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	President of the Jury
Pr. Berah Smail	Thesis Supervisor
Dr. Djemame Safia	Co-Supervisor
Dr. ACHIRI Leila	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

الملخص :

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 بوجود وبِدْمان وبدونه. الهدف هو تعزيز أمان البيانات في الشبكات الكمومية مع ضمان كفاءة النقل، مما يمهد الطريق لأنظمة اتصال كمومية أكثر قوة وموثوقية.

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

First part

0.1 General Introduction:

In a time where knowledge is a valuable resource, data transfer security has become crucial. Even with their advanced features, classical cryptography systems are inevitably susceptible to increases in processing capacity, particularly as quantum computing becomes more and more prevalent. Quantum algorithms that can solve the challenges that underlie the security of algorithms like RSA and ECC in polynomial time have the potential to make once-unbreakable algorithms obsolete.

Interest in quantum cryptography, a cutting-edge science that uses the basic principles of quantum mechanics to ensure secure communication, has increased as a result of this growing vulnerability. The strength of quantum cryptography is derived from physical concepts such the Heisenberg uncertainty principle, quantum entanglement, and the no-cloning theorem, in contrast to classical cryptography, which bases its security on mathematical complexity. Because of these principles, some quantum protocols are intrinsically resistant to undetected eavesdropping, regardless of the adversary's computational capabilities.

Quantum entanglement, a phenomena where particles become connected to the point where their states instantly influence one another regardless of their distance from one another, is at the core of this new frontier. Entanglement makes it possible to create new cryptographic protocols that are both theoretically safe and physically verifiable. A paradigm change in secure communication is provided by entanglement-based quantum key distribution (QKD) methods such as E91, which allow users to identify any possible spy or eavesdropper by looking for variations in predicted quantum correlations.

In this thesis, the application and theoretical foundations of entanglement protocols for secure communication are examined, both with and without an adversary, or "with and without a spy." We discuss the practical difficulties of deploying entangled photons, the behaviour of entangled quantum systems under different situations, and the response of various protocols to observation or interference. By doing this, we hope to draw attention to the advantages, drawbacks, and prospects of entanglement-based quantum communication.

This study offers a conceptual and technical guide to comprehending how quantum entanglement may become the cornerstone of the next generation of secure communication by first providing a strong foundation in classical and quantum cryptography and then moving into in-depth protocol analysis.

Chapter 1

Cryptographic Paradigms and Their Evolution

1.1 Classical Cryptography and Its Limits

1.1.1 Overview of classical encryption techniques: symmetric (AES, DES) and asymmetric (RSA, ECC)

Cryptography is a technique used for the conversion of plain text into cipher text for providing the security of data and information on different devices [1].
Cryptography includes various techniques like word-image fusion and other methods for providing secure data transmission. It is the study of techniques for secure communication in the presence of attackers. Modern cryptography concerns itself with the following objectives[2]:

1. **[a]. Confidentiality:** Securing the data so that no other person other than the intended user can understand the data [3].
2. **[b].Integrity:** The data can't be modified or accessed by the unauthorized user without being noticed when it is in transit or storage [4].
3. **[c].Non-repudiation:** The sender has to bear the responsibility for the data transmitted so that in the later stages he/she can't deny it [5].
4. **[d].Authentication:** The identity of the sender and receiver has to be confirmed by each other[6].

Cryptography Algorithms Considered for Evaluation

1. Advanced Encryption Standard (AES) :
AES is the symmetric encryption algorithm based on the Substitution Permutation Network (SPN) structure [7]. It is a symmetric encryption standard used for secure data transfer between the initiator and receiver [8]. It is a block cipher consisting of different key lengths 2^8 bits, 192 bits, and 2^8 bits. It contains four basic tasks: Sub Bytes, Shift Rows, Columns, and Round key[9].

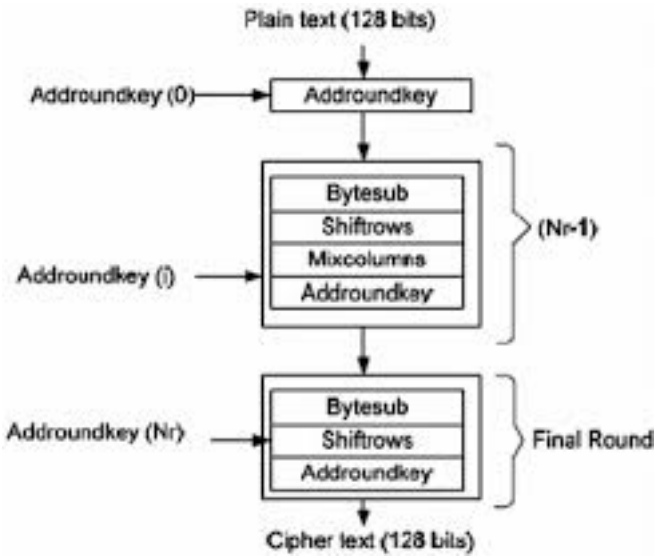

Figure :1.1 AES Encryption Algorithm Structure]10.[

2. DATA ENCRYPTION STANDARD (DES) :

It is a block cipher based on SKE [11]. At the encryption site, DES generates a 64-bit ciphertext from a 64-bit plaintext, and at the decryption site, DES generates a 64-bit block of plaintext from a 64-bit ciphertext. Both encryption and decryption use the same 56- bit cipher key. The DES network is based on the Feistel network (FN). The algorithm is strengthened throughout 16 rounds. DES was built for hardware; it is fast in hardware but only moderately fast in software [12].

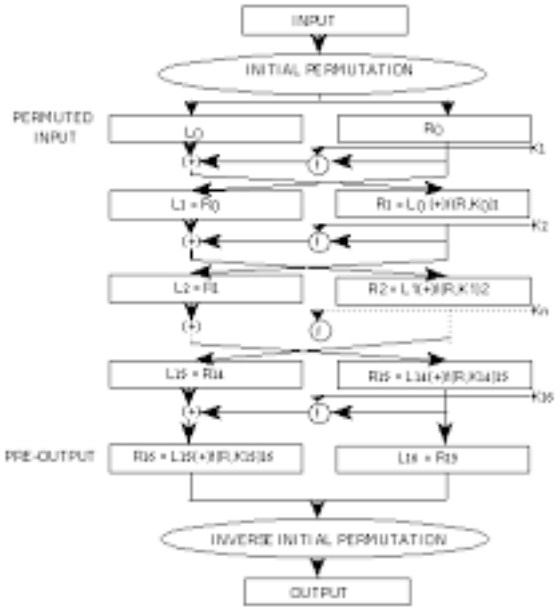

Figure :1.2 Structure of DES Encryption Algorithm]13.[

3. Rivest Shamir Adlmen (RSA) :

RSA is considered the most secure way of encryption. RSA uses prime numbers and exponents. The integers used in this method are quite large making it difficult to decrypt. Here we use 2 keys i.e., public and private. RSA is used in SSL, MIME, RSA signature, and verification. The key distribution problem is solved in RSA and it removes the problem of authentication and confidentiality that we had in symmetric key cryptography [14].

RSA provides us with digital signatures so that no unauthorized user can tamper with the data. The public key used in RSA is shared over the network but the private key is not shareable [15].

Data in RSA cannot be modified. RSA is used with DSA to solve the problem of authentication and integrity of the message.

RSA keys are mainly 2 10 to 211 bits and increasing the key size increases the encryption strength exponentially. Key generation is slow in RSA and the algorithm fails if the message length is greater than the key size [16].

4. Elliptic Curve Cryptography (ECC):

ECC is gaining a lot of popularity as an alternative to RSA. ECC is a PKC based on an elliptic curve. It gives us faster, smaller, and more efficient cryptography keys using the elliptical curve equation. ECC generates keys that are mathematically harder to decrypt. ECC keys are harder to decrypt since they are very difficult to generate as well as decode [18]. Victor Miller and Neil Koblitz discovered ECC in 1985. Security in ECC is obtained from an elliptic curve logarithm. In constrained devices like mobile phones and wireless devices having limited bandwidth, memory, and battery life a public key cryptosystem must be chosen so that it is efficient in terms of Computing cost, storage cost, and key size [19]. ECC provides the highest security per bit as compared to other cryptography algorithms. Smaller key size helps to reduce and save bandwidth memory and processing power. RSA having 1024 bits is equivalent to 256-bit ECC in terms of security. ECC keys are difficult to break. Cryptographic resistance per bit in ECC is much greater than other cryptography algorithms present, it requires lesser memory storage, has greater encryption and signing speed in both hardware and software implementation, and is also ideal for small-size hardware implementation [20].

1.1.2 Issues with Key Distribution and Authentication

The implementation of 1- and 2-photon quantum communication protocols in km long optical fibers suffers from several decoherence mechanisms. In this contribution we review the main ones and illustrate how one can control them. Photons are characterized by three (non independent) parameters: their temporal coherence, their polarization and their frequency spectrum. In the next three sections decoherence affecting each of these parameters are presented, together with counter-measures. The first one, in the time domain, leads to a useful measurement method of polarization mode dispersion. Mastering the second one, depolarization, leads to a practical implementation of quantum cryptography. Finally, the phenomenon of two-photon chromatic dispersion cancelling opens the route to long distance Bell experiments.

Polarization Mode Dispersion: Decoherence in the time domain:

Real fibers are not perfectly circular. Consequently, the two polarization modes are not degenerate and propagate at different phase and group velocities. The Difference in group velocities results in **Polarization Mode Dispersion (PMD)**. The phenomenon of PMD is presently a very severe limitation to high speed optical communication. In addition to the presence of two group velocities, PMD is characterized by random polarization mode coupling: some energy of the fast mode couples to the slow mode and vice-versa. The locations where such couplings take place and their extend are very sensitive to thermal and mechanical variations. Hence, in practice, the coupling is described as a random phenomenon [1, 2]. The magnitude of the dispersion ranges from a few tenths of a picosecond up to tens of picoseconds. Because of its stochastic nature, PMD is measured in units of $\mathrm{ps}/\sqrt{\mathrm{km}}$.

Direct measurement of PMD is a non trivial task. When light with a short coherence time (typically light from a LED with $\tau_c \approx 0.05$ ps) propagates down a fiber, the dispersion is larger than the coherence, producing decoherence. However, coherence can be recovered by connecting an interferometer at the end of the fiber, see figure 1. When the

interferometer is unbalanced, light that went out of coherence in the fiber by precisely the amount of imbalance of the interferometer can be brought back into coherence. This leads to interference fringes even when the interferometer's imbalance is larger than the source coherence, see figure 2. This simple technique to recohere light is widely used by the telecom industry to measure PMD [3].

An interesting generalization using 2-photon interferometry was demonstrated by A. Sergienko and A. Muller, see [4, 5].

Chromatic Dispersion: Decoherence in the frequency domain :

For long distance Bell experiments, the use of polarization correlation is unpractical because of the depolarization mechanism described in the previous section (see however [13] where the distance and the photon spectrum were reduced to limit depolarization). Moreover, the use of Faraday Mirrors is incompatible with the requirement that the two detectors and the source should be at three widely separated locations. In 1989, Jim Franson [14] proposed an elegant two-photon interferometer free of the depolarization problem and suitable for tests of the Bell inequality over long distance, see figure 5 (actually, in this scheme polarization has to be controlled inside the two distant interferometers, but depolarization in the long fibers connecting the source and interferometers is irrelevant [15, 16]).

However, chromatic dispersion, the fact that different optical frequencies (wavelengths) propagate at different speeds, imposes severe limitations to the fringe visibility in Franson interferometers. Indeed, the two photons, emitted precisely at the same time by spontaneous parametric down-conversion in a nonlinear crystal, must be detected in coincidence, within a time window of typically 300 ps. This time window must be short enough so that one can distinguish the cases when the two photons took both the short or both the long arm of their interferometer, from the cases when they took different arms. For stability reasons it is reasonable to have arm length differences of some tens of cm, corresponding to a few ns. But if chromatic dispersion (or any other cause of dispersion) reduces the time correlation between the photons, then a coincidence detection no longer guarantees that both photons took the same path. Hence, chromatic dispersion severely reduces the 2-photon interference visibility.

In a dispersive media, like the silica of optical fibers, the chromatic dispersion vanishes for a wavelength close to 1310 nm (the exact value depends on details of the manufacture). In our long distance Bell experiment, the single photons had a spectral width of about ± 35 nm. Hence, for a fiber length of 17 km[1], the chromatic dispersion is of the order of 500 ps, large enough to reduce the fringe visibility down below the threshold set by Bell inequality (Bell inequality is violated for visibilities larger than $1/\sqrt{2} \approx 71\%$).

One way around this decoherence mechanism is the following. In good approximation, chromatic dispersion is a linear function of the wavelength λ (this approximation is valid over several tens of nm). Hence the differential group delay is a quadratic function of λ, with its minimum at λ_0, the wavelength of zero chromatic dispersion. Accordingly, if the central wavelength of the photon pair is precisely at λ_0, then, thanks to the frequency correlation of the two photons, both photons are at wavelengths symmetrically above and below λ_0. Both photons undergo thus

the same differential group delay, hence arrive at the analyzer in perfect coincidence. This phenomenon, called *2-photon chromatic dispersion cancellation* [17], is essential for long distance Bell experiments using optical fibers.

Note that we made two approximations: first that chromatic dispersion is approximately a linear function of wavelength, next that the frequency correlation $\nu_1 + \nu_2 = \nu_{\text{pump}}$ (due to energy conservation) implies the approximate wavelength correlation $\lambda_1 + \lambda_2 \approx \lambda_{\text{pump}}$ (this second approximation is not necessary, as all the discourse could be phrased in terms of frequency, but traditionally chromatic dispersion is expressed in wavelengths).

1.1.3 Motivation for Quantum Approaches :

The fundamental limitations of classical cryptographic systems have driven the development of quantum-based solutions, particularly in the domain of secure key distribution. Traditional public-key cryptography relies on computational complexity assumptions that may become vulnerable with advances in algorithm design or computational power Shor1997. In contrast, quantum key distribution (QKD) offers information-theoretic security based on the laws of quantum physics rather than computational assumptions.

The security foundation of QKD stems from two key quantum principles:

- The *no-cloning theorem* prevents perfect copying of unknown quantum states
- Measurement-induced disturbance ensures that any eavesdropping attempt introduces detectable anomalies

As demonstrated by Scarani2009, practical QKD implementations can achieve robust security even when accounting for real-world experimental imperfections. Their comprehensive review establishes that:

$$\epsilon_{\text{sec}} \leq 2^{-s} + \epsilon_{\text{cor}} \qquad (1.1)$$

where ϵ_{sec} represents the security failure probability, s is a security parameter, and ϵ_{cor} accounts for correction terms. This rigorous framework has enabled the deployment of QKD systems that are:

- Provably secure against arbitrary attacks
- Compatible with existing telecom infrastructure
- Capable of achieving key rates suitable for practical applications

The quantum approach becomes particularly compelling when considering long-term security requirements, as it provides forward secrecy against future advances in computing technology. Recent developments in measurement-device-independent QKD and twin-field QKD have further extended the practical range and security guarantees of these systems Lo2012, Lucamarini2018.

1.2 The Quantum Computer :

1.2.1 Architecture and Working Principles :

Quantum computers represent a paradigm shift from classical computing by leveraging quantum mechanical phenomena to process information. Unlike classical bits, which exist in states of 0 or 1, quantum bits or qubits can exist in superpositions of both states simultaneously. This capability enables quantum computers to perform complex calculations more efficiently than classical counterparts.

components of a quantum computer include:

1. **Qubits and Quantum Registers:**

    - Quantum information is stored in qubits, which can be implemented using various physical systems such as photons, trapped ions, or superconducting circuits.

2. **Quantum Gates and Circuits:**

   - Quantum logic gates, such as the Hadamard gate, CNOT gate, and Pauli gates, form the fundamental building blocks of quantum circuits. These gates manipulate qubit states based on quantum mechanics.

3. **Quantum Memory and Quantum Processor:**

   - Quantum memory stores quantum information while the quantum processor executes operations on qubits through sequences of quantum gates.

4. **Quantum Measurement and Readout:**

   - Measurement collapses qubits into definite states (0 or 1), producing classical data from quantum states.

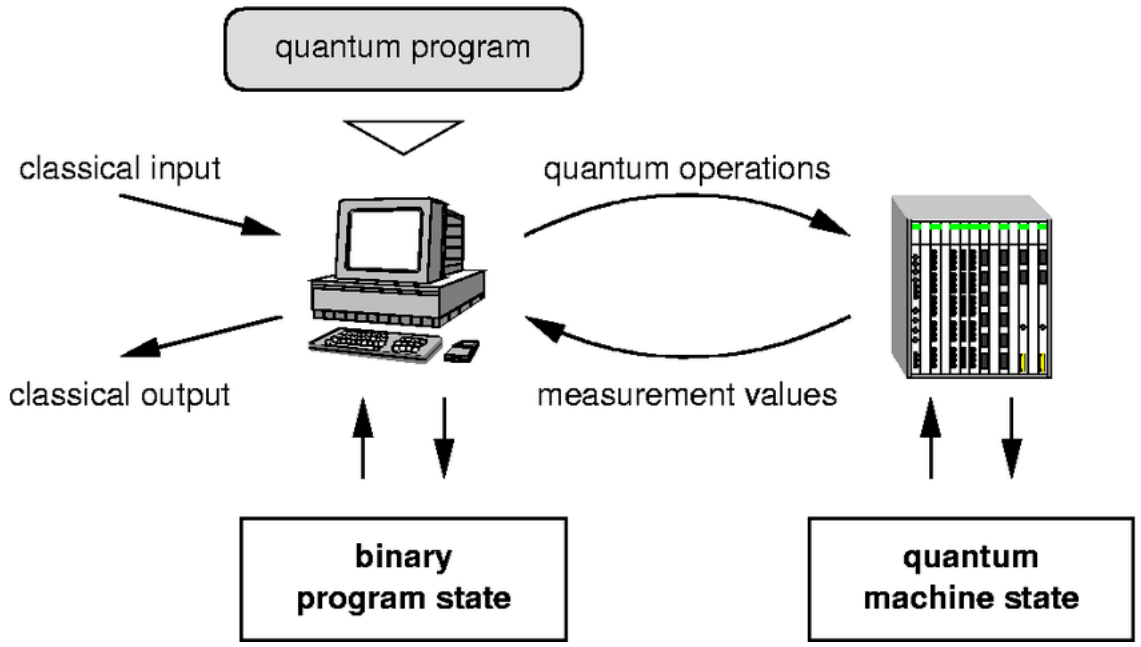

Figure :1.3 Hybrid architecture for a quantum computer which consists of a classical computer and a quantum memory with the ability to apply unitary operators and perform measurements at the disposal of the classical system

1.2.2 Superposition and Parallelism:

A fundamental principle of quantum computing is **superposition**, where qubits can exist in multiple states simultaneously, represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1.2)$$

where α and β are complex probability amplitudes such that:

$$|\alpha|^2 + |\beta|^2 = 1 \qquad (1.3)$$

Superposition enables quantum computers to perform **parallel computations**, exploring multiple potential solutions simultaneously, exponentially increasing computational power [25].

