor connected as a fail-safe mechanism as illustrated in Figure 4.13.

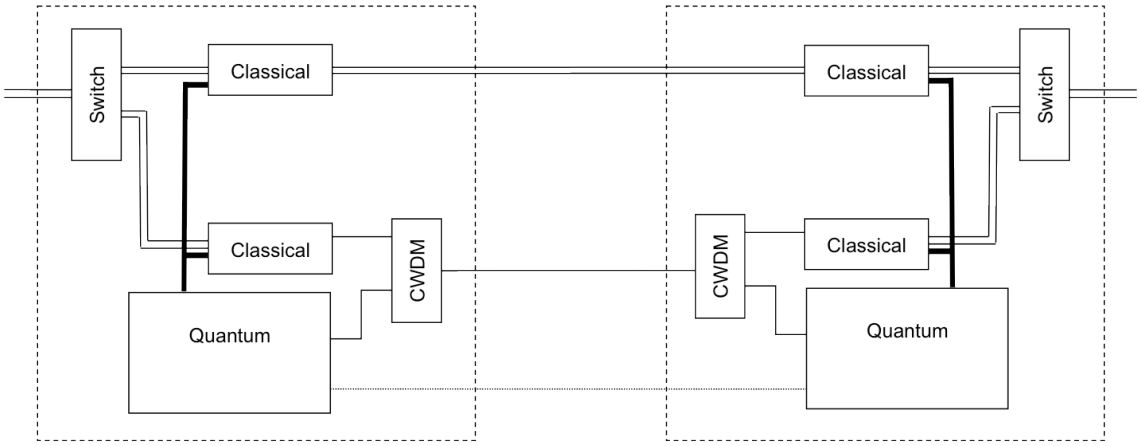

Figure 4.13: A schematic of the QuantumStadium link is presented. Due to the critical nature of the information transferred along this link, both the primary and redundant pairs of fibres were encrypted. One fibre from the primary pair was used for the quantum key exchange process while the other remaining fibre served as a classical communication over a duplex, Coarse Wavelength Division Multiplexed (CWDM) fibre. A switch provides the failsafe mechanism.

The network was a two-node network linking the Venue Operations Centre at the Moses Mabhida Stadium to the Joint Operation Centre in the City of Durban through two independent links as illustrated in Figure 4.14. The redundant fibre pair (red) connected between the two nodes to reduce any downtime on the link. In the primary fibre pair (green), one strand is used for the raw QKD process, while the second fibre runs in duplex mode to facilitate the QKD post processing and transfer the encrypted data.

The primary link, on which the QKD system connected, was 2.62 km in length with one patch at the Old Fort road police station. The attenuation was compounded due to the patch cords and was rated at 1.9 dB.

Figure 4.14: Network structure of the QuantumStadium project linked the on-site Venue Operations Centre (VOC) to the off-site Joint Operations Centre (JOC). A dual link was used to prevent any downtime during the operation of the units.

The statistics of the stability of the QKD solutions duration of the 2010 FIFA World Cup™ is presented in Figure 4.15 and Figure 4.16. The measurements are depicted as a daily average. The visibility of the system was calculated at 99.3%. It remained stable for the duration of the measurements. The stability of the system was assisted by the fact that the fibre was laid underground thus minimizing mechanical stresses.

The SKR fluctuated between 400 bps and 1800 bps during the event. A spike in the QBER on 22 June 2010 was associated with fibre maintenance conducted at Old Fort road police station on that day. The theoretical estimate of the SKR, as calculated in Section 2.3.4 on page 22, depicted in red in Figure 4.15 is closely followed by the experimental data. The variation maybe attributed to the uncertainty associated with the QBER.

