UNIVERSITI PUTRA MALAYSIA

A METHOD FOR AUTHENTICATION OF MULTI-USER KEY MANAGEMENT USING QUANTUM KEY DISTRIBUTION OVER NOISELESS CHANNEL

ABUDHAHIR BUHARI

FSKTM 2015 12

A METHOD FOR AUTHENTICATION OF MULTI-USER KEY MANAGEMENT USING QUANTUM KEY DISTRIBUTION OVER NOISELESS CHANNEL

By

ABUDHAHIR BUHARI

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

February 2015

DEDICATIONS

This thesis is dedicated to my family who waited patiently for me

Tomy loving Mother Raheela Banu,

To my caring Father Buhari,

To my supportive Sister Sirin,

To my helping Brother Mohammed Azaruddeen,

To my beautiful and caring Wife Thohirah.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A METHOD FOR AUTHENTICATION OF MULTI-USER KEY MANAGEMENT USING QUANTUM KEY DISTRIBUTION OVER NOISELESS CHANNEL

By

ABUDHAHIR BUHARI

February 2015

Chairperson: Associate Prof. Zuriati Ahmad Zukarnain, PhD
Faculty: Computer Science and Information Technology

Quantum Cryptography (QC) is the emerging field of the current world and the potential player of the future. Quantum Key Distribution (QKD) is the matured discipline of QC and available in the market to establish a secret key between parties. In order to achieve in multiparty, basically quantum entanglement has been applied over a theoretical settings. However, due to practical limitation, entanglement based research has a feasible difficulty with current technology.

The thesis principal goal is to propose a framework for quantum protocol layer for secure key management without entanglement over multiparty environment. In the secret key management, conference key or Multiparty QKD (MQKD) and joint-venture key or Public Shared Secret Quantum Key (PSSQK) protocols acted as a top layer and quantum user authentication scheme as a middle layer and the standard QKD operation as a bottom layer.

The proposed secrete key management protocols are based on secret key between parties using QKD, modified error correction code and linear independent matrix. These protocols require only classical communication and yield higher secret key rate regardless of distance and noise. The security analysis using guessing entropy has applied and results shows only negligible amount information can be extracted during eavesdropping.

The challenge-challenge response technique has been applied to proposed quantum user authentication scheme for verification of quantum user. This is a bidirectional authentication scheme and requires both quantum and classical channel to execute and has two modes of operation, i.e., initial and session authentication.Due to deterministic key distribution orientation, the efficiency of protocol reaches up to 100% in terms of reduction of photon wastage during communication. Further, this scheme is resilient to

various quantum security attacks However, this scheme requires noiseless quantum channel in order to detect the insider and outsider attacks during authentication.

A GUI based discrete event simulation has developed using OptiSystem™ in order to test the practical feasibility of proposed quantum cryptography protocol layer. The polarized based discrete variable QKD protocols have been designed and analyzed. Due to lack of real receiver setup, the results have showed lower quantum bit error rate. Further, we analyzed the impact of polarization structure of qubit due to noise, loss and distance over fiber optics and free space. A multiparty QKD setuphas been designed based on frequency division multiplexing (FDM) centralized quantum channel server. This approach reduces the requirement of total quantum channel from $N*(N-1)/2$ to N and each party requires one quantum channel to communicate with all other parties. The bit commitment protocol and message authentication in the layer has considered for the future research direction.

Abstrak tesis yang dikemukakan oleh Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

KAEDAH PENGESAHAN MULTI PENGGUNA MENGGUNAKAN KUNCI PENGAGIHAN KUANTUM MELALUI SALURAN TANPA GANGGUAN

Oleh

ABUDHAHIR BUHARI

Februari 2015

Pengerusi: Profesor Madya Zuriati Ahmad Zukarnain, PhD
Fakulti: Sains Komputer dan Teknologi Maklumat

Kriptografi kuantum adalah bidang baru di dalam dunia semasa dan berpotensi menjadi keutamaan dari segi penggunaannya di masa hadapan.Pengagihan kunci kuantum adalah disiplin yang agak matang di dalam kriptografi kuantum dan didapati di dalam pasaran untuk mewujudkan satu kunci rahsia di antara pihak-pihak tertentu. Untuk dicapai oleh berbilang pihak, pada asasnya simpulan atau *entanglement* kuantum telah digunakan di dalam penetapan teoritikal. Bagaimanapun, disebabkan had praktikal, penyelidikan berasakan simpulan sukar dilaksanakan dengan teknologi semasa.

Matlamat utama tesis ialah untuk mencadangkan satu rangka kerja bagi lapisan protocol kuantum untuk pengurusan kunci rahsia tanpa simpulan ke atas persekitaran berbilang pihak. Dalam pengurusan kunci rahsia, protocol-protokol kunci persidangan mahupun pengagihan kunci kuantum pelbagai pihak dan kunci usaha sama atau kunci rahsia kuantum awam yang dikongsi bersama bertindak di lapisan atas dan skim pengesahan pengguna di lapisan tengah dan operasi standard pengagihan kunci kuantum di lapisan bawah.

Protokol-protokol pengurusan kunci rahsia yang dicadangkan adalah berdasarkan kunci rahsia diantara pelbagai pihak yang menggunakan pengagihan kunci kuantum, kod pembetulan ralat yang diubahsuai dan matriks bebas linear. Protokol-protokol ini memerlukan komunikasi yang klasik dan menghasilkankadar kunci rahsia yang lebih tinggi tanpa mengira jarak dan gangguan.Analisis sekuriti yang menggunakan kaedah meneka entropy telah digunakan dan hasil penggunaannya menunjukkan hanya maklumat yang tidak penting mahupun boleh diabaikan boleh diekstrak semasa intipan.

Teknik sambutan cabaran telah digunakan untuk mencadangkan skim pengesahan penggunakuantum mengesahkan pengguna kuantum. Ia adalah skim pengesahan dwiarah dan memerlukan kedua-dua kuantum dansaluran klasik untuk melaksanakannya dan mempunyai dua cara operasi, iaitu, awal danpengesahan sesi. Disebabkan orientasi pengedaran kunci yang berketentuan, kecekapan protokolmencapai sehingga 100% dalam kadar pengurangan pembaziran foton semasakomunikasi. Tambahan pula, skim ini kukuh mahupun bertahan kepada pelbagai

serangan keselamatan kuantum.Walau bagaimanapun, skim ini memerlukan saluran kuantum yang tanpa gangguan untuk mengesan serangan luaran dan dalaman semasa pengesahan.

Satu antara muka pengguna grafik berpangkalan simulasi acara yang diskret telah dibangunkan menggunakan OptiSystem™ untuk menguji kebolehlaksanaan praktikal lapisan protokol kriptografi kuantum yang dicadangkan.Pembolehubah protokol-protokol diskret pengagihan kunci kuantum yang berasaskan polarisasi telah direka bentuk dan dianalisis. Disebabkan kekurangan persediaan penerima yang sebenar, keputusan yang diperolehi mencerminkan kadar ralat bit kuantum yang lebih rendah. Tambahan pula, kami juga menganalisis kesan struktur polarisasi qubit yang disebabkan oleh gangguan, kehilangan dan jarak ke atas optik gentian dan ruang bebas. Pengagihan kunci kuantum berbilang pihak telah dibangunkan dan direka bentuk berdasarkan pemultipleksan pembahagian frekuensi yang memusatkan pelayan saluran kuantum. Pendekatan ini mengurangkan keperluan jumlah saluran kuantum dari $N*(N-1)/2$ kepada N dan setiap pihak memerlukan satu saluran kuantum untuk berkomunikasi dengan pihak-pihak yang lain. Protokol komitmen bit dan pengesahan mesej di dalam lapisan boleh diterokai untuk penyelidikan masa depan.

ACKNOWLEDGEMENTS

Foremost of all, all thanks to Almighty Allah who is the source of my strength and my life. I thank Allah for his immense grace and blessing every stage of my entire life. Peace and blessings of Allah be upon our Prophet Muhammad Sallallahu Alaihi Wasallam, who was sent for mercy to the world.

I owe tremendous debts of gratitude to the following:

- My supervisor Associate Prof. Dr. Zuriati Ahmad Zukarnain, who has supported and encouraged me during the entire process, and also introduce me to the technology entrepreneur field.
- My committee memberAssociate Prof. Dr. Shamala K Subramaniam, who taught performance modelling and the source of interest in discrete variable simulation. She always encouraged me during my tough times.
- My committee member AssociateProf. Hisham Zainuddin, who taught me first about quantum mechanics. He has helped me in understanding the complexity of quantum mechanics.
- My committee member Dr. Suhairi Saharudin for his wonderful effort to bring me into experimental fiber optic course. The interest of experimental simulation has begun during that course.
- I would like to special thanks to Attila Pereszlényi who taught me quantum key distribution from his QCircuit simulator. He responded patiently for all my novice questions during the interaction.
- I wish to thank my all my friends and well-wishers those willingly shared their knowledge and research skills which enable me to accomplish my thesis.
- My department colleagues and fellow students, and extend my gratitude also to the Faculty of Computer Science and Information Technology and the School of Graduate Studies.
- Sincere appreciation and gratitude are extended to many people who have assisted and encouraged me along the way.
- Last but least, My parents for nurturing, encouragement and their willingness to allow me to take things apart, while knowing that I might not succeed in putting them back together.

I certify that a Thesis Examination Committee has met on 13 February 2015 to conduct the final examination of Abudhahir Buhari on his thesis entitled "A Method for Authentication of Multi-User Key Management using Quantum Key Distribution Over Noiseless Channel" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Hamidah binti Ibrahim, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Ramlan bin Mahmod, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Mohamed Ridza Wahiddin, PhD
Professor
International Islamic University Malaysia
Malaysia
(External Examiner)

Kwek Leong Chuan, PhD
Professor
National University of Singapore
Singapore
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 17 June 2015

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

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Shamala K.Subramaniam, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Hishamuddin Zainuddin, PhD
Associate Professor
Faculty of Science and Environmental Studies
Universiti Putra Malaysia
(Member)

Suhairi Saharudin, PhD
Research Head,
Photonics Lab,
MIMOS Berhad, Malaysia
(Member)

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

Date:

Declarationby graduate student

I hereby confirm that:

- This thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of the thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceeding, 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.: ____

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature:
Name of Chairman of Supervisory Committee:
Zuriati Ahmad Zukarnain, PhD

Signature:
Name of Member of Supervisory Committee:
Shamala K.Subramaniam, PhD

Signature:
Name of Member of Supervisory Committee:
Hishamuddin Zainuddin, PhD

Signature:
Name of Member of Supervisory Committee:
Suhairi Saharudin, PhD

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BIT	Binary DigIT
CIANR	Confidentiality, Authentication, Integrity and Non-Repudiation
COW	Coherent One Way
CQKD	Counterfactual QKD
CVQKD	Continuous Variable QKD
CW	Coherent Way
Db	Discard bits
DES	Discrete Event Simulation
DIQKD	Device Independent QKD
DPS	Differential Phase Shift
DVQKD	Discrete Variable QKD
ECC	Error Correction Codes
IB	Identification Block
IGK	Identification Group Key
IK	Identification Key
KDF	Key Derivation Function

LED	Light-Emitting Diode
MDIQKD	Measurement Device Independent QKD
MQKD	Multiparty QKD
NP	Non-Polynomial time
NPC	Non-deterministic Polynomial Complete
NP-hard	Non-deterministic Polynomial-time, hard
OSI	Open System Interconnection
OT	Oblivious Transfer
OTP	One Time Pad
PBS	Polarization Beam Splitter
PbSQK	Public Secret Quantum Key
PbSSQK	Public Shared Secret Quantum Key
PMD	Polarization Mode Dispersion
PrSQK	Private Secret Quantum Key
PSSQK	Public Shared Secret Quantum Key
QBER	Quantum Bit Error Rate
QC	Quantum Cryptography
QIS	Quantum Information Science

QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
QS	Quantum Signature
QSDC	Quantum Secure Direct Communication
QSSK	Quantum Shared Secret Key
QUBIT	Quantum BIT
Sn	Total no. of Sets
SPIR	Symmetrical Private Information Retrieval
Tm	Total number of Matrices
UTP	Untrusted Third Party
VCSEL	Vertical Cavity Surface Emitting Laser

CHAPTER 1

INTRODUCTION

1.1 Background

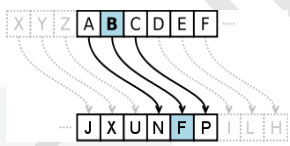
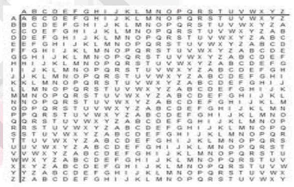
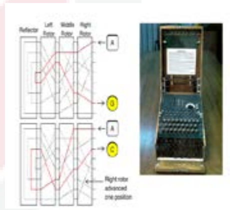
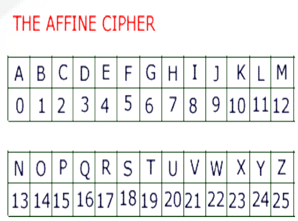
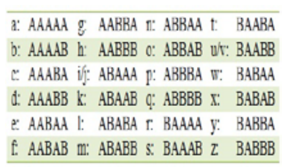
Cryptography is the mechanism to provide users with the four main factors of security which are confidentiality, authentication, integrity and non-repudiation (CIANR). Depends upon the applications, there is a trade-off among the factors. One of the important branches and the ever challenging task of cryptography is the secure transmission.