1.2.3 Quantum Logic Gates and Circuits

Quantum gates are the building blocks of quantum circuits, analogous to classical logic gates but operating on qubits. Quantum gates are **unitary operations**, meaning they are reversible and conserve probability amplitudes.

Common Quantum Gates:

- **Hadamard Gate (H):**

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (1.4)$$

- **Pauli Gates (X, Y, Z):** Apply spin-flip and phase shift operations.

- **CNOT Gate:** Entangles two qubits, implementing controlled operations.

Quantum circuits are constructed by combining these gates to perform specific operations [25].

1.2.4 Quantum Algorithms: Shor and Grover

Quantum algorithms harness quantum properties to solve specific problems more efficiently than classical algorithms.

1. **Shor Algorithm:** Shor's algorithm factors large integers in polynomial time, making it a threat to cryptographic systems based on RSA [25].

2. **Grover Algorithm:** Grover's algorithm searches an unsorted database in $O(\sqrt{N})$ time, providing a quadratic speedup over classical search algorithms [25].

1.3 Basic Notions of Quantum Mechanics

1.3.1 Superposition, Measurement Postulate, and Probability Amplitudes

Quantum mechanics challenges classical intuitions by allowing particles to exist in multiple states simultaneously. This phenomenon, known as superposition, forms the foundation of quantum computing and cryptography. **Superposition: The Foundation of Quantum Computing** According to Shankar (1994), a quantum system can exist in a superposition of states, described mathematically as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where:

- $|\psi\rangle$: Quantum state vector,
- $|0\rangle$ and $|1\rangle$: Basis states (analogous to classical bits),
- α and β: Complex probability amplitudes.

Unlike classical bits that are either 0 or 1, qubits can exist in a combination of both states simultaneously. The probabilities of measuring each basis state are given by:

$$P(|0\rangle) = |\alpha|^2, \quad P(|1\rangle) = |\beta|^2$$

The sum of probabilities must always equal 1, ensuring that the quantum system exists in one of the defined states upon measurement:

$$|\alpha|^2 + |\beta|^2 = 1$$

Implications of Superposition in Quantum Systems:

- In quantum cryptography, superposition enables qubits to encode multiple states simultaneously, exponentially increasing computational power.
- In quantum communication, superposition allows for the encoding of multiple bits of information within a single qubit, enhancing the efficiency of data transmission.

Measurement Postulate: Collapsing Superposition Measurement in quantum mechanics is fundamentally different from classical systems. According to Shankar, when a quantum state is measured, the superposition collapses into one of the basis states with a probability determined by the square of the amplitude.
For instance, if the state is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

- The probability of measuring $|0\rangle$ is:

$$P(|0\rangle) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} = 0.5$$

- The probability of measuring $|1\rangle$ is:

$$P(|1\rangle) = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} = 0.5$$

This balanced probability distribution demonstrates the inherent probabilistic nature of quantum mechanics, where measurement outcomes are fundamentally uncertain until observed. [21]

1.3.2 Heisenberg Uncertainty Principle:

The Heisenberg Uncertainty Principle asserts that it is fundamentally impossible to simultaneously measure certain pairs of physical properties, such as position and momentum, with absolute precision. Formulated by Werner Heisenberg and further elucidated by Shankar (1994), it is mathematically expressed as:

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

where:

- Δx: Uncertainty in position,
- Δp: Uncertainty in momentum,
- $\hbar$: Reduced Planck constant ($\hbar = \frac{h}{2\pi}$).

Implications of the Uncertainty Principle:

1. **Quantum Cryptography:**
   - The uncertainty principle ensures that any attempt to measure a quantum state introduces unavoidable disturbances. In the context of quantum key distribution (QKD), this principle forms the basis for detecting eavesdroppers.

2. **Quantum Communication:**

   - If an intruder attempts to intercept a qubit during transmission, the measurement process will disturb the quantum state, altering the probability distribution and exposing the presence of the intruder.

[21]

1.3.3 No-Cloning Theorem

The No-Cloning Theorem, as formulated by Wootters and Zurek (1982), is a cornerstone of quantum mechanics that prohibits the creation of identical copies of an unknown quantum state. This is mathematically expressed as:

$$U(|\psi\rangle \otimes |e\rangle) \neq |\psi\rangle \otimes |\psi\rangle$$

where:

- U: Unitary operation (quantum gate),
- $|\psi\rangle$: Arbitrary quantum state to be cloned,
- $|e\rangle$: Initial "blank" state of the target qubit,
- $\otimes$: Tensor product (denotes composite quantum systems).

This inequality shows that there exists no unitary operation U that can perfectly clone an arbitrary unknown quantum state $|\psi\rangle$.

Why Cloning is Impossible:

- Cloning would require a linear operator that replicates the quantum state without altering it. However, such an operation would contradict the linear nature of quantum mechanics, violating the superposition principle.
- If cloning were possible, it would enable an eavesdropper to intercept and duplicate quantum states without detection, undermining the security of quantum cryptographic protocols like BB84.

Application in Quantum Cryptography:

- In QKD, the no-cloning theorem prevents an eavesdropper from replicating qubits without detection, as any cloning attempt would alter the state probabilities, revealing the intrusion.

1.4 Properties of Quantum Information

1.4.1 Irreversibility of Measurement

In quantum mechanics, the act of measurement is fundamentally irreversible. Unlike classical systems where information can be observed and then restored to its original state, measuring a quantum state collapses its superposition to a single outcome.

Understanding Measurement Irreversibility:

- In classical physics, observing a system does not inherently alter its state. For instance, measuring the speed of a car does not change its speed.
- In quantum mechanics, however, the act of measurement collapses a superposition of states into a single, definite state. This collapse is irreversible.

Quantum Measurement Example:

- Suppose a qubit is in the superposition state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Upon measurement, the state collapses to either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$
- The measurement process is irreversible - once collapsed, the original superposition is lost and cannot be fully recovered. This demonstrates the fundamental difference between quantum and classical information.

1.4.2 Entanglement and Nonlocality:

Quantum entanglement is a phenomenon where two or more qubits become interconnected such that the state of one qubit cannot be fully described without considering the state of the other(s), regardless of the distance between them. This concept is deeply explored in Peres (1995).

What is Entanglement?

Consider two qubits, A and B, in the entangled Bell state:

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Key properties:

- **Correlation**: The qubits are perfectly correlated - measuring both always gives either 00 or 11
- **Non-locality**: If the qubits are separated and qubit A is measured:
  - Getting $|0\rangle_A$ collapses B to $|0\rangle_B$
  - Getting $|1\rangle_A$ collapses B to $|1\rangle_B$

  This occurs *instantaneously*, regardless of distance
- **No Classical Analog**: Einstein called this "spooky action at a distance" as it violates classical locality

Entanglement enables quantum technologies like:

- Quantum teleportation
- Superdense coding
- Quantum cryptography

Peres (1995) Analysis: Peres (1995) discusses how entanglement serves as a resource for quantum communication and quantum cryptography:

- **Bell Inequality:** Demonstrates that the correlations observed in entangled states cannot be explained by classical local hidden variables.
- **Quantum Teleportation:** Shows how entanglement enables the transfer of quantum states without physically transmitting particles.[23]

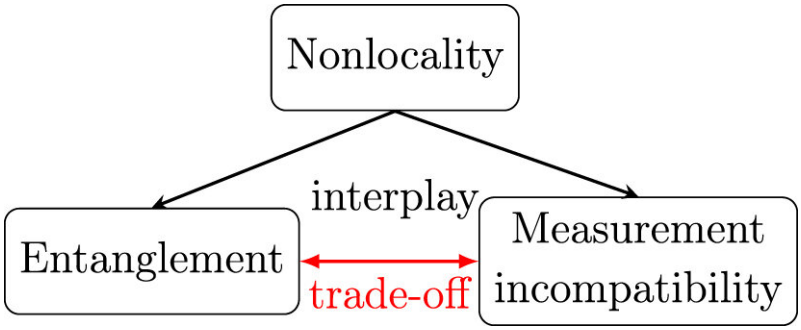

Figure :1.4 The Role of Nonlocality in Entanglement Estimation and Measurement Incompatibility

1.4.3 No-Broadcasting Theorem

The No-Broadcasting Theorem states that it is impossible to create multiple identical copies of a quantum state that is mixed or non-pure. This extends the no-cloning theorem to mixed states and has significant implications for quantum communication and cryptography.

Understanding the No-Broadcasting Theorem:

- In classical systems, information can be easily duplicated and distributed.
- In quantum systems, however, copying a state without disturbing it is fundamentally impossible, as demonstrated by the no-cloning theorem.
- The no-broadcasting theorem further extends this limitation to mixed states, preventing them from being distributed without introducing noise or disturbance.

1.5 Qubit

1.5.1 Particularity of the Qubit

Imagine holding a coin in your hand. In the classical world, the coin can either be heads or tails. But in the quantum world, that coin can be in a state of both heads and tails simultaneously — a concept known as superposition.

A qubit, short for quantum bit, is the quantum version of a classical bit, capable of existing in multiple states at once. Unlike classical bits that are strictly 0 or 1, qubits can exist as a combination of both states until they are measured. This unique property gives qubits their computational advantage, allowing them to process multiple possibilities simultaneously.

Mathematical Representation of a Qubit:

A qubit is represented as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where:

- $|\psi\rangle$: Quantum state of the qubit,
- α and β: Complex probability amplitudes,
- $|0\rangle$ and $|1\rangle$: Basis states, similar to binary 0 and 1,
- The condition $|\alpha|^2 + |\beta|^2 = 1$ ensures that the probabilities sum to 1.

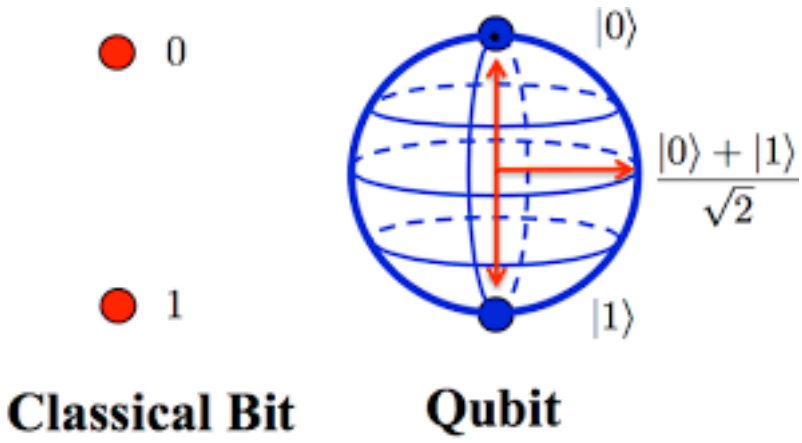

Figure :1.5 The representation of QUBIT

Bloch Sphere Representation:

The state of a single qubit can be visualized as a point on the surface of a unit sphere (the Bloch sphere):

- **Poles**:
  - North Pole: $|0\rangle$ state
  - South Pole: $|1\rangle$ state
- **General State**: Any pure qubit state can be written as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

where:

  - $\theta \in [0, \pi]$: Polar angle (latitude) controls amplitude balance
  - $\phi \in [0, 2\pi)$: Azimuthal angle (longitude) controls quantum phase
- **Key Features**:

- States on opposite points are orthogonal
- Equator represents equal superposition states
- Phase difference appears as rotation about z-axis

Preskill Lecture Notes:

Preskill further emphasizes the versatility of the qubit in his lecture notes from the California Institute of Technology, illustrating that the qubit ability to exist in a superposition is what gives quantum computers their power. Unlike classical bits, which can only hold one state at a time, qubits can hold an infinite number of states, making them essential for algorithms like Shor and Grover algorithms.[25] [26]

1.5.2 Entangled States

Imagine two people holding two halves of a torn piece of paper. No matter how far apart they are, if one person looks at their half, they instantly know what the other half says.

In quantum mechanics, this mysterious connection is called entanglement. When two qubits become entangled, the state of one qubit becomes inextricably linked to the state of the other, even if they are separated by great distances.

- A pair of qubits A and B can be prepared in the **entangled state**:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- If qubit A is measured to be $|0\rangle$, then qubit B will **instantly collapse** to $|0\rangle$, regardless of the distance between them.
- This phenomenon puzzled even Einstein, who famously referred to it as *spooky action at a distance.*

Horodecki Analysis: Quantum Entanglement Review

In 2009, Horodecki et al. published a comprehensive review of quantum entanglement in the Reviews of Modern Physics. They discuss:

- How entanglement is a fundamental resource for quantum communication and quantum cryptography.
- How entanglement can be measured using metrics like concurrence and entanglement entropy.
- The role of entanglement in quantum teleportation, where one qubit state is transmitted to another location without physical transfer.[27]

1.6 Photon (Polarizations, etc.)

Introduction

From quantum perspective, light consists of particles called photons. photon carries electromagnetic energy and momentum, as well as intrinsic angular momentum (or spin) associated with its polarization properties. It can also carry orbital angular momentum. The photon has zero rest mass and travels at c0, the speed of light in vacuum; its speed in dielectric materials is reduced to c< c0. A photon concomitantly has a wavelike character that determines

its localization properties in space and time, and governs how it interferes and diffracts. The notion of the photon initially grew out of an attempt by Max Planck in 1900 to resolve a long-standing conundrum concerning the spectrum of blackbody radiation emanating from a cavity held at a fixed temperature T. Planck ultimately resolved the problem by assuming that the allowed energies of the atoms in the walls of the cavity were quantized to discrete values. In 1905, Albert Einstein proposed that the quantization be imposed directly on the energy of the electromagnetic radiation, rather than on the atoms, which led to the concept of the photon. This enabled Einstein to successfully explain the photoelectric effect. The term "photon" was introduced by Gilbert Lewis in 1926. The concept of the photon and the rules of photon optics are introduced by considering light inside an optical resonator (cavity). This is a convenient choice because it restricts the space under consideration to simple geometry. However, the presence of the resonator turns out not to be an important feature of the argument; the results can be shown to be independent of the form of the resonator, and even of its presence.

in the realm of quantum mechanics, the photon is not just a particle of light—it is a fundamental carrier of quantum information. Understanding its behavior, particularly its **polarization properties**, is essential for advancements in **quantum cryptography**, quantum computing, and secure communication. This section explores the quantum nature of photons and how their polarization enables the encoding, transmission, and measurement of quantum bits (qubits).

We begin by examining the **wave-particle duality of photons**(Section 1.1), establishing why they behave as quantum objects rather than classical particles. Next, we discuss **polarization states—horizontal**, vertical, diagonal, and circular—and how they form the basis for qubit representation . From there, we explore how these states are used to **encode qubits** (Section 1.3) and how **superposition and measurement in different bases**introduce probabilistic behavior critical for quantum security (Section 1.4). Finally, we describe the **optical components—such as polarizers**, wave plates, and beam splitters—that allow precise control over photon polarization (Section 1.5). This foundation is crucial because:

- **Quantum cryptography (e.g., BB84 protocol)** relies on the fact that measuring a photon's polarization disturbs its state, making eavesdropping detectable.
- **Quantum computing**uses polarization-encoded qubits for processing information in ways classical bits cannot.
- **Optical quantum networks** depend on manipulating single photons with high precision.

By the end of this section, you will understand how photons serve as the backbone of quantum communication and why mastering their polarization is key to unlocking the potential of quantum technologies.

1.6.1 Nature of a Photon as a Quantum Particle

Introduction to Quantum Optics and Photon Behavior

Quantum optics is the branch of physics that explores the interaction between light and matter at the smallest scales, where classical wave theories of light give way to quantum mechanical descriptions. At the heart of this field lies the **photon**, the fundamental quantum particle of light. Unlike classical electromagnetic waves, photons exhibit both**particle-like and wave-like properties**, a duality that lies at the core of quantum mechanics.

A photon is a mass-less, charge-less particle that travels at the speed of light ($\approx 299,792$ km/s in a vacuum) and carries discrete packets of energy given by $E = h\nu$, where h is Planck's constant and ν is the photon's frequency. This quantization of energy was first proposed by **Max Planck** in 1900 to explain blackbody radiation and later

formalized by **Albert Einstein** in 1905 to explain the photoelectric effect—work that earned him the Nobel Prize. These discoveries shattered the classical wave theory of light, proving that light could behave as both a particle and a wave.

Wave-Particle Duality and Quantum Superposition

One of the most striking features of photons is their **wave-particle duality**. In some experiments, such as the **double-slit experiment**, photons produce interference patterns characteristic of waves. Yet, when detected, they arrive as discrete particles. This duality is mathematically described by quantum mechanics, where a photon's state is represented by a wavefunction ψ, which encodes probabilities of measurement outcomes.

A photon can exist in a **superposition** of states, meaning it does not have a definite polarization or path until measured. For example, a diagonally polarized photon

$$+ = \frac{1}{\sqrt{2}}(H + V)$$

is neither purely horizontal (H) nor purely vertical (V) but a combination of both. Only upon measurement does it "collapse" into one of these states—a phenomenon central to quantum cryptography protocols like **BB84**.

