UNIVERSITI PUTRA MALAYSIA

ALTERNATIVE DISCRETE VARIABLE PROTOCOL FOR POINT TO POINT QUANTUM KEY DISTRIBUTION SYSTEM

LIZAL ISWADY AHMAD GHAZALI

ALTERNATIVE DISCRETE VARIABLE PROTOCOL FOR POINT TO POINT QUANTUM KEY DISTRIBUTION SYSTEM

By

LIZAL ISWADY AHMAD GHAZALI

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

October 2012

DEDICATION

All praises are due to ALLAH SWT the most beneficent and merciful.

This work is dedicated to the quantum key distribution community whom benefit most from the work.

To my wife, Dr.Makhfudzah Bt. Mokhtar, my both parents Hj Ahmad Ghazali B. Abu Hassan Ashaari, Hjh Siti Zaleha Bt. Ayob, Hj Mokhtar B. Hashim, Hjh Mariam Bt. Abu Bakar, for their doa and moral support. May ALLAH (SWT) grant them Hasanah, Amin.

May ALLAH helps to revive Muslim Ummah back to becoming true teacher to the entire being and foster a strong brotherhood among Muslims. Brotherhood is the foundation to glory.

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

ALTERNATIVE DISCRETE VARIABLE PROTOCOL FOR POINT TO POINT QUANTUM KEY DISTRIBUTION SYSTEM

By

LIZAL ISWADY AHMAD GHAZALI

October 2012

Chair: Assoc. Prof. -Ing Ahmad Fauzi Abas, PhD

Faculty: Engineering

Quantum Key Distribution (QKD) is an enabling technology to current modern cryptography which utilizes nature properties of light to transfer key information safely over an unsecured channel. Via this application, both communicating parties can share an identical secret key for their chosen cryptographic scheme in various applications which demand a protection to their highly important message.

A designated key bits reconciliation method is known as QKD protocol. The first ever protocol introduced and popularly used is the Bennett and Brassard 1984 (BB84) protocol. However the implementation with current technology has restricted its primary capability to guarantee the security of secret key establishment. As a result, it is vulnerable to Eavesdropping attack. This leads many works on practical protocol and the most significant contribution having used the same setup as the

BB84 protocol is the Scarani, Acin, Ribordy and Gisin 2004 (SARG04) protocol. The SARG04 is more robust against photon number splitting attacks and double the BB84 critical transmission distance. Nevertheless SARG04 protocol still has lower percentage of sifted key bit compared to BB84 protocol.

Therefore this study has embarked its objectives on identifying and proposing a new QKD protocol which can improve the robustness while allowing higher final key length. The alternative protocol is designed by combining the existing SARG04 decoding with improved SARG04 decoding (ISARG04). Unlike SARG04 which discards any inconclusive result from his measurement, ISARG04 will always accept the non orthogonal state with half probability of error.

The robustness of the proposed protocol is simulated based on simple Intercept Resend attack and photon number splitting attacks in quantum key distribution. This new protocol is robust up to two photons per pulse and has an improvement to secure transmissions of bits at higher link loss, up to 26.7 dB.

In summary, this work has presented an improved discrete variable protocol which improved the sifted key length and robust to eavesdropping. It is hope that, this contribution might be a breakthrough for near future QKD protocol.

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

PPROTOKOL PEMBOLEHUBAH DISKRET ALTERNATIF UNTUK SISTEM PENGAGIHAN KEKUNCI KUANTUM DALAM GENTIAN OPTIK TITIK KE TITIK

Oleh

LIZAL ISWADY AHMAD GHAZALI

Oktober 2012

Pengerusi: Prof Madya -Ing Ahmad Fauzi Abas, PhD

Fakulti: Kejuruteraan

Pengagihan Kekunci Kuantum (QKD) adalah suatu teknologi mampan kepada kriptografi moden pada masa kini dimana ia memanfaatkan sifat-sifat semulajadi cahaya untuk memindahkan maklumat tentang kekunci tersebut dengan selamat melalui talian yang tidak dilindungi. Melalui aplikasi ini, kedua-dua pihak yang berhubung mampu berkongsi kekunci rahsia yang sama bagi kegunaan skim kriptografi untuk pelbagai aplikasi yang memerlukan perlindungan kepada data atau mesej yang sangat penting.

