ENHANCED WINNOW KEY RECONCILIATION FOR BENNETT-BRASSARD 84 QUANTUM KEY DISTRIBUTION PROTOCOL

RIAZ AHMAD QAMAR

FACULTY OF COMPUTING
UNIVERSITI TEKNOLOGI MALAYSIA

ENHANCED WINNOW KEY RECONCILIATION FOR BENNETT-BRASSARD 84 QUANTUM KEY DISTRIBUTION PROTOCOL

RIAZ AHMAD QAMAR

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

AUGUST 2013

Dedicated to my beloved mother, sister Farhat Nasima, dearest wife and daughter for their enduring love, motivation and support.

ACKNOWLEGEMENT

All praise to Almighty Allah for his blessings and to conduct this research. I am highly grateful to my main supervisor, Professor Dr. Mohd Aizaini Maarof and co-supervisor Associate Professor Dr. Subariah Ibrahim for their encouragement, guidance, criticism and academic freedom during the working in this research study. The high standards set by them have not only greatly contributed to the quality of this work but also helped me become a better person.

I would like to express my gratitude to Universiti Teknologi Malaysia for the financial aid, facilities and opportunity given to me to pursue this study.

I would also like to thank all staff of Department who have encouraged and assisted me throughout this study to make this thesis success.

I wish to extend my gratitude to my parents and my family for their inspiration and continuing support.

ABSTRACT

Quantum cryptography specifically called Quantum Key Distribution (QKD) provides acceptable levels of secure communications by utilising established laws of quantum mechanics. QKD protocol distributes a raw key through quantum channel between two cryptography users and then it removes errors occurred during communication from the distributed key by passing messages via public channel. Most popular error reconciliation protocols such as Binary, Cascade and Winnow are used to remove errors in a secure way. Among these three protocols, Buttler's Winnow has the advantage of less communication complexity, however it is less effective at high error rates in a key and has the disadvantage of introducing errors during error reconciliation, and hence, causes reduction in reconciled key size and/or leave errors in the reconciled key. Winnow can handle quantum bit error rates a maximum up to 18 percent. However, after 13 percent error rate, Winnow becomes highly interactive and it may fail to reconcile the key. The deficiencies of high interactivity, reduction in reconciled key size, leaving errors in the reconciled key and failure of Winnow can be removed by enhancing the error reconciliation protocol by employing modified Bose, Chaudhuri, Hocquenghem (BCH) channel coding techniques. The enhanced BCH encoding algorithm is designed to handle a key at higher quantum bit error rates. BCH error detection and correction algorithms are enhanced to minimise the error percentage in the reconciled key. The modified block interleaver is introduced in the reconciliation protocol to obtain a long-size reconciled key with minimum iterations. The enhanced error reconciliation protocol can reconcile the key up to 50 percent initial bit error rate and reduces public channel communications. Finally, a long sized identical shared secret key with minimal error rate approaching zero is obtained within two iterations. The attained key can be used with secret key cipher to encrypt and decrypt information.

ABSTRAK

Kriptografi kuantum secara khususnya dikenali sebagai Pengagihan Kekunci Kuantum (QKD), menyediakan tahap komunikasi selamat yang boleh diterima dengan menggunakan undang-undang mekanik kuantum yang telah mantap. Protokol QKD mengagihkan kekunci mentah melalui saluran kuantum di antara dua pengguna kriptografi dan kemudian ia membuang ralat yang berlaku semasa komunikasi dari kekunci teragih dengan menghantar mesej melalui saluran umum. Protokol penyelarasan ralat yang paling popular seperti Binary, Cascade dan Winnow digunakan untuk membuang ralat secara selamat. Antara ketiga-tiga protokol ini, Winnow Buttler mempunyai kelebihan dengan mempunyai komunikasi yang kurang rumit, walau bagaimanapun, ia kurang berkesan pada kekunci yang mempunyai kadar ralat yang tinggi dan mempunyai kelemahan dalam memperkenalkan ralat semasa penyelarasan ralat. Dengan itu menyebabkan pengurangan saiz kekunci terselaras dan/atau meninggalkan ralat dalam kekunci terselaras. Winnow boleh mengendalikan kadar ralat bit kuantum sehingga maksimum 18 peratus. Tetapi, selepas 13 kadar ralat peratus, Winnow menjadi sangat interaktif dan ia mungkin gagal untuk menyelaras kekunci. Kekurangan interaktiviti yang tinggi, pengurangan dalam saiz kekunci terselaras, meninggalkan ralat dalam kekunci terselaras dan kegagalan Winnow boleh dibuang dengan mempertingkatkan protokol penyelarasan ralat dengan menggunakan teknik pengkodan saluran Bose, Chaudhuri, Hocquenghem (BCH) yang diubahsuai. Algoritma pengekodan BCH yang telah dipertingkatkan direka untuk mengendalikan kekunci pada kadar ralat bit kuantum yang lebih tinggi. Algoritma pengesanan dan pembetulan ralat BCH dipertingkatkan untuk meminimumkan peratusan ralat dalam kekunci terselaras. Blok selang-seli yang diubahsuai diperkenalkan dalam protokol penyelarasan untuk mendapatkan kekunci terselaras yang bersaiz panjang dengan lelaran minimum. Protokol penyelarasan ralat yang telah dipertingkatkan boleh menyelaras kekunci sehingga 50 peratus kadar ralat bit awalan dan mengurangkan komunikasi saluran umum. Akhirnya, kekunci rahsia berkongsi serupa yang bersaiz panjang dengan kadar ralat minimum menghampiri sifar diperolehi dalam dua lelaran. Kekunci yang diperolehi boleh digunakan dengan sifer kekunci rahsia untuk menyulit dan menyahsulit maklumat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