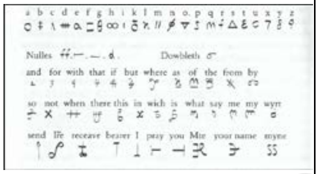
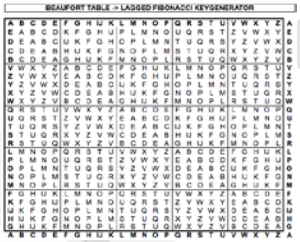
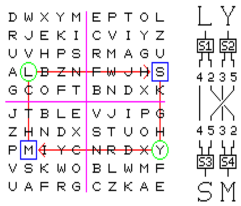
The field of secure transmission has a long cloak-and-dagger history with various turning points. In 1917, Vernam introduced the One-Time Pad (OTP) encryption, which uses a symmetric random secret key shared between sender and receiver. This scheme in principle is unbreakable, if the key is not reused. Later in 1948, Claude Shannon presented the concept of perfect secrecy in his ground- breaking thesis. Shannon listed out various conditions to achieve perfect secrecy and also pointed out OTP is optimal, if satisfied the prescribed conditions. However, the concept of perfect secrecy is not practically feasible due to different serious drawbacks as follows,

- Perfect random OTP
- Secure generation and transmission of OTP
- Secure storage and treatment

Therefore, perfect secrecy is only possible in theory. Currently no cryptosystem offers a perfect secrecy in real implementations. But the development of unconventional cryptography based on quantum and DNA promise to break the barriers and reach the door of perfect secrecy. So far, quantum based cryptography has achieved random generation and secure key distribution. Thus, perfect secrecy will be no more fiction in the future. Despite its promises, Quantum Cryptography (QC) is still in the early stage of the development phase from the emerging field of Quantum Information Science (QIS). To reach the height of conventional cryptography or digital cryptography's pinnacle of success, QC needs to undergo various challenges and tasks. This thesis focuses mainly on authenticated secret key distribution using a combination of quantum protocols and digital cryptography techniques. Thus, the contributions suit towards hybrid cryptography of QC and digital cryptography. For completeness, a tabular summary of the history of classical, modern or digital cryptography with the importance of the key distribution problem is presented in Table1.1 and Table 1.2.

Table 1.1 History of classical cryptosystem. Source: (A.Weis, 2007)

No	Name	Year / Inventor	Mechanism	Picture / Illustration
1	Scytale		Transposition	
2	Ceaser Cipher		Substitution	
3	Vigenere Cipher	Giovan Battista Bellaso : 1553 Blaise de Vigenère : 19 century	Polyalphabetic substitution	
-4	Rotor based cipher		Polyalphabetic	
5	Affine cipher		Mono-alphabetic substitution cipher	
6	Baconian	Sir Francis Bacon	Substitution cipher	

7	Codes & Nomenclature Cipher	15 century ~ 18 century		
8	Beaufort Cipher	Sir Francis Beaufort ~ 1838	polyalphabetic substitution cipher	
9	Four-square cipher	Felix Delastelle 1902	Encrypts pair of letter : Significant stronger than Substitution cipher and much resistant to frequency analysis attack	
10	Play fair cipher	Charles Wheatstone 1852	First practical digraph substitution cipher	A B C D E s e c r t F G H I K a b d f g L M N O P h i k l m Q R S T U n o p q u V W X Y Z v w x y z k e y w o A B C D E r d a b c F G H I K f g h i l L M N O P m n p q s Q R S T U t u v x z V W X Y Z Playfair Tableau
11	ADFGVX Cipher	Colonel Fritz Nebel : 1918		A D F G V X A S U B J E C D T A D F G H F I K L M N O G P Q R V W X V Y Z 0 1 2 3 X 4 5 6 7 8 9

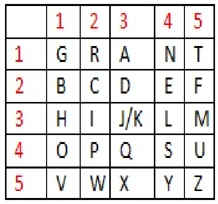
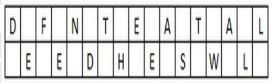
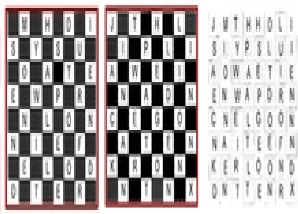
12	Bifid Cipher	Felix Delastelle	Polybius square with transposition, and uses fractionation to achieve diffusion	
13	Trifid Cipher	Felix Delastelle	Combines substitution with transposition and fractionation	
14	Rail fence cipher		Simple transposition cipher	
15	Straddle Checkerboard Cipher		Variable substitution changing an alphabetic plaintext into digits while simultaneously achieving fractionation. A kind of information diffusion. Data compression relative to other schemes using digits. It is also known as a monôme-binôme cipher.	

Table 1.2 Overview of digital cryptography & problem. Source: (A.Weis, 2007)

No	Cryptosystem / Problems	Description
1	Classical Cryptography	o Modern computers became nemesis to pen and paper, and mechanical cryptosystem. o Construction were unplanned and no available security proofs for the public o Only military and intelligence unit has the cryptographic knowledge

		o **Key distribution:** The number of keys in the system grows quadratically with the number of parties increases.
	Modern Cryptographic Epoch • Standardization of cryptographic primitives • Invention of public key cryptography • Formalization of security definitions • Growth of computing and the internet • Liberalization of cryptographic restrictions	
2	Diffie-Hellman Key Exchange	Diffie-Hellman-Merkle (1976) / Williamson (1974):
	<u>Generate a shared secret with a stranger over a public channel.</u> 1. Alice picks a group G, generator g, and a random value x 2. Alice computes A = g^x and sends Bob (G, g, A) 3. Bob picks a random y, computes B = gy, and sends Alice B 4. Alice computes K = B^x = g^(xy) 5. Bob computes K = A^y = g^(xy)	
	Eve's Information and Complexity	
	Eve's : (G, g, A, B) = (G, g, g^x, g^y) Hardness to compute g^(xy)	
	Problems	
	• Need to establish n^2 keys for n people or conduct • Interactive key exchange protocols for each message. • Expensive Computation over appropriate groups. • Vulnerable to a man in the middle attack	
3	**Public Key Encryption**	
	A public key cryptosystem consists of (G, E, and D). 2. Alice generates a key pair: G(r)→(PK_a, SK_a) 3. Alice publishes her public key PK_a 4. Bob encrypts a message with her public key: E(PK_a,m) → c 5. Alice decrypts a cipher text with her secret key: D(SK_a,c) →m	Only one key per person, not per pair. Can communicate with a stranger without agreeing on a key.

	Problem	
	• To *get al*ice's public key • To trust the cipher text	
4	**RSA Encryption**	Published in 1977 / Cocks 1973
	<u>Based on hardness of factoring products of large primes.</u> 1. Setup: n = pq, PK = (e, n), SK = d, ed = 1 mod (p-1)(q-1) 2. E(PK, m) = m^e (mod n) = c 3. D(SK, c) = c^d (mod n) = m^(ed) (mod n) = m	
	Problems	
	• Fixed size of cipher text • Expensive Computation • Trust of modified of cipher text • No semantic secure	
	Authentication	
	• Verification of Alice is Alice • Verification of orientation of message • Confidentiality of Alice message during transmission	
5	**Message Authentication Codes**	
	Alice and Bob share a secret key k. Either can sign (or MAC) a message: Sign(k, m)→ σ The recipient can verify the signature: Verify(k, m, σ) Often built from other primitives Similar key distribution problems to ciphers	
6	**Public Key Signatures**	
	Only you can sign messages, but anyone in the world can verify them. Public-key analog of a MAC.	
	A public key signature scheme consists of (G, Sign, Ver). 2. Alice generates a key pair: G(r)→(VKa, SKa) 3. Alice publishes her verifying key VKa 4. Alice signs a message: Sign(SKa, m) → σ 5. Bob verifies a signature with her verifying key: Ver(VKa,m)	
	Problems	
	Feasibility of public key signature scheme Distribution of verification keys	

	RSA is fixed size. Issues of sign of big messages
7	**Message Digests**
	Message digests compress input to fixed length strings. No keys involved. One-way: It is hard to find an input that hashes to a pre-specified value. Collision resistance: Finding any two inputs having the same hash-value is difficult. Fixed-length public signature schemes can sign digests instead of the actual message.
7	**Key Distribution: Evergreen Problem**
	<u>Problem: To verify the owner of the public key</u> o Current Solutions: Certificates - A signature on a public key or another certificate o PKI: A graph of relationships between keys. o Certificate authorities : A "web-of-trust" social graph <u>Revocation of keys</u> o Expiration dates o Certificate Revocation Lists

Most of digital cryptography based security protocols are based on hard prime factorization which takes Non-Polynomial time (NP Problem) to solve. From the view of computational complexity theory, is a branch of the theory of computation in theoretical computer science and mathematics that focuses on classifying computational problems according to their inherent difficulty, and relating those categories to each other. A computational problem is solved by a computer. Non-deterministic Polynomial-time, hard (NP-hard) is a class of problems and as at least as hard as any NP-problem. The examples are decision subset sum problem, halting problem and often attempted in areas which are rule-based languages.

NPC (Non-deterministic Polynomial Complete) is a class of problem which is mostly dealing with decision problems. There are many sets of problems studied under this class, namely, isomorphism problems, graph problem and the decision problem, such as Knapsack problem, travelling salesman problem, vertex problem, clique problem, Hamiltonian graph problem and so on so forth. Hence, digital cryptography offers a computational security which means a security mechanism which is bounded by technology limit. On the other hand, key distribution using quantum mechanics so-called quantum key distribution (QKD) offers an unconditional security which means a security mechanism is not bounded by technology limit.

QIS deals with several disciplines of information science through quantum mechanics principles. A brief classification of QIS is presented in Figure 1.1. The strong cruxes of QKD are No-Cloning theorem and the Heisenberg Uncertainty Principle. In the following section, we will briefly discuss some aspects of quantum theory relevant for quantum information science.

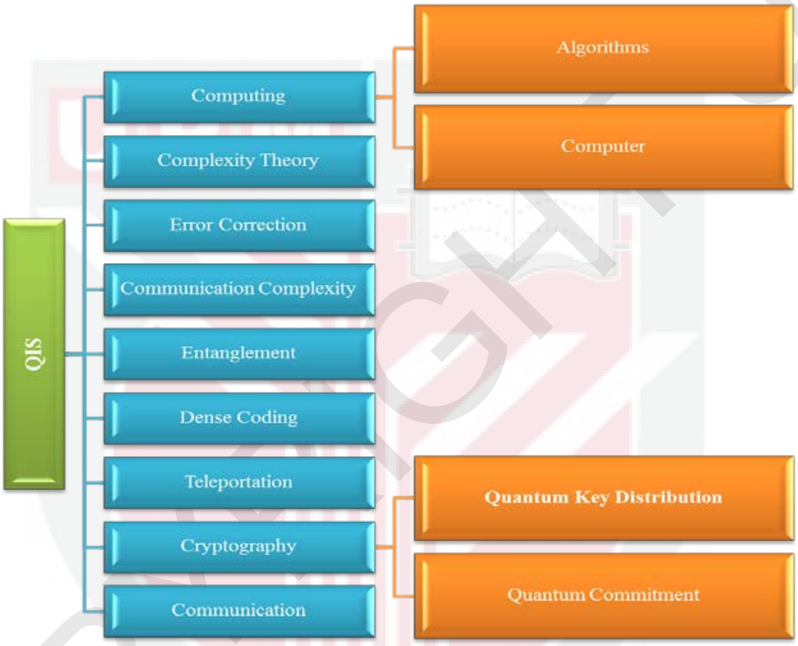


Figure 1.1 Fields of Quantum Information Science

In computer, bit (binary digit) is the smallest unit of data which represents a single binary value either 0 or 1. Likewise, in quantum world the basic unit of quantum information is referred as qubit (quantum bit). Basically, qubit is a two-state quantum-mechanical state such as polarization (horizontal or vertical) of a single photon (elementary particle). Further, a qubit can be represented in geometrical coordinates of a sphere and commonly illustrated in the Bloch Sphere as shown in Figure 1.2. However, quantum mechanics allows qubit to have a third state called superposition which is a mixture of both states at the same time. This property distinguishes the application based on quantum mechanics and holds the key for qubit phenomenal properties, i.e., parallel process, entanglement, teleportation and etc.

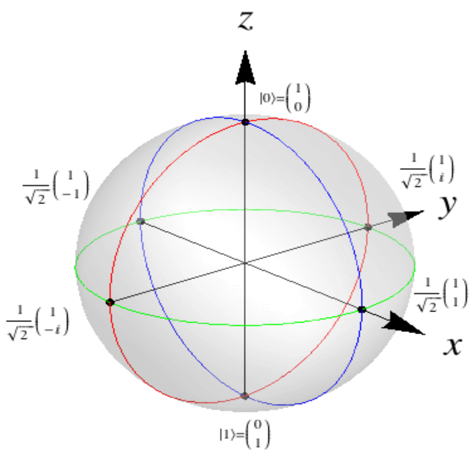


Figure 1.2 Qubit's Bloch Sphere View. Source: (Sphere, 2009)

No-Cloning theorem:

This is a type of no-go theorem of quantum mechanics which prohibits the creation of identical copies of an arbitrary unknown quantum state. This property is also the core of quantum computing and perfectly varies from the digital world.

Heisenberg Uncertainty Principle:

This is another dazzling property of quantum mechanics which makes its application is quite subtle. The correct result can be only obtained by correct measurement. Specific to QKD, the right (or correct) polarization of a photon (qubit) can be measured only by right polarizer otherwise, photon collapse itself. Any wrong measurement of photon (qubit) results in wrong outcome.

1.1.1 Limitations of Digital Cryptography

The property of the Heisenberg Uncertainty and No-Cloning theorems of quantum mechanics builds QKD's pillars of unconditional security and totally distinguish from the digital cryptography. In digital communication, a bit can be copied as many as possible without any notification. In quantum communication, a qubit cannot copy perfectly and measure (read) the value with wrong measurement causes a qubit loss its complete original information. In other words, the self-destruction of information occurs in the case of wrong measurement. Thus, detection of eavesdropping is an intrinsic property of QKD and outsmarts the digital communication. Moreover, digital cryptography is highly vulnerable due to perfect copy of data without any notification. Brute force technique is a simple but powerful technique to break the current cryptosystem provided by digital cryptography. A brief summary of hacking activities on digital cryptography and its impact is presented in Table 1.3, Table 1.4 and Table 1.5. Cyber hacking threat trends are represented in Figure 1.2 and Figure 1.3.