Teknik pemadanan bagi bit-bit kuantum yang mewakili maklumat kekunci tersebut dikenali sebagai protokol QKD. Protokol yang terawal dan paling popular diaplikasikan sehingga kini ialah protokol BB84. Walau bagaimanapun pelaksanaannya dengan menggunakan teknologi masa kini adalah sangat terhad dan di bawah keupayaan sebenar yang boleh dicapai oleh protokol ini iaitu bagi

menjamin perlindungan di dalam penghasilan kekunci rahsia. Ini mengakibatnya ia mudah terdedah kepada serangan penceroboh. Keadaan ini telah mendorong lebih banyak penyelidikan untuk menghasilkan protokol yang praktikal dan di antara sumbangan terpenting di dalam penyelidikan tersebut ialah pengenalan kepada protokol SARG04 yang boleh diaplikasikan menggunakan tatacara pemasangan yang serupa seperti protokol BB84. SARG04 lebih kebal terhadap serangan penyisihan nombor foton dan menawarkan dua kali ganda jarak penghantaran kritikal protokol BB84. Walaupun begitu, protokol SARG04 masih menghasilkan kadar peratusan sisihan bit kekunci yang rendah berbanding protokol BB84.

Oleh itu kajian ini telah memfokuskan kajiannya kepada pengenalan protocol alternatif yang dapat menambah kekebalan jarak selamat penghantaran kekunci di samping menghasilkan kekunci akhir yang lebih panjang. Protokol yang dicadangkan ini telah menggabungkan kaedah ayakan bit SARG04 dengan kaedah saringan ISARG04. Tidak seperti SARG04 yang terpaksa menyisihkan pengukuran yang tidak pasti, ISARG04 menerima hasil pengukuran yang tidak ortogonal tersebut dengan kebarangkalian separuh ralat.

Kekebalan protokol ini disimulasi berdasarkan serangan mudah ‘halang dan hantar semula’ dan serangan pecahan bilangan foton. Protokol ini kebal terhadap serangan penceroboh pada kadar dua foton bagi satu denyut isyarat dan mempunyai penambahbaikan untuk melindungi penghantaran bit kekunci pada kehilangan talian kritikal yang lebih tinggi sehingga 26.7 dB.

Secara keseluruhnya, kajian ini telah mengemukakan suatu penambahbaikan protokol yang dapat meningkatkan panjang bit kekunci saringan dan kebal terhadap serangan penceroboh. Adalah diharapkan cadangan ini mampu menawarkan penyelesaian praktikal baru pada masa terdekat kepada protokol Pengagihan Kekunci Kuantum.

ACKNOWLEDGEMENTS

All praises are due to Allah (SWT), the almighty, Lord of the worlds, the Most Beneficent, the Most Merciful.

I would like to profoundly thank my supervisor, Dr.-Ing. Ahmad Fauzi Abas, without whose help and support, this dissertation may not be a reality. Dr.-Ing. Ahmad Fauzi consorts and motivates us at hard and easy time. He is always available to us despite his busy schedule as a researcher, lecturer, a leader in his society organization and also a small leader in his family. He always listens and offer prompt solutions to whatever problem we confronted him with. To Dr.-Ing. Ahmad Fauzi, I say thank you. May Allah (SWA) guide, support and pour His blessings upon you and your family.

I would also wish to express my deepest gratitude and appreciation to another gentlewoman, Dr Wan Azizun Wan Adnan. She has contributed immensely to the success of this dissertation. I also benefitted tremendously from her moral and financial support and wide and vast knowledge in the field of not only information security but other aspects of general knowledge. May Allah Help and Reward her abundantly.

I also deeply appreciate the contributions, guidance and support of my supervisory committee member, Prof Dr Mohd Adzir Mahdi.

I appreciate the help and assistance of my colleagues in our research group, Shafiqul Islam, Abdul Hadi, and others. I cherish the support with which we faced throughout the study. I would also want to thank all staffs and other students of the Photonic and Fiber Optic System Laboratory (PFOSLab), for their help and support. Equally, I would like to thank all the other staffs of the Computer and Communication Systems Engineering department.

Finally to my families who support my long period of study while I am pursuing the Master degree, I say thank you for understanding. May Allah Bless you all. Amin.

I certify that an Examination Committee has met on **XX^{h} XXX 2012** to conduct the final examination of **Lizal Iswady Ahmad Ghazali** on his degree thesis entitled **"Alternative Discrete Variable Protocol for Point to Point Fiber Optics Quantum Key Distribution System"** in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the Master of Science.