Polarization States and Qubit Encoding

Polarization is a key property that makes photons ideal for quantum information processing. A photon's polarization describes the orientation of its electric field oscillations:

- **Linear polarization**: Horizontal (H) and vertical (V) are the most common basis states.
- **Diagonal polarization**: Superpositions such as

$$+ = \frac{1}{\sqrt{2}}(H + V)$$

and

$$- = \frac{1}{\sqrt{2}}(H - V)$$

Circular Polarization

Right (R) and left (L) circularly polarized states, representing phase-shifted superpositions:

$$R = \frac{1}{\sqrt{2}}(H + iV), \quad L = \frac{1}{\sqrt{2}}(H - iV)$$

These states can be used to encode **quantum bits (qubits)**, the fundamental units of quantum information. Unlike classical bits (which are strictly 0 or 1), a qubit can be in a superposition, enabling quantum parallelism and secure communication.

Quantum Measurement and the Observer Effect

A fundamental principle of quantum mechanics is that **measurement disturbs the system**. When a photon's polarization is measured, the act of detection forces it into one of the basis states. For example:

- If a + photon is measured in the $\{H, V\}$ basis, it randomly collapses to H or V with 50% probability.

- If measured in the diagonal $\{+, -\}$ basis, it remains unchanged.

This property is crucial for **quantum cryptography**, as any eavesdropper (Eve) attempting to measure photons introduces detectable errors, ensuring security.

Photon Statistics and Quantum Interference

Photons exhibit unique statistical behaviors:

- **Single photons** follow **anti-bunching** (they arrive one at a time, a key feature of true single-photon sources).
- **Coherent laser light** follows Poisson statistics, sometimes emitting multiple photons per pulse.
- **Entangled photons** (e.g., from SPDC) exhibit quantum correlations, violating classical Bell inequalities.

Quantum interference effects, such as **Hong-Ou-Mandel (HOM) interference**, demonstrate the indistinguishability of photons, a critical feature for quantum computing and teleportation.

Applications in Quantum Technologies

Understanding photon behavior has led to revolutionary technologies:

- **Quantum Key Distribution (QKD):** Uses photon polarization to create unhackable encryption.
- **Quantum Computing:** Photons serve as stable qubits in optical quantum computers.
- **Quantum Sensing:** Enables ultra-precise measurements beyond classical limits.

The photon, as a quantum particle, defies classical intuition, blending wave and particle behaviors while enabling groundbreaking technologies. Its polarization, superposition, and measurement properties form the foundation of **quantum optics**and secure communication. As research advances, harnessing single photons and entanglement promises even more transformative applications in computing, cryptography, and beyond.

1.6.2 Polarization States: Horizontal, Vertical, Diagonal

Polarization is a fundamental property of light that describes the orientation of the electric field vector in an electromagnetic wave as it propagates. In classical physics, light can be considered a transverse wave, with the electric field oscillating perpendicular to the direction of propagation. The polarization of such light can take many forms: linear, circular, or elliptical. However, in quantum optics, where individual photons are treated as quantized particles of the electromagnetic field, polarization becomes a quantum degree of freedom. This makes it one of the most practical and widely used methods for encoding and manipulating quantum information. Photon polarization states are central to quantum information protocols such as quantum key distribution (QKD), quantum teleportation, and various implementations of quantum logic gates. The polarization state of a single photon is described as a two-level quantum system, or qubit, making it directly analogous to a spin-½ particle or a two-level atom. This compatibility with qubit formalism makes polarization not only intuitive but also experimentally accessible with mature optical technologies.
In the quantum mechanical description, a photon can exist in a well-defined polarization state, such as horizontal ($|H\rangle$) or vertical ($|V\rangle$), or in a superposition of both. The states $|H\rangle$ and $|V\rangle$ form what is known as the **rectilinear**

basis, a standard basis for describing linear polarization. A photon in the $|H\rangle$ state has an electric field oscillating horizontally with respect to a defined coordinate frame, while a photon in the $|V\rangle$ state oscillates vertically. These two states are orthogonal, meaning they can be perfectly distinguished through measurement using a polarizing beam splitter (PBS) aligned to the horizontal-vertical axis. This binary distinction forms the basis for using polarization to represent qubits: $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$. In the quantum mechanical description, a photon can exist in a well-defined polarization state, such as horizontal ($|H\rangle$) or vertical ($|V\rangle$), or in a superposition of both. The states $|H\rangle$ and $|V\rangle$ form what is known as the **rectilinear basis**, a standard basis for describing linear polarization. A photon in the $|H\rangle$ state has an electric field oscillating horizontally with respect to a defined coordinate frame, while a photon in the $|V\rangle$ state oscillates vertically. These two states are orthogonal, meaning they can be perfectly distinguished through measurement using a polarizing beam splitter (PBS) aligned to the horizontal-vertical axis. This binary distinction forms the basis for using polarization to represent qubits: $|0\rangle \equiv |H\rangle$ and $|1\rangle \equiv |V\rangle$.
However, quantum mechanics allows for more than just these orthogonal basis states. Photons can exist in **superpositions** of $|H\rangle$ and $|V\rangle$, leading to other linear polarization states, such as **diagonal (ID)** and **antidiagonal (IA)**. These states form the **diagonal basis**, where:

- $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$,
- $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$.

In these cases, the electric field oscillates at +45°or -45°to the horizontal, respectively. The diagonal and rectilinear bases are **mutually unbiased**, meaning a measurement in one basis of a state prepared in the other yields completely random outcomes with equal probability. This property is crucial in quantum key distribution protocols such as **BB84**, where a sender (Alice) and receiver (Bob) randomly switch between polarization bases to create a secure key.

Because of the **no-cloning theorem** and the **collapse of quantum states upon measurement**, any eavesdropper (Eve) attempting to intercept the photons introduces detectable disturbances if she measures in the wrong basis.

Quantum information encoded in polarization can also use the **circular polarization basis**, composed of left-circular ($|L\rangle$) and right-circular ($|R\rangle$) polarization:

- $|L\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$,
- $|R\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$.

These states represent photons whose electric field vectors rotate in time as they propagate. Like the diagonal basis, the circular polarization basis provides another set of orthogonal states, expanding the versatility of polarization encoding in quantum systems.

The state of a photon in any polarization basis can be represented as a **quantum state vector** in a two-dimensional Hilbert space. A general state $|\psi\rangle$ can be written as a linear combination:

$$|\psi\rangle = \alpha|\mathrm{H}\rangle + \beta|\mathrm{V}\rangle,$$

where α and β are complex probability amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$. This form makes polarization a natural and elegant representation of a qubit. The ability to prepare arbitrary superpositions allows for rich

quantum behaviors like interference and entanglement, both of which are foundational to quantum computation and communication.

To manipulate and measure polarization states, a variety of **optical components** are used. A **polarizing beam splitter (PBS)** separates incoming photons based on their linear polarization, transmitting $|\mathrm{H}\rangle$ and reflecting $|\mathrm{V}\rangle$, making it a fundamental tool for polarization measurement. **Wave plates**, such as half-wave and quarter-wave plates, are birefringent optical elements that introduce phase shifts between polarization components. A half-wave plate can rotate the polarization direction, for example turning $|\mathrm{H}\rangle$ into $|\mathrm{V}\rangle$ and vice versa, or converting $|\mathrm{D}\rangle$ into $|\mathrm{A}\rangle$. A quarter-wave plate, on the other hand, converts linear polarization into circular and vice versa. These components allow for dynamic control over a photon's polarization state, enabling experiments that require precise preparation, transformation, or analysis of quantum states.

Experimentally, polarization-encoded qubits are relatively easy to work with. Lasers produce coherent beams that can be attenuated to produce single-photon-level outputs. These single photons are then passed through polarizers, wave plates, and beam splitters to prepare and measure specific polarization states. In real-world systems, fiber optics and free-space channels are used to transmit these polarization-encoded qubits over distance. However, maintaining polarization stability over long distances can be challenging due to birefringence in optical fibers or atmospheric turbulence in free space, which can rotate or degrade the polarization state. Thus, active polarization compensation techniques or polarization-maintaining fibers are employed in practical implementations of quantum communication.

The choice of polarization basis not only determines how quantum information is encoded and decoded but also plays a direct role in the security and robustness of quantum communication protocols. Because non-orthogonal quantum states cannot be perfectly distinguished, an eavesdropper cannot measure a qubit in transit without introducing detectable errors. This forms the cornerstone of quantum cryptography, where secure keys can be generated and verified by comparing polarization measurement results over a public channel.

In summary, polarization is a versatile and powerful property of photons that lends itself naturally to qubit representation in quantum optics. The ability to prepare, manipulate, and measure polarization states with high precision using mature optical technology makes it one of the most practical approaches in experimental quantum information science. Whether in the lab or in real-world quantum networks, polarization-encoded photons form the backbone of many key technologies in quantum cryptography, quantum computing, and quantum metrology.

1.6.3 Qubits Encoded via Polarization

Photon Polarization

As indicated earlier, light is characterized by a set of modes of different frequencies, directions, and polarizations, each occupied by an integral number of photons. For each monochromatic plane wave traveling in a particular direction, there are two polarization modes. The polarization of a photon is that of the mode it occupies. For example,the photon may be linearly polarized in the x direction, or right circularly polarized. Since the polarization modes of free space are degenerate, they are not unique. One may use modes with linear polarization in the x and y directions, linear polarization in two other orthogonal directions, say x' and y', or right- and left-circular polarizations. The choice of a particular set is a matter of convenience. A problem arises when a photon occupying a given mode (say linear polarization in the x direction) is to be observed in a different set of modes (say linear polarization in the x' and y' directions). Since the photon energy cannot be split between the two modes, a probabilistic interpretation is called for.

In classical electromagnetic optics, the state of polarization of a plane wave is described by a Jones vector, whose components $\{A_x, A_y\}$ are the components of the complex envelope in the x and y directions, respectively . The same wave may also be represented in a different coordinate system (V, V), e.g., one that makes a 45°angle with the initial coordinate system, by a Jones vector with components .[36]

$$A_{x'} = \frac{1}{\sqrt{2}}(A_x - A_y), \quad A_{y'} = \frac{1}{\sqrt{2}}(A_x + A_y),$$

Therefore, a wave that is linearly polarized in the x direction is described by a Jones vector with components $(\mathrm{A0}, 0)$ in the x-y coordinate system, where Ao is the complex envelope. In the $(xr, y1)$ coordinate system, the Jones vector has components $(\frac{1}{\sqrt{2}}A_0, \frac{1}{\sqrt{2}}A_0)$.

The state of polarization of a single photon is described by a Jones vector with complex components (Ax, Ay), normalized such that $|AE|^2 + |\mathrm{Ay}|^2 = 1$. The coefficients Ax and Ay are interpreted as complex probability amplitudes, and their squared magnitudes, $|\mathrm{AX}|^2$ and $|\ \mathrm{Ay}|^2$, represent the probabilities that the photon is observed in the x and y linear polarization modes, respectively.

Linearly Polarized Photon

The components (Ax, Ay) are transformed from one coordinate system to another in the same manner as ordinary Jones vectors, and the new components represent complex probability amplitudes in the new modes. Thus, a single photon may exist, probabilistically, in more than one mode. This concept is illustrated by the following examples. A photon is linearly polarized in the x direction. In terms of the x—y linearly polarized modes, the photon is described by a Jones vector with components (1,0). In a set of linearly polarized modes in the x' and y' directions at 45°, these components are$(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$, so that the probabilities of observing the photon in a linear polarization mode along the x' or y' directions are both 1/2.

A photon is linearly polarized in the x direction. In terms of the x—y linearly polarized modes, the photon is described by a Jones vector with components (1,0). In a set of linearly polarized modes in the x' and y' directions at 45°, these components are (-1= -±=) so that the probabilities of observing the photon in a linear polarization mode along the x' or y' directions are both |12|. This is illustrated schematically in Fig 2.6. [36]

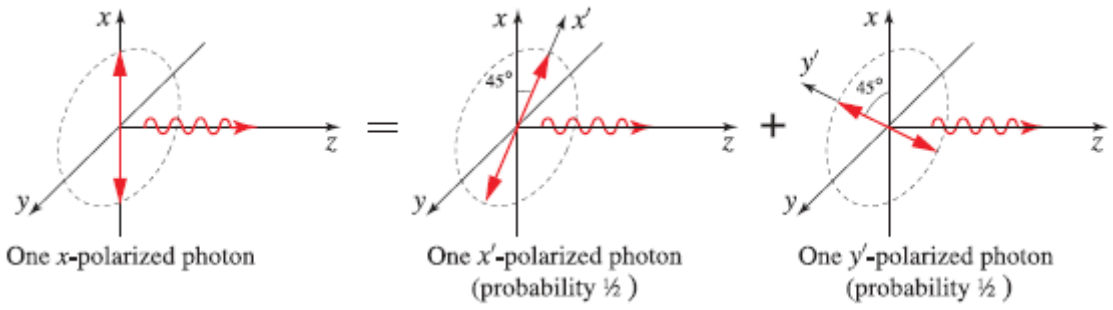

Figure :1.6 A photon in the x linear polarization mode is the same as a photon in a superposition of the x' and y' linear polarization modes, each with probability 1/2

Circularly Polarized Photon

A circularly polarized photon is described by a Jones vector that has components $\frac{1}{\sqrt{2}}(1, \pm j)$, where the + and – signs correspond to right- and left-handed polarization, respectively. This description is based on an x-y coordinate system, i.e., linearly polarized modes. Therefore, the probability of the photon passing through a linear polarizer pointing in either the x or y direction is 1/2. It can also be shown that this result prevails whatever the direction of the linear polarizer. The circularly polarized photon may be regarded as equivalent to the probabilistic superposition of one photon with linear polarization in the x direction and another in the y direction, each with probability $\frac{1}{2}$ light. Right- and left-circular polarizations may also be used as modes (as a coordinate system). In that description, a linearly polarized photon may be regarded as a probabilistic superposition of right- and left-circularly polarized photons, each with probability $\frac{1}{2}$, as illustrated in Fig 2.7.

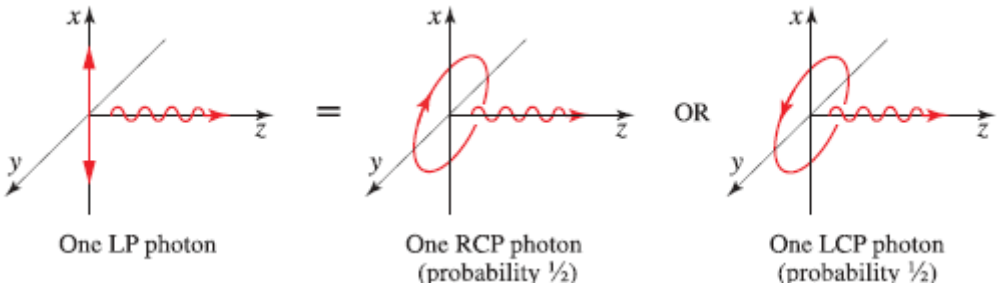

Figure :1.7 A photon in the x linear polarization mode is the same as a photon in a superposition of the x' and y' linear polarization modes, each with probability 1/2

[36]

1.6.4 Superposition and Measurement in Dffierent Bases

The Schrodinger Equation – Superposition Core Concept

Imagine a particle of mass m, constrained to move along the x axis, subject to some specified force $F(x,t)$ (Figure 2.8). The program of classical mechanics is to determine the position of the particle at any given time: $x(t)$. Once we know that, we can figure out the velocity ($v = dx/dt$), the momentum ($p = mv$), the kinetic energy ($T = (1/2)mv^2$), or any other dynamical variable of interest. And how do we go about determining $x(t)^2$. We apply Newton's second law:

$$F = ma.$$

(For conservative systems-the only kind we shall consider, and, fortunately, the only kind that occur at the microscopic level-the force can be expressed as the derivative of a potential energy function,

$$F = -\partial V/\partial x,$$

and Newton's law reads

$$md^2x/dt^2 = -\partial V/\partial x.$$

This, together with appropriate initial conditions (typically the position and velocity at $t = 0$), determines $x(t)$.

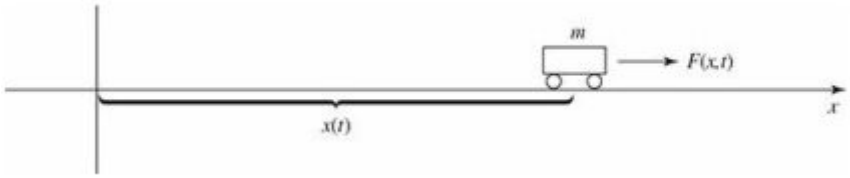

Figure :1.8 A "particle" constrained to move in one dimension under the influence of a specfiied force.

Quantum mechanics approaches this same problem quite differently. In this case what we're looking for is the particle's wave function, $\Psi(x,t)$, and we get it by solving the Schrödinger equation:

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi}{\partial x^2} + V\Psi$$

Here i is the square root of -1, and $\hbar$ is Planck's constant-or rather, his original constant (b) divided by 2π:

$$\hbar = \frac{h}{2\pi} = 1.054573 \times 10^{-34}\ \text{J s.}$$

The Schrodinger equation plays a role logically analogous to Newton's second law: Given suitable initial conditions (typically, $\Psi(x,0)$), the Schrödinger equation determines $\Psi(x,t)$ for all future time, just as, in classical mechanics, Newton's law determines $x(t)$ for all future time.[37]

Measurements and expectation values

We have already pointed out that physically measurable quantities are represented by operators in quantum mechanics. Each operator $\mathcal{O}^\wedge$ has its own set of eigenfunctions and eigenvalues, which are found by solving the corresponding eigenvalue equation:

$$\hat{O}\varphi_i = O_i\varphi_i$$

As was the case for the Hamiltonian operator, the eigenfunctions $\{\phi i\}$ form a complete orthonormal basis, so that an arbitrary state ψ can always be expressed at a specific time as a sum according to:

$$\psi = \sum_i c_i\varphi_i$$

where the coefficients $\{c_i\}$ are, in general, complex numbers. is interpreted as meaning that if we make a measurement of the observable property represented by the operator O on a system prepared in the state ρ_i, the result O_i will be obtained. In other words, if the particle enters the apparatus in one of the eigenstates of $\hat{O}$ (e.g. Y_i), the result will be equal to the corresponding eigenvalue (i.e. O_i). This is true no matter how many times the measurement is made.

