

People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Ferhat Abbas University

Faculty of sciences



Master's Thesis

To obtain the diploma of **Master's Degree**

Field of Study: **Computer Science**

Specialisation: **Quantum Computing**

Theme

An entanglement protocol study within and without spy

Presented by :

Ghedjati Houcine

Hadjidj Walid

Defended on: *[Juin, 2025]*

in front of the jury composed of:

Dr. Djemame Safia

Pr. Berah Smail

Dr. Djemame Safia

Dr. ACHIRI Leila

President of the Jury

Thesis Supervisor

Co-Supervisor

Examiner

Academic Year: **2024/2025**

DEDICATIONS:

Through this modest work we show our gratitude to our parents and our families for their moral and financial support.

THANKS :

First of all, we would like to thank Professor Berrah Smail for kindly directing this work, for guiding and preciously advising us. We also thank:

1. *The members of the jury for agreeing to judge this work.*
2. *All the teachers who have contributed to our training.*
3. *Our dear friends and the promo M2-QC-2025*

Thank you so much

June 2025

Contents

List of Figures	6
Summary	8
0.1 General Introduction:	11
1 Cryptographic Paradigms and Their Evolution	12
1.1 Classical Cryptography and Its Limits	12
1.1.1 Overview of classical encryption techniques: symmetric (AES, DES) and asymmetric (RSA, ECC)	12
1.1.2 Issues with Key Distribution and Authentication	14
1.1.3 Motivation for Quantum Approaches :	16
1.2 The Quantum Computer :	16
1.2.1 Architecture and Working Principles :	16
1.2.2 Superposition and Parallelism:	17
1.2.3 Quantum Logic Gates and Circuits	18
1.2.4 Quantum Algorithms: Shor and Grover	18
1.3 Basic Notions of Quantum Mechanics	18
1.3.1 Superposition, Measurement Postulate, and Probability Amplitudes	18
1.3.2 Heisenberg Uncertainty Principle:	19
1.3.3 No-Cloning Theorem	20
1.4 Properties of Quantum Information	20
1.4.1 Irreversibility of Measurement	20
1.4.2 Entanglement and Nonlocality:	21
1.4.3 No-Broadcasting Theorem	22
1.5 Qubit	22
1.5.1 Particularity of the Qubit	22
1.5.2 Entangled States	24

1.6	Photon (Polarizations, etc.).....	24
1.6.1	Nature of a Photon as a Quantum Particle.....	25
1.6.2	Polarization States: Horizontal, Vertical, Diagonal.....	27
1.6.3	Qubits Encoded via Polarization.....	29
1.6.4	Superposition and Measurement in Different Bases.....	31
1.7	Single Photon Source.....	33
1.7.1	How Do Single Photon Sources Work?.....	33
1.7.2	The Importance of Single Photons in Quantum Cryptography.....	36
1.7.3	Types of Single-Photon Sources.....	38
1.8	Attenuated Laser Sources.....	39
1.8.1	Principle of Weak Coherent Pulses.....	40
1.8.2	Approximation to Single-Photon States.....	41
1.8.3	Photon Number Splitting (PNS) Attack Vulnerability – Detailed Explanation.....	41
1.9	Conclusion.....	42
2	conception	43
2.1	Principle of Quantum Cryptography.....	43
2.1.1	Overview of Quantum Key Distribution (QKD).....	43
2.1.2	BB84 Protocol Encoding and Basis Choice.....	46
2.1.3	Quantum vs Classical Security Approaches.....	50
2.1.4	Comparison Table: Quantum vs Classical Security [53][54].....	51
2.1.5	Challenges of Quantum Cryptography.....	51
2.1.6	Toward a Post-Quantum Future.....	51
2.2	The Quantum Channel.....	52
2.2.1	Role of Quantum Channel in Transmitting Qubits.....	52
2.2.2	Losses, Decoherence, and Noise in Optical Fibers.....	54
2.3	The Classical Channel.....	56
2.3.1	Role in Key Reconciliation and Error Correction.....	57
2.3.2	functions of the Classical Channel in QKD.....	58
2.3.3	Security Considerations.....	59
2.4	Entanglement Protocols.....	60
2.4.1	B92 Protocol (1992).....	60
2.4.2	Six-State Protocol (SSP).....	61
2.4.3	SARG04 Protocol.....	61

2.4.4	GV95 Protocol	61
2.4.5	KMB09 Protocol.....	61
2.4.6	S9 Protocol.....	61
2.4.7	E91 Protocol (1991).....	61
2.4.8	BBM92 Protocol	61
2.4.9	Coherent One-Way Protocol (COW).....	62
2.4.10	Bell Inequality Tests for Eavesdropping Detection	62
2.4.11	Entanglement Swapping and Quantum Repeaters	62
2.4.12	Use Cases: "Within and Without a Spy" Scenario	63
3	Implementation	66
3.1	Introduction.....	66
3.1.1	Tools and Technologies.....	66
3.1.2	3.2 Development of Artificial Intelligence	67
3.2	Simulation and Results.....	68
3.2.1	Overview.....	68
3.3	Tools and Technologies	68
3.4	Workflow Organigram	68
3.5	Simulation Algorithm	69
3.6	Simulation Results	69
3.7	Conclusion.....	69
4	Annex	71
	Bibliography	75