Members of the Examination Committee were as follows:

Name of Chairperson, PhD
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Name of Examiner 1, PhD
Faculty of Engineering
University Putra Malaysia
(Internal Examiner)

Name of Examiner 2, PhD
Faculty of Engineering
University Putra Malaysia
(Internal Examiner)

Name of External Examiner, PhD
Faculty of Engineering
University Putra Malaysia
(External Examiner)

Seow Heng Fong, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master Science. The members of the Supervisory Committee were as follows:

Ahmad Fauzi Abas, PhD, -Ing
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Mohd Adzir Mahdi, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

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

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

_____

LIZAL ISWADY AHMAD GHAZALI

Date:

TABLE OF CONTENTS

		Page
DEDICATION		ii
ABSTRACT		iii
ABSTRAK		v
ACKNOWLEDGEMENTS		viii
APPROVAL		x
DECLARATION		xii
TABLE OF CONTENTS		xiii
LIST OF TABLES		xv
LIST OF FIGURES		xvi
LIST OF ABBREVIATIONS		xvii
CHAPTER		
1	**INTRODUCTION**	1
	1.1 Evolution of Information Security	1
	1.2 Problem Statement	4
	1.3 Objectives	6
	1.4 Scope of Work	7
	1.5 Organization of the Thesis	9
2	**LITERATURE REVIEW**	10
	2.1 Introduction	10
	2.1.1 Quantum Bits and Quantum States	10
	2.1.2 Understanding Quantum Measurement	12
	2.2 Implementation Issues	13
	2.2.1 Photon Sources	13
	2.2.2 Quantum Channels	14
	2.2.3 Photons Detectors	15
	2.2.4 Random Number Generator	17
	2.2.5 Photon Number Splitting (PNS) Attack	17
	2.2.6 Protocols	20
	2.3 QKD protocol: Discrete Variable Coding	21
	2.3.1 BB84 Protocol	21
	2.3.2 B92 Protocol	24
	2.3.3 Six States Protocol	25
	2.3.4 SARG04 Protocol	26
	2.4 Critical Review	28
	2.5 Summary	30
3	**METHODOLOGY**	32
	3.1 Introduction	32
	3.2 The Development of Proposed Protocol	39
	3.2.1 Optimal Probability in Selecting ISARG04 Decoding Scheme	36
	3.2.2 Algorithm for the Proposed Protocol	40
	3.3 Intercept Resend Attack on the Proposed QKD Protocol	49
	3.4 PNS Attack on the Proposed QKD Protocol	50

3.4.1 Intercept Resend (IR) with Unambiguous State Discrimination (IRUD) Attack on the Proposed QKD Protocol 52
3.4.2 Storage Attack on the Proposed QKD Protocol 54
3.4 Errors in Transmission 56
3.5 Summary 57

4 **RESULTS AND DISCUSSION** 58
4.1 Introduction 58
4.2 Performance of the Proposed Scheme against IR Attack 58
4.3 Performance of the Proposed Scheme against Intercept Resend with Unambiguous State Discrimination (IRUD) Attack (Ideal Case) 62
4.4 Performance of the Proposed Scheme against Storage Attack (Ideal Case) 63
4.5 Evaluation on Eve Effective Attack (Ideal Case) 65
4.6 Performance of the Protocol against Storage Attack (Practical Case) 66
4.7 Reviewed criteria 68
4.9 Summary 69

5 **CONCLUSION AND FUTURE WORK** 70
5.1 Conclusion 70
5.2 Recommendation for Future Work 72

REFERENCES/BIBLIOGRAPHY 73
APPENDICES 76
BIODATA OF STUDENT 85
LIST OF PUBLICATION 86

LIST OF TABLES

Table		Page
2.1	Reviewed Criteria of Single Photon Detectors	17
2.2	Reviewed Criteria of QKD Protocols	30
4.1	Theoretical Results of Average Sifted Key and Expected Error	59
4.2	Performance of Proposed Protocol without Basic IR Attack	60
4.3	Performance of Proposed Protocol against Basic IR with Eve	60

LIST OF FIGURES

Figure		Page
1.1	Research Overview	8
2.1	Denoting a qubit state	11
2.2	Pulse Path Over Single Mode and Multimode Optical Fiber	15
2.3	Research Focus on QKD Protocols	20
2.4	Operation Illustration of BB84 Protocol	23
2.5	Operation Illustration of SARG04 Protocol	27
3.1	Research Methodology	33
3.2	Venn Diagram of Proposed Work	37
3.3	Alice Encoding Part of Proposed Scheme	42
3.4	Qframes Structure	45
3.5	Bob Decoding Part of Proposed Protocol	47
3.5a	SARG04 Decoding Scheme	48
3.5b	ISARG04 Decoding Scheme	48
4.1	Robustness against Intercept Resend on Proposed Protocol	60
4.2	Robustness against Intercept Resend on SARG04 Protocol	61
4.3	Robustness against Intercept Resend Unambiguous Discrimination (IRUD) Attack (Ideal Case)	63
4.4	Robustness against Storage Attack (Ideal Case)	64
4.5	Robustness against Two PNS Attacks (Ideal Case)	65
4.6	Interpolation of Practical Robustness of Proposed Scheme at (Practical Case)	67

