UNIVERSITI PUTRA MALAYSIA

MODELLING AND SIMULATION OF IMPROVED SCARANI-ACIN-RIBORDY-GISIN-04 PREPROCESSING TECHNIQUE

RINIE NARINIE BINTI MOHD NASIR

MODELLING AND SIMULATION OF IMPROVED SCARANI-ACIN-RIBORDY-GISIN-04 PREPROCESSING TECHNIQUE

By

RINIE NARINIE BINTI MOHD NASIR

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

November 2015

COPYRIGHT

DEDICATIONS

I want to thank my grateful to ALLAH SWT, alhamdulillah all praises to HIM the most beneficient and merciful.
To my parents, Mohd Nasir bin Abu Samah and Nik Rosmah binti Mustapha for being supportive to me and give moral advises from the beginning until the end.
To my siblings especially my sister, Nurfarizza Surhada binti Mohd Nasir for always being there for me. May Allah bless them and grant their prayers.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master Science

MODELLING AND SIMULATION OF IMPROVED SCARANI-ACIN-RIBORDY-GISIN-04 PREPROCESSING TECHNIQUE

By

RINIE NARINIE BINTI MOHD NASIR

November 2015

Chair: Makhfudzah Mokhtar, PhD
Faculty: Engineering

Quantum Key Distribution (QKD) can be considered as the best secured technology that appreciates the quantum mechanics principals in terms of information transmission over vulnerable quantum channel. QKD ensures that both parties can share the matched secret key through particular designated method in order to protect the shared key from the intruders to eavesdrop the information.

Every procedure needs its own protocol to carry out the work accordingly and there are many QKD protocols in the quantum system that can be used in the transmission. In this study, the Scarani, Acin, Ribordy and Gisin 2004 (SARG04) protocol has been choosen because of its robustness against Photon Number Splitting (PNS) attack compared to Bennet and Brassard 1984 (BB84) protocol.

It is more likely that by improving secret key rate, the system can be more robust. Therefore, enhancing the secret key rate is one of the best way to enhance the security and authentication of the communication system. The Improved SARG04 (ISARG04) was introduced in a thesis by Ghazali (2012) in order to enhance secret key rate and its confidentiality from unauthorized parties. However, the studies were not being compared with SARG04 preprocessing technique. Therefore in this study, a mathematical modeling and a comparison between the secret key rate of the preprocessing of the existing SARG04 and the proposed technique of ISARG04 will be investigated in more details.

The results of this study show that the preprocessing technique of ISARG04 protocol is robust within the range of Quantum Bit Error Rate (QBER) between 0.14625 and 0.14880. The ratio of secret key rate between ISARG04 and SARG04 is exceeds one, hence the modification is improved. This outcome has shown an improved secret key rate against PNS attack. In consequence, it is expected that this study will bring an aspiration and contribution for future QKD protocol.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

MEMODELKAN DAN SIMULASI PENAMBAHBAIKAN SCARANI-ACIN-RIBORDY-GISIN-04 MENGGUNAKAN TEKNIK PRA PEMPROSESAN

Oleh

RINIE NARINIE BINTI MOHD NASIR

November 2015

Pengerusi: **Makhfudzah Mokhtar, PhD**
Faculti: **Kejuruteraan**

Pengagihan Kekunci Kuantum (QKD) boleh dikatakan sebagai teknologi yang paling selamat yang menggunakan prinsip kuantum mekanik dalam penghantaran maklumat melalui media kuantum yang terdedah. QKD memastikan bahawa kedua-dua pihak dapat berkongsi kekunci rahsia yang berpadanan melalui kaedah pemadanan untuk melindungi kekunci tersebut daripada penceroboh yang ingin mendapat maklumat.

Setiap prosedur memerlukan protokolnya yang tersendiri untuk menjalankan kerja dengan baik dan terdapat banyak protokol QKD di dalam sistem kuantum yang dapat digunakan semasa penghantaran. Dalam penyelidikan ini, protokol Scarani, Acin, Ribordy and Gisin 2004 (SARG04) telah dipilih disebabkan oleh kekebalannya terhadap serangan penyisihan nombor foton berbanding dengan protokol Bennet and Brassard 1984 (BB84). Protokol SARG04 lebih kebal terhadap serangan tidak bersambung oleh penceroboh.

