Contents

Acknowledgement **I**
Dedication **II**
Abstract **III**
Contents **IV**

Chapter one: Introduction and basic concepts

1-1 Introduction 1
1-2 Cryptography 2
1-2-1 Restricted cryptography algorithm 3
1-2-1 Key based cryptography algorithm 3
1-2-2-1 Asymmetric 4
1-2-2-1 Symmetric 4
1-2-2-2-a Block 4
1-2-2-2-b Stream 5
1-3 Classical key distribution 5
1-3-1 RSA cipher 6
1-3-1-1 Security of RSA 7
1-3-2 One time pad 8
1-4 Quantum mechanical background 8
1-4-1 Operators 9
1-4-2 Formalism 10
1-4-3 Dirac’s notation 12
1-4-4 Completeness 15
1-4-5 Spin 16
1-4-6 Polarization 20
1-4-7 Measurement 21
1-4-8 Quantum superposition 22
1-4-9 Qubit 23
1-4-10 Single qubit transformation 25
1-4-11 No- cloning theorem 26

Chapter Two: Quantum Cryptography

2-1 Basic and classification 28
2-2 Quantum cryptography based on faint laser pulses 31
2-2-1 polarization encoding protocol (BB84) 31
2-3 Quantum cryptography based on photon pairs 36
2-3-1 Source of entangled photons 41
2-3-2 Types of entanglement 43
2-3-3 Ekert or EPR protocol 50

2-4 Transmission of raw key 51
2-4-1 Bell's inequality 53
2-4-2 Quantum calculation of the correlation in Bell's theorem 55
2-5 Security criteria 59
2-6 Error correction stage 61
2-7 Privacy amplification 63
2-7-1 privacy amplification subtraction parameter 64
2-7-2 privacy amplification parameters 66

Chapter Three: Simulation Work

3-1 introduction 68
3-2 General view of the simulation work 68
3-3 Simulation of the initialization stage 70
3-4 simulation algorithm of quantum transmission stage 75
3-5 Error correction stage 75
3-6 Simulation of the encrypted message stage 78
3-7 Separated program 79

Chapter Four: Results and Discussions

4-1 Introduction 83
4-2 Effective involved EPR pairs 83
4-3 Point wise privacy amplification parameters 89
4-4 Failure probability 92
4-5 Encryption and Decryption of the message 94
4-6 Conclusions 97
4-8Future work 98
References