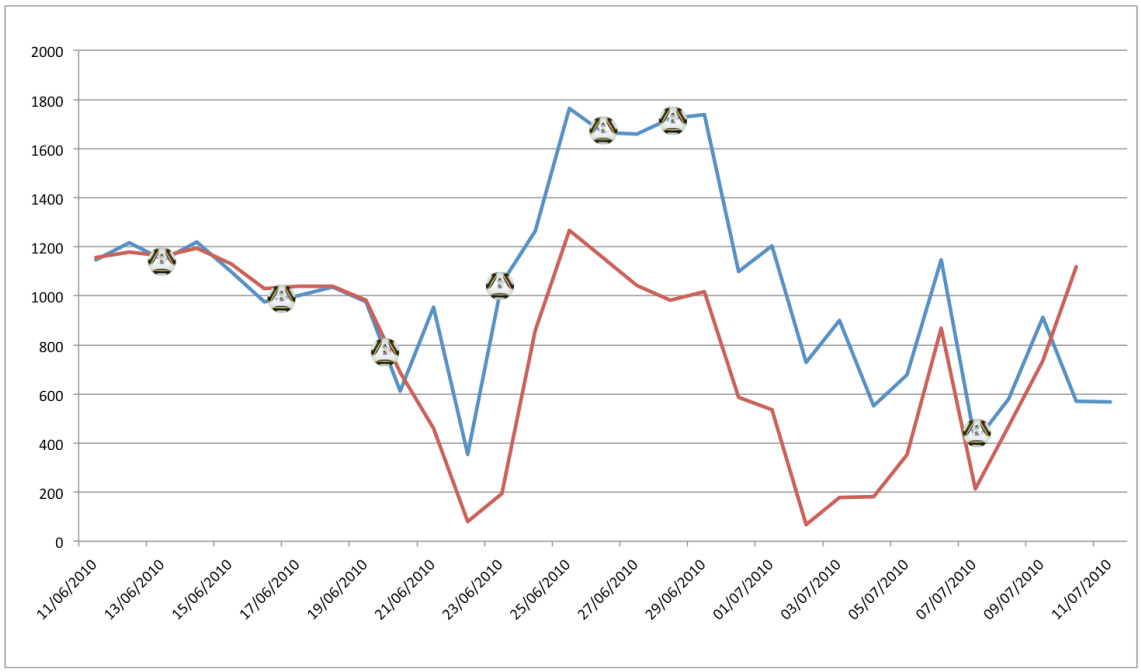

Figure 4.15: The Secure Key Rate (SKR) of the QKD system implemented during the 2010 FIFA World Cup™. The rate is depicted as a daily average and the soccer balls denote match days at the Moses Mabhida Stadium. The blue graph represents the experimentally measure SKR while the red graph represents the theoretical values as calculated by the Raw Key Rate and the QBER.

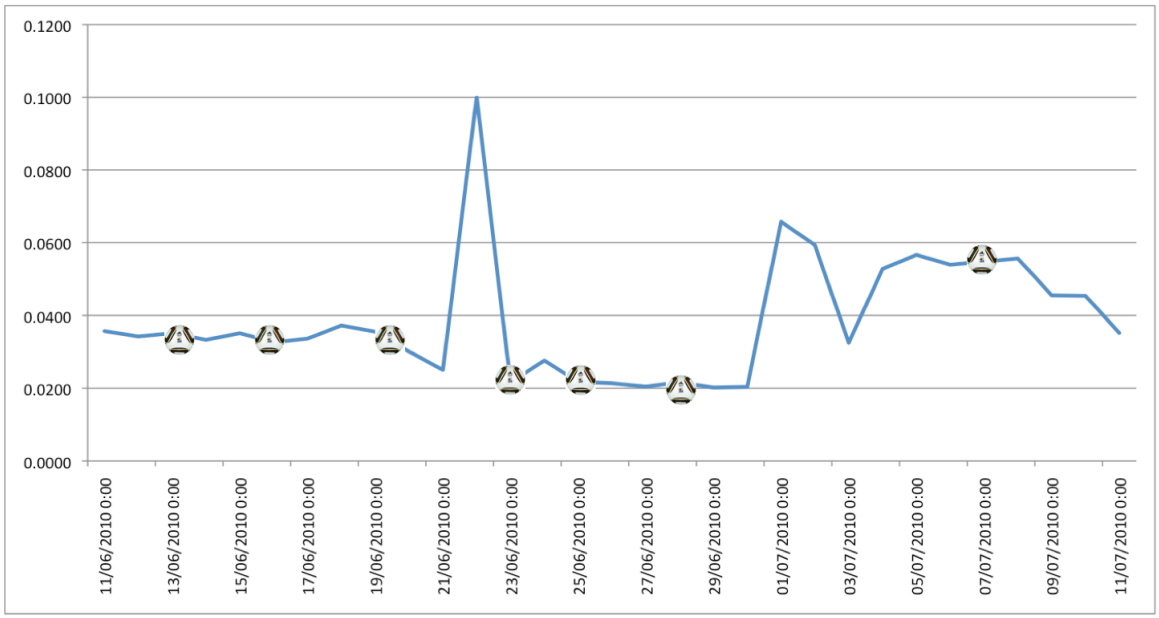

Figure 4.16: The Quantum Bit Error Rate (QBER) of the QKD system implemented during the 2010 FIFA World Cup™. The rate is depicted as a daily average and the soccer balls denote match days at the Moses Mabhida Stadium.