Apabila menambaik kadar kekunci rahsia, sistem boleh menjadi lebih kebal. Oleh itu, menambahbaik kadar kekunci rahsia adalah satu cara yang terbaik untuk memelihara dan mengesahkan sistem komunikasi. Penambahbaikan SARG04 (IS-ARG04) telah diperkenalkan dalam tesis yang telah ditulis oleh Ghazali (2012) untuk menambahbaik kadar kekunci rahsia dan kerahsiaannya daripada pihak yang tidak diberikan kuasa pengesahan. Walau bagaimana pun, penyelidikan ini belum pernah lagi dibandingkan dengan pra pemprosesan SARG04.

Hasil keputusan penyelidikan ini menunjukkan bahawa protokol ISARG04 adalah kebal dari segi kadar kekunci rahsia dalam lingkungan Kadar Ralat Bit Kuantum (QBER) di antara 0.14625 dan 0.14880. Nisbah kadar kekunci rahsia antara ISARG04 dan SARG04 melebihi satu, justeru , ia menunjukkan satu penambahbaikan. Dapatan ini telah menunujukkan peningkatan kadar kekunci rahsia terhadap serangan penyisihan nombor foton. Sehubungan dengan itu, kajian ini dijangka dapat mendatangkan aspirasi dan sumbangan kepada protokol Pengagihan Kekunci Kuantum pada masa hadapan.

ACKNOWLEDGEMENTS

All praises are due to ALLAH (SWT), the almighty, the most beneficent, most merciful.

First of all, I would like to thank my supervisor, Dr. Makhfudzah Mokhtar for giving the guidelines throughout my master degree. Without her support, this thesis would not be an achievement. She always come out with good advises whenever I came to face with difficulties. She is generous in providing whatever needed in this research. Also, I would like to thank the other co-supervisor in Universiti Putra Malaysia (UPM), Dr. Wan Azizun Wan Adnan and Dr. Hafiz Abu Bakar for their moral support. May Allah grant all their prayers.

Next, I would like to give my special thanks to my another co-supervisor from International Islamic University Malaysia (IIUM), Dr. Jesni Shamsul Shaari for giving his best to guide me in this research. I was in IIUM Kuantan campus for more than one year with Dr. Jesni Shamsul Shaari in order to finish this research. He always came out with excellent ideas whenever we were puzzled in the middle of our research. To Dr. Jesni Shamsul Shaari, thank you for all the knowledge you have given to me. May Allah bless him and his family.

I would like to thank all the staff of the Computer and Communication System Engineering department of UPM and department of physics of faculty of Science of IIUM for all the contribution and support.

Finally to my families for their endless moral support,warm words and understanding my passionate for pursuing my master degree. Thank you so much. May Allah bless you all. Amin.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science.

The members of the Supervisory Committee were as follows:

Makhfudzah Mokhtar, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Wan Azizun Wan Adnan, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Muhammad Hafiz Abu Bakar, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Jesni Shamsul Shaari, PhD
Associate Professor
Kuliyaah of Science
International Islamic University Malaysia
(Member)

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work.
- quotations, illustrations and citations have been duly referenced
- the thesis has not been submitted previously or concurrently for any other degree at any institutions
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be owned from supervisor and deputy vice – chancellor (Research and innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software

Signature: _____ Date: _____

Name and Matric No: Rinie Narinie Binti Mohd Nasir GS34684

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

QC	Quantum Crypthography
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adlemen
QBER	Quantum Bit Error Rate
EPR	Einstein-Podolsky-Rosen
EDP	Entanglement Distillation Protocol
B92	Bennett Protocol
BB84	Bennett and Brassard Protocol
SARG04	Scarani-Acin-Ribordy-Gisin-04 Protocol
ISARG04	Improved Scarani-Acin-Ribordy-Gisin-04 Protocol
SSMF	Standard Single Mode Fiber
SMMF	Standard Multi Mode Fiber
PNS	Photon Number Splitting
IR	Intercept Resend

CHAPTER 1

INTRODUCTION

1.1 Background of Quantum Key Distribution

The modern world nowadays is already well-known up to the extent where by the communication is inseparable with human beings as described by Kasera et al. (2005). It has been ages that the researchers have been continuously finding ways to upgrade the information transmission and managed to convey and receive the message efficiently and effectively. There are some information that can be publicly shared with others and some are too confidential due to safety reasons. As some of the information needed for high security, the idea of protecting the information exchange happened since ages. Therefore, it is very crucial for them to secure their messages from being intercepted by the eavesdropper.