ABBREVIATIONS

AES	Advance Encryption System
APD	Avalanche Photo Diode
B92	Bennett 1992
BB84	Bennett and Brassard 1984
dB	Decibel
DES	Data Encryption System
DSS	Decoding Scheme Selection
IR	Intercept Resend attack
IRUD	Intercept Resend with Unambiguous Discrimination
Km	Kilometer
LD	Laser Diode
Mbps	Mega bits per second
mW	mili Watt
Nm	Nanometer
OTDV	Optical Time Domain Visualizer
P&M	Prepare and Measure
PD	Photon detector
PMT	Photomultiplier tube
PNS	Photon Number Splitting
QBER	Quantum Bit Error Rate
QC	Quantum Cryptography
QKD	Quantum Key Distribution
RSA	Rivest, Shamir and Adleman

SARG04	Scarani, Acin, Ribordy and Gisin 2004
SMMF	Standard Multimode Fiber
SNSPDs	Superconducting nanowire single-photon detectors
SPAD	Single-photon avalanche photodiodes
SSMF	Standard Single Mode Fiber
TES	Transition-edge sensors

CHAPTER 1

INTRODUCTION

1.1 Evolution of Information Security

Communication is a part of natural desire that the human being need to interact, transfer and share information between them. A communication system is based on the fundamental basis of exchanging data between two parties. The development of communication technology has undergone many stages and advances . As far as important information is concerned, various ways of concealing private information have also been introduced over times. This act of hiding the information such that only the rightful users can share the original message is known as cryptography [1].

Cryptography is a combination of Greek`s words, kryptos (hidden or secret), and graphein (to write) respectively [1]. A cryptographic algorithm, known as cipher, is used to define the information conversion [2]. An anonymous or unintended user that try to forge the information, fall into other category called as cryptanalysis which is an art of breaking the code. Both areas of cryptography and cryptanalysis are called cryptology [3].

Dated back before 3000 CE, ancient Egypt kingdoms had developed a non-military cryptography known as hieroglyphics to record information [4]. Later, the development of different cryptography extends its application in military-based cryptography. Among

the early known cryptography been used was the skytale cipher. It was believed to be the first transposition cipher introduced for military campaign by the ancient Greeks and Spartans [1], [2].

The merging of computer science and data communications between 1970s and 1980s has changed the way cryptography work [5]. Modern cryptography schemes namely symmetry key cryptography and public key cryptography have been introduced which extend its application in public services such as electronic banking, securing patients medical records, delivering votes in municipal elections and so on.

A symmetric key cryptography development period covers both traditional (precomputer era) and modern era [3]. This type of conventional cryptography allows only an identical key for both users to perform encryption and decryption, meaning that both sender and receiver must have the same key. The traditional period are based on the substitution or transposition techniques. In modern era, the symmetric key cryptography involves multiple stage of substitution and transposition of an encryption [3]. Hence, it resulted in the algorithm to be more secured in term of its robustness against cryptanalysis. An example of deploying this principle has been seen in a system known as rotor machines. It is a mechanical machine that is driven by electricity that outputs unique ciphertext every time a letter is fed at the input. Moreover this idea has paved the way to the introduction of Data Encryption Standard (DES) in modern era of symmetric key cryptography [3].

The introduction of DES was adopted in 1977 as information security standard and over times, many new schemes (such as 3DES, Advance Encryption System (AES)) were introduced with response to the weaknesses by previous design. The fact that the security that makes up symmetric key cryptography is based on key length has opened the possibility of attack. This is true since the hardware prices will continue to drop as the processing speed increases that will benefit the cryptanalysis [3]. The only solution is to have the length of a secret key as large as the message and reused is not permitted [2], [3]. One time pad is the only proven secure cipher but impractical as it needs a huge and constant supply of key to encryption process [2], [3], [6]. Moreover, the main limitation to this cryptography is to distribute the key within legal users. Conventional methods such as face to face meeting or courier services might not suitable especially for long distance communication and bare risks. For that matter, the public key cryptography has been introduced to cater the key distribution problem [3], [7]. The public key cryptography provides two types of keys to the respective users who want to share confidential information together. One is the private key which owned only by recipient while the other is known as public key which is used by sender to encrypt the data. Rivest-Shamir-Adleman (RSA) is widely used and is the pioneering public cryptography scheme [3].

Basically all public key cryptography algorithms are based on mathematical functions. For that matter, its security relies on the key length and computational work to break the cipher. In other word, both keys is related by mathematical one way function that make it hard to deduce a private key from a known public key [1]. The term 'hard' connotes the time taken to do the factoring are huge, thus making the secret information no more

valuable to the attacker as both user already finished their business. However the probability of having an efficient factoring algorithm cannot be ruled out as it may significantly reduce the time taken and will benefit the attacker. In addition, Peter Shor (person who introduce Shor's algorithm in 1994 which runs on a quantum computer to break public-key cryptography schemes)[8] has devised a quantum computer algorithm to reduce factoring time and therefore inventing quantum computer is possible in near future [9]. With the realization of quantum computer, most current public-key cryptosystem will end up broken within seconds and highly important data will be at stake.