Table 1.3 Hash functions security summary. Source: (Wikipedia, 2014c)

Algorithm	Output size (bits)	Best known attacks (Complexity: rounds) [c 2]		
		Collision	Second Preimage	Preimage
GOST	256	Yes (2105)	Yes (2192)	Yes (2192)
HAVAL	256/224/192/160/128	Yes	No	No
MD2	128	Yes (263.3)	No	Yes (273)
MD4	128	Yes (3)	Yes (264)	Yes (278.4)
MD5	128	Yes (220.96)	No	Yes (2123.4)
PANAMA	256	Yes	No	No
RadioGatún	Up to 608/1,216 (19 words)	With flaws (2352 or 2704)	No	No
RIPEMD	128	Yes (218)	No	No
RIPEMD-128/256	128/256	No	No	No
RIPEMD-160	160	Yes (251 :48)	No	No
RIPEMD-320	320	No	No	No
SHA-0	160	Yes (233.6)	No	No
SHA-1	160	Yes (251)	No	No
SHA-256/224	256/224	Yes (228.5 :24)	No	Yes (2248.4:42)
SHA-512/384	512/384	Yes (232.5 :24)	No	Yes (2494.6:42)
SHA-3	224/256/384/512[c 3]	No	No	No
Tiger(2)-192/160/128	192/160/128	Yes (262 :19)	No	Yes (2184.3)
WHIRLPOOL	512	Yes (2120 :4.5)	No	No

Table 1.4 Block cipher security summary. Source: (Wikipedia, 2014a)

Cipher	Security claim	Best attack	Attack date	Comment
AES128	2128	2126.1 time, 288 data,	2011-	Independent biclique

		28 memory	08-17	attacks
AES192	2192	2189.7 time, 280 data, 28 memory		
AES256	2256	2254.4 time, 240 data, 28 memory		
Blowfish	2448	4 of 16 rounds	1997	The author recommends using Twofish instead.
DES	256	239 – 243 time, 243 known plaintexts	2001	Linear cryptanalysis. In addition, broken by brute force in 256 time, no later than 1998-07-17, see EFF DES cracker. Cracking hardware is available for purchase since 2006.
Triple DES	2168	2113 time, 232 data, 288 memory	1998-03-23	
KASUMI	2128	232 time, 226 data, 230 memory, 4 related keys	2010-01-10	The cipher used in 3G cell phone networks. This attack takes less than two hours on a single PC, but isn't applicable to 3G due to known plaintext and related key requirements.
Serpent-128	2128	10 of 32 rounds (289 time, 2118data)	2002-02-04	Linear cryptanalysis
Serpent-192	2192	11 of 32 rounds (2187 time, 2118data)		
Serpent-256	2256			

Twofish	2128 – 2256	6 of 16 rounds (2256 time)	1999-10-05	

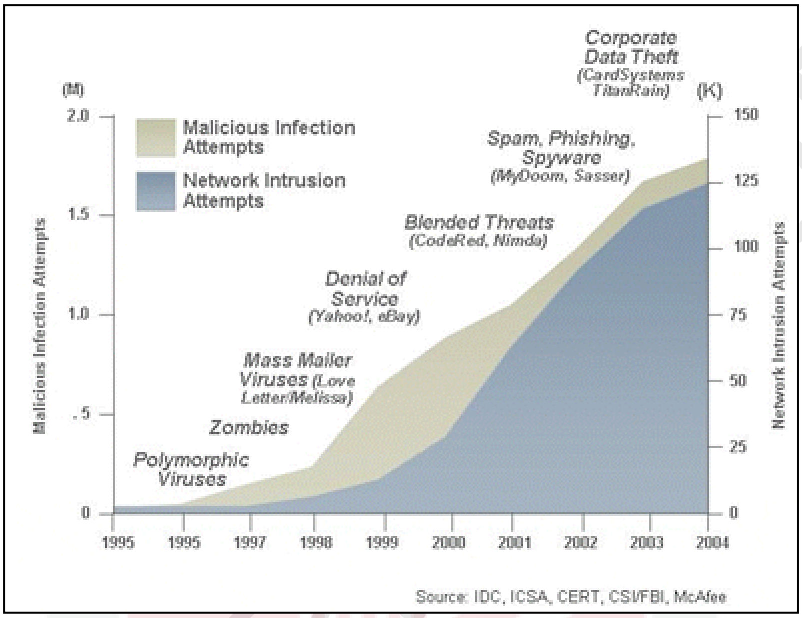


Figure 1.3 Progress of Cyber Security Threats. Source: (Baylor, 2006, September 1)

Table 1.5 Anatomy of hacking. Source: (TWINCLING™, 2013)

No	Stages	Techniques
1	Reconnaissance	Preparatory phase: Monitoring and Probing Network Foot printing, Pre-scanning & Enumeration
2	Scanning	Port scanning:
3	Gaining Access	System Hacking , Sniffers, Social Engineering Denial of Service, Session Hijacking, Buffer Overflows, Rootkits, Hacking Web servers, Web application vulnerabilities, Web based password cracking, SQL injection, Hacking Wireless networks, Virus and Worms, Evading IDS, firewalls, Honeypots, Cryptography
4	Maintaining Access	Rootkits, Trojans and Backdoors
5	Clearing tracks	Tunneling, Altering/Clearing log files, Disabling auditing

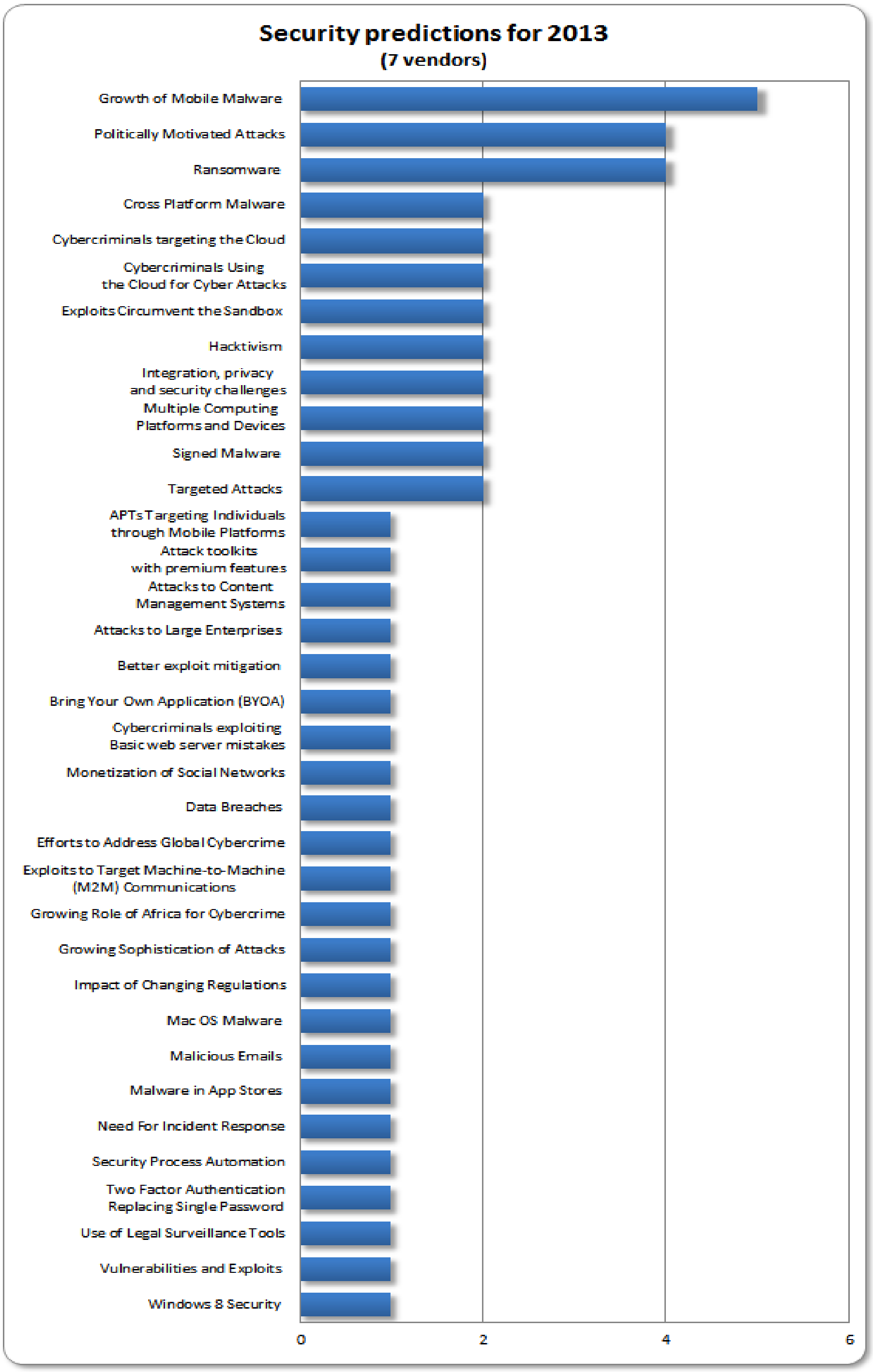


Figure 1.4 Security Issues – 2013. Source: (Micro, 2013)

Presently, digital world grows at an exponential way in which ubiquitous computing, smart technology, sensor mechanism, broadband communication are all evolved into borderless world and inevitable part of the life. For all these technologies, the sole security mechanism is provided by digital cryptography. However, the current digital cryptographic mechanism has vulnerable threats from both quantum computer and smart phone technology. Smart phones potent are already making serious threats (Zineddine & Kindi), while quantum computer on its way to reach its full form (Ladd *et al*., 2010). Thus, an alternative security solution is imminent for current world. On the other hand, QC promises unconditional security. Further, QC is the mature application of quantum mechanics.

1.1.2 BB84 Protocol – Birth of QKD

In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol (Bennett & Brassard, 1984). The fundamental concept for this protocol is that Alice can transmit a random secret key to Bob by sending a string of photons where the secret key's bits are encoded in the polarization of the photons. Heisenberg's uncertainty principle can be used to guarantee that an eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a noticeable way thus revealing her existence.

Figure 1.5 illustrates how a bit can be encoded in the polarization state of a photon in BB84. Binary 0 is characterized as a polarization of 0 degrees in the rectilinear bases or 45 degrees in the diagonal bases (CKI, 2001; Nicolas Gisin, Ribordy, Tittel, & Zbinden, 2002). Similarly a binary 1 can be 90 degrees in the rectilinear bases or 135 in diagonal bases. Thus a bit can be represented by polarizing the photon in either one of two bases.

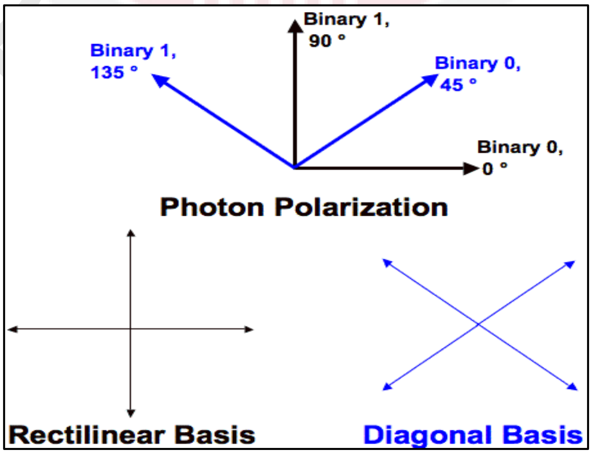


Figure 1.5 BB84 Bit Encoding. Source:(Haitjema)

In the first stage, Alice transmits to Bob over a quantum channel. Alice begins by choosing a random string of bits and for each bit, Alice will randomly choose a basis, rectilinear or diagonal, by which to encode the bit. She will transmit a photon for each bit with the corresponding polarization, as just described, to Bob. For every photon Bob receives, he will measure the photon's polarization by a randomly chosen basis. If, for a particular photon, Bob chose the same basis as Alice, then in principle, Bob should measure the same polarization and thus he can correctly deduce the bit that Alice calculated to send. If he chose the wrong basis, his result, and thus the bit he reads, will be wrong.

In the second stage, Bob will notify Alice over any insecure channel what basis he used to measure each photon. Alice will report back to Bob whether he chose the correct basis for each photon. At this point Alice and Bob will discard the bits corresponding to the photons which Bob measured with a different basis. Provided no errors occurred or no one manipulated the photons, Bob and Alice should now both have an identical string of bits which is called a sifted key. The example below shows the bits Alice chose, the bases she encoded them in, the bases Bob used for measurement, and the resulting sifted key after Bob and Alice discarded their bits as just mentioned (Wikipedia, 2014f). The operation of sifted key is presented in Figure 1.6.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 1.6 Sifted Key. Source:(Haitjema)

Prior to the end, Alice and Bob agree upon a random subset of the bits to compare to ensure consistency. If the bits agree, they are discarded and the remaining bits form the shared secret key. In the absence of noise or any other measurement error, a disagreement in any of the bits compared would indicate the presence of an eavesdropper on the quantum channel. This is because if the eavesdropper, Eve, were attempting to determine the key, she would have no choice but to measure the photons sent by Alice before sending them on to Bob. This is true because the no cloning theorem assures that she cannot replicate a particle of unknown state (Wootters & Zurek, 1982). Since Eve do not know what bases Alice used to encode the bit until after Alice and Bob discuss their measurements, Eve will be forced to guess. If she measures on the incorrect bases, the Heisenberg's uncertainty principle ensures that the information encoded on the other bases is now lost. Thus when the photon reaches Bob, his measurement will now be random and he will read a bit incorrectly 50% of the time. Given that Eve will choose the measurement basis incorrectly on average 50% of the time, 25% of Bob's measured bits will differ from Alice (Rieffel & Polak, 2000). The chance that an eavesdropper learned the secret is thus negligible if sufficiently long sequences of the bits are compared.