4.4 Global Quantum Network Initiatives

This section draws extracts from [106] that represents original work by the author.

A global QKD network will consist of quantum Metropolitan Area Networks (MAN) linked together through mobile trusted relays. The relays would form a Global Area Network (GAN) providing global connectivity to the participating MANs. The MANs will plug into the quantum GAN through a trusted gateway. These gateways will be responsible for key storage and allocation across the quantum GAN.

The necessary requirements for a quantum GAN are high throughput communications and a global coverage. The mobile nodes and access points to the GAN through the gateway are considered to be trusted currently. The development of quantum memories will relax this condition.

Both satellites and aircrafts fulfill the above conditions, however the access points to an aircraft-based quantum GAN host a distinct advantage.

Satellite-based quantum GAN

The use of satellite technology in achieving a global quantum secured communication network has been of interest in the past few years. Many feasibility tests have been conducted [84, 85, 87, 107] however various challenges still need to be addressed prior to the realisation of a ground to satellite QKD link. These challenges are mainly associated with spatial and temporal synchronisation of the stations. The use of LEO satellites permits an uplink time for QKD synchronisation of approximately 10 minutes per session. A high-speed synchronisation will therefore be required for an efficient and stable communication link. An advanced tracking system is therefore critical to such an implementation [87]. Due to the relatively high speeds of the satellite the Doppler effect and time variations due to relativity must also be compensated. Together with the above, the general challenges of atmospheric parameters (temperature, visibility, weather and background noise) that are associated with free-space communication may further limited and degrade the contact time for the quantum key exchange.

In this technique the satellites are considered to be trusted nodes. The nodes travel between various MANs creating a global backbone encryption key resource. The satellite network therefore requires an access point at each participating MAN network. The access point will require, further to a robust QKD link, the communication infrastructure to provide gateway functionality to the Metropolitan area. Unfortunately, most sites that are good for ground-to-satellite links are in relatively remote and isolated in their surroundings. Although this ensures better visibility, it lacks the infrastructure to support a commercially viable global access point.

Aircraft-based quantum GAN

The commercial aircrafts' network is another secure transport mechanism to support the global quantum GAN. Commercial airliners create an ideal alternate global network for key distribution in terms of coverage, reliability and gateway uptime time. Further the airports at each connected city have the appropriate supporting infrastructure to serve as an access point for the MANs to the global network.

The QKD process, implemented in the proposed scheme, will occur whilst the aircraft is docked at the airport. This allows a simple fibre-based QKD system to be used for the key distribution process. Due to the use of a fibre channel, the solution bypasses the additional synchronisation techniques required when using a satellite-based network. The frequency and reliability of the link, further enhances the opportunities that this option has to offer.

The commercial airliners provide global linkages between the MANs of participating cities. Hence the respective airports serve as gateways to the quantum GAN. Each aircraft is to be fitted with a tamper-proof QKD unit in the communications hub in the hull of the aircraft. This is a highly restricted zone and therefore can be assumed as a secure location. This unit will be responsible for the quantum-secured key distribution between itself and the sister unit stationed in the respective airport through an authentication process. The secure key management center, within the airport building, will then manage the storage and distribution of keys. This, in total will provide the access point to the MAN. Information can be encrypted on site and safely propagated through conventional communication networks or the keys sold onwards to the respective clients.

The QKD procedure for the aircraft-based quantum GAN will employ the general algorithm for trusted relays as follows:

The qubit source, the QKD transmitter, will be installed into the carrier aircraft and the detectors, QKD receiver, into the participating airports.

The carrier aircraft will dock at a gate for disembarkment, preparation for the next flight and boarding of passengers. During this time the diagnostics cable will be connected to the aircraft. This will also contain the dark fibre for the QKD process.

- QKD will be conducted between the aircraft and the departing airport while docked at the Airport A.
- This initial key, k_A generated between the aircraft and airport A, will then be stored in a secured memory within the QKD station in the aircraft.
- After docking at the arriving airport, Airport B, a second key is generated between the aircraft and Airport B, k_B.
- An XOR function is then employed to encrypt k_A with k_B using a One Time Pad. This securely transfers k_A to the Airport B.

- The two airports then share a secure key ready to be used. The secure key management layer will control the flow and distribution of these keys.
- The local quantum MAN may then be used to distribute the keys further to end users within the network using local QKD links.