The expertise from the earliest discoveries started the secret messages by designing the cryptography which is a way of secret communication that only the intended receiver can receive the information or bit. Such examples are called transposition ciphers that used to reposition the order of letters while sending a message to the receiver. The other examples are substitution ciphers which used to substitute the letters with another letters. They designed the encoding and decoding procedure as mentioned in Loepp and Wotters (2006). This cryptography happened in the classical world with the assumption that classical cryptography is entirely depends on the complex factorization. However, in 1997 Peter Shor managed to solve it in based on algorithm and it has changed the idea that any cryptography which depends on those classical operations would be possible to break as quantum computing becomes real as explained in Chuang and Nielsen (2000).

As for the quantum world is described by the quantum mechanics concept, it is theoretically impossible to break the information. The message is transmitted in quantum system called as quantum cryptography (QC). The eavesdropper may attack to steal information by attacking during the transmission. Thus, various of ways have been designed to make the the communication system robust to the attacks.

Quantum key distribution (QKD) is one good example of quantum cryptography where by it is the process of exchanging the secure information that only happen in the Hilbert space of the quantum system. QKD is said to be secured because of the properties of quantum physics namely the no-cloning theorem. This is because Eve has to apply a quantum mechanics measurement whenever she wants to probe the signals in the quantum channel. This action will leave traces where by it can be detected and thus abort the transmission of the information as described by Bruβ and Leuchs (2007). The original idea of QC was proposed by Stephen Wiesner and Charles Bennet in the 1970s. After several attempts to publish their ideas, Charles Bennet and Gilles Brassard managed to publish it in 1983 as described by Brassard (2005).

The principle work of QKD involves two parties of Alice as the transmitter and Bob as the receiver in order to transmit codes or else known as secret key. Assuming Eve as the eavesdropper who will interrupt the secret message to be delivered she will attack the signals of secret key in many ways. This is where both Alice and Bob need to secure their secret key to prevent Eve from obtaining the information. Both parties use two mediums of communication which are quantum channel (one way communication) and public channel (two way communication).

In quantum channel, Alice will send the polarized photons which represent as qubits and Bob will measure the received qubits. During the end of the transmission, they will manage to compare publicly the operators that used and only keep the matched operators. Then, both of them will simulate a communication via public channel. Alice and Bob will clarify their measurements at this time with or without the presence of Eve which is called as the parameter estimation. They will estimate the quantum bit error rate (QBER) which indicates how differ their keys are. Then, Alice and Bob will commit to error correction as mentioned in Gisin et al. (2002). The final stage is the privacy amplification where by Alice and Bob manage to produce the final key which Eve has very minimal or zero information about it as explained by Renner et al. (2005). Only then, it is said that the information is genuinely secured.

1.2 Problem Statement

One has to assume that they will always be noise in quantum channel. This noise can be caused by Eve as mentioned in Renner et al. (2005). The type of noises can be included as depolarizing of photons, bit-flip, phase flip, bit-phase-flip and dark counts. These noises will affect the qubits through the quantum channel. Eve has many possible attacks during Alice and Bob's transmission such as individual attack (incoherent attack) and collective attack (coherent attack). Individual attack occurred as Eve interrupt her probe individually in each qubit at one time. Meanwhile, as for collective attack, she attaches her probes in several qubit at a time as described in Gisin et al. (2002). Since in practice, more than one photon may appear during the transmission, it will make things more easier for Eve to measure the information without letting Alice and Bob know about the disturbance that Eve has made. So, this is the challenge to prevent Eve from being able to able to measure the length of the information.