Free space QKD was first demonstrated in 1989 by Bennett and his co-workers over 30 cm optical link (Bennett, Bessette, Brassard, Salvail, & Smolin, 1992). The first experimental implementation of QKD was proposed in (Buttler *et al*., 1998), since then a lot of research effort has been dedicated by researchers to develop the technology for use in future optical communication systems, to support security critical information flows. While the experimental setup was able to send quantum signal over distances of 100 km in optical fiber link, in free-space quantum signal was sent over a distance of 23.3 km. Recently, advances have led to demonstrations of QKD over point-to-point optical links (Christian Kurtsiefer *et al*., 2002). These rather promising transmission distances have stressed the high possibility of obtaining practical QKD systems. In order to implement QKD between any two locations on the globe, a satellite is needed to be used as a secure relay station. Feasibility studies by researchers have shown that the ground-to-satellite, satellite-to-ground and satellite-to-satellite QKD demonstrations are feasible (Hughes, Nordholt, Derkacs, & Peterson, 2002; Rarity, Tapster, Gorman, & Knight, 2002). In (J. Zhu & Zeng, 2005) a stratospheric quantum communication model based on the characteristics of the stratosphere was proposed. Besides, a study by (Gabay & Arnon, 2006) on the effect of turbulence on a quantum key distribution system can be found in (Gabay & Arnon, 2005). Moreover, to improve the transmission bit rate of free space systems, two authors conducted a study on quantum key distribution by free-space MIMO system (Gabay & Arnon, 2006). Furthermore, to evaluate the performance of various QKD systems, the QBER and secure communication rate are considered as important criteria.

The QBER which is indicative of the security and post-error-correction communication key rate is taken in to account when evaluating the link performance. Any information learnt by an unauthorized third party about the exchanged key leads to an increase in the QBER. A high QBER enables an unauthorized user or more correctly the eavesdropper to learn more information about the transmitted key at the expense of the legitimate recipient. Thus, it should be taken into account that obtaining high QBER values in QKD systems can resultantly lower the secure communication key rate during error correction stage of the protocol. It has been shown that, as long as the QBER of the sifted key is below a certain threshold, Alice and Bob can still distill a secure key by means of classical error correction and privacy amplification. Besides, past studies have shown that any QBERs of the sifted key above 15% give room for an eavesdropper to actually learn more information than the intended recipient. When the obtained QBER is more than 15%, no form of classical privacy amplification techniques can be used effectively (Kumavor, Beal, Yelin, Donkor, & Wang, 2005).

Thus, any proper design a QKD link should ensure a baseline QBER of below 15 % threshold if privacy amplification strategies are to be used to eliminate any knowledge gained by the eavesdropper. If the QBER goes above 15% limit value, depending on the restrictions on the eavesdropper's abilities, it will no longer be possible to extract as secure communication bit rate. This baseline QBER considers a QKD link in which a one-way classical processing by Alice and Bob is observed.

1.1.3 Limitations of Quantum Cryptography

The comparison between the quantum cryptography and the digital cryptography is like a comparison between a novice and expert. Still, QC is in an early stage of the limelight, but with various developments in quantum hardware shows promising transformation from novice to expert. QC is still lacking in a comprehensive structure of digital cryptography. Moreover, QC cannot provide any full crypto-system and so far secure transmission is the milestone achievement.

Secure key transmission / generation is the stronghold of QC and commonly refer as QKD. For the current digital world security mechanism, secret key is the most vital for any crypto-system. Further, the generation rate, reusability, secure storage, cost, secure transmission and privacy are all performance metric or attributes of the secret key. Current security mechanism requires a higher rate key to accomplish its task. Therefore, key rate with minimum cost is the first and foremost priority of the crypto-system.

QKD offers unconditional secure key transmission, but due to the lower key rate, only small scope set of jobs is possible to achieve. In contrast to digital cryptography, the cost of key generation in QKD is expensive and even incomparable.

The critical factors, i.e. noise and distance are the main hurdles in the QKD to perform like its counterpart digital cryptography’s key distribution mechanism. In fact, both factors are directly related to the intrinsic properties of QKD’s components and need for efficient source, detectors, and quantum storage and quantum repeaters. Different with the computer bit, quantum bits or qubits are sensitive to channel and apparatus. Further, the development of photonic components to produce results like theoretical QKD’s result is another major research area. This clearly shows that still a long road to achieve the heights of digital cryptography. However, the recent progress in the development of photonic components is the promising sign to achieve the height. Indeed, QKD only achieved short distance transmission over fiber and free-space. As the distance grows qubits' drops its composure and extinct. Entanglement and repeaters are the ultimate solution for this problem. However, the recent improvements in the photonic devices are clearly showing that QKD can be achieved over large distances in near future.

QKD's hardware improvements would surely bring achievements into another height. However, usage of digital cryptography key derivation function (KDF), Error Correction Codes (ECC), and key strengthening in QKD algorithms would aid or improve the key generation rate.

This thesis mainly focuses on the QKD in the multi-party environment without the use of entanglement. In some research papers, the term multi-party refers to multi-user. As a matter-of- fact, QKD is strong in two-party or two-user system to establish a secret key. However, with quantum entanglement property, secret key distribution is possible for many users. Indeed, QKD mechanism is not a deterministic process, but rather it is a stochastic process.

Multiparty QKD (MQKD) is an analogue of conference key sharing in digital cryptography. The distribution of conference key to all users is an easy achievable task in digital cryptography, but in quantum cryptography is still hard. To achieve a conference key using QKD without entanglement is a challenging task. Most of the current QKD market products are not based on entanglement mechanism, so without or with small changes in current market QKD product to attain MQKD would be beneficial to the end users as well as developers. Another secure key management task is shared secret key or joint-venture key. Joint-venture secret key management plays vital role in many aspects of day-to-life. A shared secret key management is a secret key which is divided into many parts and each part of the key is held by an authorized user. In quantum terminology, joint-venture key mechanism refers as quantum shared secret key (QSSK). The foundation for QSSK research is the various types of entangled states.

QKD mechanism without utilizing entanglement suffers big blow in reaching reusable and higher rate secret key. Further, in the multi-party environment, it escalates the deficiency and prone to more challenges, namely dishonest party, topology, channel management in addition to basic problems such as eavesdropper issues, imperfect devices, losses and noise factors. Hence, if any mechanism or algorithm by using the standard QKD operation can solve the above problems then, it considers as a milestone in the QKD history.

The authentication process is the norm for any security mechanism. Certainly, quantum message authentication researches have attracted many and still on-going active research areas. Message authentication scheme using entanglement can cover both user and message at a same time. Recently, quantum hacking activities prove that an attacker can attack the quantum user apparatus or hardware components. This widens man-in-the-middle based attacks with assorted options. There is an urgent need of a quantum user authentication scheme in every QKD operation. Further, in multi-party system, the situation is worse due to presence of dishonest member.

The composable quantum cryptography protocol researches are widely based on entanglement. However, these schemes are not applicable to the current QKD market product to overcome the quantum hacking activities. Here, in the thesis, we propose MQKD, QSSK , quantum user authentication protocols based on key derivation function (KDF), challenge-response scheme, error correction code (ECC) and linear independent matrix and combined as a single protocol suite, which can operate similar to conventional network layering protocols and fulfill the composable quantum cryptography (Müller-Quade & Renner, 2009).

Basically, there is a big gap between theoretical QKD research and experimental QKD research. This gap is studied and presented by various research groups. Recent research shows that theoretically QKD is proven secure, but that implementation is totally insecure against a strong eavesdropper that has a one-time access to the receiver's equipment(Boyer, Gelles, & Mor, 2012). Further, practical limitations are ignored in the QKD's security proofs.

One of the main limitations in QC research is the absence of effective simulation study to evaluate the performance of the experimental QKD setup. Simulation study is the de facto evaluation approach in all fields of science. Especially, computer network research highly dependable on simulation study for analysis the performance of protocols. Further, simulation study can act as a bridge between theoretical and practical quantum research. Therefore, a framework for the experimental QKD setup simulation is developed in our research to facilitate the study on photonic components and eavesdropper techniques.

1.2 Motivations

Quantum Cryptography has evolved into a mature field during recent years. However, the applicability of QC is still limited. On the other hand, digital cryptography plays a central role in everyday life. This is due to the trustable, complex and sophisticated architecture. Further, digital cryptography craves simplicity, suitability, maintainability and robustness. Digital cryptography is the most predominant applicable in digital transaction and internet transaction.

There are various features in the digital cryptography; one of them is supporting of protocol layering. In concern with the computer networking, protocols are classified according to layer. The predominant open system interconnection (OSI) layer contains of seven layers and each layer performs specific functions (Wikipedia, 2014e). This layering concept encapsulates from top to bottom structures. In other words, the protocol layering concept offers a total support from hardware equipment’s to the software application. Each layer is acting as a hub between upper layer and lower layer. Digital cryptography protocols are usually at the top layer called application layer. The conversion of information into digital is done in physical layer or lowest layer. Other layer supports each other with a specific role.

The main motivation of this thesis is to construct quantum cryptography protocols as layering protocols. Since, the quantum cryptography protocols are in its early development stage, designing a simple and effective layering system would be the first step towards the big goal. This layering concept not only to combines the QC protocols, but it also provides a systematic flow of information.

The principal concern of this research is to combine quantum authentication scheme and multi-party quantum key distribution protocols. Hence, in every set of transaction, quantum user authentication can be achieved.

QC protocols achieved more success in a two-party system rather in a multi-party system, especially in the domain of quantum key distribution (QKD) protocols. Basically, to achieve QKD in a multi-party system applies the quantum entanglement concept. However, entanglement based QKD protocols suffers low practical realization. The available QKD products are variations of fainted laser or near single photon model. Further, quantum shared secret key (QSSK) or joint-venture key in the digital cryptography’s jargon system is achieved by entanglement property. To devise an efficient protocol based on a shared secret key by QKD protocols to achieve a higher key rate multiparty QKD (MQKD) and QSSK without entanglement, using one-way public communication and resilient to sophisticated attacks are the propelling factors in this research. The main objective of this thesis is to propose a systematic framework to achieve user authenticated MQKD and QSSK by a single photon concept over a noiseless channel.

QKD is a combination of hardware (i.e. photonic and optical telecom components) and software (protocols & post quantum methods) to accomplish the unconditional security for secret key distribution. The intrinsic property of QKD is the detection of eavesdropping makes it a distinguished application in compare with digital cryptography applications.

Most research on QKD are analytically oriented and rests are experimental. Due to the cost factor, the experimental type researches are not equivalent to analytical counterparts. On the other hand, an analytical or mathematical research has numerous limitations, which affect the efficiency of the performance analysis. Further, it usually ignores the importance of accurate hardware losses. Additionally, for the fresh researchers to understand, the QKD operation makes difficult. In contrast, understanding the digital cryptography or digital network protocols is simple due to the availability of simulation option. These researches have been efficient in analytical or experimental researches, but also they have effective simulation programs. In particular, discrete event simulation of the network protocol is de-facto standard for evaluating the performance metrics.

Generally, the study and evaluation of the quantum computers and its algorithms' various methods are available. The options range from new functional programming language, a library of high-level language, online services, framework, interactive simulation, GUI oriented - circuit oriented simulators, emulators and visualization. On the other hand, the study of the QKD operations are very few and inefficient. There is a lack in the efficient simulation study tool for QKD protocols. Another motivational behind this research is the need to develop an effective GUI based discrete event simulation (DES) to simulate the experimental QKD setup.

Figure 1.7 represents the typical multi-party QKD environment setup. Both public channel and private channel (quantum channel) are available. Public channel is in a star topology while quantum channel is a full mesh topology.

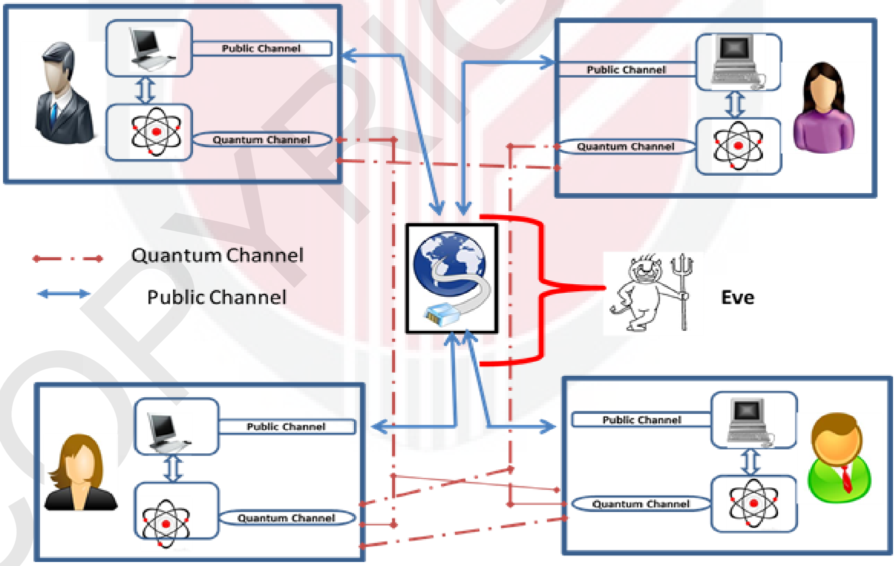


Figure 1.7 Multiparty QKD System with Eve Presence

Channel calculations for Figure 1.7.