Benefits of the aircraft-based quantum GAN

There are major components to the quantum GAN, namely:

- the GAN nodes,
- the access point between the MAN and GAN and
- the link between the access point and the GAN.

Both the quantum GAN implementations mentioned in this thesis utilise mobile trusted relays as the GAN nodes. Both serve to produce a global coverage however satellites-based networks will have access to remote locations (such as a military outpost) while the aircraft-based network will have a wider coverage between cities. The use of airports as an access point to the quantum GAN is ideal for due to the facilities offering ample redundancy, connectivity and storage for both the MAN and GAN. Quantum communication with a satellite will dictate that the ground station be situated in a relatively isolated area to ensure that the communication is not disrupted through light saturation.

The most promising benefit of the aircraft-based quantum GAN is the fibre link at the gateway of the GAN as opposed to a free-space link for ground to satellite linkages. Due to the fibre links, the MAN gateway will be more reliable and robust as such connections are not weather dependent. It further allows one to strategise and manage the keys more effectively as the key production rates and frequencies are periodic and predictable.

The above system is intended to be the next extension to the QuantumCity initiative.

5. CONCLUSION

The engagement of photonics and quantum physics is merging to shape a revolutionary new trend in ICT. Creating a technology platform for the control and manipulation of quantum systems will establish the capabilities to participate in the development of Quantum Information Processing and Communication (QIPC). The growth of such a knowledge pool is critical as we head towards a nanotechnology revolution of the ICT industry.

The research presented in this thesis represents various aspects of a practical QKD solution. The thesis summarises the experimental efforts in QKD by the Centre for Quantum Technology at the University of KwaZulu-Natal. The Centre investigates both aspects of the QKD system, such as random number generators and polarisation compensation and tracking, as well as optimising the deployment of quantum communication solutions as part of the QuantumCity initiative.

The focus of the investigations was the adaptation of conventional optical technology to suit the needs of quantum communication. A strategic set of research initiative have been undertaken to create a robust Quality of Service of the quantum photonics enabled network. In particular, the coverage, reliability, delay and bandwidth of the network have been considered. This conventional-quantum hybrid technology is an ideal short-term solution to engage quantum communication with mainstream ICT. The efforts towards this compatibility will remain transparent to the emerging quantum technology based devices such as quantum memories and repeaters. The culmination of all the above creates a complete technology platform for QIPC devices.

The author has been the principal researcher for the solution deployment based investigations presented in Chapter 4 and a co-researcher for the system development initiatives presented in Chapter 3 of this thesis.

5.1 Critical Assessment

The development the QKD system has focused on aspects including the prototyping of components, the investigation of encoding mechanisms and system optimisation techniques. This thesis focused on the development of a physical random number generator based on the shot noise of a Zener diode. While the generator does not involve quantum optics for the production of quantum random number sequences it promotes a cheap and easily implementable product that has a quantum mechanical base for the randomisation process. The generator produces a good quality of random sequences as has been demonstrated through various tests. Due to the electronic nature of the random number generator, electromagnetic shielding and the robustness of the physical design are still to be developed and tested.

Polarisation-encoded QKD in fibre has been actively researched for many years. The polarization compensation technique presented in this thesis differentiates from previous works due to the analytical technique used to find the inverse rotational transformation. The technique uses an active method of isolating the plane of polarisation through a step search rather than just a point on the Poincaré sphere. This allows for a reduction in equipment in the setup and hence the cost of the unit. While the initial calibration of the system takes longer than the previous efforts, the proposed system can, in principle, compensate for any two bases. Together with a system development, this compensation technique will allow future investigations into free space-fibre coupled QKD links.

Polarisation tracking is an integral component for mobile QKD units, in particular satellite stations. The proposed tracking technique allows the QKD unit to orientate itself in alignment with the transmitters polarisation axis. This technique is simple in its implementation but does not account for elliptical polarisation. The lack of birefringence in the atmosphere allows the current setup to provide suitable results for laboratory-based experiments. The next iteration of system development will take further polarisation changes into account. This needs to be investigated due to the possibility of various contaminants within the atmosphere and possible line of sight links that may cause phase retardation of light.

5.2 Future Work

The QuantumCity initiative is a long-term project supported by the eThekwini Municipality. The network has been in operation since 2009 and currently one of the three links is still operational. The remaining links are waiting to be recommissioned.