It is one of the fundamental postulates of quantum mechanics that the result of a measurement of an observable property represented by the operator O is always equal to one of the eigenvalues of O. The act of measurement 'collapses the wave function' in such a way that, if the particle enters the apparatus in an arbitrary state ψ, it emerges in the state with the eigenfunction corresponding to the result obtained. This means that if we obtain the result O_i,

the particle will emerge with the wave function pi-Subsequent measurements will therefore always give the same result O_i.

The probability for obtaining the result O_i for a particle that enters the apparatus in an arbitrary state ψ is found by expanding the wave function over the eigenstates of $\hat{O}$ as in eqn. It is then apparent that the result O_i will be obtained with a probability equal to $|c_i|^2$. If the experiments repeated many times on an ensemble of particles each prepared in the same state ψ, the average of the results will be equal to:

$$(\hat{O}) = \int \psi^* \partial\psi \, d^3r$$

This average result is called the expectation value of the operator. The spread of the results about the expectation value can be obtained from the mean square variation (the variance):

$$(\Delta O)^2 = \int \psi^* (O - \langle O' \rangle)^2 \psi \, d^3r$$

$$= \langle O^2 \rangle - \langle O^2 \rangle^2$$

The variance represents the average deviation from the mean value, and can be understood as the uncertainty in the quantity that is being measured. An important implication of the collapse of the wave function associated with the measurement process is that the act of measurement generally changes the state of the system.
Therefore, in general it is not possible to measure a property and leave the system undisturbed in the process. Measurements on quantum systems are therefore invasive. The invasiveness of the measurement process is the fundamental principle underlying the security of quantum cryptography systems.

1.7 Single Photon Source

1.7.1 How Do Single Photon Sources Work?

An application of the techniques for the generation of antibunched light is the development of a triggered single-photon source, these sources are needed to improve the security in quantum cryptography experiments. The basic idea of a single-photon source is that the source should emit exactly one photon in response to a trigger pulse, which can be either electrical or optical. The operating principle is shown in Fig. 2.9. The source consists of a single emissive species (say an atom), and the trigger pulse excites the atom to an upper excited state, as shown in Fig. 2.9(a). The atom then emits a cascade of photons as it relaxes to the ground state. Since the photons have different wavelengths, it is possible to select the photon from a particular transition by filtering the fluorescence. There will only ever be one photon emitted from a specific transition in each cascade. Consider now the timing of the photons emitted by this process. An intense trigger pulse will rapidly promote an electron to the excited state.[38]

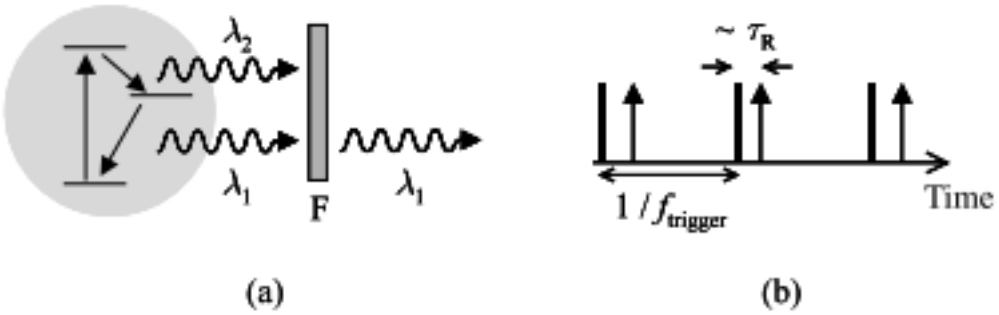

Figure :1.9 Excitation - emission cycle from a single atom in response to trigger pulses.

and the atom will emit exactly one photon after a time roughly equal to the radiative lifetime R, as shown schematically in Fig. 2.9(b). No more photons can be emitted until the next trigger pulse arrives, when the process repeats itself. The time separation of the trigger pulses is determined by the frequency ftrigger at which the trigger source operates. If the time separation between the pulses is significantly longer than R, the trigger pulses control the separation of the photons in the fluorescence. We thus have a source that emits exactly one photon of a particular wavelength whenever a trigger pulse is applied.

The easiest way to make a triggered single-photon source is to use an optical trigger from a suitable laser. However, in the long run it will be important to develop electrically triggered devices. Figure 2.10 illustrates one such implementation incorporating a single quantum dot as the lightemitting species. The device consisted of a GaAs light emitting diode (LED) with a layer of InAs quantum dots inserted within the active region. The quantum dots were excited by a programmed sequence of

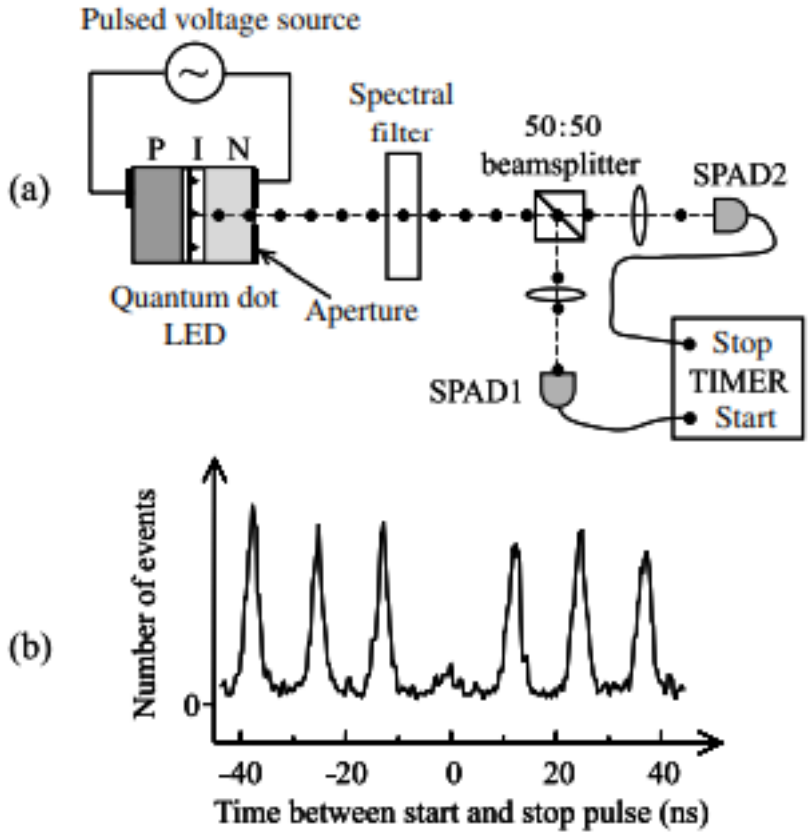

Figure :1.10 An electrically driven triggered single-photon source. (a) Schematic representation of the experiment.

Current pulses produced by a pulsed voltage source. The current pulse injected electrons and holes into the device, and the quantum dots then emitted a light pulse in response to each trigger pulse. An aperture in the top contact ensured that the light from only a few of the InAs quantum dots was collected. The emission wavelength of a quantum dot depends on its size, which varies from dot to dot due to statistical fluctuations related to the crystal growth. Hence the wavelength varied slightly from dot to dot, which allowed the light emitted from a particular emission line of an individual quantum dot to be selected by using a spectrometer as a spectral filter. In these circumstances, we expect the light to be antibunched, as demonstrated previously in Fig. 2.11. Figure 2.10(b) presents the results of the HBT experiment performed on the filtered light emitted from the device using fast single-photon avalanche photodiodes (SPADs) as the detectors. These results can be understood as follows. Let us suppose a photon strikes SPAD1 and generates a trigger pulse to start the timer. The timer will then measure the time that elapses before another photon strikes SPAD2 and generates the stop signal. This second photon may have come from the same light pulse as the first one, or from a different one. In the former case, we will record an event near $\tau = 0$. In the latter case, we will record an event near $\tau = m/f_{\text{trigger}}$, where m is an integer and $f_{\text{trigger}} = 80\,\text{MHz}$ is the frequency of the trigger pulse sequence. Hence the histogram of events will show peaks separated by 12.5 ns in these experiments. The key feature of the results is the very small number of events recorded near $\tau = 0$. This indicates that the source is emitting only one photon in each pulse, because there would have to be at least two photons in the pulse in order to register events at $\tau = 0$. In other words, we must have achieved a single-photon light source.[37]

The results shown in Fig. 2.11 represent a substantial step towards the development of a convenient source for generating single photons on demand. At the present time, the main experimental difficulties that have to be overcome before these single-photon sources find more widespread applications is the low overall quantum efficiency and the

operating temperature, which was 5 K for the data presented in Fig. 2.10. An elegant experiment demonstrating the wave–particle duality of light using a single-photon source is shown schematically in Fig. 2.11. The light from a quantum dot single-photon source was divided equally with a 50 : 50 beam splitter and sent either to a Michelson interferometer or to a HBT experiment. The data from the HBT experiment was collected simultaneously with the fringe pattern from the interferometer. Clear interference fringes demonstrating the wave nature of light were observed at the same time as antibunching, which is a purely photon (i.e. particle) effect. Although it is clear that the individual photons go either to the interferometer or to the HBT experiment, it is very unlikely that the presence of one piece of apparatus can affect the results of the other. Therefore, the simultaneous observation of fringes and antibunching during a data collection run is a good demonstration of the wave–particle duality of light. [38]

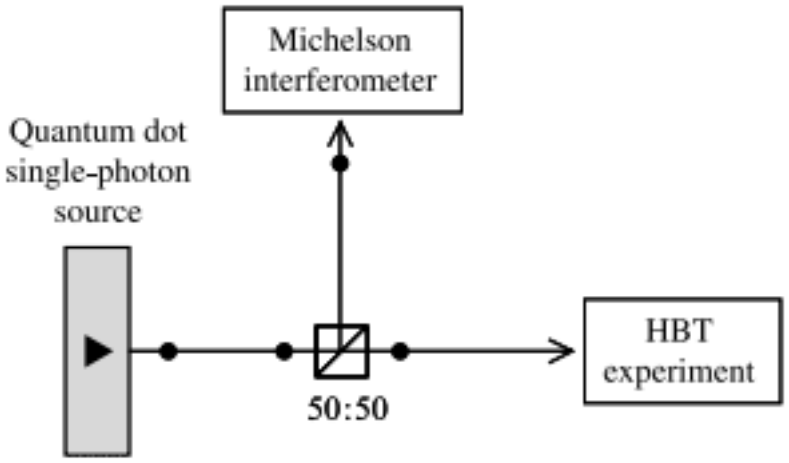

Figure :1.11 Demonstration of the wave–particle duality of light using a quantum dot single-photon source

1.7.2 The Importance of Single Photons in Quantum Cryptography

Quantum cryptography represents a paradigm shift in secure communication, offering theoretical security rooted in the fundamental principles of quantum mechanics. At the heart of this technology lies the single photon, a quantum of light that behaves both as a particle and a wave. Unlike classical signals composed of large numbers of photons, quantum cryptographic protocols rely on the precise control and manipulation of individual photons. This section explores why single photons are essential to the security and functionality of quantum cryptographic systems, with a focus on the widely known BB84 protocol and the vulnerabilities that arise when true single-photon sources are not used.

Quantum Cryptography: A Brief Overview

Quantum cryptography, particularly Quantum Key Distribution (QKD), enables two parties (commonly referred to as Alice and Bob) to establish a shared, secret cryptographic key over an insecure channel. The security of QKD does

not rely on computational hardness assumptions (like factoring large integers, which underlie RSA), but instead on the laws of quantum physics. Specifically, it exploits two key principles:

1. **The No-Cloning Theorem** It is impossible to create an exact copy of an unknown quantum state.
2. **Measurement Disturbs the System**– Any attempt to observe a quantum state alters it, revealing the presence of an eavesdropper (Eve).

Single photons are critical to enforcing these principles during communication

Role of Single Photons in QKD Protocols

The most established QKD protocol is BB84, introduced by Charles Bennett and Gilles Brassard in 1984. In this protocol:

- Alice encodes classical bits (0 or 1) in the polarization states of single photons, using one of two conjugate bases (e.g., rectilinear: horizontal/vertical or diagonal: $\pm 45°$).
- Bob randomly selects a measurement basis for each incoming photon and records the result.
- After transmission, Alice and Bob share their chosen bases over a classical channel and discard bits where the bases did not match.

The critical requirement here is that each bit of information is encoded in a single photon, ensuring that any eavesdropping attempt introduces detectable anomalies

Photon Number Splitting (PNS) Attack

In practical implementations, many QKD systems do not use perfect single-photon sources. Instead, they often rely on attenuated laser pulses, which emit a low average number of photons per pulse. However, due to the Poissonian statistics of photon emission in such lasers, there is still a non-zero probability of emitting two or more photons in a single pulse.
This imperfection creates a loophole known as the Photon Number Splitting (PNS) attack. In this strategy:

- Eve intercepts multi-photon pulses and splits off one photon, storing it in a quantum memory.
- She then allows the remaining photons to proceed to Bob, undisturbed.
- After Alice and Bob disclose their measurement bases, Eve can measure her stored photon in the correct basis and recover the bit without detection.

The presence of such multi-photon events therefore undermines the very foundation of QKD security.

True Single-Photon Sources: A Solution

The use of true single-photon sources addresses this vulnerability directly. A source that emits exactly one photon per pulse, and no more, ensures that:

- No additional photons are available for Eve to intercept undetected.
- Any attempt to measure or clone the photon disrupts its quantum state, alerting Alice and Bob to the intrusion.
- The integrity of the key generated between Alice and Bob remains uncompromised.

As a result, the security of QKD becomes unconditional, resting solely on the principles of quantum theory rather than device limitations or mathematical assumptions.

Practical Benefits of Single-Photon Sources

Beyond improved security, single-photon sources also offer the following advantages:

- **Higher Key Rates**: Reduced need for privacy amplification due to lower error rates.
- **Longer Communication Distances**: Enhanced fidelity of transmission in lossy channels such as optical fibers.
- **Device-Independent QKD**: Some protocols assume minimal trust in the devices used; true single-photon sources are vital for such schemes.
- **Quantum Network Integration:** For emerging quantum internet applications, single-photon communication between nodes is essential

1.7.3 Types of Single-Photon Sources

Single-photon sources are crucial components in quantum optics, particularly in quantum communication, quantum cryptography, and quantum computing. The ideal single-photon source should emit one and only one photon on demand, with high purity (low probability of multiple photons), high brightness (emission efficiency), and indistinguishability (photons are identical in all degrees of freedom like frequency, polarization, and timing). Achieving all three properties simultaneously is challenging, and various physical systems have been developed to address this task, each with its own advantages and limitations.
This section outlines the main types of single-photon sources used in modern quantum technologies, categorized based on their physical principles and methods of photon generation.

- **Spontaneous Parametric Down-Conversion (SPDC)** Spontaneous Parametric Down-Conversion is a nonlinear optical process in which a high-energy photon (usually from a laser) interacts with a nonlinear crystal (like beta-barium borate, BBO), and splits into two lower-energy photons known as the signal and idler photons. These photons are produced in an entangled state and conserve both energy and momentum.

  #### Heralded Photon Generation:

  SPDC is not a true deterministic single-photon source because it relies on spontaneous events, and sometimes no photons or multiple photon pairs are generated. However, it can be used in a heralded configuration: by detecting one photon of the pair (e.g., the idler), we ”herald” the presence of its twin (the signal), ensuring a single-photon event in that channel.
  Advantages:

  - Relatively simple and inexpensive to set up

- Widely used in quantum optics laboratories
- Can generate entangled photons for quantum communication

  Limitations:
- Probabilistic process, not truly deterministic
- Multi-photon events can still occur, which compromises security in some applications
- Requires phase matching and precise alignment

- **Quantum Dots (QDs)**

  Quantum dots are nanoscale semiconductor particles that confine electrons and holes in all three spatial dimensions, creating discrete energy levels similar to those in atoms. When an electron-hole pair (exciton) recombines in a quantum dot, it emits a single photon. By optically or electrically exciting the quantum dot, one can induce this recombination on demand.

  Materials: Common materials used for QDs include InAs/GaAs (indium arsenide/gallium arsenide) and CdSe (cadmium selenide). These structures are often embedded in microcavities to improve collection efficiency and emission directionality.

- **Nitrogen-Vacancy (NV) Centers in Diamond**

  An NV center is a point defect in a diamond crystal lattice, consisting of a nitrogen atom adjacent to a vacancy (missing carbon atom). When optically excited (e.g., with a green laser), NV centers can emit single photons with high stability.

  Room Temperature Operation:

  One of the main attractions of NV centers is their ability to emit single photons at room temperature, which makes them more practical for certain real-world applications compared to sources requiring cryogenics.

  Isolated Atomic or Ionic Systems

  In this method, individual atoms or ions are trapped using magnetic or optical fields in vacuum environments (e.g., ion traps or optical tweezers). Upon laser excitation, the atom emits a single photon as it relaxes from an excited state. The atomic system can be precisely controlled, and transitions are well-defined.

1.8 Attenuated Laser Sources

Quantum key distribution (QKD) relies on transmitting quantum states, typically encoded in photons. While ideal single-photon sources are desirable, they are not always available or practical. As a result, attenuated laser sources which emit weak coherent pulses are commonly used. These sources are cost-effective and compatible with existing optical infrastructure, making them popular in real-world QKD deployments. However, they also introduce unique security challenges, especially when multi-photon pulses are unintentionally emitted.[51][52]

1.8.1 Principle of Weak Coherent Pulses

In practical quantum key distribution (QKD) systems, the generation of perfect single-photon states remains a significant technical challenge. As a result, weak coherent pulses (WCPs), derived from standard laser sources, are often used as an effective approximation to single-photon sources. These WCPs are created by heavily attenuating laser pulses so that the mean photon number per pulse, denoted by the symbol μ, is much less than one typically in the range of $\mu \approx 0.1$.[51][52]

Lasers naturally emit coherent states, which are quantum states that exhibit classical-like behavior while maintaining a probabilistic structure in terms of photon number. These states can be expressed as a superposition of Fock states (number states) and follow Poissonian photon number statistics, meaning the number of photons in each pulse is governed by the probability distribution:

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}$$

Where:
- $P(n)$ is the probability of finding n photons in a given pulse, - μ is the average photon number per pulse, - e is Euler's number (2.718), - $n!$ is the factorial of n.