B92	-	Bennett protocol published in 1992
BB84	-	Bennett-Brassard protocol published in1984
BBBSS	-	Bennett-Bessette-Brassard-Salvia-Smolin
BCH	-	Bose, Chaudhuri, Hocquenghem
CB	-	corrected blocks
EC	-	error correction
ECC	-	error correction codes
EEA	-	enhanced encoding algorithm
EECA	-	enhanced error correction algorithm
EEDA	-	enhanced error detection algorithm
FEC	-	forward error correcting codes
FLT	-	full size lookup table
GF	-	Galois field
GG02	-	the protocol of Grosshans and Grangier published in 2002
IEC	-	interactive error correction
LDPC	-	low-density parity check code
LCM	-	lowest common multiple
MLTs	-	multiple lookup tables
NB	-	no-error blocks
PGZ	-	Peterson-Gorenstein-Zierler
PNS	-	photon number splitting
QBER	-	quantum bit error rate
QKD	-	quantum key distribution protocol
REM	-	remainder of division
RLT	-	refined lookup table
RSLT	-	reduced size lookup table

SA	-	standard array
SARG04	-	Scarani-Acin-Ribordy-Gisin protocol published in 2004
SB	-	swapped blocks
SB_p	-	swapped blocks' positions
SET	-	simplified encoding table
UB	-	uncorrected blocks
UB_p	-	uncorrected blocks' positions
WM	-	weighted method
XOR	-	exclusive OR operation (modulo-2)

LIST OF SYMBOLS

A	-	Alice's message blocks
a	-	subscript used for Alice
B	-	Bob's message blocks
BCH(n,k,t)	-	BCH code with code length n, message length k and error correcting capacity t
b	-	subscript used for Bob
C	-	Channel capacity
$c(X)$	-	code polynomial
d_{min}	-	minimum Hamming distance
e	-	error pattern
E	-	error rate
$F(X)$	-	factor polynomial
G	-	generator matrix
G_{sys}	-	systematic generator matrix
$g(X)$	-	generator polynomial
H	-	parity check matrix
$H(X)$	-	Shannon's entropy
h	-	hash function
i	-	used for indices, index i
j	-	used for indices, index j
k	-	message block length
L	-	length of sifted key
m	-	degree of primitive polynomial
M	-	message vector
$m(X)$	-	message polynomial
n	-	code word length, number of bits in a code word

N_h	-	length of a block in bits
p	-	probability
P	-	parity vector
$p(X)$	-	primitive polynomial
q	-	q-ary (q=2) 2 binary digits
$q(X)$	-	quotient polynomial
R	-	received vector
r	-	code rate
$r(X)$	-	remainder polynomial
S	-	syndrome
S_d	-	syndrome difference
t	-	number of errors
V	-	vector space
w	-	weight of a message block (number of non-zero bits)
X_i	-	bit at *i*th position
$\oplus$	–	the mod 2 bitwise addition of bit strings or bit vectors
$\lfloor\ \rfloor$	-	floor brackets, rounds number to lower integer e.g.; $\lfloor 7.3 \rfloor = 7$
$\sum$	-	sigma, sum of all values in range of series

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In today's world, where large amount of information travels through communication networks for commerce, strategic and military use, a secure data transfer is essential (Nguyen *et al.*, 2006). Over time, various methods have been adopted for secure information transfer from one legitimate party to another. Currently, cryptography, a branch of science that deals with information security, is playing an important role to meet commerce, strategic and military requirements. One of the mechanisms to secure information in cryptography is called encryption. Encryption is a method of transforming information that conceals its meaning. The reverse process of encryption is termed as decryption and an algorithm that encrypts and decrypts information is called a cipher. A cryptosystem consists of information to be encrypted/decrypted, an algorithm and a key. A good cryptographic algorithm should provide confidentiality/privacy, integrity, authentication and non-repudiation. The concept of cryptography evolved soon after humans learned to communicate through writing, since then a number of cryptography techniques ranging from basic shifting of alphabetical letters to complex mechanical and electronic encryption methods have been used. Historical ciphers, which are known as paper and pen ciphers, used substitution and transposition methods for information encryption or decryption (Katz and Lindell, 2008). The conventional cryptography has three elements namely algorithm, message and key. In conventional ciphers, key is most important element of cryptography and it is nearly impossible to get back the original message without it. A cryptography key is exchanged secretly between two users through a secured communication channel. The cryptographers' community agrees to keep the key secret and to publish encryption algorithms. The purpose of publishing encryption algorithm is to identify the flaws and to make it more robust against attackers. Among other factors, Kerckhoff's principle enunciates that the security of a cryptosystem should rely on the secrecy of the key instead, the secrecy of the algorithm (Van Assche, 2006). In the 1970s, IBM designed the most common encryption scheme, which is termed as Data Encryption Standard (DES). DES was adopted by the National Bureau of Standards, presently named as the National Institute for Standards and Technology (NIST), in 1977 (Kessler, 2003). Cryptography entered into a new era when Charles Bennett and Gilles Brassard developed a quantum key distribution protocol, named BB84 in 1984, after reading a "conjugate coding" paper written by Stephen Weisner in early 1970s.