N = Total Number of Users

C_Q= *Total Number of quantum channel*

C_P= *Total Number of Public Channel*

C_Q= N (N-1)/2 [Triangular number formula]

Let say,

N = 5;

then C_Q= 10

C_P= 5 [All users are connected to Internet Cloud]

1.3 Problem Statements

The application of secure key transmission through QKD in the real world scenario is limited. The practicable QKD system provides unconditional security towards two-party system over a shorter distance with a lower key rate. Further, due to the imperfect devices, noises in the channel and losses during the transmission have reduced the efficiency. Moreover, there is a lack of efficient QKD mechanism for multi-party environment and robust against attacks. Generally, secret key distribution in the multiparty environment is mostly based on quantum entanglement. Entanglement based full QC research is only applicable in theoretical setting. However recent improvements in the hardware, entanglement based applications is possible in near future (Aktas, Fedrici, Labonté, & Tanzilli, 2014; G. Gao, 2014).

Authentication is prior task for any secure communication. Recently, quantum identity verification research has got much attention (Goorden, Horstmann, Mosk, Škorić, & Pinkse, 2013; T. H. Lin & Hwang, 2014; Tan & Jiang, 2014; Waseda, 2013). This is due recent hack activities and hardware attacks on QKD experiments. Further, user authentication is a topmost process in the multiparty environment. However, the entanglement based solution for both user and message authentication has an implementation problem with current technology. Further, there is a deficiency of efficient quantum user authentication scheme to resist insider and outsider attacks, less complex key derivation cycle, reduced usage of photons and feasible with current technology.

The secret key rate of practical QKD in the quantum network is mainly affected by detection rate and distillation rate. Basically, QKD established secret key between parties with a lower secret key rate and wastage of heavy photons during quantum transmission and error correction. Furthermore, quantum based secret key management protocols, i.e. conference key and joint-venture key protocols cause higher wastage of photons due to collective noise and security attacks, lower secret key rate, security compromise due to dishonest member and Eve and less reusable of secret key. Quantum secret sharing based on error correction codes has advantages over key rate. However, no authentication mechanism during the quantum transmission will leads to Denial of Service and Trojan horse attacks.

Basically, designing the QKD experiments is expensive due to involvement of sensitive photonics component. Currently, most of QKD's experiment components are imperfect which includes lack of single photon LASER source, birefringent and dispersion oriented fibers channels and lossy free space optics and inefficient photodetectors. Typically, QKD security analysis assumes devices are perfect which results in a huge difference in practical and theoretical setup outputs. Simulation study is the de facto standard for the performance evaluation for various sciences. There is a lack of effective simulation study on quantum experiment setups in order to study the performances prior to implementation. An effective simulation tool can reduce the cost and time for the development of the QKD experiments.

The composability of quantum cryptographic protocols is an active research area in order to build a complete crypto system using quantum mechanics. The quantum composability cryptography includes combination authentication, secret key distribution, and bit commitment protocols in a protocol suit. However, there is a lack of study in development of composable quantum cryptography schemes which is feasible with current technology (Müller-Quade & Renner, 2009).

In this thesis, a quantum user authentication is based on challenge-response scheme over noiseless quantum channel and secret key management protocols are based on modified ECC and linear independent matrix in order to achieve the non-linear key derivation and resist towards security attacks. Further, a quantum cryptography protocol layer for an authenticated higher key rate multiparty secrete key management protocols, i.e., conference key and joint-venture key over noiseless quantum channel is proposed.. However, both protocols required shared secret key between parties using standard QKD protocol. Further, the practical feasibility of the authenticated multiparty QKD is studied through photonic simulation software called OptiSystem™.

1.4 Research Objectives

- To propose an efficient quantum user authentication scheme over noiseless channel based on pre-shared secret key between the parties, pre-calculated quantum bit error rate (QBER) verification and modified digital challenge-response scheme. The efficiency is measured in terms of reduction of photon wastage and resistance towards security attacks.

- To develop higher key rate MQKD and QSSK protocols based on modified KDF and pre-shared secret key. Here on, the proposed QSSK protocol is called as public shared secret quantum key (PSSQK). Since private shared secret keys among the parties are converted into a shared secret key. The higher key rate is measured in terms of conversion of shared secret key among parties with few losses.

- ü To design a simulation framework based on OptiSystem™ which is a commercial simulation tool to design and simulate the polarized based discrete variable experimental QKD setups and design then multiparty QKD environment.

- ü To propose a quantum protocol stack or composable quantum protocol layer which describes the systematic flow of operation for all proposed protocols, viz. Authentication, MQKD, PSSQK and standard QKD. The efficiency of this stack is a detailed description of actions and mitigation process in the real-world scenario.

1.5 Research Scope

This section lists the assumptions have made for the research. Moreover, the detailed assumptions are presented in each chapter.

- All users are established short-shared secret key (private key) between them using standard QKD mechanism. Therefore, total number of keys = $N(N-1)/2$.
- Classical channel is authenticated and Eve can only listen to the message.
- Eve has full control over quantum channel, i.e. she is not bound by any computational limit.
- Prerequisite of noiseless quantum channel: In fact, this assumption makes the proposed scheme into a weaker position in the achievement of practical feasibility. But relying on the current research developments in the field of QKD hardware is promising.
- Prerequisite of single photon and ideal detector: Again, this assumption makes the proposed authentication scheme into impracticable. Nonetheless, if the value of noise and losses caused by the channel and the detector are pre-determined, then proposed scheme can be optimized.

Both proposed secret key management schemes can be considered as a hybrid of quantum and digital cryptography. Hereon, hybrid cryptography denotes the combination of quantum and digital cryptography. Actually, except the secret key establishment process which is done by QKD process, all other processes involved in secret key management have no relationship with quantum mechanics. Further, data distribution between the users is done using only public channel. The underlying techniques of proposed schemes are based on KDF and matrix manipulation operations.

The proposed quantum user authentication scheme is also under the hybrid cryptography. The fundamental function is based on digital challenge-response scheme. Both quantum and public channels are required. The proposed schemes for both secret key management and user authentication have utilized polarized based discrete variable (DV) QKD operation, especially BB84 setting quantum communication. Therefore, standard BB84 security proofs are only required.

The proposed simulation models are developed under the basis of BB84 experimental setup. However, only source and channel models are similar to the experimental settings while the detector is considered as ideal. All the components applied in the simulation models are intrinsic component of the simulation itself. Therefore, inbuilt parameter settings are the most vital for various types of simulations. However, some of the results are anti-correlated with experimental setups due to unavailable of components in the simulator. The proposed simulations are based on polarized based discrete variable QKD.

Figure 1.8 depicts the areas are covered in the thesis in order to achieve the goal of authenticated quantum cryptography protocol layer for secret key management.

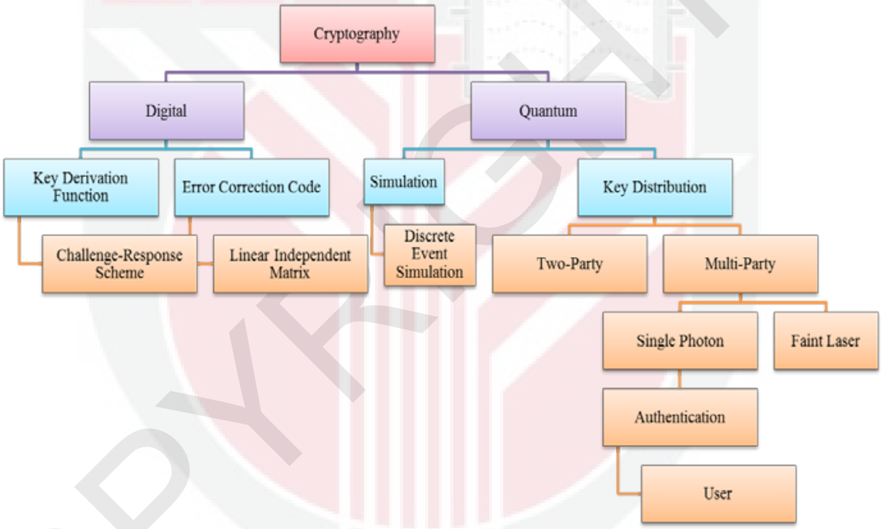


Figure 1.8 Coverage of Research Topics in Thesis

1.6 Thesis Organization

Chapter 2 focuses on literature review, which includes related research work and other developments in the field of QKD and an overview of research methodology is presented in chapter 3.

Chapter 4 illustrates the building blocks of proposed quantum user authentication protocols with the discussion of performance evaluation.

Chapter 5 presents the mechanism and performance evaluation of the proposed secure key management protocols i.e., the MQKD and PSSQK and the proposed QKD simulation architecture and respective QKD protocols based on OptiSystem™ is presented in Chapter 6.

Finally, Chapter 7 concludes with the merits and limitation of this research and a brief summary of future enhancements.

REFERENCES

A.Weis, S. (2007). Theory and Practise of Quantum Crytpography Retrieved 17 August 2014, from http://saweis.net/crypto.html

Aktas, D., Fedrici, B., Labonté, L., & Tanzilli, S. (2014). *Entanglement-based quantum key distribution in standard telecom channels for long-distance multi-user network implementation.* Paper presented at the 23rd Int. Laser Physics Workshop (LPHYS'14).

Altenkirch, T., & Grattage, J. (2005). *A functional quantum programming language*.

Anders, J., Ng, H. K., Englert, B.-G., & Looi, S. Y. (2005). The Singapore Protocol: Incoherent Eavesdropping Attacks. *arXiv preprint quant-ph/0505069*.

Anders, J., Ng, H. K., Englert, B. G., & Looi, S. Y. (2005). The Singapore Protocol: Incoherent Eavesdropping Attacks. *Arxiv preprint quant-ph/0505069*.

Bagherinezhad, S., & Karimipour, V. (2003). Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers. *Physical Review A, 67*(4).

Barnum, H. (2001). Quantum message authentication codes. *Arxiv preprint quant-ph/0103123*.

Barnum, H., Crépeau, C., Gottesman, D., Smith, A., & Tapp, A. (2002). *Authentication of quantum messages.* Paper presented at the Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on.

Barnum, H. N. (1999). Quantum secure identification using entanglement and catalysis. *Arxiv preprint quant-ph/9910072*.

Barrett, J., Colbeck, R., & Kent, A. (2013). Memory attacks on device-independent quantum cryptography. *Physical Review Letters, 110*(1), 010503.

Bartlett, S. D., de Guise, H., & Sanders, B. C. (2002). Quantum encodings in spin systems and harmonic oscillators. *Physical Review A, 65*(5), 052316.

Baylor, K. (2006, September 1). Evolution of Hacker Threat, from http://www.securitypronews.com/evolution-of-the-hacker-threat-2006-09

Beaver, D. (1995). Precomputing oblivious transfer *Advances in Cryptology—CRYPT0'95* (pp. 97-109): Springer.

Bechmann-Pasquinucci, H., & Gisin, N. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A, 59*(6), 4238.

Beige, A., Englert, B. G., Kurtsiefer, C., & Weinfurter, H. (1999). Secure communication with a publicly known key. *Acta Physica Polonica A, 101*, 357.

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters, 68*(21), 3121.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (1992). Experimental quantum cryptography. *Journal of cryptology, 5*(1), 3-28.

Bennett, C. H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing.* Paper presented at the Proceedings of IEEE International Conference on Computers, Systems and Signal Processing.

Bennett, C. H., Brassard, G., Crépeau, C., & Skubiszewska, M.-H. (1992). *Practical quantum oblivious transfer.* Paper presented at the Advances in Cryptology—CRYPTO'91.

Bennett, C. H., Brassard, G., & Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. *Physical Review Letters, 68*(5), 557.

Bin, G., Chuan-Qi, L., Fei, X., & Yu-Lin, C. (2009). High-capacity three-party quantum secret sharing with superdense coding. *Chinese Physics B, 18*(11), 4690.

Blakley, G. R. (1899). *Safeguarding cryptographic keys.* Paper presented at the Managing Requirements Knowledge, International Workshop on.

Bogdanski, J., Ahrens, J., & Bourennane, M. (2009). Sagnac secret sharing over telecom fiber networks. *Optics Express, 17*(2), 1055-1063.

Bogdanski, J., Rafiei, N., & Bourennane, M. (2008). Experimental quantum secret sharing using telecommunication fiber. *Physical Review A, 78*(6).

Bowen, W. P., Schnabel, R., Lam, P. K., & Ralph, T. C. (2003). Experimental investigation of criteria for continuous variable entanglement. *Physical Review Letters, 90*(4), 043601.

Boyer, M., Gelles, R., & Mor, T. (2012). Attacks on fixed apparatus quantum key distribution schemes *Theory and Practice of Natural Computing* (pp. 97-107): Springer.

Branciard, C., Gisin, N., Lutkenhaus, N., & Scarani, V. (2006). Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *arXiv preprint quant-ph/0609090*.

Brassard, G., Bussieres, F., Godbout, N., & Lacroix, S. (2003). *Multiuser quantum key distribution using wavelength division multiplexing.* Paper presented at the Applications of Photonic Technology.

Brassard, G., & Crépeau, C. (1991). Quantum bit commitment and coin tossing protocols *Advances in Cryptology-CRYPT0'90* (pp. 49-61): Springer.

Brida, G., Cavanna, A., Degiovanni, I. P., Genovese, M., & Traina, P. (2012). Experimental realization of counterfactual quantum cryptography. *Laser Physics Letters, 9*(3), 247-252.

Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters, 81*(14), 3018.

Buttler, W., Hughes, R., Kwiat, P., Lamoreaux, S., Luther, G., Morgan, G., . . . Simmons, C. (1998). Practical free-space quantum key distribution over 1 km. *Physical Review Letters, 81*(15), 3283.

Cabello, A. (2000). Multiparty key distribution and secret sharing based on entanglement swapping. *arXiv preprint quant-ph/0009025*.

Cabello, A. (2000). Quantum key distribution in the Holevo limit. *Physical Review Letters, 85*(26), 5635.

Cachin, C. (1997). *Entropy measures and unconditional security in cryptography.* Swiss Federal Institute of Technology Zurich.