For example, if $\mu = 0.1$, then:
- 90.5% of pulses contain zero photons (vacuum), - 9% contain one photon, - 0.5% contain two or more photons. This distribution means that while most pulses will be empty or contain a single photon, a non-negligible fraction may contain multiple photons, which poses a security risk.
Use in QKD Protocols WCPs are commonly employed in protocols like BB84, where quantum bits (qubits) are encoded in the polarization or phase of individual photons. Although WCPs are not ideal single-photon sources, they offer several advantages:

- Ease of implementation with off-the-shelf laser diodes,
- Compatibility with existing fiber-optic infrastructure,
- High repetition rates, supporting fast key generation.

To mitigate the risks posed by multi-photon emissions, modern QKD protocols often incorporate decoy-state techniques. In this approach, the sender (Alice) varies the intensity (i.e., the value of μ) of each pulse between "signal" and "decoy" levels. This randomization prevents an eavesdropper from reliably exploiting multi-photon pulses without detection, thereby enhancing security.[51][52]

Benefits and Limitations

Advantages:

- Simple and cost-effective hardware,
- Scalable and robust for real-world QKD networks.

Limitations:

- Multi-photon emission vulnerability (exploitable via photon number splitting attacks),
- Not truly deterministic—emission of a photon is probabilistic.

Despite these limitations, weak coherent pulses remain the backbone of commercial QKD systems. Their reliability, combined with effective security enhancements like decoy states and advanced error correction, makes them a practical solution for secure quantum communication over fiber-optic links and free-space channels.

1.8.2 Approximation to Single-Photon States

Weak coherent pulses (WCPs) are often used in quantum key distribution (QKD) systems as practical substitutes for ideal single-photon sources. Although they do not emit exactly one photon per pulse, WCPs can closely approximate single-photon states when carefully engineered and used with appropriate protocols.

Coherent States vs. Single-Photon States

A true single-photon state is described by the Fock state $|1\rangle$, which contains exactly one quantum of light energy (one photon). These states are essential in quantum information protocols because of their non-classical behavior and indivisibility.

In contrast, a coherent state $|\alpha\rangle$ (produced by a laser) is a quantum superposition of photon number states $|n\rangle$ with Poissonian distribution, as shown in Section 3.1. When the mean photon number

$$\mu = |\alpha|^2$$

is very small, the probability of having more than one photon in a pulse becomes negligible. For instance, when:

- $\mu = 0.1$, then $P(2) = 0.005$
- $P(3)$ and higher terms are even smaller.

Thus, for sufficiently low μ, the dominant non-zero term is the one-photon state, making the WCP effectively behave like a probabilistic single-photon source.

Importantly, security analyses of QKD protocols like BB84 are modified to account for the Poissonian distribution of WCPs. This includes treating the multi-photon components separately and bounding their impact on security.[51][52]

1.8.3 Photon Number Splitting (PNS) Attack Vulnerability — Detailed Explanation

What Is a PNS Attack?

In Quantum Key Distribution (QKD), particularly in systems using weak coherent pulses (WCPs), one major vulnerability arises from the fact that some pulses may contain more than one photon. These multi-photon pulses—though rare—open the door to a specific type of eavesdropping: the Photon Number Splitting (PNS) attack.[51][52]

In a PNS attack:

1. Eve (the eavesdropper) intercepts the quantum channel between Alice (sender) and Bob (receiver).
2. She monitors incoming pulses and identifies multi-photon pulses (those containing 2 or more photons).
3. Instead of destroying the pulse, Eve splits off one photon and allows the rest to proceed to Bob undisturbed.

4. Eve stores her photon in quantum memory and waits until Alice and Bob publicly announce their measurement bases.
5. She then measures her photon in the correct basis—thus gaining perfect knowledge of the bit without introducing detectable errors.

This type of attack is particularly dangerous because it can be performed passively, without alerting Alice and Bob, unless protective measures are in place.[51][52]

Real-World Demonstration

According to Ashkenazy and Idan (2023), a realistic implementation of the PNS attack can be realized using cavity-enhanced atomic systems and Raman interactions. These systems can isolate and extract a photon from a pulse in a way that preserves quantum coherence. Though technically demanding, the researchers suggest such attacks could be feasible with advancements in near-term quantum technology.
They also found that these attacks might cause a slight increase in the quantum bit error rate (QBER), which could be used as an indirect indicator of an ongoing attack especially in tightly monitored systems.
Defense: Decoy State Protocol
To counter PNS attacks, Decoy State QKD protocols are implemented. This strategy was developed specifically to nullify the benefits an eavesdropper might gain from multi-photon pulses.[51][52]

1.9 Conclusion

In this chapter, we have laid the groundwork for understanding the evolution of cryptography from classical to quantum paradigms. We began by reviewing traditional encryption techniques, such as symmetric (AES, DES) and asymmetric (RSA, ECC) algorithms, highlighting their strengths and limitations—particularly in the face of emerging quantum threats. The shortcomings in key distribution and vulnerability to quantum algorithms like Shor's underscore the need for more secure approaches.

We then explored the foundational principles of quantum computing and quantum mechanics that distinguish quantum systems from classical ones. Concepts like superposition, entanglement, no-cloning, and measurement irreversibility not only define quantum information but also enable the development of inherently secure communication protocols.

Finally, we examined the physical implementation of quantum bits (qubits), particularly through photon polarization, which forms the basis for quantum key distribution. Understanding how photons can be manipulated, measured, and used to encode quantum information sets the stage for deeper discussions in the following chapters.

This conceptual foundation is essential for analyzing entanglement-based protocols and understanding the technical and physical requirements for secure quantum communication in scenarios with and without an eavesdropper.

Chapter 2

conception

2.1 Principle of Quantum Cryptography

2.1.1 Overview of Quantum Key Distribution (QKD)

We have seen above that present-day cryptographic systems using public-key encoding are not totally secure. For example, the RSA encryption scheme will become obsolete as soon as someone finds an efficient way to factorize large numbers.

This inevitably leads us to look for alternative ways to encrypt the data with a higher degree of security. It is obvious that the whole encryption system would be much safer if the interested parties were to encrypt their message with a secret private key, known only to them, rather than with a public one know to everyone. The data encrypted with the private key are secure provided that no-one else has the key.

The purpose of quantum cryptography is to provide a reliable method for transmitting a secret key and knowing that no-one has intercepted it along the way. The method is founded on the fundamental laws of quantum physics, and the process of sharing a secret key in a secure way is called quantum key distribution.

There are two basic schemes that have been devised for carrying out quantum cryptography. The first relies on the basic principles of quantum measurements on single particles, while the second relies on the properties of entangled states. In this chapter we shall only discuss the first type of quantum cryptography, since it is the easiest to understand and is the one which is most commonly implemented in the field.

In discussing quantum cryptography, we invariably encounter three characters: Alice (A), Bob (B), and Eve (E). Alice and Bob are the two people who wish to exchange information. Eve is the eavesdropper who is trying to intercept the message and steal it without disclosing her presence. The task of quantum cryptography is to provide a scheme that enables Eve's activity to be detected.

Quantum cryptography does not protect against eavesdropping attacks, but it does provide a failsafe way for knowing when the message has been intercepted. This allows Alice and Bob to set up a system for transferring private keys with the confidence of knowing that the key really is private. If they detect the presence of an eavesdropper, they can simply discard the bits transferred while Eve was listening in, and start again. Once they have successfully shared the private key, they can use it for encrypting a secret message that can be transmitted across public channels at high data rates. Provided they encrypt with a new key for every message, then they are effectively using a one-time-pad cipher and their message is totally secure against eavesdropping attacks by unwanted third parties.

Let us suppose that Alice wants to send a message to Bob by using a conventional telecommunications system as shown in Fig. 2.12(a). The data signals will be sent as pulses of light along the optical fibre. Strong pulses represent binary '1', while weak pulses, or no pulse at all, represents binary '0'. In this arrangement, there is nothing that Alice and Bob can do to prevent Eve from stealing a copy of the data while it is being transferred down the fibre. All Eve has to do is to intercept the signal, and keep a copy of it without disclosing her presence to Bob. Figure 2.12(b) shows one way in which this might be done. Eve inserts a 50 : 50 beam splitter (BS) followed by an optical amplifier with a gain of 2 into the fibre. The signal received by Bob is unaffected by Eve's presence, but Eve has obtained a copy which she can then process using her own detection system. In classical data transmission systems such as the ones shown in Fig. 2.12, there is in principle no way that Alice and Bob can know of Eve's presence. This is because there is no physical law that prevents us from measuring the data signal and making an exact duplicate without affecting it in the process. On the other hand, we know that quantum mechanics tells us that in general it is not possible to make measurements on single particles without affecting their state in some way or other. For example, we cannot detect a photon, extract all the quantum information from it, and then transmit another photon which is an exact quantum copy of the first one. This is called the quantum no-cloning theorem. Now an eavesdropper will have to make some form of measurement on the data stream in order to extract information from it. This means that if we encode the data in a quantum-mechanical way, the eavesdropper will in principle have to reveal her presence by the invasive way in which she makes the measurement. This is the basic principle behind quantum cryptography. [38]

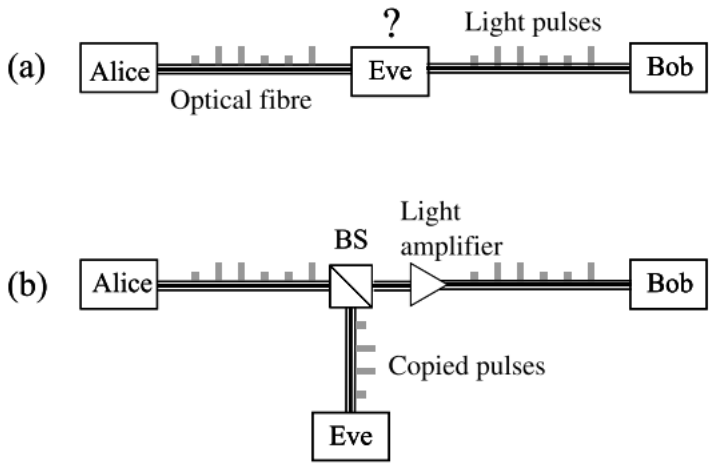

Figure :2.1 (a) In a classical telecommunication system, Alice sends a message to Bob by transmitting high power pulses of light down an optical fibre.

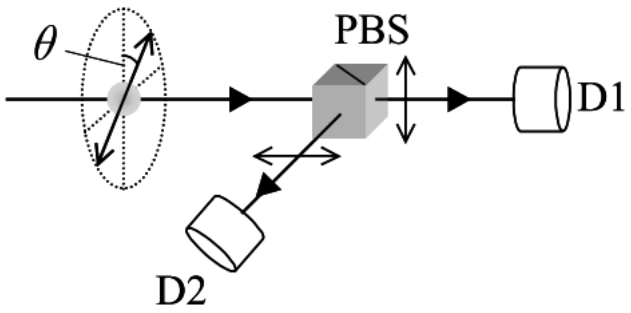

Figure :2.2 Apparatus to measure the polarization state of a single photon using a polarizing beam splitter (PBS) and two single-photon detectors D1 and D2.

We can illustrate this point by considering the experimental arrangement shown in Fig. 2.13. This arrangement is designed to measure the polarization state of a single photon. As we shall see below, this is in fact one of the methods that are used for the data encoding in practical quantum cryptography systems. The apparatus consists of a polarizing beam splitter (PBS) and two single-photon detectors D1 and D2. The PBS has the property that it transmits vertically polarized light but diverts horizontally polarized light through 90°. This arrangement is conceptually similar to the Stern–Gerlach experiment in which a magnet is used to deflect a particle with a spin quantum number of 1/2. It is found experimentally that the particle is either deflected up or down depending on the initial state of the incoming particle. The spin up and spin down states of the spin–1/2 particle in the Stern–Gerlach experiment are analogous to the vertical and horizontal polarization states of the photon considered here. Let us suppose that the incoming photon is linearly polarized with its polarization vector at an unknown angle of θ with respect to the vertical axis. If $\theta = 0°$, we have vertically polarized light and the photon will be registered by detector D1. Similarly, if $\theta = 90°$, we have horizontally polarized light and the photon will be registered by detector D2. In all other cases we have to resolve the polarization vector into its horizontal and vertical components. Let us represent the quantum state for vertically and horizontally polarized photons by $|\uparrow\rangle$ and $|\leftrightarrow\rangle$, respectively. We can then write the quantum state $|\theta\rangle$ of a photon with arbitrary polarization angle as a superposition of the two orthogonal polarization states according to:

$$|\theta\rangle = \cos\theta|\uparrow\rangle + \sin\theta|\leftrightarrow\rangle.$$

The probability that the photon is transmitted towards D1 is then given by:

$$\mathcal{P}_v = |\langle\uparrow|\theta\rangle|^2 = \cos^2\theta.$$

Similarly, the probability that the photon is diverted towards D2 is equal to $|\langle\leftrightarrow|\theta\rangle|^2 = \sin^2\theta$. Now let us suppose that we are trying to determine θ and then transmit another photon with the same polarization angle, as shown in Fig. 2.14. This is exactly what the eavesdropper has to do in the quantum cryptography systems that we shall be discussing below. The measurement could be made by using the arrangement shown in Fig 2.13 . In each measurement the only information Eve receives is whether detector D1 or D2 registers.

Detector D1 will register with a probability equal to $\cos^2\theta$ and D2 with probability $\sin^2\theta$. If

detector D1 registers then the most sensible thing Eve can do is to send on a vertically polarized photon. Similarly, if D2 registers she will transmit a horizontally polarized photon. However, the state of the second photon is only the same as the first one for the special cases where $\theta = 0°$ or $90°$. For all other values of θ, the act of trying to extract the information about the polarization angle leads Eve to transmit the second photon with a different polarization angle θ' to the first one. This implies that, if measurements are made on the outgoing photon generated by Eve, they can give different results from the ones obtained on the original photon.

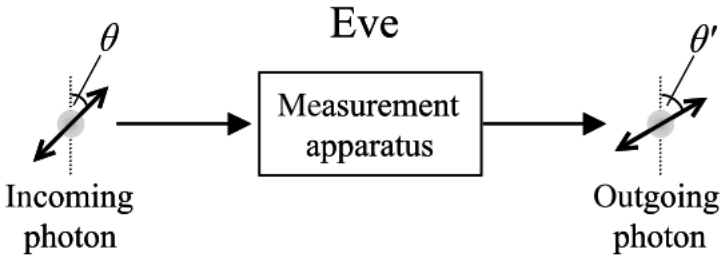

Figure :2.3 Schematic arrangement for eavesdropping on data encoded as the polarization state of a single photon. In order to extract useful information,

The conclusion of this argument is that it is not possible to extract information from a quantum system without saltering its state in the process. This is a consequence of the invasive nature of quantum measurements. The eavesdroppers must reveal their presence though the disturbance they make through their measurements, which affects the results of subsequent measurements on the photons that are received at the final destination. It could be argued that the eavesdropping scheme we have considered here is very simple and that Eve might devise a more sophisticated way to tap in to the data stream. However, no matter how hard she tries, she will always be subject to the general principles and must give away something in making the measurement. We shall see how this works in practice in the next section. process. This is a consequence of the invasive nature of quantum measurements. The eavesdroppers must reveal their presence though the disturbance they make through their measurements, which affects the results of subsequent measurements on the photons that are received at the final destination. It could be argued that the eavesdropping scheme we have considered here is very simple and that Eve might devise a more sophisticated way to tap in to the data stream. However, no matter how hard she tries, she will always be subject to the general principles and must give away something in making the measurement.

2.1.2 BB84 Protocol Encoding and Basis Choice

In the previous section we explained the general point that eavesdroppers must reveal their presence through the invasive nature of the measurements they make. We shall now see how this principle is used in practical implementations of quantum cryptography. The idea is to distribute the private key in a secure way so that Alice and Bob can subsequently use it to encrypt secret messages transmitted over public channels. There have been several schemes proposed in the literature and implemented in the laboratory, the two most important of which are:

- the Bennett–Brassard 84 (BB84) protocol
- the Bennett 92 (B92) protocol.

In what follows we restrict our attention to the BB84 protocol, which will be sufficient to explain the basic principles.[38]

Basis	Binary 1	Binary 0
$\oplus$	$\lvert\updownarrow\rangle$ $\theta = 0°$	$\lvert\leftrightarrow\rangle$ $\theta = 90°$
$\otimes$	$\lvert\nearrow\rangle$ $\theta = 45°$	$\lvert\nwarrow\rangle$ $\theta = 135°$

Figure :2.4 Data representation values in the BB84 protocol for the two choices of polarization basis

In the simplest version of the BB84 protocol, the data are encoded as the polarization states of single photons, with binary '1' and '0' represented by orthogonal polarization states. Thus we could represent 1 by the $\theta = 0$ vertical polarization state and 0 by the $\theta = 90°$ horizontal polarization state, where the polarization angle θ is defined in Fig. 2.13. However, we are not restricted to choosing the axes of the polarization states to be horizontal or vertical. Any orthogonal pair of angles will do. In the BB84 protocol two sets of polarization states called the $\oplus$ and $\otimes$ bases are used:

The $\oplus$ basis: Binary 1 and 0 corresponds to photons with polarization angles of 0° and 90°, respectively.

The $\otimes$ basis: Binary 1 and 0 corresponds to photons with polarization angles of 45° and 135°, respectively.