Conventional ciphers are categorized, more commonly, on bases of the type of key used. Symmetric key ciphers, which are known as secret-key ciphers (Kessler, 2003), use the same key for encryption and decryption while asymmetric key ciphers, also known as public-key ciphers, use two different but co-related keys for encryption and decryption. Symmetric key encryption is required to share a secret key between two cryptography users in order to exchange messages secretly. DES and Advanced Encryption Standards (AES) are symmetric key ciphers whereas Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA) and Elliptic curve ciphers are well known asymmetric key ciphers. Symmetric cryptography is more secure but exchange of secret key is usually inconvenient so, asymmetric cryptography provides an alternative. In public key cryptography (asymmetric) two keys are used, a public key for encryption and a private key for decryption. Public key ciphers are based on hard computational problems, for example RSA cipher relies on the difficulty of factorization. Elliptic curve cryptography offers a comparable security but with shorter key length. Thus, presently hybrid cryptographic system is used to exchange messages more efficiently and securely. In this system the key is exchanged by using an asymmetric-key cipher, and the message is encrypted using a symmetric-key cipher. Major Joseph Mauborgne and Gilbert Vernam invented a perfect secure cipher “one time pad” in 1917. One-time pad cipher has a strong evidence of security but requires a key length equal to that of a plaintext message. However, practically it was considered inconvenient, especially for longer messages. Secret key ciphers are considered more secure but the key distribution is a major problem in these ciphers. Quantum cryptography, more precisely called quantum key distribution (QKD), has solved the problem of key distribution of conventional cryptography by using quantum information science. In contrast with conventional cryptography that uses unproven mathematical techniques (Elboukhari *et al.*, 2009; GÜMÜŞ, 2012); quantum cryptography employs proven secure laws of quantum mechanics. Thus, quantum cryptography provides acceptable levels of secure distribution of a key, which is used with secret-key cipher or with one-time pad.

The first quantum key distribution protocol BB84 was developed by Gilles Brassard and Charles Bennett in 1984 (Bennett and Brassard, 1984). BB84 comprises of two main steps that are quantum state transmission and conventional post processing. In the quantum state transmission, one party generates a sequence of random bits (0 or 1) called raw key and transmits it to a second party through quantum channel by encoding quantum carriers, e.g.; photons or laser pulses, into polarization state using randomly selected two basis – rectilinear and diagonal. Second party decodes quantum carriers and obtains a raw key. It is quite possible that both parties, conventionally called Alice and Bob, may have different versions of raw key because of errors produced in the raw key. The source of errors may be imperfections or malfunctioning of quantum channel devices or presence of a potential eavesdropper at the quantum channel. These errors in the raw key are removed in a post quantum transmission phase, which is known as conventional post processing phase. In conventional post processing phase, key sifting and key distillation processes are carried out by exchanging messages through unsecure public communication channels such as wireless, internet or telephone lines. In key sifting process both parties compare their basis and discard all bits from their list for which the basis are unequal. The key obtained in the key sifting process is known as sifted key. Key distillation process is further divided into two phases namely error reconciliation (also called key reconciliation) and privacy amplification. In error reconciliation phase errors are removed from the sifted key whilst privacy amplification is used to diminish the knowledge of eavesdropper about the key. The progressive steps of a QKD protocol are given in Figure 1.1, and are discussed in subsequent chapters. This study is focussed on error reconciliation.

Quantum cryptography is being used by some government agencies and banks. Previously, the longest distance over which an encrypted key could send, along fiber cables or through the atmosphere, was approximately 100 kilometers (Optical Society of America, 2010). However, optical key distribution via these channels is limited to distances of less than 200 km due to signal losses along the way (Ludwig-Maximilians-Universitaet Muenchen, 2013). In 2007, Ludwig-Maximilians-Universitaet Muenchen (LMU) physicist Harald Weinfurter and his group successfully transmitted a key over 144 km of free space between ground stations on the islands of Tenerife and La Palma. Georgia Tech team developed a new technology that arranges series of quantum devices – arrayed like Christmas lights on a string -- could reach distances in excess of 1,000 kilometers via glass-fiber cable (Optical Society of America, 2010). A team led by Weinfurter and Sebastian Nauerth at the Physics Faculty at LMU Munich, in collaboration with the German Center for Aeronautics and Space Research (DLR), has now succeeded in optically transmitting quantum information between a ground station and a plane in

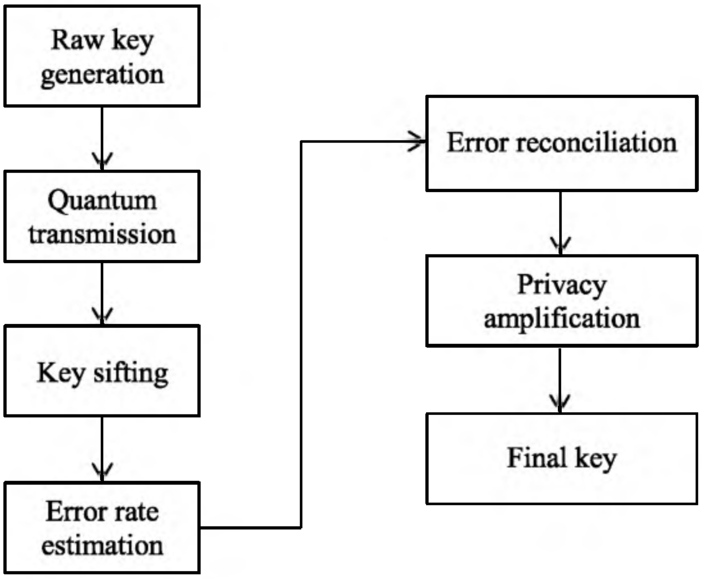

Figure 1.1: Quantum key distribution protocol BB84

flight. This is the first time that quantum cryptography has been used for communication with a mobile transmitter (Ludwig-Maximilians-Universitaet Muenchen, 2013).