The network has provided substantial insight into the long-term stability of QKD systems and the versatility of the applications it may serve. The QuantumCity network achieved stable long-term results for both the QBER and SKR. Due to the current limitations of the QKD systems, in particular power and bandwidth requirements and cost implications, the network architecture

needs to be reconsidered. The optimal configuration of hybrid channels and devices must remain confined within the physical layer of the network. Secure transport protocols for key management need to be integrated into the QuantumCity network.

As the QuantumCity project focuses on *adapted conventional networking technology*, a further investigation into the routing of qubits within an optical network is to be considered. This includes the use of untrusted conventional networks through current optical networking tools such as switches, multiplexers and cross connects to establish connection-orientated linkages. WDM must play an integral role in this deployment for the combination of quantum and bright signals on a single optical fibre. Such all-optical implementations parameterise the network for a natural progression towards *quantum enhanced networking technology* to generate improved Quality of Service of quantum communication.

6. BIBLIOGRAPHY

1. Mollin, R., *An Introduction to Cryptography*. Second ed, 2007, USA: Chapman & Hall CRC.
2. Konheim, A., *Cryptography: A Primer,* 1981: John Wiley & Sons Inc.
3. Gisin, N., et al., *Quantum Cryptography.* Review of Modern Physics, 2002. **74**. p. 145-195.
4. Schneier, B., *Applied Cryptography,* 2007: John Wiley & Sons.
5. Ferguson, N. and B. Schneier, *Practical Cryptography,* 2003: John Wiley & Sons Inc.
6. Kahn, D., *The Code Breakers,* 1967: Macmillian Pub. Co.
7. Shannon, C., *Communication Theory of Secrecy Systems.* Bell System Technical Journal, 1949. **28**: p. 656–715.
8. Blahut, R., *Principles and Practice of Information Theory,* 1987: Addison-Wesley.
9. Wiesner, S., *Conjugate Coding.* SIGNAT News, 1983. **15**(1): p. 78-88.
10. Bennett, C.H. and G. Brassard. *Quantum cryptography: Public Key Distribution and Coin Tossing*. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984. Bangalore, India. (1984), pp. 175-179.
11. Lenhart, G., *ETSI QKD ISG*, 2008. Available online from: http://www.etsi.org/website/technologies/qkd.aspx.
12. Renner, R., *Security of quantum key distribution.* International Journal of Quantum Information, 2008. **6**(01): p. 1-127.

13. Mirza, A. and F. Petruccione. *Centre for Quantum Technology*. 2011; Available online from: http://quantum.ukzn.ac.za.
14. Bhatt-Chauhan, D., *Using quantum cryptography for network security*, in *From science to business,* 2011, Institute of Physics: UK. p. 3-4.
15. Mirza, A., F. Petruccione, G. Lenhart and G. Ribordy, *Quantum Key Distribution - A World First for Durban.* Quantum Journal, 2010, **10**(5): p. 11-12.
16. Furuta, A., *Tokyo network startup to production quantum cryptography.* Scientific American (Japanese Edition), 2011. **2011**(1): p. 86-91.
17. Bennett, C., *The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working!* SIGNAT News, 1989. **20**(4): p. 78-82.
18. Qian, Y. and Z. Sheng-mei, *Quantum key distribution based on Orbital Angular Momentum*, in *12th IEEE International Conference on Communication Technology (ICCT),* 2010: Nanjing, China. IEEE. p. 1228-1231.
19. FBI *Annual Report on Cybercrime*. 2009; Available online from: http://www.ic3.gov/media/annualreport/2009_ic3report.pdf.
20. Davis, L., et al. *2011 Top Cyber Security Risks Report*. 2011; Available online from: http://www.hpenterprisesecurity.com/cybersecurityrisks.
21. Bogdanov, A., D. Khovratovich, and C. Rechberger, *Biclique cryptanalysis of the full AES.* Advances in Cryptology–ASIACRYPT 2011, 2011: p. 344-371.
22. Dunkelman, O., N. Keller, and A. Shamir, *A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony*. In *Advances in Cryptology – CRYPTO 2010*, Ed. T. Rabin. 2010, Springer Berlin Heidelberg. p. 393-410.
23. Rivest, R., A. Shamir, and L. Adelman, *A method of obtaining digital signatures and public key cryptosystems.* The Communications of the ACM, 1977. **21**: p. 120-126.
24. Shay, W., *Understanding Communication Networks,* 2004: Thomson.
25. Scarani, V., *Quantum Physics: A First Encounter: Interference, Entanglement, and Reality,* 2006, Oxford UK: Oxford University Press.
26. DeBroglie, L., *Matter and Light-The New Physics,* 2007: Campbell Press.
27. Krane, K., *Modern Physics,* 1996: John Wiley & Sons Inc.
28. Nielsen, M.A. and I.L. Chuang, *Quantum Information Processing and Communication*2002, United Kingdom: Cambridge University Press.
29. Zettili, N., *Quantum Mechanics: Concepts and Applications,* 2009: John Wiley & Sons Inc.
30. Koashi, M., *Unconditional security of quantum key distribution and the uncertainty principle*, in *Journal of Physics: Conference Series.* 2006, IOP Publishing **36**(1) p. 98.