The two polarization states for the $\oplus$ basis can be represented in Dirac notation by $\lvert\uparrow\rangle, \lvert\leftrightarrow\rangle$, while the two states for the $\otimes$ basis are represented by $\lvert\nearrow\rangle$, and $\lvert\searrow\rangle$ respectively. These assignments are summarized in Fig 2.15

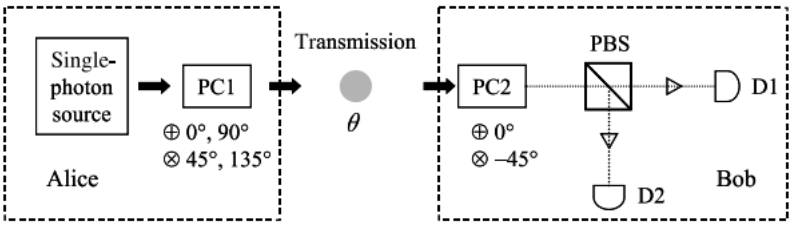

Figure :2.5 Data encoding scheme according to the BB84 protocol.

An experimental scheme for quantum cryptography according to the BB84 protocol is shown in Fig. 2.16. Alice's apparatus consists of a source of vertically polarized photons and a

Pockets cell PC1. Alice synchronizes her Pockets cell with the single-photon source and applies the correct voltages to produce polarization rotations of 0°, 45°, 90°, or 135°. In this way she can send a string of binary data which is encoded in either of the two polarization bases at her choice.

The photons emerging from Alice's apparatus are received by Bob who has a polarization measurement arrangement similar to the one shown in Fig. 2.13. Bob's apparatus includes a second Pockets cell PC2 in front of the PBS. Bob applies the correct voltage to this Pockets cell to rotate the polarization vector of the incoming photon by either 0° or −45° at his choice. These two choices are equivalent to detecting in the 1 and 2 bases, respectively. Bob does not know the basis that Alice has chosen to encode the individual photons. He therefore has to choose the detection basis at random. If he guesses the right basis, he will register the correct result. This occurs when Alice chooses the 1 basis and Bob chooses the 0° detection angle, and also when Alice chooses the 2 basis and Bob chooses the −45° rotation angle. If Alice's choice of basis is random, this correct matching of bases will occur 50% of the time. For the remaining 50% of the time Bob will be detecting in the wrong basis and will get random results. Thus, for example, if the incoming photon is polarized at +45° and Bob is detecting in the 4 basis (rotation angle = 0°), he will register results on either of his detectors with an equal probability of 50%. In the BB84 protocol the following steps are taken.

1. Alice encodes her sequence of data bits according to the scheme in Fig 2.15, switching randomly between the $\oplus$ and $\otimes$ bases without telling anyone what she is doing. She then transmits the photons to Bob with regular time intervals between them.
2. Bob receives the photons and records the results using a random choice of $\oplus$ and $\otimes$ detection bases as determined by the rotation angle of his Pockels cell.
3. Bob communicates with Alice over a public channel (e.g. a telephone line) and tells her his choice of detection bases, without revealing his results.
4. Alice checks Bob's choices against her own and identifies the subset of bits where both she and Bob have chosen the same basis. She tells Bob over the public channel which of the time intervals have the same choice of basis, and both Alice and Bob discard the other bits. This leaves them both with a set of sifted data bits.
5. Bob transmits to Alice over a public channel a subset of his sifted bits. Alice checks these against her own and performs an error analysis on them.
6. If the error rate is less than 25%, Alice deduces that no eavesdropping has occurred and that the quantum communication has been secure. Alice and Bob are then able to retain the remaining bits as their private key.

Table 2.1 shows an example of how these six steps of the protocol are implemented. The first line shows the original set of the data that Alice wishes to send to Bob. The second line shows the random choice of polarization basis that she makes, which gives rise to the polarization angle encoding of the photons shown in the third line using the criteria given in Table 2.15. The fourth line gives Bob's random choice of detection basis. This will coincide with Alice's for half of the bits on average. In these cases Bob will register the correct result, provided no eavesdropper is present (see below). In the other half of the cases, Bob will only get the right result with a probability of 50%. This does not matter, however, because these data are never used for the key. The next step involves the comparison of the two bases. Bob publicly announces his choice of bases without revealing his

results. Alice checks this against her choices and identifies the cases where the two choices coincide. These are identified with the 'y' label in the sixth row of Table 2.1. Alice tells Bob which bits these are, and they discard the other bits. This now leaves them both with the sifted bits shown in the seventh row of the table. Bob now sends a subset of his sifted bits to Alice, again over a public channel. In the example shown, he sends every other bit. Alice can check these against her own list, and carry out an error analysis. [38] This is the stage at which the

Table :2.1 Representative sequence of data choices according to the BB84 protocol.

A's data	1	0	0	1	1	1	0	0	1	0	0	1
A's basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$
θ (°)	0	135	90	45	45	0	90	135	0	135	135	0
B's basis	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$
B's result	1	0	0	0	1	1	0	1	1	0	1	1
Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
Sfited bits		0	0		1	1			1	0		
Data check ?	y	n	y	n				y	n			
Private key		0		1					0			

eavesdropper reveals her presence. It is easiest to understand what happens if we assume that Eve has the same apparatus as Alice and Bob. She can then detect the photons sent by Alice using a copy of Bob's apparatus, and transmit new photons to Bob using a copy of Alice's apparatus, as shown schematically in Fig. 2.17. Since she cannot know what choice of basis Alice is making, she must choose her detection basis randomly. Half the time she will guess correctly and accurately determine the polarization state of the photon. She can then send an identically polarized photon on to Bob without anyone knowing about it. For the remaining half of the bits, she will guess incorrectly, and register a result on either of her detectors with an equal probability of 50%. She will then send a photon to Bob which is polarized with her choice of detection basis, rather than Alice's. This means that Eve will alter the polarization basis angle by 45° for 50% of the bits. In the cases where Bob has chosen the same basis as Alice and Eve has guessed incorrectly, Bob will register random results on his detectors with a probability of 50%. He will thus register errors even when he has guessed Alice's basis correctly. The error probability P_{error} is given by:

$$P_{\text{error}} = P_{\text{Eve has wrong basis}} \times P_{\text{Bob gets wrong result}},$$

$$= 50\% \times 50\%,$$

$$= 25\%.$$

This high error rate of 25% will be easily recognizable when Alice carries out her error analysis in the final step of the process. She will thus be able to detect the presence of the eavesdropper, and therefore know whether the private key distribution has been secure.

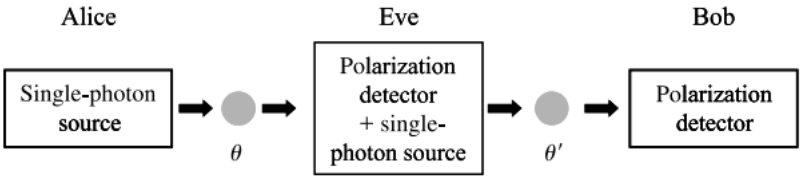

Figure :2.6 An eavesdropper between Alice and Bob tries to measure the polarization angle of the photon sent by Alice and send an identical photon on to Bob]38[

2.1.3 Quantum vs Classical Security Approaches

Cryptography has always been at the heart of secure communication. Traditional or classical cryptographic systems rely on mathematical algorithms and assumptions about computational difficulty. In contrast, quantum cryptography leverages the fundamental laws of quantum mechanics to achieve security. This section explores the philosophical and technical differences between these two paradigms, highlighting how quantum mechanics allows for provable security independent of computational power.[53][54]

Classical Security: Computational Assumptions

Classical cryptographic systems such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are built on the assumption that certain mathematical problems are intractable. For example:

- RSA relies on the difficulty of factoring large integers.
- Diffie-Hellman is based on the hardness of the discrete logarithm problem.
- ECC uses the difficulty of solving elliptic curve discrete logarithms.[53][54]

These algorithms are widely used today in securing digital communications, online banking, digital signatures, and more. However, their security is not absolute—it is computational.
If an adversary acquires enough computational power or a breakthrough algorithm is developed, these systems can be compromised.
Risks to Classical Cryptography:

- Quantum Computing Threats: Quantum algorithms like Shor algorithm can efficiently factor large numbers and compute discrete logarithms, making RSA and similar systems vulnerable.
- Advancing Hardware: Even without quantum computers, increasing classical computational power can pose risks over time.
- Long-Term Confidentiality Risk: Encrypted data intercepted today could be decrypted years later.

Quantum Security: Physics-Based Guarantees

Quantum cryptography, and particularly Quantum Key Distribution (QKD), operates under entirely different principles. Rather than relying on computational hardness, it uses laws of quantum mechanics to ensure security:
Key Quantum Principles in Security:

- Heisenberg Uncertainty Principle: Measurement of a quantum state inevitably disturbs it.
- No-Cloning Theorem: It is impossible to make an exact copy of an unknown quantum state.
- Superposition Entanglement: Enable secure correlations and state verification.

In quantum cryptography, the security is information-theoretic, meaning it holds regardless of the adversary's computational resources.[53][54]

Advantages of Quantum Cryptography:

- Provable Security: Based on physical laws rather than computational assumptions.
- Eavesdropping Detection: Any attempt to intercept a quantum signal introduces detectable errors.
- Forward Secrecy: Even if an adversary gains future computational power, previously exchanged keys remain secure.

2.1.4 Comparison Table: Quantum vs Classical Security]53][54[

Feature	Classical Cryptography	Quantum Cryptography
Security Basis	Computational complexity	Laws of quantum mechanics
Main Examples	RSA, ECC, AES, Dffiie-Hellman	BB84, E91, B92 QKD protocols
Vulnerable to Quantum	Yes (e.g., by Shor's algorithm)	No (resilient by design)
Eavesdropping Detection	Not possible	Intrinsic to protocol
Key Distribution	Public-key algorithms or physical keys	Quantum Key Distribution (QKD)
Assurance	Assumed hard problems	Provably secure
Post-Quantum Safe	Only with new (PQ) algorithms	Naturally secure

2.1.5 Challenges of Quantum Cryptography

- Technological Maturity: Requires advanced hardware like single-photon sources and detectors.
- Distance Limitations: Photon loss in optical fibers limits QKD range.
- Cost and Integration: Current systems are expensive and not easily integrated.
- Side-Channel Vulnerabilities: Practical implementations may introduce loopholes.

2.1.6 Toward a Post-Quantum Future

As quantum computers approach practicality, the world of cryptography is evolving:

- Post-Quantum Cryptography (PQC): Classical algorithms resistant to quantum attacks.
- Hybrid Systems: Combining classical and quantum methods for added security.
- Global Research Efforts: Organizations like NIST are standardizing PQ algorithms.

Quantum cryptography offers a revolutionary shift in secure communication by providing unconditional security based on the unchangeable laws of quantum physics. While classical cryptography has served us well, its future is uncertain in the face of advancing technology. A combination of quantum and post-quantum classical systems may define the next era of secure communication. [53][54]

2.2 The Quantum Channel

The quantum channel refers to the physical medium or system that carries quantum information most often encoded in qubits—between two or more parties. Unlike classical communication channels, quantum channels must preserve fragile quantum states like superposition and entanglement, which are essential to quantum communication. This chapter explores the different aspects of quantum channels, including how they transmit qubits, the challenges they face, and how those challenges are mitigated.

2.2.1 Role of Quantum Channel in Transmitting Qubits

A quantum channel is the physical medium by which quantum information, usually encoded in qubits, is transmitted between remote senders and recipients. In contrast with classical communication, where information is transmitted by bits in electrical or optical signals, quantum communication uses quantum states of particles-most commonly photons-to represent and carry information. These quantum states are fragile, and the channel required to transmit them has to preserve their integrity and coherence throughout their transit time.

Transmission Mediums

In practical realizations, the quantum channel may take one of the following forms:
Optical fibers are cylindrical dielectric waveguides made typically of ultra-pure silica glass, designed to transmit light over long distances with minimal loss. In quantum communication systems—especially those based on Quantum Key Distribution (QKD)—optical fibers serve as the primary medium for transmitting quantum states encoded in single photons.
Key Advantages:

1. **Low Transmission Loss** Modern optical fibers, especially at the telecom wavelength of 1550 nm, exhibit very low attenuation—about 0.2 dB/km for standard single-mode fibers like SMF-28. This allows for relatively efficient transmission of quantum states over tens of kilometers without significant degradation.
2. **Integration with Classical Infrastructure** Optical fibers are already widely deployed in telecommunications. Quantum signals can, in some cases, coexist with classical data using techniques such as wavelength division multiplexing (WDM), although care must be taken to avoid cross-talk and noise from classical signals.
3. **Stability in Controlled Environments** When deployed in underground or enclosed conduits, optical fibers are shielded from atmospheric effects, providing a more stable environment than free-space links. This is particularly beneficial for minimizing decoherence and environmental noise.

Free-space optical links

In free-space quantum cryptography, the photons sent by Alice travel through the air towards Bob's receiver apparatus. The basic arrangement is shown schematically in Fig. 2.18. The data are encoded as the polarization state of the photon, and Alice and Bob both have the same apparatus as shown in Fig. 2.16. Alice fires her photons into a telescope which expands, collimates, and directs the beam towards Bob's receiver. Bob himself has another telescope which allows him to collect the photons efficiently. These telescopes are needed to minimize the effects of beam expansion caused by diffraction when Alice and Bob are separated by long distances. Without the telescopes, the fraction of the photons that would fall upon the detector area would be unacceptably low.[38]

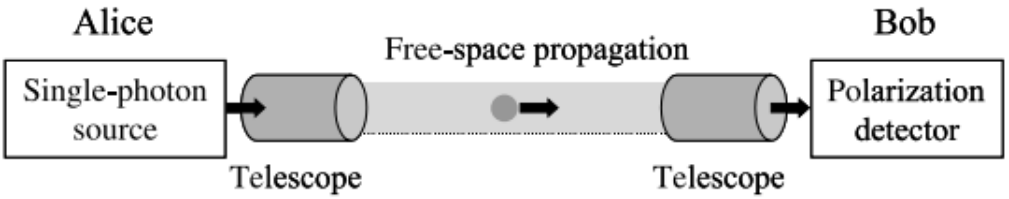

Figure :2.7 Schematic representation of free-space quantum cryptography[38[

The first practical demonstration of quantum cryptography used free-space propagation and was reported by Bennett, Brassard, and co-workers in 1992. They used strongly attenuated pulses from a lightemitting diode operating at 550 nm and transmitted the photons across an air gap of 0.32 m. Much progress has been made since this first proofof-principle experiment. Free-space quantum cryptography systems have now been demonstrated across distances of 10 km in both daylight and at night. In another experiment, the quantum key was distributed across 23 km between the summits of two Alpine mountains at night. The long-term aim of these experiments is to develop quantum cryptography systems for communicating with satellites in low earth orbits. Feasibility studies indicate that there are no fundamental obstacles that should prevent this from becoming a reality.

The long-range free-space systems implemented so far have been carried out at wavelengths in the range 600–900 nm. At these wavelengths, the atmospheric losses are small, and low-noise detectors with high quantum efficiencies are readily available. In these conditions there are two **main sources of error:**

- **Air turbulence**: this causes random deviations in the direction and timing of the light pulses. The effects of these random deviations are well-known from the twinkling of stars. The effects of air turbulence can be minimized by sending a bright (classical) pulse in front of the encoded photon. This allows Alice and Bob to compensate for the beam wandering and timing jitter.
- **Stray light**: background light from the sun, moon, or street lamps, causes unwanted detector counts. The stray light signal can be reduced by placing suitable filters in front of the detectors and triggering the detectors so that they are only switched on for the short time interval in which the encoded photon is expected to arrive.

It is important to realize that most of the deleterious effects due to atmospheric turbulence occur in the first few km from the ground. Hence the demonstration of cryptography over similar distances at ground level is a significant step towards the long-term goal of overcoming the problems associated with communicating with satellites.[38]

Photon-Based Qubit Encodings

Commonly single photons are used to encode quantum information in several degrees of freedom, which include:

- Polarization: Horizontal and vertical polarizations represent logical $|0\rangle$ and $|1\rangle$ states.
- Phase: Information is encoded in the phase difference between two optical paths.
- Time-bin: Photons are sent in discrete time slots; an early or late arrival corresponds to a particular state.
- Frequency: Photon's spectral features are used for encoding.

The above-mentioned encoding schemes provide flexibility and robustness for the transmission of quantum states, over different kinds of quantum channels. [55]

Entanglement Distribution

Quantum channels have also proved very useful for entanglement distribution, whereby pairs of entangled photons need to be distributed between distant parties. Entanglement serves as a prime resource for quantum communication protocols such as:

- Quantum key distribution (QKD) with entangled pairs, for instance, in the Ekert Protocol
- Quantum teleportation, an interface that transmits a quantum state of a particle without a physical transfer of the particle itself
- Quantum networking, where entangled states play a role in distributed quantum computing or sensing
- The quantum channel must maintain the entanglement and should not introduce decoherence or noise that may destroy the shared quantum correlations for the above protocols to function in their intended manner.Thus, in summarising, the quantum channel plays an important role in transmitting quantum information. By carrying qubit transport, maintaining coherence, and allowing entangled distribution, it thus forms the cornerstone of many practical and theoretical applications iPolarization: Horizontal and vertical polarizations represent logical |0 and |1 states.
- Phase: Information is encoded in the phase difference between two optical paths.
- Time-bin: Photons are sent in discrete time slots; an early or late arrival corresponds to a particular state.
- Frequency: Photon's spectral features are used for encoding.

n quantum communication, a field that is witnessing rapid growth.

2.2.2 Losses, Decoherence, and Noise in Optical Fibers

The successful transmission of qubits over long distances through optical fibers is central to practical quantum communication. However, this process is fundamentally constrained by physical phenomena such as photon loss, decoherence, and noise, which can degrade or destroy the quantum information encoded in photons.

Photon Losses

Optical fiber quantum communication is significantly impeded by photon losses, which have a direct consequence on the reliability and distance over which quantum information can be transmitted. Whenever single-photon transmissions take place, their propagation through an optical fiber is hindered by attenuation, which is defined as the gradual reduction in signal strength due to various physical effects.