Although the realization is expected to take tens of years, the threat must be dealt in serious manner. Any new threat due to the advancement of technology will result in further compromise to the secrecy of data such as in military, banking, and so on. Fortunately the introduction of quantum key distribution in 1984 has relief many, in such a way it helps to solve the security of a cryptographic key faced by the available cryptography schemes as mention earlier and not vulnerable against quantum computer. Based on the fundamental law of quantum mechanics, this new enabling innovation will promise an unconditional security to the threat faced by modern cryptography [9], [10], [8], [11].

1.2 Problem Statement

Quantum cryptography (QC) or quantum key distribution (QKD) has become an important technology in the world of cryptology. The unique feature of protection to

encrypt keys distribution underlined by the quantum mechanics theorems, made this technology possible to be implemented to any available modern encryption system by adding the safety feature imposed by the current demand of data protection [9], [10], [12].

Since its introduction in 1984, it has endured various challenges to date. The early stage of its milestones involves developing foundation concept of QKD. These include the introduction of Bennett and Brassard 1984 (BB84), entangle states and Bennett 1992 (B92) protocols. The first in-principle demonstration of the BB84 protocol was the first laboratory work done experimentally to realize the idea physically [13]. As a result of the work, it has sparked an era of competition between the experimentalist and theorists. The experimentalists were actively involved in bringing out the laboratory experimental work to deploying it in the real world. They have achieved to demonstrate QKD deployment over increasing distance. Meanwhile the theorists with the same motivation have proposed various protocols and security proofs derivation. The effect from this competition has broadened the gap between the different parties such that the security proofs were derived for idealized setup while the practical setup implementation were done without considering seriously security perspective [9].

Fortunately, the awareness of this gap got noticed as a result of discovery of photon number splitting (PNS) attacks. The groups later began to cooperate in making the QKD implementable with available technology yet guarantee the security with reasonable proofs. Works on making QKD practical with existing infrastructure is a thoroughgoing research, thus making rooms for improvements in several sectors such as the photon sources, photons detectors, quantum channels and protocols [9], [10].

Among the significant contribution through the cooperation yield methods to minimize the PNS threat such as the introduction of SARG04 [9]. The SARG04 is more robust against photon number splitting attacks and its ultimate limit of robustness (in the case of zero errors) is shifted from approximately 50 km up to 100 km (as compared to BB84) [14]. Nevertheless SARG04 protocol still has lower percentage of sifted key bit compared to BB84 protocol.

Thus, having a shared key with longer final key while ensuring its security during key distribution are substantially essential [9], [10]. Therefore this study has embarked its objectives on identifying and proposing an alternative technique for SARG04 protocol which can improve the robustness while allowing higher final key length.

1.3 Objectives

In general, the main objective of this research is to design and develop a new QKD protocol which offers improvement to the sifted key rate and secure key transmission distance against common Eve attacks. In specific, the objectives of this thesis are:

i. To study and analyze the strength and weakness of in-used prepare and measure with discrete variable coding QKD protocol.
ii. To design an algorithm for implementing new decoding rules.
iii. To propose a protocol using the new decoding rules and SARG04 for better performance in term of robustness.

iv. To evaluate the performance of the proposed protocol and compare against the most popularly deployed QKD protocol.

1.4 Scope of Work

This thesis covers the system theoretical modeling and simulations. Details of the scope are shown in the K-Chart [15] shown in Figure 1.1. The figure summarizes the whole study including the scope of study, methodology, design and performance parameters used in the analysis.

The scope of this research focuses on prepare and measure protocol for point to point fiber optics quantum key distribution where a new protocol is introduced. In order to carry out the work, a methodology has been underlined in developing a new decoding scheme and modeled the way the protocol determines its final output. Then the protocol is simulated in term of its working principle and robustness against common attacks which considering ideal and real scenario of a QKD set-up.

All the results are clearly categorized under certain design and performance parameters as specified in the Figure 1.1. The results are important in evaluating the protocol for each methodology.