31. Chen, G., et al., *Quantum Computing Devices: Principles, Designs, and Analysis,* 2006, USA: Chapman & Hall CRC.
32. Bužek, V. and M. Hillery, *Quantum copying: Beyond the no-cloning theorem.* Physical Review A, 1996. **54**(3): p. 1844–1852
33. Lo, H.-K., *Proof of unconditional security of six-state quantum key distribution scheme.* arXiv preprint quant-ph/0102138, 2001.
34. Ekert, A., *Quantum cryptography based on Bell's theorem.* Physical Review Letters, 1991. **67**(6): p. 661-663.
35. Scarani, V., et al., *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations.* Physical Review Letters, 2004. **92**(5): 57901.
36. Lo, H.-K., X. Ma, and K. Chen, *Decoy State Quantum Key Distribution.* Physical Review Letters, 2005. **94**(23): 230504.
37. Mach, E., *The principles of physical optics: an historical and philosophical treatment*. 1926: Taylor & Francis.
38. Shannon, C.E., *A mathematical theory of communication.* ACM SIGMOBILE Mobile Computing and Communications Review, 2001. **5**(1): p. 3-55.
39. Ribordy, G., et al., *Fast and user-friendly quantum key distribution.* Journal of Modern Optics, 2000. **47**: p. 517-531.
40. Hiskett, P.A., et al., *Long-distance quantum key distribution in optical fibre.* New Journal of Physics, 2006. **8**(9): 193.
41. Schmitt-Manderbach, T., et al., *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km.* Physical Review Letters, 2007. **98**(1): p. 010504.
42. Alleaume, R., et al., *Topological optimization of quantum key distribution networks.* New Journal of Physics, 2009. **11**(7): 075002.
43. Peev, M., et al., *The SECOQC quantum key distribution network in Vienna.* New Journal of Physics, 2009. **11**(7): 075001.
44. Tanenbaum, A.S., *Computer Networks*. Forth ed, 2007, New Dehli: Prentice-Hall of India.
45. Mirza, A., *Towards Practical Quantum Cryptography*, MSc Dessitation, 2009, University of KwaZulu-Natal: Durban.
46. Mirza, A. and F. Petruccione, *Recent Findings from the Quantum Network in Durban*, in *QCMC 2010*, T. Ralph and P.K. Lam, Editors. 2010, American Institute of Physics: Brisbane, Australia. p. 35-38.

47. Elliott, C., et al., *Current status of the DARPA quantum network* in *Quantum Information and Computation III*, E. Donkor, A. Pirich, and H. Brandt, Editors. 2005, SPIE. p. 138-149.

48. Peev, M., et al., *The SECOQC quantum key distribution network in Vienna.* New Journal of Physics, 2009. **11**(7), 075001.

49. Pillay, S., A. Mirza, and F. Petruccione, *Polarisation encoded quantum key distribution in fibre*, in Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, edited by I. Basson and A.E. Botha (University of South Africa, Pretoria, 2011), pp. 426 - 431. ISBN: 978-1-86888-688-3. Available online from: http:\\www.saip.org.za

50. Schindler, W. and W. Killmann, *Evaluation criteria for true (physical) random number generators used in cryptographic applications.* Cryptographic Hardware and Embedded Systems-CHES 2002, 2003: p. 431-449.

51. Marsaglia, G., A. Zaman, and W. Wan Tsang, *Toward a universal random number generator.* Statistics & Probability Letters, 1990. **9**(1): p. 35-39.

52. Marsaglia, G., *DIEHARD Test suite*, 1998, Technical report, http://www.stat.fsu.edu/pub/diehard.

53. Soto, J., and L. Bassham. *Randomness testing of the advanced encryption standard finalist candidates*. Booz-Allen and Hamilton Inc. McLean VA, 2000.