The three mechanisms causing attenuation include:

- **Rayleigh scatting**: The interruption of microscopic variations in refractive index along the fiber results in scattering of the photon in all interstitial directions.
- **Material absorption**: These are losses due to impurities or inherent/built-in absorption in the glass material of the fiber.
- **Bending losses**: Occurs due to excess coil/tightness in fiber wiring, which leads to lose of photons from the fiber core or escape out of it.

Standard single-mode telecom fibers such as SMF-28 are optimized to obtain lower losses within a wavelength premise of 1550 nm, at which the attenuation reaches approximately 0.2 dB/km. Despite low losses, the cumulative effect over long distances is quite serious. For example, in a 100 km fiber, only about 1% of the originally transmitted photons remain, assuming no amplification or error correction is being used .[55]

An exponential loss limitation is primarily at the core of the distance restriction for quantum communication in optical fiber. Unlike classical communication systems that can use ordinary amplifiers, quantum systems cannot do this due to the No-Cloning Theorem, which denies copying unknown quantum states. Quantum repeaters or other forms of transmission must therefore be employed to overcome that limitation and provide the reach of quantum networks.[55]

Decoherence

Decoherence is a fundamental challenge in quantum communication, referring to the degradation of a quantum system's coherence due to interactions with its surrounding environment. In the context of fiber-optic quantum communication, decoherence leads to the loss of the well-defined quantum phase relationships that are essential for maintaining the integrity of qubits during transmission.

In optical fibers, decoherence can be induced by several physical phenomena:

- **Thermal fluctuations**: Changes in temperature alter the refractive index of the fiber material, affecting the propagation speed of photons and introducing phase noise.
- **Mechanical stress and vibrations**: External pressure, bending, or mechanical disturbances can deform the fiber, disturbing the qubit state.
- **Polarization Mode Dispersion (PMD)**: Arises from random imperfections in the fiber geometry, which cause different polarization modes to travel at slightly different speeds, leading to temporal broadening and interference.
- **Chromatic dispersion:** Variations in photon group velocities at different frequencies can lead to temporal spreading of the qubit wave packet, especially for broadband sources.

For polarization-encoded qubits, even slight changes in the fiber's birefringence—caused by environmental perturbations—can result in unpredictable rotation of the polarization state. This severely impacts the fidelity of quantum communication protocols like Quantum Key Distribution (QKD), which rely on preserving the exact polarization state of photons during transmission .

On the other hand, time-bin encoding, which encodes qubits in the relative arrival times of photon pulses, is significantly more resilient to polarization-related disturbances. Because it is less affected by birefringence or polarization drift, time-bin encoding is widely used in long-distance quantum communication systems over optical fibers .

Overall, mitigating decoherence requires advanced stabilization techniques and careful selection of encoding schemes, both of which are essential for the realization of scalable and secure quantum networks.

Noise

Quantum communication over optical fibers is also challenged by various sources of noise—unwanted signals or events that can interfere with the detection and interpretation of qubits. These noise sources can distort, mask,

or imitate actual quantum signals, contributing significantly to the degradation of quantum communication systems. Key sources of noise in quantum channels include:

- **Background light**: In free-space quantum communication, particularly under daylight or atmospheric conditions, ambient photons can enter the receiver, mimicking or overwhelming the true quantum signals.
- **Detector dark counts**: These are spurious counts generated by single-photon detectors in the absence of incoming photons, often due to thermal fluctuations or imperfections in the detection system.
- **Fiber imperfections**: Microscopic defects, splices, or impurities in the fiber can introduce random scattering and phase noise, reducing the fidelity of transmitted qubits.

These noise effects increase the **Quantum Bit Error Rate (QBER)**—a measure of the discrepancy between the sent and received qubits. A high QBER reduces the effectiveness of quantum key distribution (QKD) and may compromise the overall **security and reliability** of the communication link .

Mitigation Techniques

To ensure reliable transmission of quantum information over practical distances, several **engineering techniques and material innovations** are employed to mitigate noise, losses, and decoherence:

- **Low-loss optical fibers**: Advanced fiber types, such as **ultra-pure silica fibers** or **hollow-core photonic crystal fibers**, exhibit significantly reduced attenuation and scattering, preserving photon counts over long distances.
- **Active polarization stabilization**: Real-time feedback systems monitor and correct polarization drift caused by environmental changes, ensuring consistent transmission of polarization-encoded qubits.
- **Environmental isolation**: **Temperature-controlled enclosures** and **vibration-damping systems** help minimize decoherence by reducing environmental perturbations.
- **Spectral filtering and time-gating**: Narrowband optical filters and precisely timed detection windows are used to block unwanted photons and reduce detector dark counts, improving signal-to-noise ratios.

These mitigation strategies are crucial for maintaining the **coherence**, **fidelity**, and **detectability** of quantum states over long-distance fiber links. As quantum networks evolve, these techniques will become increasingly essential for enabling **scalable**, **high-performance quantum communication** systems .[55]

2.3 The Classical Channel

In a quantum communication system, particularly in Quantum Key Distribution (QKD) protocols like BB84, the classical channel plays a critical supporting role alongside the quantum channel. Although qubits are transmitted via the quantum channel, the establishment of a shared secret key between two parties—commonly referred to as Alice and Bob—also requires classical communication to reconcile, verify, and refine the quantum-derived information.

2.3.1 Role in Key Reconciliation and Error Correction

In quantum communication systems—especially in Quantum Key Distribution (QKD) protocols—the classical channel is a crucial companion to the quantum channel. While the quantum channel carries quantum states (typically photons encoding qubits), the classical channel handles the post-processing of the quantum measurements, including steps such as basis reconciliation, error correction, and privacy amplification.

The classical channel is defined as public but authenticated. This unique configuration presents specific requirements and characteristics:

Public but Authenticated

- **Public Accessibility**: The classical channel is openly accessible, meaning that any third party (such as a potential eavesdropper, Eve) can monitor or record the communication. This transparency is intentional and allowed by the security model of QKD.
- **Authentication Requirement**: Despite being public, the channel must be authenticated, meaning that messages exchanged between the legitimate parties (commonly Alice and Bob) must be verifiably genuine. Eve should not be able to:
  - Forge messages pretending to be Alice or Bob.
  - Modify the content of messages undetected.
  - Replay old messages to disrupt the communication.

Authentication protects against man-in-the-middle (MITM) attacks, where an attacker impersonates both parties and attempts to intercept and manipulate messages in real time. In QKD, such attacks can break the integrity of the protocol even if the quantum channel is perfectly secure.

Why Confidentiality Is Not Required ?

Unlike in classical cryptographic systems, confidentiality of the classical messages is not required in QKD. This is because:

- The quantum channel already ensures the secrecy of raw key material through quantum mechanical principles (e.g., the no-cloning theorem and measurement-induced disturbance).
- The classical channel is used only for supporting operations that don't reveal the final secret key directly.
- If Eve listens to the classical communication but cannot tamper with it, she cannot gain useful information to compromise the final secret key.

Authentication Method

To achieve authentication, QKD implementations use cryptographic authentication mechanisms, such as:

- **Message Authentication Codes (MACs)** based on universal hashing (e.g., Wegman-Carter authentication).
- **Digital signatures** in some implementations, although they require more computational resources.
- **Pre-shared secret keys** for authentication, often exchanged via a trusted initial setup or bootstrap method.

These authentication keys can be refreshed using a portion of the QKD-generated secret key in future sessions, ensuring long-term security and sustainability without reliance on classical key distribution methods.

Security Implications

If the classical channel is not properly authenticated, the entire security guarantee of QKD collapses. An attacker could:

- Inject or alter messages during basis reconciliation or error correction.
- Cause Alice and Bob to derive different keys without detection.
- Mount a denial-of-service or key mismatch attack.

Thus, authentication is as vital as quantum transmission itself in practical QKD systems.

The authenticated public classical channel is a cornerstone of secure quantum key distribution. While it does not carry sensitive quantum data or the secret key itself, it facilitates critical post-processing steps. Its authentication mechanisms ensure the reliability, integrity, and trustworthiness of communication between legitimate users, effectively closing the door to impersonation and active interference by adversaries. Without this secure classical layer, the foundational promises of QKD would not hold in real-world implementations.

2.3.2 functions of the Classical Channel in QKD

The classical communication channel plays an indispensable role in the successful execution of Quantum Key Distribution (QKD) protocols. After the initial transmission of quantum bits (qubits) over the quantum channel, several critical processing steps must be carried out through interactive classical communication. Although this channel is public, all communications over it must be authenticated to prevent tampering or impersonation.

The core functions of the classical channel in QKD can be categorized as follows:

1. **Basis Reconciliation** QKD protocols, such as BB84, involve encoding and measuring qubits in randomly chosen bases—for example, rectilinear (Z-basis) and diagonal (X-basis). Since neither Alice (the sender) nor Bob (the receiver) knows in advance which basis the other party will choose:
   - After the quantum transmission phase, Alice and Bob publicly exchange their **basis choices** over the classical channel.
   - They **compare their measurement bases** and identify which bits were measured in matching bases.
   - Bits corresponding to mismatched bases are **discarded**, and the remaining bits form the **sifted key**.

   This step is essential to extract meaningful and correlated information from the inherently probabilistic nature of quantum measurements.
2. **Error Correction** Even after basis reconciliation, some discrepancies may still exist between Alice's and Bob's sifted keys. These errors can arise due to:
   - Photon loss or scattering in the quantum channel
   - Detector inefficiencies
   - Environmental noise or decoherence

   To synchronize their keys, Alice and Bob engage in a classical error correction protocol. Common techniques include:

- **Cascade Protocol**: An interactive method involving multiple rounds of parity checks and binary searches to identify and correct errors.
- **Low-Density Parity-Check (LDPC) Codes**: A more efficient, forward-error- correcting approach that uses sparse parity-check matrices.

These protocols must be carefully designed to correct errors without leaking too much information to a potential eavesdropper.

3. **Privacy Amplification** Even after error correction, it is possible that an eavesdropper (Eve) has gained partial knowledge of the shared key due to imperfections in the system or unavoidable information leakage during reconciliation. To eliminate any residual knowledge that Eve may have:
   - Alice and Bob apply privacy amplification, which involves compressing the corrected key into a shorter, more secure final key.
   - This is typically done using universal hash functions, which reduce Eve's possible information to a negligible amount—even if she had some prior knowledge of the original key.

   This step is performed over the classical channel, using authenticated communication to ensure that no adversary interferes with the process.

Security Requirements

All of the above operations—basis reconciliation, error correction, and privacy amplification—require secure and authenticated use of the classical channel. Authentication ensures that:

- Messages are indeed from the claimed sender (Alice or Bob)
- The contents of the communication have not been tampered with
- Protocol steps cannot be disrupted or manipulated by an adversary

If the classical channel is not properly authenticated, attackers could mount man-in-the-middle (MITM) attacks, corrupt the reconciliation process, or inject incorrect error correction data—undermining the entire security guarantee of QKD.

2.3.3 Security Considerations

Although the classical channel in Quantum Key Distribution (QKD) does not carry quantum information, its security is integral to the overall protocol correctness and integrity. A compromised classical channel can lead to protocol failure, incorrect key agreement, or even the undetected influence of an adversary. As such, robust authentication mechanisms are essential to defend against classical communication threats such as:

- **Message modification**: Altering messages in transit to distort the protocol.
- **Spoofing**: Pretending to be one of the legitimate communicating parties.
- **Replay attacks**: Resending previously captured messages to confuse or mislead the system.

To prevent such vulnerabilities, QKD implementations adopt cryptographic authentication methods, which ensure that the messages exchanged over the classical channel are genuine and unaltered. Common techniques include:

- **Message Authentication Codes (MACs):** Hash-based or block cipher-based authentication tags attached to messages.
- **Universal Hash Functions:** Used for unconditionally secure authentication schemes with provable bounds on adversary success.
- **Digital Signatures:** Employed in some scenarios to verify identity and message integrity, especially in asymmetric authentication settings.

It is important to note that many authentication schemes require an initial pre-shared secret between the communicating parties. While this might appear to contradict the ideal of key distribution from scratch, it is typically considered a reasonable and minimal assumption in QKD systems, especially since this shared secret can be refreshed and strengthened in future rounds using keys generated by the QKD protocol itself.

The classical communication channel, while not responsible for transmitting quantum states, is a critical enabler of secure quantum key distribution. It supports key operations such as basis reconciliation, error correction, and privacy amplification, all of which are essential to transforming raw quantum measurement outcomes into a robust, shared secret key.

The security of the classical channel must be rigorously enforced through authentication techniques to preserve the trustworthiness of the communication and ensure that protocol steps cannot be hijacked or manipulated by an adversary. Without authenticated classical messaging, the security guarantees of QKD protocols—rooted in the laws of quantum physics—cannot be fully realized in practice.

Thus, the classical channel stands as a foundational element of practical quantum communication systems, linking quantum mechanics with classical information theory to achieve unconditionally secure key exchange.

2.4 Entanglement Protocols

Entanglement-based quantum key distribution (QKD) protocols are a cornerstone of secure quantum communication. They exploit the quantum phenomenon of entanglement to allow two distant users to share cryptographic keys with security guaranteed by the fundamental laws of physics. In this section, we explore the principles and mechanisms of entanglement-based QKD, including the E91 protocol, the use of Bell inequality tests for eavesdropping detection, the role of entanglement swapping and quantum repeaters in extending communication range, and two primary use cases: communication within a spy scenario and without a spy scenario. This analysis aligns with the broader objective of this study: to investigate how parameters such as distance, bit rate, and wavelength affect entangled photon transmission in optical fiber, both in ideal and compromised settings.[56]

2.4.1 B92 Protocol (1992)

Inventor: Charles Bennett

A simplified variant of BB84, using only two non-orthogonal quantum states. It relies on unambiguous state discrimination for security. While simpler to implement, it is more vulnerable to photon loss and requires more advanced detection techniques.[56]

2.4.2 Six-State Protocol (SSP)

Inventor: Dagmar Brub
An extension of BB84 using three mutually unbiased bases (MUBs), leading to six possible quantum states. This increases the protocol's sensitivity to eavesdropping and improves error detection, at the cost of increased complexity in measurement.[56]

2.4.3 SARG04 Protocol

Inventors: Scarani, Acin, Ribordy, and Gisin
A modification of BB84 designed to enhance robustness against photon-number splitting attacks. It uses the same quantum states as BB84 but applies different classical post-processing to generate the secret key, making it more suitable for implementation with weak coherent pulses.[56]

2.4.4 GV95 Protocol

Inventors: Goldenberg and Vaidman
A QKD protocol that uniquely uses orthogonal states for encoding, exploiting interference and timing for security instead of basis randomness. It does not require basis reconciliation and is based on quantum superposition and precise control over the transmission times.[56]

2.4.5 KMB09 Protocol

Inventors: Khan, Murphy, and Beige
An entanglement-based QKD protocol designed for quantum networks, utilizing single-photon interference. It emphasizes practical implementation and device independence, improving real-world security models.[56]

2.4.6 S9 Protocol

Inventors: Slutsky et al.
A protocol using nine polarization states, expanding upon the Six-State Protocol. The larger state space increases resistance to eavesdropping and improves noise tolerance, but it also requires more complex measurement systems.[56]

2.4.7 E91 Protocol (1991)

Inventor: Artur Ekert
An entanglement-based QKD protocol relying on violations of Bell's inequality to detect eavesdropping. Security is rooted in quantum non-locality, and the protocol enables device-independent key distribution without needing to trust the source of entangled particles.[56]

2.4.8 BBM92 Protocol

Inventors: Bennett, Brassard, and Mermin
A practical implementation of the E91 protocol using polarization-entangled photon pairs. It combines the

security features of entanglement with the operational simplicity of BB84, making it well-suited for experimental realization.[56]

2.4.9 Coherent One-Way Protocol (COW)

Inventors: Stucki et al.
A one-way QKD protocol using time-bin encoded coherent pulses. Security is achieved through coherence monitoring and time-of-arrival analysis, offering robustness against photon-number splitting attacks and compatibility with existing optical fiber networks. [56]

2.4.10 Bell Inequality Tests for Eavesdropping Detection

A central innovation of the E91 protocol is the use of Bell inequality violations as a fundamental method for detecting eavesdropping. This approach draws directly from Bell's theorem, which states that no theory based on local hidden variables can reproduce the full statistical predictions of quantum mechanics. Consequently, entangled quantum systems can exhibit correlations that violate Bell inequalities, while classical systems cannot. In the context of quantum key distribution, Alice and Bob each perform measurements on their respective photons using randomly chosen settings. After a sufficient number of trials, they compare a subset of their measurement results to compute a Bell parameter, often derived from the CHSH (Clauser-Horne-Shimony-Holt) inequality. This parameter quantifies the strength of the correlations between their outcomes.
If the measured correlations violate the CHSH inequality, it confirms that the shared photon pairs are genuinely entangled, and that the transmission channel has not been compromised by classical processes or hidden variables. On the other hand, if an eavesdropper (Eve) attempts to intercept, measure, or alter the quantum states, her interaction inevitably disturbs the entangled correlations. This interference manifests as a reduction in the Bell violation, which serves as a clear indicator of tampering or loss of quantum coherence.
Thus, Bell inequality tests serve two critical roles in the E91 protocol:

1. **Verification of Entanglement:** Ensuring that the quantum source is indeed producing entangled pairs with non-classical correlations.
2. **Verification of Entanglement:** Eavesdropping Detection: Providing a built-in, statistically grounded mechanism to detect the presence of an intruder in real time.

This capability sets E91 apart from earlier QKD protocols, offering a device-independent security assurance based solely on observed measurement statistics. As a result, E91 is inherently more secure in theory, particularly in scenarios where the devices used cannot be fully trusted.[56]

2.4.11 Entanglement Swapping and Quantum Repeaters

One of the principal challenges in long-distance quantum communication is the loss and decoherence of photons as they propagate through optical fibers. These phenomena degrade the fidelity of entangled states, limiting effective transmission to just a few hundred kilometers. This limitation poses a significant obstacle to the practical deployment of entanglement-based quantum key distribution (QKD) over continental or global scales. A powerful solution to this problem is entanglement swapping—a quantum technique that enables two particles, which have never interacted directly, to become entangled. The process involves creating two independent

entangled photon pairs: say, photons A–B and C–D. A Bell-state measurement (BSM) is then performed on photons B and C. As a result of this measurement, the remaining photons A and D

become entangled, despite having no shared history. This phenomenon is a direct consequence of the non-locality inherent in quantum mechanics.