1.2 Background of the Study

Error reconciliation is an important phase in the key distillation process because an identical key for secret-key ciphers or one-time pad is required. In this phase, protocols are used to reconcile a key by exchanging messages between two users e.g.; Alice and Bob, through a public channel. The popular error reconciliation protocols are developed for error correction in the key. In 1992 five researchers, Bennett, Brassard, Bessette, Salvail and Smolin, put their research together and developed an error reconciliation protocol and they named it Binary. Binary protocol uses binary search to correct discrepancies in the key. Binary search is a simple way to detect and correct one error per block. Alice and Bob start a binary search upon the blocks for mismatching parties. They bisect blocks into sub-blocks and publicly compare the parities of each sub-block. This process is continued until an error is detected in the block. Binary corrects one error in a block and uses several iterations.

Brassard and Salvail (1994) developed Cascade protocol, the second famous error reconciliation protocol, which is an improved version of Binary protocol. The choice of block size has a great significance in Cascade protocol and it depends on the estimated error in the key. For small block size, the parity bits are needlessly disclosed to an eavesdropper for the blocks containing no error and large sized block needs more iterations to correct all errors. After comparing parities of blocks, Binary is used to correct errors. Another difference between Cascade and Binary can be seen in second and onward iterations where block size becomes double as in the previous iteration. From second iteration onwards, every iteration corrects two errors for every erroneous bit detected. Brassard and Salvail claimed in his original paper that four such iterations are sufficient to correct all errors in a key for realistic initial error rates. Since the publication of Cascade, it has been thoroughly studied and many enhancements have been proposed (Calver, 2011). Sugimoto and Yamazaki (2000) suggested applying alternate block strategy after two iterations; since most of the errors have been removed after second iteration. This improves the protocol efficiency compared with the original one. A dynamic block size selection was proposed by Rass and Kollmitzer in 2009 with the use of enhanced permutation function between two iterations (Bellot and Dang, 2009). The rate of interactivity in Cascade is very high due to the necessary parity exchanges. Cascade uses random bit permutations after each pass to distribute errors. These permutations my accumulate errors in a block instead to distribute therefore, size of the reconciled key is unpredictable in Cascade.

Winnow, an error reconciliation protocol, was proposed by Buttler *et al.*, (2003) for QKD which offers lower interactivity and better throughput. Like Binary and Cascade, it also partitions binary string into blocks. Alice and Bob exchange parities of all their blocks and thus determine the blocks that contain odd number of errors. For blocks of diverging parity, Alice sends Bob the syndrome of a Hamming code calculated over her block. A syndrome is an error indicator that is calculated by multiplying message vector with a parity check matrix of the code. Unlike Binary and Cascade, which use a bisection, the correction of a block using the Hamming code does not necessarily reduce the number of errors in that block. The Hamming code proposed in Winnow allows Alice and Bob to correct one error. If more than one error is present in a block, Bob's attempt may actually increase the number of errors in that block, thus, block size should be chosen in such a way that it globally reduces the number of errors. Unlike Cascade, the iterations of Winnow are independent of each other and so an exhaustive search could be performed at a low complexity using dynamic programming. Later on error correction capability of Winnow protocol was analysed and estimated by (Zhao *et al.* 2007). They believed that Winnow protocol removed errors efficiently at higher initial error rates (>7%), for smaller block size such as k = 8 bits (Zhao *et al.* 2007). (Yan *et al.* 2009) analysed the efficiency of Winnow protocol and suggested the optimal block size theoretically and experimentally for different error rate. In Winnow protocol, error rate is estimated by publicly comparing a random subset of sifted key bits. Lustic (2011) suggested a probabilistic approach for error estimation instead of publicly comparing and discarding sifted key bits. He also gave an efficient block-size schedule at given initial error rate. Even though Winnow is a fast and efficient protocol, it has the following discrepancies:

i. Cascade protocol performs better than Winnow for quantum bit error rate (QBER) up to about 10%, while between 10% and 18%, Winnow is more efficient but it does not perform well above 18% error rate. From 18% to 25% Cascade is used (Van Assche, 2006).

ii. In Winnow protocol, both legitimate parties compute syndromes of their respective blocks separately using a Hamming code. After exchanging syndromes, they calculate syndrome difference as $S_d = S_a \oplus S_b$ ($\oplus$ means exclusive OR). The syndrome difference S_d does not distinguish between single- and multiple-bit errors in a block. Therefore, an additional error is introduced in a block when applying Hamming error correction method if $S_d \neq \{0\}^m$ so the block already contains more than one error.

iii. Winnow is not applied to the blocks containing an even number of errors because it uses parity check method for error detection. Moreover, Hamming algorithm always corrects any single error within a k-bit block.

iv. Interactivity of Winnow protocol increases (requires many iterations) with increase in QBER and/or error-bursts in the sifted key, which reduces the key-security and hence reduces the size of final key.

The present research addresses the aforementioned issues of Winnow protocol by augmenting methods of encoding, error detection and correction algorithms.

1.3 Statement of Problem

An error reconciliation protocol corrects errors in a sifted key, which are produced due to imperfection of devices used in a quantum channel and/or presence of an adversary during quantum communications. Cascade protocol is an improved version of the first reconciliation protocol that is BBBSS. Both protocols, BBBSS and Cascade, use binary search to single out the error in a block of bits and then flip the erroneous bit to correct error. Cascade is more efficient than BBBSS to correct errors because it keeps the record of previously investigated blocks and search back the investigated blocks to correct errors from those. Cascade can only correct one error in a block of any size. Because, Cascade protocol uses binary search to detect error in a block therefore, it is highly interactive protocol. Many interactions (parity exchanges) are required between Alice and Bob. Winnow, an error reconciliation protocol, performs efficiently in removing errors as compare to Cascade. Winnow uses Hamming error correcting method to detect and correct errors and it is comparatively less interactive. It detects errors in a block by using parity comparison of receiver and sender's block. If a block contains an even number of errors, the parity comparison claims that the block has no error. In other words, Winnow can only detect erroneous blocks that have an odd number of errors. Furthermore, Winnow protocol relies on Hamming error correcting code, which can correct only one error in a block of any size. If a block contains an odd number of errors greater than one, Hamming code introduces one more error instead of removing the error within the block. Either this situation increases the number of iterations to correct errors or Winnow may fail at high quantum bit error rates. In addition, the performance of Winnow decreases with increases in error-bursts in the sifted key.

