Thesis Report

Transition from traditional to modern cryptography: quantum key distribution

---

Submitted To

School of Systems & Technology

In Partial Fulfillment of the Requirements

For Degree Of

MASTER OF SCIENCE (SOFTWARE ENGINEERING)

Submitted by:

Fauzia Durrani(15007114010)

Session 2015-17

Supervised By

Dr. Muhammad Masroor Ahmad

In the Name of Allah

The most Beneficent & Most Merciful

FINAL APPROVAL

It is certified that the research work presented in this thesis entitled,"Transition From Traditional To Quantum Cryptography: Quantum Key Distribution"has been carried out and completed by Fauzia Durrani, under the supervision of Dr. Muhammad Masroor Ahmad at the University of Management and Technology Lahore, Pakistan in December 2017 to fulfill the requirement for the degree of MS Software Engineering.

1. **Supervisor**
   Dr. Masroor Ahmad _____
   Assistant Professor,
   School of Systems & Technology, Lahore

2. **Director Graduate Studies**
   Dr. Shoaib Farooq _____
   HEC approved PHD Supervisor
   Associate Professor,
   School of Systems & Technology,

3. **DEAN SST**
   Dr. Shaukat Iqbal, _____
   Professor,
   School of Systems & Technology,
   University of Management & Technology, Lahore

,

DECLARATION

I FAUZIA DURRANI D/O MUHAMMAD ASLAM DURRANI ID: 15007114010, Session 2015-2017, herby certify that this thesis titled "**Transition from Traditional to Quantum Cryptography: Quantum Key Distribution**" is being submitted in partial fulfillment of the requirement for the MS degree in Software Engineering. This thesis, apart from the recognized assistance of my supervisor, is my original work. The data plus material presented here, to the best of my knowledge, has not been previously submitted as research work, thesis or publication in any form in any other University, research institution etc. in Pakistan or abroad to obtain a research diploma or degree.

Signature: _____

Date: _____

FauziaDurrani

ACKNOWLEDGEMENTS

This thesis owns many thanks to a number of people for their assistance, patience and kindness. Indeed, without their support, I could not have accomplished my goal.

I would like to express my gratitude to ALLAH ALMIGHTY for His help and blessings. I would also like to thanks and appreciate all the people who directly or indirectly assist me in the completion of my work.First and foremost, I would like to express my heartfelt thanks to my supervisor, Dr. Masroor Ahmad for the continuous support for my MS study and related research work, for his patience, motivation, and the vast knowledge. His kind guidance helped me all the time during my research work and lettering of this thesis. I could not have imagined having a better advisor for my MS study.

Finally, I am sincerely grateful to my beloved mother for her continuous support, assistance, patience and encouragement she provided me for during my work.