The SARG04 protocol is more robust in terms of incoherent attack such as photon number splitting (PNS) attack compared to other protocols as explained in Scarani et al. (2004). The SARG04 protocol is similar with BB84 protocol which both of them are using four quantum states to send the qubits. The only difference is during post classical processing procedure where SARG04 is using the non-orthoganal states in sending the qubits from Alice to Bob.

Improving the secret key rate is one of the best way to keep the security and authentication of the communication system. The Improved SARG04 (ISARG04) was introduced by in a thesis by Ghazali (2012) in order to enhance secret key rate and its confidentiality from unauthorized parties. However, the studies was not being compared in SARG04 preprocessing technique. Therefore in this study, a mathematical modeling, a comparison between the secret key rate of the preprocessing of the existing SARG04 and the proposed technique of ISARG04 will be investigated in more details.

1.3 Aim and Objectives

Aim

To improve the secret key rate of preprocessing SARG04 by using an improved technique of SARG04 protocol.

Objectives

1. To reanalyze the existing preprocessing technique of SARG04 protocol.

2. To model the preprocessing of improved SARG04 protocol based on optimal incoherent attack.

3. To evaluate the performance of the ISARG04 preprocessing with a comparison to the existing SARG04 preprocessing.

1.4 Scope of Work

This thesis consists of theoretical modeling, numerical calculation and simulations. The scope of this research is more focusing in analyzing the secret key rate of ISARG04 that will enhance the robustness of the preprocessing SARG04 system. In order to achieve that, a methodology has been made in which the algorithm is improvised to be placed into the measuring observable. Then, its robustness is tested by using the simulation software in order to verify the improvement of the model.

All of the results are vital as they will be evaluated and compared with the original preprocessing SARG04. From there, the success of this improved preprocessing technique will be determined at the end of the research.

1.5 Organization of the Thesis

The organization of the thesis is arranged as below:
Chapter 1 starts with introduction of quantum cryptography and quantum key distribution, followed by the problem statement that need to overcome, aim and objectives of the research and scope of the work.

In Chapter 2, a general picture of QKD is further explained. A mathematical modeling of quantum operation is shown to understand how it works in the quantum system. After that, the implementation of QKD is thoroughly described to see other alternatives to carry out the sources, followed by possible attacks which will harm the secret keys and lastly, the protocols that are enable in QKD system. Among of those protocols, SARG04 protocol is discussed as a whole and reasons of choosing it.

As for Chapter 3, the introduction of methodology used in this research is shown. The design and performance parametes are determined followed by modification of pre-processing technique. All the theoretical modeling and numerical calculations can be seen thoroughly in SARG04 and also Improved SARG04.

In Chapter 4, the graphs from the simulation are shown to evaluate the performance of the robustness, followed by discussion. The results of Improved SARG04 is compared to the original preprocessing SARG04 protocol.

Finally, the conclusions and the recommendation for future works are discussed in Chapter 5.

1.6 Research Overview

Figure 1.1 depicts a thorough picture of this research in which each section represents the sub-topics that will be described in the next chapters.