The study developed a protocol which resolves issues of secret key reconciliation of quantum key distribution process. The research question is:

"*How to devise a fast and efficient method that provides a higher key generation rate so that the minimum final error probability approaches to zero in the secret-reconciled key at higher quantum bit error rate (QBER).*"

To answer this question, the following assumptions are made:

i. Sifted key comprises of binary digits.

ii. The conventional communication channel is a binary symmetric channel (BSC), for example, the entropy of the channel does not exceed the theoretical limit of Shannon's entropy.

iii. The channel is an authenticated public channel.

In addition, several sub-questions are raised as follows:

i. How do the existing error reconciliation protocols e.g.; Binary, Cascade and Winnow compare to each other at given initial sifted key error rate? And in case of burst errors in the sifted key?

ii. How to modify an error correction code to enhance error correction capability?

iii. What is the effect of block size on effectiveness of reconciliation protocol?

iv. How does an interleaver increase length of a reconciled key?

1.4 Purpose of Study

The aim of the research is to enhance secret key reconciliation to obtain a long-sized shared identical secret key by enhancing error reconciliation protocol.

1.5 Objectives of Study

Quantum key distributions protocol in theory offers unconditional security for key exchange but in reality, there are some technical limitations. For example, practical systems cannot achieve flawless quantum transmission that is required in an ideal quantum key distribution protocol. In addition to this, interference by an eavesdropper cannot be ignored, which leads to produce errors in the transmitted key. These errors must be resolved prior to applying key for cryptography. Efficiently reconciling these errors is the focus of this study. Specifically, this thesis will first enhance the BCH codes and then use these Enhanced BCH codes for efficient error reconciliation. The following objectives are set to achieve the aim of this research:

i. To increase the initial error handling capacity of error reconciliation protocol by designing an enhanced BCH encoding algorithm and plugging it into existing Winnow protocol.

ii. To minimize the final key bit error rate by design of enhanced BCH error detection and error correction algorithms and replacing the Hamming algorithm in Winnow protocol by the enhanced BCH error detection and error correction algorithms. The Winnow protocol with enhanced BCH encoding, error detection and correction algorithms is known as enhanced reconciliation protocol.

iii. To increase length of the reconciled secret key by designing and implementing a modified block interleaver in between two passes (iterations) of the enhanced reconciliation protocol.

1.6 Scope of Study

This research engaged in an in-depth study of components of quantum cryptography used for securing information in networks. The error reconciliation phase of quantum cryptography is an important part of this research. The information and coding theory is a basic component of error reconciliation process. Therefore, this research also focuses on channel coding e.g.; encoding and decoding methods, modifying existing BCH (Bose, Chaudhuri, Hocquenghem) error correction codes. Modifying existing BCH codes means enhancing BCH encoding, error detection and error correction algorithms and their implementation in error reconciliation protocol. In addition, this study designs a modified block interleaver and implementing it in the enhanced reconciliation protocol.

1.7 Significance of the Study

Symmetric cryptography is considered, presently, a more secure information communication technique. The key for symmetric cryptosystem is distributed between users by encrypting it with asymmetric ciphers such as RSA or with Diffie-Hellman key exchange algorithm. These well-known asymmetric ciphers protect key-data based on the computational difficulty techniques. Asymmetric ciphers neither provide secrecy proof nor detect eavesdropping. RSA algorithm that is mainly used for key distribution (Elboukhari *et al.*, 2009) depends upon the unproven computational assumptions. If someone finds a faster technique for factoring large integers, then the amount of computation time reduces significantly to decrypt key-data. Another flaw in RSA cipher is that any hacker can encrypt messages by utilizing public key to a legitimate recipient holding the private key. Moreover, with the advent of quantum computers the short-key encrypted messages would be decrypted by applying brute-force. In the presence of higher computational power, the encrypted-key might be broken easily. Peter W. Shor wrote an algorithm in 1994 that could run on a quantum computer to reverse a one-way function. Several developed cryptosystems, which are based on low computational power, may be failed in the presence of expected quantum computers.

Quantum cryptography is considered an absolute secure key distribution method because of employment of physics based secrecy proofs and capability of eavesdropping detection. Quantum cryptography is regarded as secure information communication technique as long as quantum mechanics laws are valid. The combination of quantum key distribution with conventional asymmetric cryptographic ciphers boosts the confidentiality of information transmissions to an unprecedented level. Quantum cryptography has a bright future and is getting its necessary attention because of its security potential. The MIT Technology Review and Newsweek magazine wrote in 2003 (Quantique, 2009), quantum cryptography as one of the “ten technologies that will change the world”. Quantum cryptography is an emerging technology currently used by both military and financial organizations (Optical Society of America, 2010). Thomas Jennewein and Brendon Higgins from the Institute for Quantum Computing at the University of Waterloo, Canada, say a quantum space race is under way to create the world's first global quantum-communication network. A team led by Weinfurter and Sebastian Nauerth at the Physics Faculty at LMU Munich, in collaboration with the German Center for Aeronautics and Space Research (DLR), for the first time, successfully transmitted a secure quantum code through the atmosphere from an aircraft to a ground station (Ludwig-Maximilians-Universitaet Muenchen, 2013). This research is considered a beginning in quantum cryptography in Universiti Teknologi Malaysia.