Fauzia Durrani

TABLE OF CONTENTS

Table of Contents

List of Figures

List of Tables

Chapter1: Introduction

1. Network Security and cryptography 16

2. Key Terminologies 17

2.1Cryptology 17

2.2Encryption 18

2.1.1. Encryption Applications 19

2.2.2. Encryption Schemes 19

2.3. Cryptanalysis 20

3. Cryptographic Eras 20

3.1. Early cryptography 20

3.2.Advancements during World War II 20

3.3. Modern Day Cryptography 21

3.4. Claude R.Shannon’s Contribution 22

3.5. Data Encryption Standards 29

3.6. Diffie. & Hellman’s Work 24

3.7. Hash Functions 24

4. Need for Cryptography: Cryptanalysis 25

5. Quantum Cryptography: A new dimension in cryptography 26

5.1. Quantum Computing 27

5.2 Quantum Cryptography: QKD 30

5.3 Main Concept and Conclusion 32

Chapter 2 32

1.Introduction 32

2.Background Concept and Working 32

2.1. Security Attacks and cryptanalysis 33

2.2.Requirements for secure encryption 34

2.3.Significance of Key 34

2.4.Classical Encryption: Symmetric Encryption 35

2.4.1. Symmetric Encryption Model 35

2.4.2. Key Generation and Distribution 36

2.4.2.1. Cryptanalysis: Scenario 37

2.4.2.2.Attacks for symmetric key encryption 38

2.5: Symmetric encryption: Classical Ciphers 39

2.5.1. Caesar Cipher 39

2.5.2. Monoalphabetic Ciphers 40

2.5.2.1. Playfair Cipher 41

2.5.2.2. Hill Cipher 42

2.5.3.Polyalphabetic Cipher 42

2.5.3.1. VigenereCipher 42

2.5.3.2. Vernam Cipher 43

2.5.3.3.One Time Pad 44

2.6. Transposition Techniques 45

2.6.1. Rotor Machines 46

2.7. Modern Cryptography 47

2.7.1. Block Ciphers 47

2.7.1.1. Fiestal Structure 48

2.7.1.2. Data encryption Standard 49

2.7.1.3. Tipple Des 50

2.7.1.4. Advanced Encryption Standard 50

2.8. Stream Ciphers 51

2.8.1. RC4 52

2.9. Issues in Symmetric Encryption 52

3.Asymmetric Cryptography 53

3.1 Symmetric Vs. Asymmetric 54

3.2 Working Mechanism of Asymmetric Crypto 55

3.3 Cryptanalysis for Asymmetric Crypto 56

3.3.1. Authentication 57

3.3.2. One Way TrapDoor Function 58

3.4. Key Distribution Problem and Asymmetric Crypto 59

3.5. Public Key Algorithms 61

3.5.1 Diffie. Hellman Key Exchange Algorithm 61

3.5.2 RSA 62

3.5.3 Hash Functions and Authentication Codes 63

4. Summary and Conclusion 64

Chapter 3 66

1.Objective 66

2. Introduction 66

3.Core Concepts 67

4. Quantum Theory: Significance and Concepts 68

5.Quantum Cryptography 69

5.1: Quantum cryptography Origins 69

5.2: Fundamental Concepts 70

5.2.1: Quantum Bit OrQuBit 70

5.2.2:HeisenBerg's Uncertainty principle 72

5.2.3: Photon Polarization 72

5.2.4: Entanglement 74

5.2.5: No Cloning Theorem 74

6. Significance of Quantum Crypto in Info Security: KEY Dist. Problem 74

Chapter 4 75

Objective 75

1:Introduction 75

2:WorkFlow 76

3:Quantum Key Distribution 76

3.1: QKD Model 76

3.2: QKD Protocols 77

4: BB84 78

4.1: Phases of BB84 78

4.1.1: Quantum communication Phase 81

4.1.2: Public Discussion Phase 82

4.1.3: Error Correction 82

4.1.4: Example of Sifting 83

5: Practical Implementations 84

5.1: QKD Simulator 85

Chapter 5 86

1. Methodology flow 86
2. Purpose and Motivation 86
3. Literature Review 86
4. Simulation 86
5. Critical analysis of QKD as a relatively novice technique 86
6. Results 86