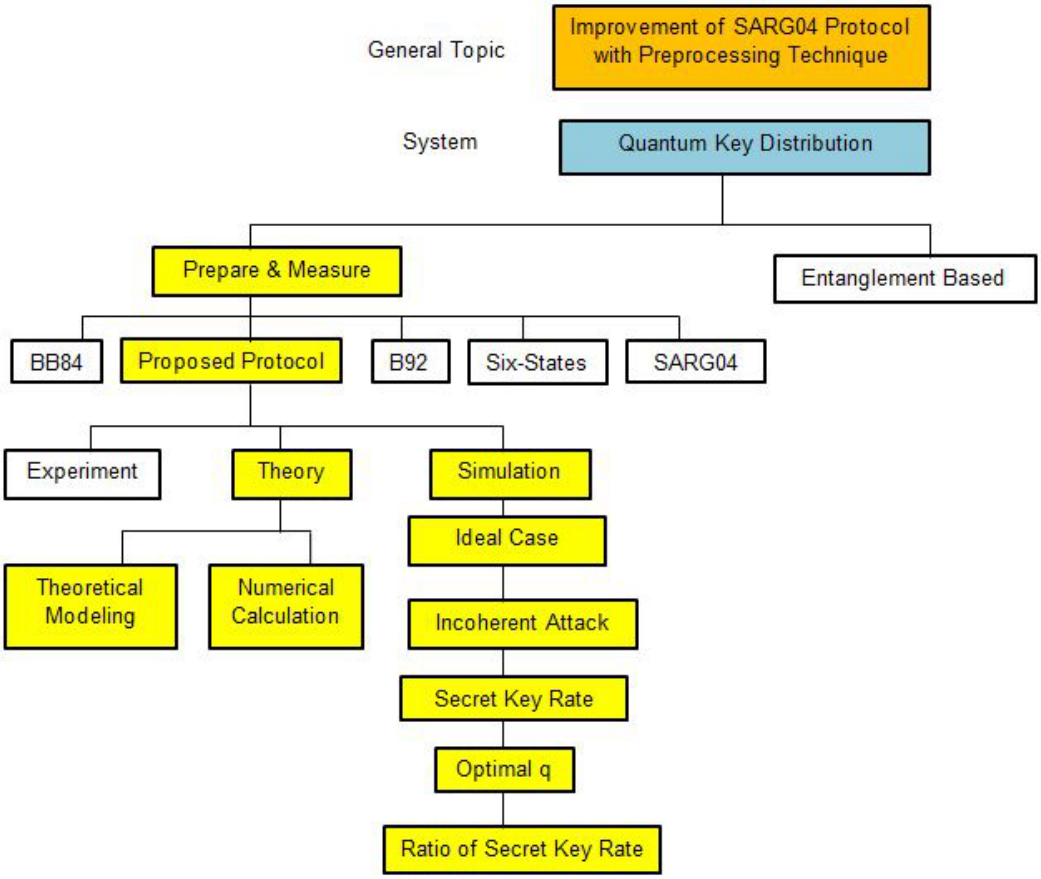

Figure 1.1: Research Overview

BIBLIOGRAPHY

Acin, A., Brunner, N., Gisin, N., Massar, S., Pironio, S. and Scarani, V. 2007. Device-Independent Security of Quantum Cryptography against Collective Attack. *Physical Review Letters* 98.

Ali, S., Mohammed, S., Chowdhury, M. S. H. and Hasan, A. A. 2012. Practical SARG04 Quantum Key Distribution. *Springer* .

Antonio, A., Gisin, N. and Scarani, V. 2004. Coherent-Pulse Implementations of Quantum Cryptography Protocols Resistant to Photon-Number-Splitting Attacks. *Physical Review A.* 69.

Bennett, C. H. 1992. Quantum Cryptography Using Any Two Nonorthogonal States . *Physical Review Letters* 68: 3121–3124.

Bennett, C. H. and Brassard, G. 1984. Quantum Cryptography : Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computer, System and Signal Processing*, 175–179. Bangalore, India.

βrub, D. 1998. Optimal Eavesdropping in Quantum Cryptography with Six States. *Physical Review Letters* 81.

Biham, E., Boyer, M., Brassard, G., Graaf, J. and Mor, T. 2002. Security of Quantum Key Distribution against All Collective Attacks. *Springer* 34.

Branciard, C., Gisin, N., Kraus, B. and Scarani, V. 2005. Security of Two Quantum Key Distribution Protocols Using The Same Four Qubit States. *Physical Review A.* 72.

Brassard, G. 2005. Brief History of Quantum Cryptography : A Personal Perspective. In *Proceedings of The IEEE Information Theory Workshop on Theory Practice in Information-Theoretic Security*, 1–5. Awaji Island, Japan.

Bruβ, D. and Leuchs, G. 2007. . In *Lectures on Quantum Information*, 270–284. Germany: Wiley-Vch.

Canale, M., Bacco, D., Calimani, S., Renna, F., Laurenti, N. and Vallone, G. 2011. A Prototype of a Free-Space QKD Scheme Based on the B92 Protocol. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication*.

Chuang, I. L. and Nielsen, M. A. 2000. *Quantum Computation and Quantum Information*. 1st edn. United Kingdom: Cambridge University Press.