54. Sizer, Richard. "Information technology security evaluation criteria." *Computer Bulletin,* **5** (1993): pt 5/7/1993, no. Ser 4

55. National Security Agency, *Common Criteria for Information Technology Security Evaluation.* DTIC Document. 2002. ADA406677

56. Matsumoto, M. and Y. Kurita, *Twisted GFSR generators ii.* ACM Transactions on Modeling and Computer Simulation (TOMACS), 1994. **4**(3): p. 254-266.

57. Severence, F.L., *System Modeling and Simulation: An Introduction* 2009, Chichester, UK: John Wiley & Sons.

58. Schmidt, H., *Quantum‐Mechanical Random‐Number Generator.* Journal of Applied Physics, 1970. **41**(2): p. 462-468.

59. Shen, Y., L. Tian, and H. Zou, *Practical quantum random number generator based on measuring the shot noise of vacuum states.* Physical Review A, 2010. **81**(6): 063814.

60. Stefanov, A., et al., *Optical quantum random number generator.* Journal of Modern Optics, 2000. **47**(4): p. 595-598.

61. Jennewein, T., et al., *A fast and compact quantum random number generator.* Review of Scientific Instruments, 2000. **71**(4): p. 1675-1680.

62. Uchida, A., et al., *Fast physical random bit generation with chaotic semiconductor lasers.* Nature Photonics, 2008. **2**(12): p. 728-732.

63. Kanter, I., et al., *An optical ultrafast random bit generator.* Nature Photonics, 2009. **4**(1): p. 58-61.

64. Argyris, A., et al., *Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit.* Optics Express, 2010. **18**(18): p. 18763-18768.

65. Williams, C.R.S., et al., *Fast physical random number generator using amplified spontaneous emission.* Optics Express, 2010. **18**(23): p. 23584-23597.

66. Schellekens, D., B. Preneel, and I. Verbauwhede, *FPGA vendor agnostic true random number generator*, in *Field Programmable Logic and Applications, 2006. FPL'06. International Conference on,* 2006, IEEE. p. 1-6.

67. Petrie, C.S. and J.A. Connelly, *A noise-based IC random number generator for applications in cryptography.* Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 2000. **47**(5): p. 615-621.

68. Bucci, M., et al., *A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC.* Computers, IEEE Transactions on, 2003. **52**(4): p. 403-409.

69. Callegari, S., R. Rovatti, and G. Setti, *Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos.* Signal Processing, IEEE Transactions on, 2005. **53**(2): p. 793-805.

70. *Zener Diode I-V Characteristics Curve*. Available online from: http://www.learningaboutelectronics.com/Articles/Zener-diode-IV-characteristics-curve.

71. Hambley, A.R., *Electrical engineering: principles and applications,* 2008: Pearson Prentice Hall.

72. Brown, Daniel P., Carl M. Danielsen, and Ezzat A. Dabbish. *Random number generator with digital feedback*. U.S. Patent No. 4,853,884. 1 Aug. 1989.

73. Soto, J. *Statistical testing of random number generators*. in *Proceedings of the 22nd National Information Systems Security Conference*. 1999. NIST Gaithersburg, MD.

74. Ramaswami, R. and K. Sivarajan, *Optical Networks: A Practical Perspective*. Second ed, 2002, San Francisco, CA, USA: Morgan Kaufmann Publishers.

75. Hecht, E. and A. Zajac, *Optics Addison-Wesley*. Reading, Mass, 1974: p. 301-305.

76. Ramaswami, R.a.S., K., *Optical Networks*. Second ed, 2002: Morgan Kaufmann Publishers.

77. Palais, J.C. *Fiber optic communications*. Prentice Hall, 1988.

78. Breguet, J., A. Muller, and N. Gisin, *Quantum cryptography with polarized photons in optical fibres.* Journal of Modern Optics, 1994. **41**(12): p. 2405-2412.

79. Liu, W., Wu, W., Liang, L., Li, C. and Yuan, J., *Polarization Encoded Quantum Key Distribution over Special Optical Fibres.* Chinese Phys. Lett, 2006. **23**(2): 287.

80. Xavier, G. B., et al. *Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation*. *New Journal of Physics.* 2009. **11**(4): 045015.

81. Vilela de Faria, G., Xavier, G. B.,Temporo, G. P., Zbinden, H., Gisin, N. and J.P. and von der Weid, *Practical Scheme for Fibre-optical QKD with Polarization Encoded Qubits using Real-time Polarization Control.* Available from: http://www.secoqc.net/downloads/abstracts/SECOQC-vonderWeid.pdf

82. Chen, J., et al. *Stable quantum key distribution with active polarization control based on time-division multiplexing*. *New Journal of Physics* 11.6 (2009): 065004.