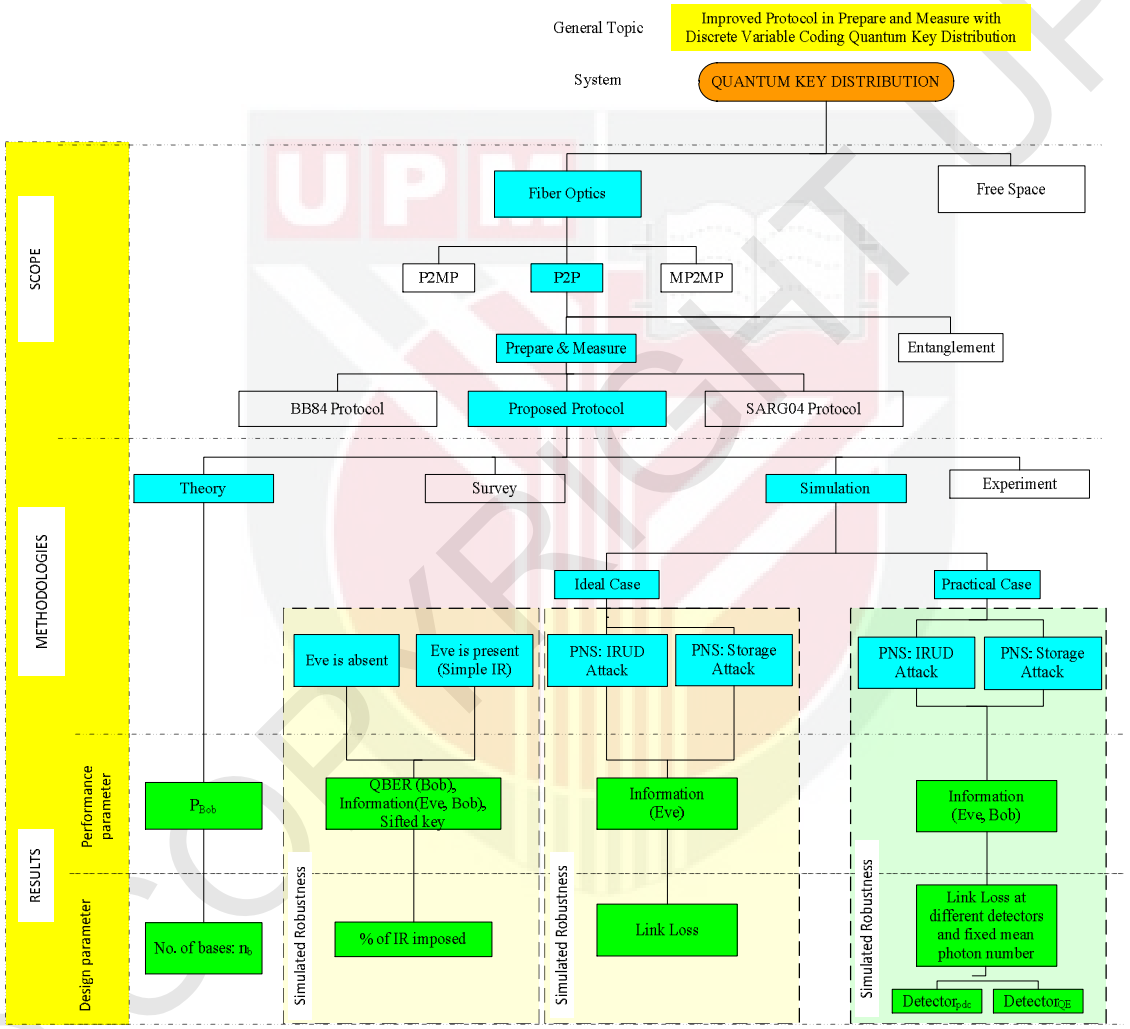

Figure 1.1. Research overview

1.5 Organization of the Thesis

The organization of this thesis is described as follows:

Chapter 1 begins with introduction and brief review on the milestone of quantum cryptography and followed by the objectives of the study, scope of the work and problem statement.

The implementation issues are described briefly in the early part of Chapter 2 while the rest part of the chapter describes in details the established QKD protocols and states the reasons of choosing the BB84 and SARG04 protocols as the main pillars in developing this new protocol.

In Chapter 3, the methodology used in this research of the proposed protocol is presented. It includes a combination of new decoding rule and the SARG04 decoding scheme, sifting process and the robustness test against basic IR and PNS attacks.

In Chapters 4, the performance evaluation of the proposed protocol is presented and discussed thoroughly. In this chapter, improved performance of the protocol is discussed based on the obtained results and is compared against the BB84 and SARG04 protocols which are the existing QKD protocols.

Finally, the conclusions and the proposed future works are drawn in Chapter 5.

REFERENCES

[1] V. Makarov, "Quantum cryptography and quantum cryptanalysis," in *Thesis for the degree doktor ingeniør* Trondheim: Norwegian University of Science and Technology, 2007.

[2] G. E. Dagmar Bruß, Tim Meyer, Tobias Riege, Jörg Rothe, "Quantum cryptography: A survey," *ACM Comput. Surv.,* vol. 39, 2007.

[3] W. Stallings, *Cryptography and Network Security*. New Delhi: Prentice-Hall of India, 2007.