1.8 Organization of the Thesis

This thesis is organized into six chapters as shown in the Figure 1.2.

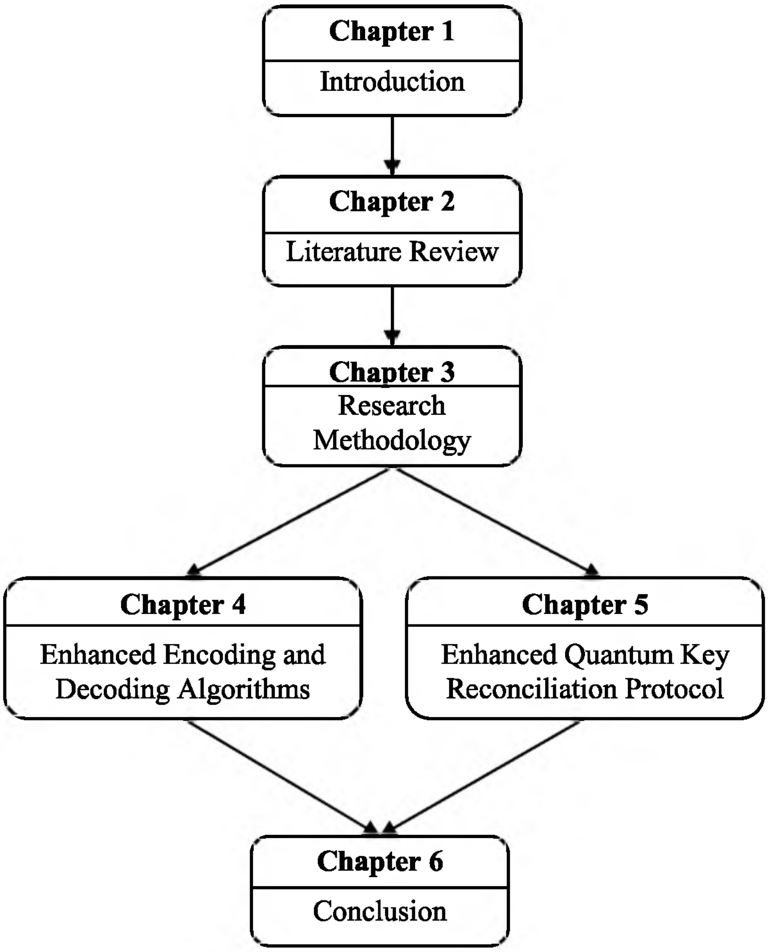

Figure 1.2: Organization of the thesis

Chapter 1 is introduction to the research. It briefly explains the problem statement, purpose of study, objectives and significance of the project. Chapter 2 represents the literature review of quantum cryptography, error reconciliation protocols and error correcting codes that leads to the formulation of the research problem. Chapter 3 is research methodology. This chapter reveals the research framework of the study and highlights the process to obtain a common secret-key for quantum cryptography. Chapter 4 provides the design of enhanced encoder, enhanced error detection and correction algorithms. Chapter 5 describes modified block interleaver, enhanced quantum key reconciliation protocol and their implementation. Chapter 6 concludes the thesis with lists of contributions, findings and recommendations for the future research.

REFERENCES

Alleaume, R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Langer, T. and Leverrier, A. (2007). SECOQC White Paper on Quantum Key Distribution and Cryptography. *arXiv preprint quant-ph/0701168.*

Bellot, P. and Dang, M.-D. (2009). BB84 Implementation and Computer Reality. *Proceedings of the 2009 Computing and Communication Technologies, 2009. RIVF'09. International Conference*: IEEE, 1-8.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J. (1992). Experimental Quantum Cryptography. *Journal of Cryptology*. 5(1), 3-28.

Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the 1984 Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*: Bangalore, India. Vol. 175, No. 0.

Bennett, C. H., Brassard, G., Crépeau, C. and Maurer, U. M. (1995). Generalized Privacy Amplification. *Information Theory, IEEE Transactions on*. 41(6), 1915-1923.

Berlekamp, E. R. (1968). *Algebraic coding theory*. (Vol. 111). New York: McGraw-Hill.

Bose, R. C. and Ray-Chaudhuri, D. K. (1960). On a Class of Error Correcting Binary Group Codes. *Information and Control*. 3(1), 68-79.

Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B. C. (2000). Limitations on Practical Quantum Cryptography. *Physical Review Letters*. 85(6), 1330-1333.

Brassard, G. and Salvail, L. (1994). Secret-key Reconciliation by Public Discussion. *Proceedings of the 1994 Advances in Cryptology—EUROCRYPT'93*: Springer. 410-423.

Buttler, W., Lamoreaux, S., Torgerson, J., Nickel, G., Donahue, C. and Peterson, C. G. (2003). Fast, efficient Error Reconciliation for Quantum Cryptography. *Physical Review A*. 67(5).

Calver, T. I. (2011). *An Empirical Analysis of the Cascade Secret Key Reconciliation Protocol for Quantum Key Distribution*. Masters Thesis. Air Force Institute of Technology, Ohio, USA.

Cerf, N. J., Levy, M. and Van Assche, G. (2001). Quantum Distribution of Gaussian Keys Using Squeezed States. *Physical Review A*. 63(5), 052311.