83. Ursin, R., et al., *Entanglement-based quantum communication over 144 km.* Nature Physics, 2007. **3**(7): p. 481-486.

84. Bonato, C., et al., *Feasibility of satellite quantum key distribution.* New Journal of Physics, 2009. **11**(4): p. 045017.

85. Hughes, R.J., et al. *Quantum cryptography for secure satellite communications*. In *Aerospace Conference Proceedings*. IEEE. **1** (2000): p. 191-200

86. Villoresi, P., et al. *Space-to-ground quantum communication using an optical ground station: a feasibility study*. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series. **5551** (2004).

87. Toyoshima, M., et al., *Polarization-Basis Tracking Scheme in Satellite Quantum Key Distribution.* International Journal of Optics, 2011. **2011**: 254154

88. Mirza, A. and F. Petruccione, *Quantum-secured Communication.* Quest Science, 2010. **6**(2): p. 50-53.

89. Mirza, A. and F. Petruccione, *QuantumCity gets a QuantumStadium.* Physics Comment, 2010. **2**(2): p. 2-3.

90. Mirza, A. and F. Petruccione, *Realizing long-term quantum cryptography.* JOSA B, 2010. **27**(6): p. A185-A188.

91. Kumavor, P.D., et al., *Comparison of four multi-user quantum key distribution schemes over passive optical networks.* Journal Light-wave Technology, 2005(23): p. 268-277.

92. Kumavor, P., et al., *Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture.* Journal of Lightwave Technology, 2006. **24**(8): p. 3103–3106.

93. Stebila, D., M. Mosca, and N. Lutkenhaus. *The case for quantum key distribution.* Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (2009): 283-296.

94. Simon, C., et al., *Quantum memories.* The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics, 2010. **58**(1): p. 1-22.

95. Julsgaard, B., et al., *Experimental demonstration of quantum memory for light.* Nature, 2004. **432**(7016): p. 482-486.

96. Beals, T.R., *Quantum communication and information processing,* Doctoral dissertation, 2008, Uni. of California, Berkeley).

97. Brassard, G., et al. *Multiuser quantum key distribution using wavelength division multiplexing*. In *Proceedings of SPIE*. 2003. **5260**: pp. 149-153.

98. Elliott, C., *The DARPA quantum network.* In Quantum Communications and Cryptography, ed. Sergienko, A., CRC Press/Taylor & Francis, Boca Raton London (2005): p. 83-102.

99. Elliott, C., et al., *Current status of the DARPA quantum network* in *Quantum Information and Computation III*, E. Donkor, A. Pirich, and H. Brandt, Editors. 2005, SPIE. p. 138-149.

100. Poppe, A., M. Peev, and O. Maurhart, *Outline of the SECOQC quantum-key-distribution network in Vienna.* International Journal of Quantum Information, 2008. **6**(02): p. 209-218.

101. Salvail, L., et al., *Security of trusted repeater quantum key distribution networks.* Journal of Computer Security, 2010. **18**(1): p. 61-87.

102. Sasaki, M., et al., *Field test of quantum key distribution in the Tokyo QKD Network.* Optics Express, 2011. **19**(11): p. 10387-10409.

103. Stucki, D., et al., *Long-term performance of the SwissQuantum quantum key distribution network in a field environment.* New Journal of Physics, 2011. **13**(12): 123001.

104. Mirza, A.R. and F. Petruccione, *Quantum Technology: A next generation solution for secure communication*. In *Military Information and Commmunication Symposium of South Africa 2011*. 2011: Pretoria, South Africa. Available online from: http://micssa.co.za/1.%20Papers%20-%20Day%201%2019%20July%202011/1-02B-3%20MICSSA%20Abdul%20Mirza%20paper.PDF

105. Odendaal, N., *Towards the digital city in South Africa: issues and constraints.* Journal of Urban Technology, 2006. **13**(3): p. 29-48.

106. Abdul Mirza and Francesco Petruccione, *Industrial application for global quantum communication*, In AIP Conference Proceedings, Quantum Africa 2010. Ed. E. Bruning, T. Konrad, F. Petruccione, Vol. 1469, pp. 58-62 (2012).

107. Pfennigbauer, M., et al., *Satellite-based quantum communication terminal employing state-of-the-art technology.* Journal of Optical Networking, 2005. **4**(9): p. 549-560.