Cai, Q. Y. (2006). Eavesdropping on the two-way quantum communication protocols with invisible photons. *Physics Letters A, 351*(1-2), 23-25.

Cai, R. (2009). *Finite Key Analysis for Quantum Cryptography, Bachelor Thesis.* National University of Singapore.

Cerf, N. J., Bourennane, M., Karlsson, A., & Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Physical Review Letters, 88*(12), 127902.

Chapuran, T., Toliver, P., Peters, N., Jackel, J., Goodman, M., Runser, R., . . . McCabe, K. (2009). Optical networking for quantum key distribution and quantum communications. *New Journal of Physics, 11*(10), 105001.

Chen, K., & Lo, H.-K. (2005). *Conference key agreement and quantum sharing of classical secrets with noisy GHZ states.* Paper presented at the Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on.

Chen, T.-Y., Wang, J., Liang, H., Liu, W.-Y., Liu, Y., Jiang, X., . . . Ju, L. (2010). Metropolitan all-pass and inter-city quantum communication network. *Optics express, 18*(26), 27217-27225.

Chen, X.-B., Niu, X.-X., Zhou, X.-J., & Yang, Y.-X. (2013). Multi-party quantum secret sharing with the single-particle quantum state to encode the information. *Quantum Information Processing, 12*(1), 365-380.

Choi, J. W., Chang, K.-Y., & Hong, D. (2011). Security problem on arbitrated quantum signature schemes. *Physical review A, 84*(6), 062330.

Choi, M.-D. (1975). Completely positive linear maps on complex matrices. *Linear algebra and its applications, 10*(3), 285-290.

Chong, S.-K., Luo, Y.-P., & Hwang, T. (2011). On the" Security analysis and improvements of arbitrated quantum signature schemes". *arXiv preprint arXiv:1105.1232*.

Chor, B., Kushilevitz, E., Goldreich, O., & Sudan, M. (1998). Private information retrieval. *Journal of the ACM (JACM), 45*(6), 965-981.

Chuang, I., & Gottesman, D. (2007). Quantum digital signatures: Google Patents.

Ciurana, A., Martinez-Mateo, J., Peev, M., Poppe, A., Walenta, N., Zbinden, H., & Martin, V. (2014). Quantum metropolitan optical network based on wavelength division multiplexing. *Optics express, 22*(2), 1576-1593.

CKI. (2001). The BB84 Quantum Coding Scheme Retrieved 17 August 2014, from http://www.cki.au.dk/experiment/qrypto/doc/QuCrypt/bb84coding.html

Cleve, R., Gottesman, D., & Lo, H. K. (1999). How to share a quantum secret. *Physical Review Letters, 83*(3), 648-651.

Collins, M. J., Clark, A., Yan, Z., Xiong, C., Steel, M. J., & Eggleton, B. J. (2014). *Quantum Random Number Generation using Spontaneous Raman Scattering.* Paper presented at the CLEO: QELS_Fundamental Science.

Collins, R. J., Hadfield, R., Fernandez, V., Nam, S., & Buller, G. (2007). Low timing jitter detector for gigahertz quantum key distribution. *Electronics Letters, 43*(3), 180-181.

Crépeau, C. (1988). *Equivalence between two flavours of oblivious transfers.* Paper presented at the Advances in Cryptology—CRYPTO'87.

Crépeau, C., & Kilian, J. (1988). *Achieving oblivious transfer using weakened security assumptions.* Paper presented at the Foundations of Computer Science, 1988., 29th Annual Symposium on.

Curty, M., Zhang, L. L., Lo, H. K., & Lütkenhaus, N. (2006). Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. *Arxiv preprint quant-ph/0609094*.

Da-Zu, H., Zhi-Gang, C., & Ying, G. U. O. (2009). Multiparty Quantum Secret Sharing Using Quantum Fourier Transform. *Communications in Theoretical Physics, 51*(2), 221-226.

De Greve, K., Yu, L., McMahon, P. L., Pelc, J. S., Natarajan, C. M., Kim, N. Y., . . . Kamp, M. (2012). Quantum-dot spin-photon entanglement via frequency downconversion to telecom wavelength. *Nature, 491*(7424), 421-425.

Deng, F.-G., Li, X.-H., & Zhou, H.-Y. (2008). Efficient high-capacity quantum secret sharing with two-photon entanglement. *Physics Letters A, 372*(12), 1957-1962. Maximally Entangled State

Denning, D. E., & Smid, M. (1994). Key escrowing today. *Communications Magazine, IEEE, 32*(9), 58-68.

Dodson, B. (2013). Quantum "spooky action at a distance" travels at least 10,000 times faster than light Retrieved 17 August 2014, from http://www.gizmag.com/quantum-entanglement-speed-10000-faster-light/26587/

Dušek, M., Jahma, M., & Lütkenhaus, N. (2000). Unambiguous state discrimination in quantum cryptography with weak coherent states. *Physical Review A, 62*(2), 022306.

Ekert, A. K. (1991). Quantum cryptography based on Bell’s theorem. *Physical Review Letters, 67*(6), 661.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., & Yeh, H. (2005). *Current status of the DARPA quantum network.* Paper presented at the Defense and Security.

Even, S., Goldreich, O., & Lempel, A. (1985). A randomized protocol for signing contracts. *Communications of the ACM, 28*(6), 637-647.

Félix, S., Gisin, N., Stefanov, A., & Zbinden, H. (2001). Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses. *Journal of Modern Optics, 48*(13), 2009-2021.

Francis, M. (2012). Quantum entanglement shows that reality can’t be local Retrieved 17 August 2014, from http://arstechnica.com/science/2012/10/quantum-entanglement-shows-that-reality-cant-be-local/

Fröhlich, B., Dynes, J. F., Lucamarini, M., Sharpe, A. W., Yuan, Z. L., & Shields, A. J. (2013). *A Multi-User Quantum Access Network.* Paper presented at the CLEO: QELS_Fundamental Science.

Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V. B., Tomamichel, M., & Werner, R. F. (2012). Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical Review Letters, 109*(10), 100502.

Furusawa, A., Sørensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J., & Polzik, E. S. (1998). Unconditional quantum teleportation. *Science, 282*(5389), 706-709.

Gabay, M., & Arnon, S. (2005). Effect of turbulence on a quantum-key distribution scheme based on transformation from the polarization to the time domain: laboratory experiment. *Optical engineering, 44*(4), 045002-045002-045006.

Gabay, M., & Arnon, S. (2006). Quantum key distribution by a free-space MIMO system. *Journal of lightwave technology, 24*(8), 3114.

Gan, G. (2009). Multiparty quantum secret sharing using two-photon three-dimensional Bell states. *Communications in Theoretical Physics, 52*(3), 421.

Gantmakher, F. R. (1959). *The theory of matrices* (Vol. 131): American Mathematical Soc.

Gao, F., Lin, S., Wen, Q. Y., & Zhu, F. C. (2008). GENERAL: A Special Eavesdropping on One-Sender Versus N-Receiver QSDC Protocol. *Chinese Physics Letters, 25*, 1561-1563.

Gao, F., Qin, S.-J., Guo, F.-Z., & Wen, Q.-Y. (2011). Cryptanalysis of the arbitrated quantum signature protocols. *Physical review A, 84*(2), 022344.

Gao, F., Wen, Q. Y., & Zhu, F. C. (2008). GENERAL: Teleportation attack on the QSDC protocol with a random basis and order. *Chinese Physics B, 17*, 3189-3193.

Gao, G. (2014). Improvement of Efficient Multiparty Quantum Secret Sharing Based on Bell States and Continuous Variable Operations. *International Journal of Theoretical Physics*, 1-5.

Gao, T., Yan, F., & Li, Y. (2009). Quantum secret sharing between m-party and n-party with six states. *Science in China Series G: Physics, Mechanics and Astronomy, 52*(8), 1191-1202.

Gay, S. J. (2006). Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science, 16*(04), 581-600.

Ghose, T. (2013a). Loophole in spooky quantum entanglement theory closed Retrieved 17 August 2014, from http://www.foxnews.com/science/2013/04/22/loophole-in-spooky-quantum-entanglement-theory-closed/

Ghose, T. (2013b). Quantum Entanglement Experiment Reconfirms Physics Phenomenon Einstein Called 'Spooky' Retrieved 17 August 2014, from http://www.huffingtonpost.com/2013/04/22/quantum-entanglement-experiment-physics-einstein-spooky_n_3130888.html

Giovannetti, V., Lloyd, S., & Maccone, L. (2010). Quantum private queries: security analysis. *Information Theory, IEEE Transactions on, 56*(7), 3465-3477.

Gisin, N., Fasel, S., Kraus, B., Zbinden, H., & Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A, 73*(2), 022320.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics, 74*(1), 145.

Goorden, S. A., Horstmann, M., Mosk, A. P., Škorić, B., & Pinkse, P. W. (2013). Quantum-Secure Authentication with a Classical Key. *arXiv preprint arXiv:1303.0142*.

Gottesman, D. (1979). On the theory of quantum secret sharing. *Commun. ACM Phys Rev A, 61*, 042311.

Gottesman, D., & Chuang, I. (2001). Quantum digital signatures. *Arxiv preprint quant-ph/0105032*.

Gottesman, D., & Preskill, J. (2001). Secure quantum key distribution using squeezed states. *Physical Review A, 63*(2), 022309.

Greene, K. (2008). The Best Photon Detector Yet Retrieved 17 August 2014, from http://www.technologyreview.com/news/411322/the-best-photon-detector-yet/page/2/

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

Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., & Grangier, P. (2003). Quantum key distribution using gaussian-modulated coherent states. *Nature, 421*(6920), 238-241.

Gu, B., Mu, L., Ding, L., Zhang, C., & Li, C. (2010). Fault tolerant three-party quantum secret sharing against collective noise. *Optics Communications, 283*(15), 3099-3103.

Gu, B., Xu, F., Ding, L., & Zhang, Y. (2012). High-Capacity Three-Party Quantum Secret Sharing With Hyperentanglement. *International Journal of Theoretical Physics, 51*(11), 3559-3566.

Haitjema, M. A Survey of the Prominent Quantum Key Distribution Protocols Retrieved 17 August 2014, from http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

Hamming, R. W. (1950). Error detecting and error correcting codes. *Bell System technical journal, 29*(2), 147-160.

Hao, L., Li, J., & Long, G. (2010). Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. *Science China Physics, Mechanics and Astronomy, 53*(3), 491-495.

He, G. P. (2007). Comment on" Experimental Single Qubit Quantum Secret Sharing". *Physical Review Letters, 98*(2), 28901.

He, G. P., Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., & Weinfurter, H. (2007). Comment on: Experimental single qubit quantum secret sharing. Authors' reply. *Physical Review Letters, 98*(2).

Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (1995). Proactive secret sharing or: How to cope with perpetual leakage *Advances in Cryptology—CRYPT0'95* (pp. 339-352): Springer.

Hillery, M. (2000). Quantum cryptography with squeezed states. *Physical Review A, 61*(2), 022309.

Hillery, M., Buzek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Physical Review A, 59*(3), 1829-1834.

Hong, C., Kim, J., Lee, H., & Yang, H. (2006). Authenticated Multiuser Quantum Direct Communication using Entanglement Swapping. *Arxiv preprint quant-ph/0601194*.

Huang, D., Chen, Z., Guo, Y., & Lee, M. H. (2007). Quantum Secure Direct Communication Based on Chaos with Authentication. *Journal of the Physical Society of Japan, 76*(12), 124001.

Huang, W., Wen, Q.-Y., Liu, B., Su, Q., & Gao, F. (2013). Cryptanalysis of a multi-party quantum key agreement protocol with single particles. *Quantum information processing*, 1-7.

Hughes, R. J., Chapuran, T. E., Dallmann, N., Hiskett, P. A., McCabe, K. P., Montano, P. M., . . . Sedillo, R. (2005). *A quantum key distribution system for optical fiber networks.* Paper presented at the Optics & Photonics 2005.

Hughes, R. J., Nordholt, J. E., Derkacs, D., & Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics, 4*(1), 43.

Hwang, T., Hwang, C.-C., & Li, C.-M. (2011). Multiparty quantum secret sharing based on GHZ states. *Physica Scripta, 83*(4), 045004.

Hwang, T., Luo, Y., & Chong, S. (2011). Enhancement on security analysis and improvents of arbitrated quantum signature. *arXiv preprint quant-ph/1109.1744*.

idQuantique. (2006). Geneva Secure Vote Retrieved 17 August 2014, from http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html

Inoue, K., Waks, E., & Yamamoto, Y. (2002). *Differential phase-shift quantum key distribution*. Paper presented at the Photonics Asia 2002.

Inoue, K., Waks, E., & Yamamoto, Y. (2003). Differential-phase-shift quantum key distribution using coherent light. *Physical Review A, 68*(2), 022317.

Jain, N., Anisimova, E., Wittmann, C., Marquardt, C., Makarov, V., & Leuchs, G. Investigating the feasibility of a practical Trojan-horse attack on a commercial quantum key distribution system. *Laser, 1*, D0.

Jakobi, M., Simon, C., Gisin, N., Bancal, J.-D., Branciard, C., Walenta, N., & Zbinden, H. (2011). Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A, 83*(2), 022301.

Jensen, J. G., & Schack, R. (2000). Quantum authentication and key distribution using catalysis. *Arxiv preprint quant-ph/0003104*.

Jia, H.-Y., Wen, Q.-Y., Gao, F., Qin, S.-J., & Guo, F.-Z. (2012). Dynamic quantum secret sharing. *Physics Letters A, 376*(10), 1035-1041. New approach.2N +1 particles to share 1 bit (or qubit) among N agents in their secret sharing

Jian, W., Quan, Z., & Chao-Jing, T. (2007). Multiparty Quantum Secret Sharing of Secure Direct Communication Using Teleportation. *Communications in Theoretical Physics, 47*, 454-458.