David, R. N. P. (2007). Introduction to Quantum Key Distribution (Lecture Notes). *Defence Science and Technology Organisation, Australia.*

Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. and Sanpera, A. (1996). Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels. *Physical Review Letters*. 77(13), 2818-2821.

Elboukhari, M., Azizi, A. and Azizi, M. (2009). Implementation of Secure Key Distribution Based on Quantum Cryptography. *Proceedings of the 2009 Multimedia Computing and Systems, 2009. ICMCS'09. International Conference*: IEEE, 361-365.

Elkouss, D., Leverrier, A., Alléaume, R. and Boutros, J. J. (2009). Efficient Reconciliation Protocol for Discrete-variable Quantum Key Distribution. *Proceedings of the 2009 Information Theory, 2009. ISIT 2009. IEEE International Symposium*: IEEE, 1879-1883.

Enzer, D. G., Hadley, P. G., Hughes, R. J., Peterson, C. G. and Kwiat, P. G. (2002). Entangled-photon Six-state Quantum Cryptography. *New Journal of Physics*. 4(1), 45.

Fung, C.-H. and Lo, H.-K. (2007). A Survey on Quantum Cryptographic Protocols and their Security. *Proceedings of the 2007 Electrical and Computer Engineering, CCECE 2007. Canadian Conference*: IEEE, 1121-1124.

Garrabrant, G. and Elliott, K. (2004). *U.S. Patent No. 6,766,490*. Washington DC: U.S. Patent and Trademark Office.

Golay, M. J. (1949). Notes on Digital Coding. *Proc. IRE*. 37(6), 657.

Grosshans, F. and Grangier, P. (2002). Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters*. 88(5), 057902.

GÜMÜŞ, E. (2012). Quantum Cryptography and Comparison of Quantum Key Distribution Protocols. *IU-Journal of Electrical & Electronics Engineering*. 8(1).

Haitjema, M. (2007). *A Survey of the Prominent Quantum Key Distribution Protocols*. URL: http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

Hocquenghem, A. (1959). Codes Correcteurs D'erreurs. *Chiffres*. 2(2), 147-156.

Hrg, D., Budin, L. and Golub, M. (2004). Quantum Cryptography and Security of Information Systems. *Proceedings of the 2004 IEEE Proceedings of the 15th Conference on Information and Intelligent System*, 63-70.

Hughes, R. J., Buttler, W. T., Kwiat, P. G., Luther, G. G., Morgan, G. L., Nordholt, J. E., Peterson, C. G. and Simmons, C. M. (1997). Secure Communications Using Quantum Cryptography. *Proceedings of the 1997 AeroSense'97*: International Society for Optics and Photonics, 2-11.

Institute of Physics (2013). Space Race Underway to Create Quantum Satellite. *ScienceDaily, March 1, 2013.*

http://www.sciencedaily.com/releases/2013/02/130228194653.htm

Kahn, D. (1996). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York:Scribner.

Katz, J. and Lindell, Y. (2008). *Introduction to Modern Cryptography*. UK, London: Chapman and Hall.

Kessler, G. C. (2003). *An Overview of Cryptography. Handbook on Local Area Networks*. Birmingham, UK:Auerbach

Koren, I. and Krishna, C. M. (2010). *Fault-tolerant Systems*. US:Morgan Kaufmann.

Lee, H. P., Chang, H. C., Lin, T. C. and Truong, T. (2008). A Weight Method of Decoding the Binary BCH code. *Proceedings of the 2008 Intelligent Systems Design and Applications, 2008. ISDA'08. Eighth International Conference*: IEEE, 545-549.

Lin, T.-C., Chang, H.-C., Lee, H.-P. and Truong, T.-K. (2010). On the Decoding of the (24, 12, 8) Golay Code. *Information Sciences*. 180(23), 4729-4736.

Lomonaco, S. J. (1999). A Quick Glance at Quantum Cryptography. *Cryptologia*. 23(1), 1-41.

Lorenz, S., Korolkova, N. and Leuchs, G. (2004). Continuous-variable Quantum Key Distribution Using Polarization Encoding and Post Selection. *Applied Physics B*. 79(3), 273-277.

Ludwig-Maximilians-Universitaet Muenchen (2013). Quantum Cryptography: On Wings of Light. *ScienceDaily*, April , 2010.

http://www.sciencedaily.com/releases/2013/04/130403071950.htm

Lustic, K. C. (2011). *Performance Analysis and Optimization of the Winnow Secret Key Reconciliation Protocol*. Masters Thesis. Air Force Institute of Technology, Ohio, USA

Marton, K., SUCIU, A. and IGNAT, I. (2010). Randomness in Digital Cryptography: A survey. *Romanian Journal of Information Science and Technology*. 13, 219-240.

Massey, J. (1969). Shift-register Synthesis and BCH Decoding. *Information Theory, IEEE Transactions on*. 15(1), 122-127.

Mathur, C. N. (2007). *A Mathematical Framework for Combining Error Correction and Encryption*. PhD Thesis, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030.

Matsumoto, M. and Nishimura, T. (1998). Mersenne Twister: a 623-dimensionally Equidistributed Uniform Pseudo-Random Number Generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*. 8(1), 3-30.

Mayers, D. (2001). Unconditional Security in Quantum Cryptography. *Journal of the ACM (JACM)*. 48(3), 351-406.

Moreira, J. C. and Farrell, P. G. (2006). *Essentials of Error-control Coding*. England: John Wiley & Sons.

Morelos-Zaragoza, R. H. (2006). *The Art of Error Correcting Coding*. (2nd ed.) Chichester, UK: John Wiley & Sons, Ltd.

Neubauer, A., Freudenberger, J. and Kuhn, V. (2007). *Coding Theory: Algorithms, Architectures and Applications*. England: John Wiley & Sons.