Chapter 6 87

1. Introduction 87

2. Analyzing Quantum bit error rate 88

3. Security Proof of BB84 90

4. Simulation Steps 90

5. Results 93

Chapter 7 96

1:Introduction 96

2:Limitations of QKD 96

2.1. Hardware Challenges 97

2.2. Distance 97

2.3. Changes in polarization 98

2.4.Digital Signatures 98

2.5. Dedicated Channel 99

2.6. Distance and free space communication 99

2.7. Chinese Breakthrough 99

2.8. Side channel Attacks 100

2.9. Intercept Resent attacks 101

3. Potential Employment Areas of QKD 102

4. Post Quantum Cryptography 102

Chapter 8 103

Conclusion, Recommendations and Future Directions 103

References 105

Lists of Figures

Fig:1.1: CIA Triad
Fig:1:2: Cryptology
Fig:1:3: Simple Encryption and Decryption
Fig:1.4: Symmetric Cryptography
Fig:1.5: Asymmetric Cryptography
Fig:1.6: Simple represenattion of an Enigma Machine
Fig:1.7: Shannon's Representation of a General secrecy system
Fig:1.8: Generic representation of a bit vs. a qubit
Fig: 1.9: Quantum Key Distribution Flow Chart
Fig:1.10: Reference QKD Architecture
Fig:2.1: Symmetric Encryption
Fig:2.2: Symmetric Crypto Model
Fig: 2.3. A Caesar Cipher
Fig:2.4. Mono Alphabetic Ciphers
Fig:2.5. An example of playfair cypher
Fig:2.6. An example of encryption using Vigenere Cipher
Fig:2.7. Rotor Machines
Fig:2. 8. Block Cipher
Fig: 2.9. Fiestal Structure- Encryption and Decryption
Fig: 2.10. DES Structure
Fig: 2.11. AES structure
Fig: 2.12. Public Key Cryptography
Fig: 2.13. Authentication and Integrity
Fig: 2.14. RSA-Key Generation Algorithm
Fig: 3.1. Binary Vs. Quantum
Fig: 3.2. Quantum Bit
Fig: 3.3. Polarization Basis

Fig:3.4: Polarization readings

Fig:4.1: Quantum Key Distribution

Fig:4.2: QKD BB84 Steps

Fig:4.3: Measuring Photon Polarization

Fig:5.1: Methodology Flow Chart

Fig:6.1: Security Proof

Fig:6.2: Table Initial configuration

Fig:6.3: Table Statistics /Overview

List of Abbreviations

DES Data Encryption Standard

AES Advanced Encryption Standard

RSA Rivist Shamir Algorith,

QC Quantum Cryptography

QKD Quantum Key Distribution

NIST National Institute of Standards and technology

PREFACE

This thesis was organized as a partial fulfillment of the requirements of acquiring the degree Master of Science in Software Engineering MS(SE), in the School of System and Technology, SST, located at the University of Management and Technology(UMT).

The thesis is comprised of eight chapters; Chapter 1 explains the introduction of the thesis related to cryptography, the problems in the existing techniques and Quantum cryptography as a new technique. Chapter 2 gives a detailed literature review of various cryptographic techniques along with some of their major issues associated with them. Chapter 3 presents quantum cryptography as a new dimension is cryptography and concepts related to the quantum physics which are at its base, along with one of its most successful application quantum key distribution. Chapter 4 describes the working mechanism of QKD in detail along with its first major protocol BB84.Chapter 5 presents research methodology. Chapter 6 presents the simulation steps and results for analyzing QKD in terms of Quantum Bit Error Rate (QBER).Chapter 7 gives an overview of the practical challenges in Quantum cryptography in general. Chapter 8 presents conclusion and future research directions.

ABSTRACT

Quantum Cryptography has emerged to be a relatively new area in the field of cryptography in recent decades. It assures the secure transmission of information between two parties on the internet in a more secure way as compared to the traditional cryptographic schemes currently being used. Existing cryptographic techniques like symmetric and asymmetric encryption schemes, majorly, are based on the mathematical models. Although these techniques provide assurance about the security of the transmitted information over a network however with the advent of more powerful computers there are possibilities that hackers would be able to breach these techniques. In such a scenario, Quantum cryptography offers a better crypto graphical solution since, instead of relying on mathematical rules; it depends upon the proven laws of physics and assures the secure transmission of information among two parties in a more secure manner as compared to traditional cryptographic schemes used.

A brief and comprehensive literature review is performed to investigate the reasons why classical or current cryptographic techniques have been failed or are vulnerable to security breaches. Why and how quantum cryptography and its technique QKD is more suitable and in which areas it could be proved useful. A comprehensive analysis is performed to elaborate its basic idea and its usage. Besides being a powerful technique why it has not been commercially much successful. What are the threats and possible attacks it is prone to.

QKD being a technique of Quantum cryptography is a powerful technique that could be used to secure one extremely sensitive data in an effective manner but it has some serious kind of challenges that need to be tackle in order to make it suitable and safe technology for use on commercial basis.

Chapter 1: Introduction

'Cryptography' generally refers to the study and practice of methods and techniques used for secure communication of information between a sender and the receiver in the presence of third party. It relies on several mathematical techniques to assure the security of the communicated information and has wide number of applications in various fields from electronic transactions to network communication. In past, it has been used to transform secret messages, to encode secret information in images and so on, however in today's computer centric world; it is most often associated with Encryption and decryption mechanisms associated with transmission of data on a network.