Jie, S., Ai-Dong, Z., & Shou, Z. (2007). Quantum secure direct communication protocol with blind polarization bases and particles' transmitting order. *CHINESE PHYSICS-BEIJING-, 16*(3), 621.

Jin, X. R., Ji, X., Zhang, Y. Q., Zhang, S., Hong, S. K., Yeon, K. H., & Um, C. I. (2006). Three-party quantum secure direct communication based on GHZ states. *Physics Letters A, 354*(1-2), 67-70.

Jingzheng, H., Zhenqiang, Y., Wei, C., Shuang, W., Hongwei, L., Guangcan, G., & Zhengfu, H. (2013). A survey on device-independent quantum communications. *Communications, China, 10*(2), 1-10.

Kanamori, Y., Yoo, S. M., Gregory, D. A., & Sheldon, F. T. (2009). Authentication Protocol using Quantum Superposition States. *International Journal*.

Karlsson, A., Koashi, M., & Imoto, N. (1999). Quantum entanglement for secret sharing and secret splitting. *Physical Review A, 59*(1), 162-168.

Kilian, J. (1988). *Founding crytpography on oblivious transfer*. Paper presented at the Proceedings of the twentieth annual ACM symposium on Theory of computing.

Knapp, A. (2013). The Space Station Could Be The Next Frontier Of Quantum Communications Retrieved 17 August 2014, from http://www.forbes.com/sites/alexknapp/2013/04/10/the-space-station-could-be-the-next-frontier-of-quantum-communications/

Koashi, M. (2004). Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters, 93*(12), 120501.

Kraus, B., Gisin, N., & Renner, R. (2005). Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters, 95*(8), 080501.

Kuhn, D. R. (2003a). A Hybrid Authentication Protocol Using Quantum Entanglement and Symmetric Cryptography. *Arxiv preprint quant-ph/0301150*.

Kuhn, D. R. (2003b). A Quantum Cryptographic Protocol with Detection of Compromised Server. *Arxiv preprint quant-ph/0311085*.

Kumavor, P. D., Beal, A. C., Yelin, S., Donkor, E., & Wang, B. C. (2005). Comparison of four multi-user quantum key distribution schemes over passive optical networks. *Lightwave Technology, Journal of, 23*(1), 268-276.

Kurtsiefer, C., Trojek, P., Schmid, C., & Bourennane, M. (2005). Experimental Single Qubit Quantum Secret Sharing. *Physical Review Letters, 95*(23), 230505.

Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P., Tapster, P., & Rarity, J. (2002). Quantum cryptography: A step towards global key distribution. *Nature, 419*(6906), 450-450.

Kye, W. H., & Kim, M. S. (2005). Security against the Invisible Photon Attack for the Quantum Key Distribution with Blind Polarization Bases. *Arxiv preprint quant-ph/0508028*.

Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. *Nature, 464*(7285), 45-53.

Lance, A. M., Symul, T., Bowen, W. P., Tyc, T., Sanders, B. C., & Lam, P. K. (2003). Continuous variable (2, 3) threshold quantum secret sharing schemes. *New Journal of Physics, 5*(1), 4.

Lancho, D., Martinez, J., Elkouss, D., Soto, M., & Martin, V. (2010). QKD in standard optical telecommunications networks *Quantum Communication and Quantum Networking* (pp. 142-149): Springer.

Lee, H., Hong, C., Kim, H., Lim, J., & Yang, H. J. (2004). Arbitrated quantum signature scheme with message recovery. *Physics Letters A, 321*(5), 295-300.

Lee, H., Hong, C., Kim, H., Lim, J., & Yang, H. J. (2004). Arbitrated quantum signature scheme with message recovery. *Physics Letters A, 321*(5-6), 295-300.

Leverrier, A. (2012). Symmetrization technique for continuous-variable quantum key distribution. *Physical Review A, 85*(2), 022339.

Li, Q., Chan, W., & Long, D.-Y. (2009). Arbitrated quantum signature scheme using Bell states. *Physical review A, 79*(5), 054307.

Li, Q., Du, R.-G., Long, D.-Y., Wang, C.-J., & Chan, W.-H. (2009). Entanglement enhances the security of arbitrated quantum signature. *Int. J. Quantum Inf., 7*(5), 913-925.

Li, Q., Li, C., Long, D., Chan, W. H., & Wang, C. (2013). Efficient arbitrated quantum signature and its proof of security. *Quantum Information Processing*, 1-13.

Li, Q., Li, C., Wen, Z., Zhao, W., & Chan, W. H. (2013). On the security of arbitrated quantum signature schemes. *Journal of Physics A: Mathematical and Theoretical, 46*(1), 015307.

Li, Q., Long, D. Y., Chan, W., & Qiu, D. W. (2011). Sharing a quantum secret without a trusted party. *Quantum Information Processing, 10*(1), 97-106.

Li, X., & Barnum, H. (2004). Quantum authentication using entangled states. *International Journal of Foundations of Computer Science, 15*(4), 609-617.

Li, X., & Chen, L. (2007). *Quantum Authentication Protocol Using Bell State*.

Li, Y., Zhang, K., & Peng, K. (2004). Multiparty secret sharing of quantum information based on entanglement swapping. *Physics Letters A, 324*(5-6), 420-424.

Lin, J., & Hwang, T. (2013). New circular quantum secret sharing for remote agents. *Quantum Information Processing, 12*(1), 685-697.

Lin, S., Wen, Q.-Y., Gao, F., & Zhu, F.-C. (2008). Improving the security of multiparty quantum secret sharing based on the improved Boström–Felbinger protocol. *Optics Communications, 281*(17), 4553-4554.

Lin, S., Wen, Q.-Y., Qin, S.-J., & Zhu, F.-C. (2009). Multiparty quantum secret sharing with collective eavesdropping-check. *Optics Communications, 282*(22), 4455-4459. QSS scheme with collective eavesdropping check, only a Bell state is used to accomplish the multi-party QSS task

Lin, T. H., & Hwang, T. (2014). Man-in-the-middle attack on quantum secure communications with authentication. *Quantum information processing, 13*(4), 917-923.

Liu, B., Gao, F., Huang, W., & Wen, Q.-y. (2013). Multiparty quantum key agreement with single particles. *Quantum information processing, 12*(4), 1797-1805.

Liu, C. L. (1968). Introduction to combinatorial mathematics.

Liu, W. J., Chen, H. W., Li, Z. Q., & Liu, Z. H. (2008). GENERAL: Efficient Quantum Secure Direct Communication with Authentication. *Chinese Physics Letters, 25*(7), 2354-2357.

Liu, X.-F., & Pan, R.-J. (2011). Cryptanalysis of quantum secret sharing based on GHZ states. *Physica Scripta, 84*(4), 045015.

Liu, Z.-H., Chen, H.-W., Xu, J., Liu, W.-J., & Li, Z.-Q. (2012). High-dimensional deterministic multiparty quantum secret sharing without unitary operations. *Quantum Information Processing, 11*(6), 1785-1795.

Ljunggren, D., Bourennane, M., & Karlsson, A. (2000). Authority-based user authentication in quantum key distribution. *Physical Review A, 62*(2), 022305.

Lo, H.-K. (1997). Insecurity of quantum secure computations. *Physical Review A, 56*(2), 1154.

Lo, H.-K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical Review Letters, 108*(13), 130503.

Lü, X., & Feng, D.-G. (2005). An arbitrated quantum message signature scheme *Computational and Information Science* (pp. 1054-1060): Springer.

Lu, X., & Feng, D. (2005). *Quantum digital signature based on quantum one-way functions.* Paper presented at the Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on.

Ma, X., & Razavi, M. (2012). Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A, 86*(6), 062319.

Majeed, M. M., Al-Khateeb, K. A., Wahiddin, M. R., & Saeb, M. M. (2010). Protocol of Secure Key Distribution Using Hash Functions and Quantum Authenticated Channels (KDP-6DP). *Journal of Computer Science, 6*(10), 1123.

Makarov, V. (2012). Quantum Hacking Retrieved 31 August 2014, from http://www.youtube.com/watch?v=5kUARd_y53w

Markham, D., & Sanders, B. C. (2008). Graph states for quantum secret sharing. *Physical Review A, 78*(4), 042309. extended the QSS based on the graph states

Massey, J. L. (1994). *Guessing and entropy*. Paper presented at the Information Theory, 1994. Proceedings., 1994 IEEE International Symposium on.

MathWorks. OptiSystem™ Retrieved 17 August 2014, from http://www.mathworks.com/products/connections/product_detail/product_35663.html

Matsumoto, R. (2007). Multiparty quantum-key-distribution protocol without use of entanglement. *Physical Review A, 76*(6), 062316.

Medeiros, R. A. C., de Assis, F. M., Júior, B. L., & Lima, A. F. (2003). Quantum authentication scheme based on algebraic coding. *Arxiv preprint quant-ph/0307095*.

Micro, T. (2013). Security Predictions for 2013 Retrieved 17 August 2014, from http://hackmageddon.com/tag/trend-micro/

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

Mosca, M., Stebila, D., & Ustaoğlu, B. (2013). Quantum key distribution in the classical authenticated key exchange framework *Post-Quantum Cryptography* (pp. 136-154): Springer.

Müller-Quade, J. (2002). Quantum pseudosignatures. *Journal of Modern Optics, 49*(8), 1269-1276.

Müller-Quade, J., & Renner, R. (2009). Composability in quantum cryptography. *New Journal of Physics, 11*(8), 085006.

Niemiec, M., Romański, Ł., & Święty, M. (2011). Quantum Cryptography Protocol Simulator. *Multimedia Communications, Services and Security*, 286-292.

Nihira, H., & Stroud Jr, C. R. (2005). Robust multipartite multilevel quantum protocols. *Physical Review A, 72*(2), 022337.

Nishioka, T., Ishizuka, H., Hasegawa, T., & Abe, J. i. (2002). " Circular type" quantum key distribution. *Photonics Technology Letters, IEEE, 14*(4), 576-578.

NIST. (2014). Random Number Generation Tool Kit Retrieved 17 August 2014, from http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

Noh, T.-G. (2009). Counterfactual Quantum Cryptography. *Physical Review Letters, 103*(23), 230501.

OptiWave. OptiSystem™ Retrieved 17 August 2014, from http://optiwave.com/resources/applications-resources/optical-communication-system-design/.

Ou, Z., Pereira, S. F., Kimble, H., & Peng, K. (1992). Realization of the Einstein-Podolsky-Rosen paradox for continuous variables. *Physical Review Letters, 68*(25), 3663.
Pan, C., Fuguo, D., & Guilu, L. (2007). Multiparty quantum secret sharing of classical and quantum messages. *自然科学口展, 17*(1).
Patel, K., Dynes, J., Lucamarini, M., Choi, I., Sharpe, A., Yuan, Z., . . . Shields, A. (2014). Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Applied Physics Letters, 104*(5), 051123.
Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., . . . Dynes, J. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics, 11*(7), 075001.
Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A., & Kurtsiefer, C. (2009). Daylight operation of a free space, entanglement-based quantum key distribution system. *New Journal of Physics, 11*(4), 045007.
Pereszlenyi, A. (2005). *Simulation of quantum key distribution with noisy channels*.

Peterson, W. W., & Weldon, E. J. (1972). *Error-correcting codes*: MIT press.
Qin, S.-J., Gao, F., Wen, Q.-Y., & Zhu, F.-C. (2008). A special attack on the multiparty quantum secret sharing of secure direct communication using single photons. *Optics Communications, 281*(21), 5472-5474.
Qin, S.-J., & Liu, F. (2014). Information leakage in quantum secret sharing of multi-bits by an entangled six-qubit state. *International Journal of Theoretical Physics*, 1-8.
Qina, S.-J., Gao, F., Wen, Q.-Y., & Zhu, F.-C. (2009). Security of quantum secret sharing with two-particle entanglement against individual attacks. *Quantum Information & Computation, 9*(9), 765-772.
Quantiki. (2014). List of Quantum Comupation Simulators Retrieved 17 August 2014, from http://www.quantiki.org/wiki/List_of_QC_simulators

Rabin, M. O. (2005). How To Exchange Secrets with Oblivious Transfer. *IACR Cryptology ePrint Archive, 2005*, 187.
Ramzan, M., & Khan, M. (2008). Multiparty quantum cryptographic protocol. *Chinese Physics Letters, 25*(10), 3543.
Rarity, J., Tapster, P., Gorman, P., & Knight, P. (2002). Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics, 4*(1), 82.

Rieffel, E., & Polak, W. (2000). An introduction to quantum computing for non-physicists. *ACM Computing Surveys, 32*(3), 300-335.
Ritter, S., Nölleke, C., Hahn, C., Reiserer, A., Neuzner, A., Uphoff, M., . . . Rempe, G. (2012). An elementary quantum network of single atoms in optical cavities. *Nature, 484*(7393), 195-200.
Sanders, J. W., & Zuliani, P. (2000). Quantum programming. *Lecture notes in computer science*, 80-99.
Sarvepalli, P., & Raussendorf, R. (2010). Matroids and quantum-secret-sharing schemes. *Physical Review A, 81*(5), 052333.
Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., . . . Tanaka, A. (2011). Field test of quantum key distribution in the Tokyo QKD Network. *Optics express, 19*(11), 10387-10409.

Scarani, V., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters, 92*(5), 057901.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301.

Scarani, V., & Kurtsiefer, C. (2009). The black paper of quantum cryptography: real implementation problems. *arXiv preprint arXiv:0906.4547*.

Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., & Weinfurter, H. (2005). Experimental single qubit quantum secret sharing. *Physical Review Letters, 95*(23), 230505.

Schoenmakers, B. (1999). *A simple publicly verifiable secret sharing scheme and its application to electronic voting*. Paper presented at the Advances in Cryptology—CRYPTO'99.

Selinger, P. (2004a). A brief survey of quantum programming languages. *Lecture notes in computer science, 2988*, 1-6.

Selinger, P. (2004b). Towards a quantum programming language. *Mathematical Structures in Computer Science, 14*(04), 527-586.