Nguyen, T. M. T., Sfaxi, M. A. and Ghernaouti-Hélie, S. (2006). 802.11 i Encryption Key Distribution Using Quantum Cryptography. *Journal of Networks*. 1(5), 9-20.

Optical Society of America (2010). Long Distance, Top Secret Messages: Critical Component of Quantum Communication Device may Enable Cryptography. *ScienceDaily,* October 20, 2010.

http://www.sciencedaily.com/releases/2010/10/101019171803.htm

Papanikolaou, N. (2005). An Introduction to Quantum Cryptography. *Crossroads.* 11(3), 3-3.

Peterson, W. W. and Weldon, E. J. (1972). *Error-correcting codes.* (2^{nd} ed.). Cambridge, Mass: MIT press.

Quantique ID. White Paper (2009). Understanding Quantum Cryptography. Ver. 1.1. URL: http://www.idquantique.com

Reed, I. S. and Solomon, G. (1960). Polynomial Codes Over Certain Finite Fields. *Journal of the Society for Industrial & Applied Mathematics.* 8(2), 300-304.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM.* 21(2), 120-126.

Roth, R. (2006). *Introduction to Coding Theory.* New York: Cambridge University Press.

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(5), 057901.

Schuler, C. (1999). *GMD Research Series.* (Vol. 21). University of Chicago: GMD - Forschungszentrum Informationstechnik GmbH.

Sergienko, A. V. (2006). *Quantum Communications and Cryptography.* USA:CRC Press.

Sharbaf, M. S. (2009). Quantum Cryptography: a new Generation of Information Technology Security System. *Proceedings of the 2009 Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference*: IEEE, 1644-1648.

Shor, P. W. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proceedings of the 1994 Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium*: IEEE, 124-134.

Shor, P. W. and Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*. 85(2), 441-444.

Silberhorn, C., Ralph, T. C., Lütkenhaus, N. and Leuchs, G. (2002). Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Physical Review Letters*. 89(16), 167901.

Singal, T. L. (2010). *Wireless Communications*. 7 West Palet Nagar, New Delhi: Tala McGraw Hill Education Private Limited.

Sugimoto, T. and Yamazaki, K. (2000). A Study on Secret Key Reconciliation Protocol. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*. 83(10), 1987-1991.

Sugiyama, Y., Kasahara, M., Hirasawa, S. and Namekawa, T. (1975). A Method for Solving Key Equation for Decoding Goppa codes. *Information and Control*. 27(1), 87-99.

Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershman, B., Bienfang, J. C., Su, D., Boisvert, R. F. and Clark, C. W. (2006). Experimental Study of High Speed Polarization-coding Quantum Key Distribution with Sifted-key Rates Over Mbit/s. *Optics Express*. 14(6), 2062-2070

Teja, V., Banerjee, P., Sharma, N. and Mittal, R. (2007). Quantum Cryptography: State-of-art, Challenges and Future Perspectives. *Proceedings of the 2007 Nanotechnology, 2007. IEEE-NANO 2007. 7th IEEE Conference*: IEEE, 1296-1301.

Tian, X. and Benkrid, K. (2009). Mersenne Twister Random Number Generation on FPGA, CPU and GPU. *Proceedings of the 2009 Adaptive Hardware and Systems, 2009. AHS 2009. NASA/ESA Conference*: IEEE, 460-464.

Tinetti, F. G. (2004). Parallel Computing in Local Area Networks. *Journal of Computer Science & Technology*, 4(2), 21.

Townsend, P. D. (1994). Secure Key Distribution System Based on Quantum Cryptography. *Electronics Letters*. 30(10), 809-811.

Van Assche, G. (2006). *Quantum Cryptography and Secret-Key Distillation*. (6th ed). New York: Cambridge University Press.

Van Assche, G., Cardinal, J. and Cerf, N. J. (2004). Reconciliation of a Quantum-Distributed Gaussian Key. *Information Theory, IEEE Transactions on*. 50(2), 394-400.

Van Dijk, M. and Van Tilborg, H. (1998). The Art of Distilling [Secret Key Generation]. *Proceedings of the 1998 Information Theory Workshop, 1998*: IEEE, 158-159.

Venkatraman, D. (2004). *Methods and Implementation of Quantum Cryptography*. MIT Department of Physics, Cambridge, England, UK.

Watanabe, Y. (2007). Privacy Amplification for Quantum Key Distribution. *Journal of Physics A: Mathematical and Theoretical*. 40(3), F99.

Wicker, S. B. (1995). *Error control Systems for Digital Communication and Storage*. (Vol. 1). Englewood Cliffs: Prentice Hall.

Yamazaki, K., Nair, R. and Yuen, H. P. (2007). Problems of the Cascade Protocol and Renyi Entropy Reduction in Classical and Quantum Key Generation. *arXiv preprint quant-ph/0703012*.

Yamazaki, K., Osaki, M. and Hirota, O. (1998). On Reconciliation Of Discrepant Sequences Shared Through Quantum Mechanical Channels. *Information Security*, 345-356. Springer Berlin Heidelberg.

Yan, H., Peng, X., Lin, X., Jiang, W., Liu, T. and Guo, H. (2009). Efficiency of Winnow Protocol in Secret Key Reconciliation. *Proceedings of the 2009 Computer Science and Information Engineering, 2009 WRI World Congress*: IEEE, 238-242.

Zhao, F., Fu, M., Wang, F., Lu, Y., Liao, C. and Liu, S. (2007). Error reconciliation for Practical Quantum Cryptography. *Optik-International Journal for Light and Electron Optics*. 118(10), 502-506.