[4] I. Leon W. Couch, *Digital and Analog Communication Systems*. New Jersey, USA: Pearson Prentice Hall, 2001.

[5] W. Stallings, *Data and Computer Communications*. upper saddle river, New Jersey, USA: Prentice-Hall, International, 1997.

[6] M. Javed, Aziz, Khurram, "A survey of quantum key distribution protocols," in *Proceedings of the 6th International Conference on Frontiers of Information Technology*, Abbottabad, Pakistan, 2009.

[7] M. Blumenthal, "Encryption: Strengths and Weaknesses of Public-key Cryptography," in *Proceedings of the Computer Science Research Symposium*, 2007, pp. 1-7.

[8] M. A. N. I.L. Chuang, *Quantum Computation and Quantum Information*. UK: Cambridge University Press, 2000.

[9] V. Scarani, Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lutkenhaus, N., Peev, M., "A framework for practical quantum cryptography," *Reviews of Modern Physics,* vol. 81, pp. 1301-1350, Sept. 2009.

[10] N. Gisin, Ribordy, G. ,Tittel, W. ,Zbinden,H. , "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, pp. 145-195, March 2002.

[11] M. Dusek, Lütkenhaus,N., Hendrych,M. , "Quantum Cryptography," in *Progress in Optics*. vol. 6, E. Wolf, Ed. New York: Elsevier, 2006, pp. 381–454.

[12] S. Singh, *The code book : the science of secrecy from ancient Egypt to quantum cryptography*. New York: Anchor Books, 2000.

[13] G. Brassard, Bennett, C. H., "Quantum Cryptography: Public key distribution and coin tossing," in *Proc. of the IEEE Int. Conf. on Comp., Sys and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[14] V. Scarani, Acín, A., Ribordy, G., Gisin, N., "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters,* vol. 92, p. 057 901, Feb 2004.

[15] N. R. M. S. Mohd Khazani Abdullah, Nordin Jamaluddin,Ahmad Samsuri Mokhtar, A. Rahim Abu Talib & Mohd Faizal Zainuddin, "K-chart: a tool for research planning and monitoring," *Journal of Quality Measurement and Analysis (JQMA),* vol. 2, pp. 123-129, 2006.

[16] T. C. R. H-A. Bachor, *A Guide to Experiments in Quantum Optics*: Wiley-VCH Verlag GmbH & Co. KGaA 2004.

[17] W. H. W. Mauerer, Ch. Silberhorn, "Recent developments in quantum key distribution: Theory and practice," *Annalen der Physik,* vol. 17, pp. 158–175, February 2008.

[18] A. Zavriyev and P. B. Alexei Trifonov, D. Mohatt, E Noonan, T. Roberts, " Practical single photon source for quantum communications," in *Proc. SPIE on Quantum Information and Computation III*, 2005, pp. 159-163.

[19] S. Barry, Vuckovic,J. , Grangier,P, "Single photons on demand," in *Europhysics News*. vol. 36, E. S. Journals, Ed., 2005.
[20] A. S. Tsuyoshi Nishioka, Toshio Hasegawa, Toyohiro Tsurumaru, Jun'ichi Abe, Shigeki Takeuchi, "Single-Photon Interference Experiment Over 80 km with a Pulse-Driven Heralded Single-Photon Source," *IEEE Photonics Technol. Lett.,* vol. 20.
[21] C. M. Kurtsiefer, S, Zarda, P, Weinfurter, H, "Stable Solid-State Source of Single Photons," *Phys. Rev. Lett.,* vol. 85, pp. 290-293, July 2000.
[22] O. T. Alibart, S. Ostrowsky, D.B, De Micheli, M.P, Baldi, P, "High performance guided-wave heralded single photon source at telecom wavelength," in *Proceedings of the SPIE*, 2005, pp. 592-601.
[23] G. V. Assche, *Quantum Cryptography and Secret Key Distillation*: Cambridge University Press, 2006.
[24] W. H. Steeb, Hardy,Y. , *Problems & Solutions in Quantum Computation and Quantum Information*: World Scientific Publishing. Co. Ptd 2004.
[25] P. Kaye, Laflamme,R. ,Mosca, M. , *An Introduction to Quantum Computing*: Oxford University Press, 2007.
[26] S. Imre, Balazs, F. , *Quantum Computing and Communications: An Engineering Approach*: John Wiley & Sons Ltd 2005.
[27] S. a. A.-K. Al-Kathiri, W. and Hafizulfika, M. and Wahiddin, M.R. and Saharudin, S, "Characterization of mean photon number for key distribution system using faint laser," in *International Conference on Computer and Communication Engineering (ICCCE)*, 2008, pp. 1237-1242.
[28] D. Pearson, Elliott, C. , "On the Optimal Mean Photon Number for Quantum Cryptography," in http://arxiv.org, 2004.
[29] J. M. Myers, Wu, T.T.,Pearson, D.S., "Entropy estimates for individual attacks on the BB84 protocol for quantum key distribution," in *Proceedings of SPIE*, 2004, p. 36.
[30] B. Slutsky, Rao,R. , Sun,P. ,Tancevski, L. ,Fainman, S. , "Defense frontier analysis of quantum cryptographic systems," *Applied Optics,* vol. 37, pp. 2869–2878, May 1998.
[31] E. Chip, Henry Yeh, "Final Tech. Rep. AFRL-IF-RS-TR-2007-180," BBN Technologies, Cambridge MA, Final2007.
[32] J. C. Palais, *Fiber optic communications*. Upper Saddle River, New Jersey: USA: Prentice-Hall Inc., 1998.
[33] Mrzeon, "Optical fiber types." vol. 2010, 2007.
[34] M. Curty, Lütkenhaus,N. , "Practical quantum key distribution: On the security evaluation with inefficient single photon detectors," *Physical Review A,* vol. 69, p. 042321, 2004.
[35] S. A. Namekata, S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," *Opt. Express,* vol. 17, pp. 6275-6282.
[36] Z. L. Yuan, Kardynal, B. E. ,Sharpe, A. W. , Shields,A. J. , "High speed single photon detection in the near infrared," *Appl. Phys. Lett. ,* vol. 91, pp. 0411141-0411143, 2007.
[37] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photonics,* vol. 3, pp. 696 - 705, December.
[38] A. Antonio, Gisin ,N., Scarani, V., "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A,* vol. 69, p. 012309, Jan 2004.