Dieks, D. 1982. Communication by EPR Devices. *Physical Review A.* 92.

Ekert. 1991. Quantum Cryptography Based on Bell's Theorem . *Physical Review Letters* 67.

Fung, C. H. F., Tamaki, K. and Lo, H. K. 2006. Performance of Two Quantum Key Distribution Protocols. *Physical Review A.* 73.

Gaintan, F. 2008. . In *Quantum Error Correction and Fault Tolerant Quantum Computing*, 20–21. New York: CRC Press, Taylor and Francis Group.

Ghazali, L. I. A. 2012. *Alternative Discrete Variable Protocol for Point to Point Quantum Key Distribuition System* . PhD thesis, Faculty of Engineering. University Putra Malaysia.

Gisin, N. and Bechmann-Pasquinucc, H. 1999. Incoherent and Coherent Eavesdropping in The Six-State Protocol of Quantum Cryptography. *Physical Review A*. 59.

Gisin, N., Ribordy, G. and Kraus. 2002. Quantum Cryptography. *Reviews of Modern Physics* 74: 1–195.

Gobby, C., Yuan, Z. L. and Shields, J. 2004. QKD over 122KM of standard telecom fiber. *Applied Physics letters* 84.

Helstrom, C. W. 1976. *Quantum Detection and Estimation Theory*. New York: Academic Press.

Kasera, S., Narang, N. and Narang, N. 2005. . In *Communication Networks Principles and Practice*, 1–3. United States of America: McGraw-Hill Communication.

Kenneth S. Schneider. 2013, Chapter 2: The Fiber Optic Data Communication Link for The Premises Environment, http://www.telebyteusa.com/foprimer/foch2.htm.

Koashi, M., Tamaki, K. and Imoto, N. 2003. Unconditionally Secure Key Distribution Based on Two Nonorthogonal States. *Physical Review Letters* 90.

Krishna, C. H. and Kumar, S. 2013. Secure QKD Scheme with EPR Sequence. *International Journal of Advanced Research in Computer Scienceand Software Engineering* 10.

Loepp, S. and Wotters, W. K. 2006. . In *Protecting Information : From Classical Error Correction to Quantum Cryptography*, 1–46. United States of America: Cambridge University Press.

Lucamarini, M., Vallone, G., Gianani, I., Mataloni, P. and Giuseppe, G. 2012. Device-Independent Entanglement Based Bennett 1992 Protocol. *Physical Review A*. 86.

Nakahara, M. and Ohmi. 2013. *Quantum Computing : From Linear Algebra to Physical Realization*. 1st edn. CRC Press, New York: Cambridge University Press.

Optical Systems Design. 2013, SM VS MM, http://www.osd.com.au/multimode-versus-singlemode/sm-vs-mm/.

Renner, R., Gisin, N. and Kraus, B. 2005. Information-Thoretic Security Proof for Quantum Key Distribution Protocols. *Physical Review A* 72: 1–17.

Scarani, V., Acin, A., Ribordy, G. and Gisin, N. 2004. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Physical Review Letters* 92 (1–4).

Shen, Y., Chen, Y., Zou, H. and Yuan, J. 2014. A Fiber-Based Quasi-Continuos-Wave Quantum Key Distribution. *Scientific Reports* .

Shor, P. W. and Preskill, J. 2000. Simple Proof of Security of The BB84 Quantum Key Distribution Protocol. *Physical Review Letters* 85.

Tamaki, K. and Lutkenhaus, N. 2004. Unconditional Security of The Bennett 1992 Quantum Key Distribution Protocol over a Lossy and Noisy Channel. *Physical Review A.* 69.

Wilde, M. M. 2013. *Quantum Information Theory*. 1st edn. United States of America: Cambridge University Press.

Wooters, W. K. and Zurek, W. H. 1982. A single quantum cannot be cloned. *Nature* 299.

Zang, C.-W., Li, C.-F. and Guo, G.-C. 1999. General Strategies for Discrimination of Quantum States. *Elsevier* .

Zoller, P., Beth, T. and Binosi, D. 2005. Quantum Information Processing and Communication : Strategic Report on Current Status, Visions and Goals for Research in Europe. *The European Physical Journal D* .