List of Figures

1.1	AES Encryption Algorithm Structure [10].	13
1.2	Structure of DES Encryption Algorithm [13].	13
1.3	Hybrid architecture for a quantum computer which consists of a classical computer and a quantum memory with the ability to apply unitary operators and perform measurements at the disposal of the classical system	17
1.4	The Role of Nonlocality in Entanglement Estimation and Measurement Incompatibility	22
1.5	The representation of QUBIT.	23
1.6	A photon in the x linear polarization mode is the same as a photon in a superposition of the x' and y' linear polarization modes, each with probability 1/2.	30
1.7	A photon in the x linear polarization mode is the same as a photon in a superposition of the x' and y' linear polarization modes, each with probability 1/2.	31
1.8	A “particle” constrained to move in one dimension under the influence of a specified force.	32
1.9	Excitation - emission cycle from a single atom in response to trigger pulses.	34
1.10	An electrically driven triggered single-photon source. (a) Schematic representation of the experiment.	35
1.11	Demonstration of the wave–particle duality of light using a quantum dot single-photon source	36
2.1	(a) In a classical telecommunication system, Alice sends a message to Bob by transmitting high power pulses of light down an optical fibre.	44
2.2	Apparatus to measure the polarization state of a single photon using a polarizing beam splitter (PBS) and two single-photon detectors D1 and D2.	45
2.3	Schematic arrangement for eavesdropping on data encoded as the polarization state of a single photon. In order to extract useful information,	46
2.4	Data representation values in the BB84 protocol for the two choices of polarization basis	47
2.5	Data encoding scheme according to the BB84 protocol.	47
2.6	An eavesdropper between Alice and Bob tries to measure the polarization angle of the photon sent by Alice and send an identical photon on to Bob [38]	50

2.7	Schematic representation of free-space quantum cryptography[38]	53
3.1	Organigram of the simulation workflow.....	68
4.1	Import Libraries and Setup Configuration [31]	71
4.2	E91 Protocol Simulation (With Without Spy)[31].....	71
4.3	Run Simulations for Trusted and Adversarial Environments[31]	72
4.4	Entanglement Verification and Feature Extraction[31].....	72
4.5	AI Spy Detection using Anomaly Detection python[31]	72
4.6	Evaluation of Spy Detection[31]	73
4.7	Visualization of Anomalies[31]	73
4.8	Run Simulations (Trusted and With Spy)[31]	73
4.9	Approximate CHSH Inequality Score for Entanglement Verification[31].....	74
4.10	Generate PDF Report of Simulation[31]	74

Summary

Summary :

As quantum computing advances, traditional encryption methods face growing security threats. This study focuses on developing and testing a quantum key distribution protocol that leverages entanglement to secure data transmission. We simulate the protocol over optical fibers to analyze how distance, bit rate, and wavelength affect communication quality. Additionally, we assess the protocol's ability to detect and resist eavesdropping by comparing scenarios with and without a spy. The goal is to enhance data security in quantum networks while ensuring efficient transmission, paving the way for more robust quantum communication systems.

Word Keys : Quantum computing • Traditional encryption • Security threats • Quantum key distribution (QKD) • Entanglement • Optical fiber • Distance • Bit rate • Wavelength • Eavesdropping • Spy detection • Quantum networks • Robust communication

ملخص:

مع تقدم الحوسبة الكمومية، تواجه طرق التشفير التقليدية تهديدات أمنية متزايدة. تركز هذه الدراسة على تطوير واختبار بروتوكول توزيع مفتاح كمومي يعتمد على التشابك الكمومي لتأمين نقل البيانات. نقوم بمحاكاة البروتوكول عبر ألياف بصرية لتحليل تأثير المسافة، ومعدل البت، والطول الموجي على جودة الاتصال. بالإضافة إلى ذلك، نقوم بتقييم قدرة البروتوكول على اكتشاف ومقاومة التنصت من خلال مقارنة السيناريوهات بوج وخدمات وبدونه. الهدف هو تعزيز أمان البيانات في الشبكات الكمومية مع ضمان كفاءة النقل، مما يمهد الطريق لأنظمة اتصال كمومية أكثر قوة و موثوقية

الكلمات المفتاحية: الحوسبة الكمومية • التشفير التقليدي • التهديدات الأمنية • بروتوكول توزيع المفتاح الكمومي • التشابك الكمومي • الألياف البصرية • المسافة • معدل البت • الطول الموجي • التنصت • اكتشاف الجاسوس • الشبكات الكمومية • الاتصال الموثوق

Résumé :

Avec l'avancement de l'informatique quantique, les méthodes de chiffrement traditionnelles sont confrontées à des menaces de sécurité croissantes. Cette étude se concentre sur le développement et les tests d'un protocole de distribution de clés quantiques basé sur l'intrication pour sécuriser la transmission des données. Nous simulons le protocole à travers des fibres optiques afin d'analyser l'impact de la distance, du débit binaire et de la longueur d'onde sur la qualité de la communication. De plus, nous évaluons la capacité du protocole à détecter et à résister à l'espionnage en comparant les scénarios avec et sans espion. L'objectif est d'améliorer la sécurité des données dans les réseaux quantiques tout en assurant une transmission efficace, ouvrant la voie à des systèmes de communication quantique plus robustes.

Mots-clés : Informatique quantique • Chiffrement traditionnel • Menaces de sécurité • Distribution de clés quantiques (QKD) • Intrication quantique • Fibre optique • Distance • Débit binaire • Longueur d'onde • Espionnage • Détection d'espion • Réseaux quantiques • Communication robuste