Sergienko, A. V. (2005). *Quantum communications and cryptography*: CRC Press.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612-613.

Shannon, C. E. (1948). A mathematical theory of communication". *Bell System Technical Journal, 27*(July and October, 1948.), 379-423, 623-656.

Sheng, Y.-B., Deng, F.-G., & Zhou, H.-Y. (2008). Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state. *The European Physical Journal D, 48*(2), 279-284.

Shi, B. S., Li, J., Liu, J. M., Fan, X. F., & Guo, G. C. (2001). Quantum key distribution and quantum authentication based on entangled state. *Physics Letters A, 281*(2-3), 83-87.

Shi, R.-h., Huang, L.-s., Yang, W., & Zhong, H. (2010). Multiparty quantum secret sharing with Bell states and Bell measurements. *Optics Communications, 283*(11), 2476-2480. Maximally Entangled state

Shi, R., Lv, G., Wang, Y., Huang, D., & Guo, Y. (2013). On Quantum Secret Sharing via Chinese Remainder Theorem with the Non-maximally Entanglement State Analysis. *International Journal of Theoretical Physics, 52*(2), 539-548.

Singh, S. K., & Srikanth, R. (2003). Unconditionally Secure Multipartite Quantum Key Distribution. *arXiv preprint quant-ph/0306118*.

Song, L., Qiao-Yan, W., & Xiao-Fen, L. (2009). Cryptanalysis and improvement of quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. *Chinese Physics Letters, 26*(12), 120307.

Soubusta, J., Haderka, O., & Hendrych, M. (2001). *Quantum random number generator*. Paper presented at the 12th Czech-Slovak-Polish Optical Conference on Wave and Quantum Aspects of Contemporary Optics.

Sphere, B. (2009). Bloch Sphere Representation of Qubit Retrieved 17 August 2014, 2014, from http://www.60pages.com/quantum-limbo-google-nasa-buckaroo-banzai-and-the-government-shutdown/

Stucki, D., Barreiro, C., Fasel, S., Gautier, J.-D., Gay, O., Gisin, N., . . . Vannel, F. (2009). Continuous high speed coherent one-way quantum key distribution. *Optics express, 17*(16), 13326-13334.

Stucki, D., Legre, M., Buntschu, F., Clausen, B., Felber, N., Gisin, N., . . . Monbaron, P. (2011). Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New Journal of Physics, 13*(12), 123001.

Stucki, D., Walenta, N., Vannel, F., Thew, R. T., Gisin, N., Zbinden, H., . . . Ten, S. (2009). High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics, 11*(7), 075003.

Sun, Y., Wen, Q.-y., & Zhu, F.-c. (2010). Improving the multiparty quantum secret sharing over two collective-noise channels against insider attack. *Optics Communications, 283*(1), 181-183.

Sun, Y., Xu, S.-W., Chen, X.-B., Niu, X.-X., & Yang, Y.-X. (2013). Expansible quantum secret sharing network. *Quantum Information Processing*, 1-12.

Sun, Z., Du, R., & Long, D. (2011). Improving the security of arbitrated quantum signature protocols. *arXiv preprint arXiv:1107.2459*.

Sun, Z., Zhang, C., Wang, B., Li, Q., & Long, D. (2013). Improvements on "multiparty quantum key agreement with single particles". *Quantum information processing, 12*(11), 3411-3420.

Tamaki, K., Koashi, M., & Imoto, N. (2003). Unconditionally secure key distribution based on two nonorthogonal states. *Physical Review Letters, 90*(16), 167904.

Tamaki, K., & Lütkenhaus, N. (2004). Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Physical Review A, 69*(3), 032316.

Tamaki, K., Lütkenhaus, N., Koashi, M., & Batuwantudawe, J. (2009). Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Physical Review A, 80*(3), 032302.

Tan, X., & Jiang, L. (2014). Identity authentication by entanglement swapping in controlled quantum teleportation. *International Journal of Embedded Systems, 6*(1), 3-13.

Tawfeeq, S. K., & Khalil, A. I. (2011). Generation of Truly Random QPSK Signal Waveforms for Quantum Key Distribution Systems Based on Phase Coding. *Iraqi Journal of Laser, 10*, 1-7.

Tittel, W., Zbinden, H., & Gisin, N. (2001). Experimental demonstration of quantum secret sharing. *Physical Review A, 63*(4), 042301.

Tosi, A., Dalla Mora, A., Zappa, F., & Cova, S. (2008). *Performance evaluation of InGaAs/InP SPAD for high clock rate QKD.* Paper presented at the Proceedings of SECOQC QKD Network Demonstration and Conference, Vienna.

Townsend, P. D. (1997). Quantum cryptography on multiuser optical fibre networks. *Nature, 385*(6611), 47-49.

TWINCLING™. (2013). Anatomy of Hacking Retrieved 17 August 2014, from http://www.studymode.com/essays/Ethical-Hacking-773150.html

Tyc, T., Rowe, D. J., & Sanders, B. C. (2003). Efficient sharing of a continuous-variable quantum secret. *arXiv preprint quant-ph/0301028*.

Tyc, T., & Sanders, B. C. (2002). How to share a continuous-variable quantum secret by optical interferometry. *Physical Review A, 65*(4), 042310.

Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., . . . Trojek, P. (2007). Entanglement-based quantum communication over 144 km. *Nature Physics, 3*(7), 481-486.

Walton, Z., Sergienko, A., Saleh, B., & Teich, M. (2005). Noise-Immune Quantum Key Distribution. *Quantum Communications and Cryptography (CRC Press, 2005)*, 211-224.

Wang, C., Deng, F. G., Li, Y. S., Liu, X. S., & Long, G. L. (2005). Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A, 71*(4), 44305.

Wang, C., Deng, F. G., & Long, G. L. (2005). Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state. *Optics communications, 253*(1-3), 15-20.

Wang, J., Zhang, Q., Liang, L.-m., & Tang, C.-j. (2005). Comment on:“Arbitrated quantum signature scheme with message recovery”[Phys. Lett. A 321 (2004) 295]. *Physics Letters A, 347*(4), 262-263.

Wang, J., Zhang, Q., & Tang, C.-j. (2007). Efficient quantum signature protocol of classical messages. *JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS, 28*(1), 64.

Wang, J., Zhang, Q., & Tang, C. (2005). Quantum signature scheme with single photons. *Arxiv preprint quant-ph/0511224*.

Wang, J., Zhang, Q., & Tang, C. (2006). Quantum secure direct communication based on order rearrangement of single photons. *Physics Letters A, 358*(4), 256-258.

Wang, S., Chen, W., Yin, Z.-Q., Zhang, Y., Zhang, T., Li, H.-W., . . . Huang, D.-J. (2010). Field test of wavelength-saving quantum key distribution network. *Optics letters, 35*(14), 2454-2456.

Wang, X.-B. (2013). Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A, 87*(1), 012320.

Waseda, A. (2013). Multiparty Simultaneous Quantum Identity Authentication Secure against Fake Signal Attacks. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 96*(1), 166-170.

Wen, X., Liu, Y., & Zhou, N. (2008). Realizable Quantum Broadcasting Multi-Signature Scheme. *International Journal of Modern Physics B, 22*(24), 4251-4259.

Wikipedia. (2014a). Block cipher security summary, 17 August 2014, from http://en.wikipedia.org/wiki/Block_cipher_security_summary

Wikipedia. (2014b). Challenge-Response Authentication, from http://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication

Wikipedia. (2014c). Hash function security summary Retrieved 17 August 2014, from http://en.wikipedia.org/wiki/Hash_function_security_summary

Wikipedia. (2014d). Key Derivation Function Retrieved 17 August 2014, from http://en.wikipedia.org/wiki/Key_derivation_function

Wikipedia. (2014e). OSI Model Retrieved 17 August 2014, from http://en.wikipedia.org/wiki/OSI_model

Wikipedia. (2014f). Quantum Cryptography Retrieved 17 August 2014, from http://en.wikipedia.org/wiki/Quantum_cryptography

Williams, J. (2013). Spooky Experiment on ISS Could Pioneer New Quantum Communications Network Retrieved 17 August 2014, from http://www.universetoday.com/101408/spooky-experiment-on-iss-could-pioneer-new-quantum-communications-network/

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature, 299*(5886), 802-803.

Xi-Han, L., Chun-Yan, L., Fu-Guo, D., Ping, Z., Yu-Jie, L., & Hong-Yu, Z. (2007). Quantum secure direct communication with quantum encryption based on pure entangled states. *CHINESE PHYSICS-BEIJING-, 16*(8), 2149.

Xiao, L., Long, G. L., Deng, F. G., & Pan, J. (2004). Efficient multiparty quantum-secret-sharing schemes. *Phys Rev A, 69*(5), 052.

Xu, F., Qi, B., Xu, H., Xuan, J., Ma, X., Lo, H.-K., & Qian, L. (2013). *A high-speed quantum random number generator prototype.* Paper presented at the CLEO: Science and Innovations.

Yang, Y.-G., Teng, Y.-W., Chai, H.-P., & Wen, Q.-Y. (2011). Verifiable quantum (k, n)-threshold secret key sharing. *International Journal of Theoretical Physics, 50*(3), 792-798.

Yang, Y.-G., Wang, Y., Chai, H.-P., Teng, Y.-W., & Zhang, H. (2011). Member expansion in quantum (< i> t, n</i>) threshold secret sharing schemes. *Optics Communications, 284*(13), 3479-3482.

Yang, Y.-G., Wang, Y., Teng, Y.-W., & Wen, Q.-Y. (2011). Universal three-party quantum secret sharing against collective noise. *Communications in Theoretical Physics, 55*, 589-593.

Yang, Y.-G., Zhou, Z., Teng, Y.-W., & Wen, Q.-Y. (2011). Arbitrated quantum signature with an untrusted arbitrator. *The European Physical Journal D, 61*(3), 773-778.

Yang, Y., Wen, Q., & Zhang, X. (2008). Multiparty simultaneous quantum identity authentication with secret sharing. *Science in China Series G: Physics, Mechanics and Astronomy, 51*(3), 321-327.

Yang, Y., Wen, Q., & Zhu, F. (2007). An efficient quantum secret sharing protocol with orthogonal product states. *Science in China Series G: Physics, Mechanics and Astronomy, 50*(3), 331-338.

Yu-Guang, Y., Qiao-Yan, W., & Fu-Chen, Z. (2007). An efficient quantum secure direct communication scheme with authentication. *CHINESE PHYSICS-BEIJING-, 16*(7), 1838.

Yu, I. C., Lin, F.-L., & Huang, C.-Y. (2008). Quantum secret sharing with multilevel mutually (un)biased bases. *Physical Review A, 78*(1), 012344.

Zeng, G., & Keitel, C. H. (2002). Arbitrated quantum-signature scheme. *Physical review A, 65*(4), 042312.

Zeng, G., & Keitel, C. H. (2002). Arbitrated quantum-signature scheme. *PHYSICAL REVIEW-SERIES A-, 65*(4; PART A), 42312-42312.

Zhan-Jun, Z., & Zhong-Xiao, M. (2005). Multiparty Quantum Secret Sharing of Key Using Practical Faint Laser Pulses. *Chinese Physics Letters, 22*, 1588-1591.

Zhang-Yin, W., Hao, Y., Gan, G., & Shou-Hua, S. (2006). Robust multiparty quantum secret key sharing over two collective-noise channels via three-photon mixed states. *Communications in Theoretical Physics, 46*(4), 607.

Zhang, D., & Li, X. (2007). *Quantum authentication using orthogonal product states*.

Zhang, S., Wnang, J., & Tang, C. J. (2012). Counterfactual attack on counterfactual quantum key distribution. *EPL (Europhysics Letters), 98*(3), 30012.

Zhang, X., Wen, Q., & Zhu, F. (2007). *Object-Oriented Quantum Cryptography Simulation Model*.

Zhang, Y. S., Li, C. F., & Guo, G. C. (2000). Quantum authentication using entangled state. *Arxiv preprint quant-ph/0008044*.

Zhang, Z., Li, Y., & Man, Z. (2001). Multiparty quantum secret sharing. *J. Phys. A Phys Rev A, 71*, 044301.

Zhang, Z. J. (2005). Multiparty quantum secret sharing of secure direct communication. *Physics Letters A, 342*(1-2), 60-66.

Zhao, S., & De Raedt, H. (2008). Event-by-event Simulation of Quantum Cryptography Protocols. *Journal of Computational and Theoretical Nanoscience, 5*(4), 490-504.

Zheng, D., Chen, K., & You, J. (2002). Multiparty authentication services and key agreement protocols with semi-trusted third party. *Journal of Computer Science and Technology, 17*(6), 749-756.

Zhong-Xiao, M., & Yun-Jie, X. (2007). Quantum secure direct communication via partially entangled states. *CHINESE PHYSICS-BEIJING-, 16*(5), 1197.

Zhu, A. D., Xia, Y., Fan, Q. B., & Zhang, S. (2006). Secure direct communication based on secret transmitting order of particles. *Physical Review A, 73*(2), 22338.

Zhu, J., & Zeng, G. (2005). *Attenuation of quantum optical signal in stratospheric quantum communication*. Paper presented at the Communications, Circuits and Systems, 2005. Proceedings. 2005 International Conference on.

Zhu, Z.-C., Hu, A.-Q., & Fu, A.-M. (2013). Cryptanalysis of a new circular quantum secret sharing protocol for remote agents. *Quantum Information Processing, 12*(2), 1173-1183.

Zineddine, M., & Kindi, H. Smart Phones: another IT Security scuffle.

Zou, X., & Qiu, D. (2010). Security analysis and improvements of arbitrated quantum signature schemes. *Physical review A, 82*(4), 042325.

Zyga, L. (2012). Quantum communication without entanglement could perform faster than previously thought possible Retrieved 17 August 2014, from http://phys.org/news/2012-10-quantum-entanglement-faster-previously-thought.html