[39] C. Branciard, Gisin, N. ,Kraus, B.,Scarani, V., "Security of two quantum cryptography protocols using the same four qubit states," *Phys. Rev. A.,* vol. 72, p. 032301, Sept 2005.
[40] I. MagiQ Technologies, in *http://www.magiqtech.com*.
[41] idquantique, in *http://www.idquantique.co:* idquantique.
[42] L. Greenemeier, "Scientific American," 2007.
[43] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *PhysRevLett,* vol. 68, pp. 3121-3124, 1992.
[44] M. K. K. Tamaki, and Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Phys. Rev. Lett,* vol. 90, p. 167904, 2003.
[45] K. Tamaki, Lutkenhaus,N., "Unconditional security of the Bennett 1992 quantum key distribution protocol over a lossy and noisy channel," *Phys. Rev. A.,* vol. 69, p. 032316, 2004.
[46] M. Koashi, "Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse," *Phys. Rev. Lett,* vol. 93, p. 120501, 2004.
[47] K. Tamaki, Lutkenhaus, N. , Koashi,M. ,Batuwantudawe, J. , "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse," *Phys. Rev. A.,* vol. 80, p. 032302, 2009.
[48] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States," *Phy Rev Lett,* vol. 81, oct. 1998.
[49] N. Gisin, Bechmann-Pasquinucc, H., "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phy Rev A,* vol. 59, june 1999.
[50] A. A. V. Scarani, G. Ribordy, and N. Gisin, "Quantum cryptography protocol," 2003.
[51] J. Calsamiglia, Barnett, S. M.,Lütkenhaus, N. , "Conditional beam-splitting attack on quantum key Distribution," *Phys. Rev. A,* vol. 65, pp. 012312.1 - 012312.12, 2002.
[52] G. Brassard, Lütkenhaus,N., Mor,T., Sanders,B.C., "Security Aspects of Practical Quantum Cryptography," *Phys. Rev. Lett.,,* vol. 85, pp. pp.1330–1333, 2000.
[53] C. H. Bennett, Bessette, F.,Brassard, G. , Salvail, L., Smolin,J. , "Experimental quantum cryptography," *Journal of Cryptology* vol. 5, pp. 3-28, 1992.
[54] A.Pereszlenyi, "Simulation of quantum key distribution with noisy channels," in *Proc. of International Conference on Telecommunication, ConTEL* 2005.
[55] V. S. A. Niederberger, N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography," *Phys. Rev. A.,* vol. 71, p. 042316, 2005.
[56] K. C. Lustic, "Performance Analysis and Optimization of the Winnow Secret Key Reconciliation Protocol," in *Department of Electrical and Computer Engineering*. vol. Master of Science Ohio: Air Force Institute of Technology, Air University, 2011, p. 106.
[57] K. C. Lustic, "Performance Analysis and Optimization of the Winnow Secret Key Reconciliation Protocol," in *AFIT/GCO/ENG11-08*: Graduate School of Engineering and Management Air Force Institute of Technology Air University 2011.
[58] I. Quantique, "Understanding quantum cryptography," Id quantique switzerland, white paper 2005.