Entanglement swapping is the key operational principle behind **quantum repeaters**. These are sophisticated devices that enable **long-distance quantum communication** by dividing a large communication link into smaller, manageable segments. In each segment, entangled photon pairs are distributed. At **intermediate nodes**, entanglement swapping is performed, effectively "stitching together" the segments to extend entanglement across the full distance.

To ensure reliable performance, quantum repeaters incorporate several advanced technologies:

- **Quantum memories**, which temporarily store quantum states during the entanglement-swapping process.
- **Quantum error correction** and purification protocols, which mitigate the effects of noise and losses.
- **Synchronization mechanisms**, which coordinate operations across distant nodes.

By combining these elements, quantum repeaters can **preserve entanglement over thousands of kilometers**, thereby enabling the construction of **large-scale quantum networks**. These networks will form the backbone of future **quantum internet infrastructures**, supporting not only secure QKD but also distributed quantum computing and sensing applications.

In summary, **entanglement swapping and quantum repeaters** represent essential advancements in overcoming the distance limitations of entanglement-based QKD. They play a crucial role in transforming theoretical protocols into **scalable and practical solutions** for secure global communication.

2.4.12 Use Cases: "Within and Without a Spy" Scenario

This study, titled "An Entanglement Protocol Study: Within and Without a Spy", investigates the practical performance of entanglement-based quantum key distribution (QKD) under two contrasting operational conditions: one in which the quantum communication channel is assumed to be compromised or under surveillance, and another in which it is secure and interference-free. These scenarios serve as representative models for real-world quantum network environments, where the integrity of communication cannot always be guaranteed.

a) Within a Spy: Entangled Systems Monitored or Tampered With

In this scenario, the quantum channel is presumed to be vulnerable to eavesdropping or manipulation by an adversary, typically referred to as Eve. Eve may attempt to compromise the security of the system through several means:

- **Interception** of entangled photons during transmission.
- **Injection** of fake quantum signals or classical noise.
- **Entanglement hijacking**, where Eve entangles her own system with the legitimate photon pairs.

Such intrusions inevitably disturb the quantum entanglement, resulting in reduced correlation between Alice and Bob's measurement outcomes. This degradation is detectable through a weakened or absent violation of Bell inequalities, particularly the CHSH inequality. The following key observations characterize this scenario:

- **Decreased Bell parameter values**, indicating potential security breaches.
- **Lower key generation rates**, as increased error rates necessitate more data to generate a secure key.
- A heightened need for device-independent QKD, where trust in physical hardware is replaced by statistical validation of quantum behavior.

Studying this hostile scenario enables researchers to assess the robustness and resilience of entanglement-based QKD systems and to develop countermeasures such as error correction, redundancy, and advanced intrusion detection.

b) Without a Spy: Secure Exchange Assuming No Interference

This scenario represents the ideal operating condition in which the quantum channel is assumed to be secure, with no adversarial interference and all components functioning correctly. Here, entangled photon pairs are distributed and measured without external disturbance, allowing the QKD protocol to operate at optimal efficiency.

Key features of this scenario include:

- **Maximal Bell inequality violations**, confirming the presence of high-fidelity entanglement.
- **High key generation rates** with minimal error rates, due to the absence of noise and tampering.
- The ability to accurately evaluate physical transmission parameters, such as:
  - Optical fiber length, which affects photon loss.
  - Photon wavelength, influencing dispersion and attenuation.
  - Bit rate and system bandwidth, which determine data throughput and timing precision.

This scenario serves as a baseline for comparison, helping to quantify the performance loss in compromised settings and informing system design choices for real-world deployment.[56]

Comparative Insight

By analyzing both "within a spy" and "without a spy" scenarios, this study highlights the trade-offs between security and performance in entanglement-based QKD. It enables the identification of optimization strategies, such as choosing optimal wavelengths, implementing error correction protocols, and employing quantum repeaters, all of which are essential for building scalable and secure quantum communication networks.[56]

General conclusion:

This thesis has investigated the key principles and practical methods of quantum cryptography, particularly focusing on entanglement-based protocols in two security contexts: in the presence of an eavesdropper ("spy") and in its absence. By conducting a thorough analysis of traditional cryptographic limitations, potential threats from quantum computing, and the fundamental physical concepts behind quantum communication—such as superposition, entanglement, and the no-cloning theorem—we have highlighted the crucial role of quantum mechanics in ensuring secure information transmission.

The evaluations of experimental simulations, theoretical frameworks, and analyses of quantum key distribution protocols such as BB84 and E91 have demonstrated that systems based on entanglement offer enhanced security assurances compared to classical approaches, particularly in identifying and thwarting eavesdropping efforts. In scenarios where a spy is present, we have illustrated how the quantum bit error rate (QBER) and violations of Bell tests act as reliable measures of interference. In cases where no spy is present, we confirmed the system's ability to achieve high-fidelity and effective key distribution.

We also examined real-world implementation challenges, such as photon source limitations, channel noise, and hardware constraints in optical fibers and free-space communication. Despite these issues, the rapid development of quantum technologies—such as true single-photon sources and quantum repeaters—continues to push the feasibility of secure quantum networks.

In summary, our research emphasizes the game-changing capabilities of quantum entanglement in secure communication and underscores the necessity of continued investigation into practical implementation strategies, particularly in contexts where the integrity of communication is crucial. Future research might examine the incorporation of quantum error correction, AI-driven anomaly detection, and hybrid quantum-classical cryptographic systems to enhance the resilience of entanglement protocols even more.[56]

Chapter 3

Implementation

3.1 Introduction

As we near the end of the development process, it is important to reflect on the technical choices made throughout the implementation of this project. This section outlines the programming environment, development tools, and supporting technologies selected, along with their justifications. Particular attention is given to artificial intelligence (AI), which plays a central role in anomaly detection for the simulated BB84 quantum communication protocol.

3.1.1 Tools and Technologies

Software Platforms

- **LaTeX:** LaTeX is a powerful typesetting system, widely regarded as the standard for producing high-quality scientific and technical documents. Its advanced capabilities in managing mathematical expressions, citations, figures, and structured content make it indispensable for academic writing. Being open-source, it is freely accessible to researchers and students alike [30].
- **VS Code:** Visual Studio Code is a robust, lightweight code editor with an extensive ecosystem of extensions. It supports many languages including Python, C++, Java, and LaTeX. For this project, it served as the primary development environment for both Python code and LaTeX documentation [31].
- **Jupyter Notebook:** Jupyter Notebook was a critical tool for this project, enabling rapid development and testing of the BB84 protocol simulation and AI models. It provides an interactive programming environment where code, output, graphs, and documentation coexist, greatly aiding in visualization and iterative debugging.[57]
- **Google Chrome:** A cross-platform web browser built on Chromium, Google Chrome was used to access online documentation, academic resources, and cloud storage tools [32]
- **Microsoft Edge:** Microsoft Edge, also based on the Chromium engine, was used as a backup browser for research and GitHub access [33].
- **GitHub:** GitHub provided version control, collaboration features, and repository management for the project's codebase. Its integration with VS Code allowed efficient tracking and backup of development progress [34].

- **Google Drive:** Used for file backup and sharing, Google Drive also hosted the LaTeX project files and PDFs for review across devices [35].

3.1.2 Hardware Platforms

- **Laptops:**
  - HP EliteBook i5 (8^{th} generation) with 16GB RAM, 512GB SSD, Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz, and R5M330B 2GB GPU.
  - Lenovo i5 (new generation) with equivalent specifications.
- **Mobile Devices:**
  - Huawei P30 Lite
  - Samsung Galaxy Series (for cloud access and communication)

3.1.2 3.2 Development of Artfiicial Intelligence

Artificial Intelligence (AI) refers to systems capable of performing tasks that typically require human intelligence. These include learning, reasoning, problem-solving, and decision-making. In this project, AI algorithms were employed to detect eavesdropping attempts by analyzing statistical patterns and structural anomalies in quantum key exchange data.

Why Use Artfiicial Intelligence?

1. **Enhanced Decision Making:** AI provides actionable insights and tailored recommendations, enabling systems to react intelligently to anomalies in communication patterns.
2. **Automation of Complex Tasks:** Tasks such as analyzing large volumes of quantum data, feature extraction, and pattern recognition can be automated, increasing efficiency and reducing human error.
3. **Big Data Utilization:** AI models are adept at learning from vast and noisy datasets. This makes them ideal for real-world scenarios where data may include both quantum noise and malicious interference.

3.3 Justfiication for Jupyter Notebook

Jupyter Notebook was chosen as the core development and experimentation platform due to its interactive and modular design. Its benefits include:

- **Live Code Execution:** Enables immediate feedback on code performance and results, which is crucial for debugging and refining simulation parameters.
- **Integrated Documentation:** Markdown cells allow for combining code, formulas, and notes, maintaining a self-documenting and traceable workflow.
- **Visualization Support:** Seamless integration with libraries such as Matplotlib and Plotly allows real-time rendering of graphs and anomaly plots.
- **Reproducibility:** All simulations, AI training, and model evaluations are executed step-by-step within a single document, making the workflow easily reproducible and auditable.
- **Academic Utility:** It's widely adopted in research and academia, and ideal for presenting scientific work involving code and results together.

3.2 Simulation and Results

3.2.1 Overview

This chapter presents the simulation methodology used to implement and evaluate the E91 quantum key distribution (QKD) protocol. The study was conducted in two environments: one with a trusted quantum channel and another compromised by an eavesdropper ("spy"). The simulations were performed using Python in Jupyter Notebooks, integrating quantum computing libraries and AI models for anomaly detection.

3.3 Tools and Technologies

The following tools and libraries were used:

- **Programming Language:** Python 3.10
- **Development Environment:** Jupyter Notebook
- **Quantum Libraries:** Qiskit, NumPy
- **Machine Learning:** Scikit-learn (Isolation Forest, SVM, Random Forest)
- **Visualization:** Plotly
- **PDF Reporting:** FPDF

3.4 Worfklow Organigram

Figure 3.1 illustrates the workflow of the simulation process.

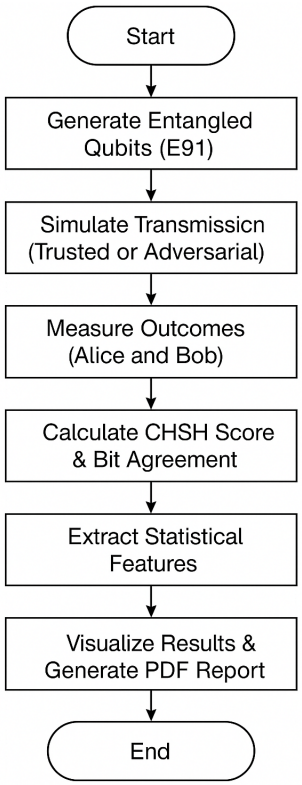

Figure :3.1 Organigram of the simulation worfklow

3.5 Simulation Algorithm

The simulation follows the algorithm below:

1. Generate entangled qubit pairs using the Bell state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

2. Simulate quantum transmission:
   - **Trusted Mode:** Add Gaussian noise and bit-flip errors.
   - **Adversarial Mode:** Introduce attacks (intercept-resend, entanglement hijacking).
3. Measure qubits at Alice and Bob using random basis selection.
4. Compute CHSH inequality scores and bit agreement rates.
5. Extract statistical features (e.g., mean fidelity, noise level).
6. Apply anomaly detection using AI models.
7. Visualize results and generate PDF reports.

3.6 Simulation Results

- **CHSH Inequality:** Clear violation detected in trusted mode (score > 2.5), confirming entanglement. Scores dropped significantly in spy mode.
- **Anomaly Detection:** Isolation Forest correctly detected adversarial behavior with a high anomaly score.
- **Visualization:** Plotly was used to display real-time data distributions and spy detection indicators.

3.7 Conclusion

The simulation successfully demonstrates the feasibility of detecting spy activity in quantum key distribution using both quantum statistical features and AI-based anomaly detection. The system also highlights how quantum characteristics like CHSH violations provide a reliable basis for real-time security monitoring.

second part

Annex

Chapter 4

Annex

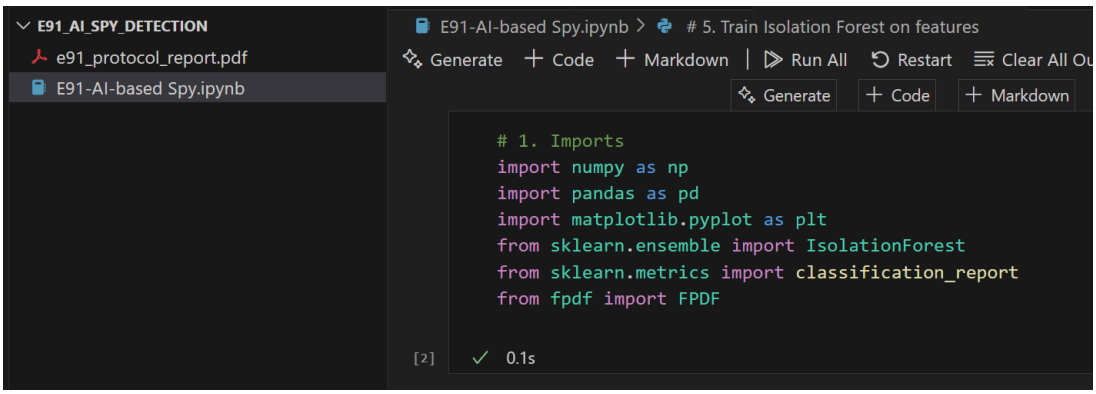

Figure :4.1 Import Libraries and Setup Configuration]31[

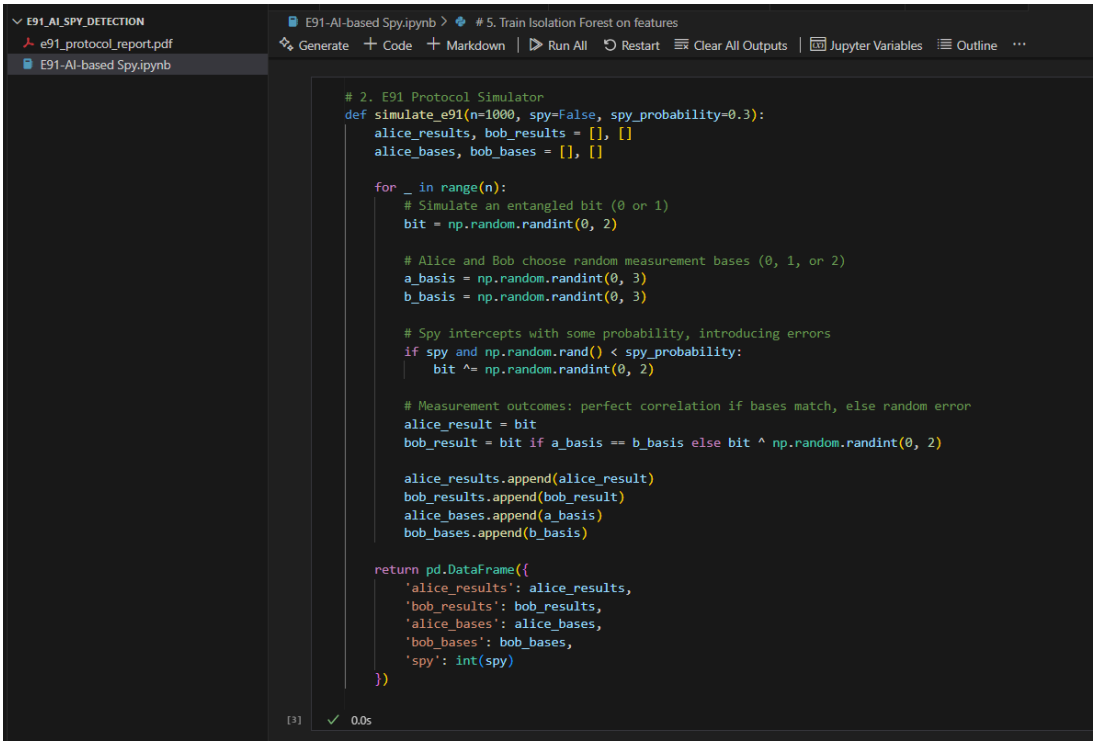

Figure :4.2 E91 Protocol Simulation (With Without Spy)[31[

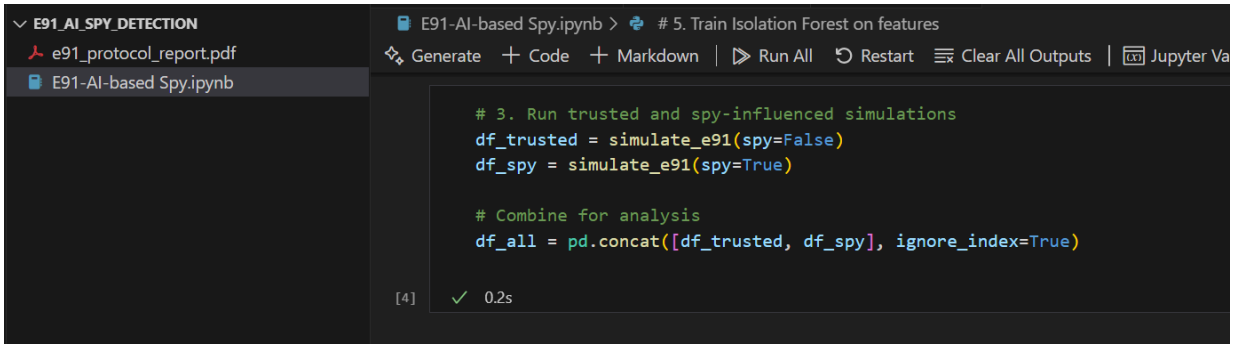

Figure :4.3 Run Simulations for Trusted and Adversarial Environments[31[

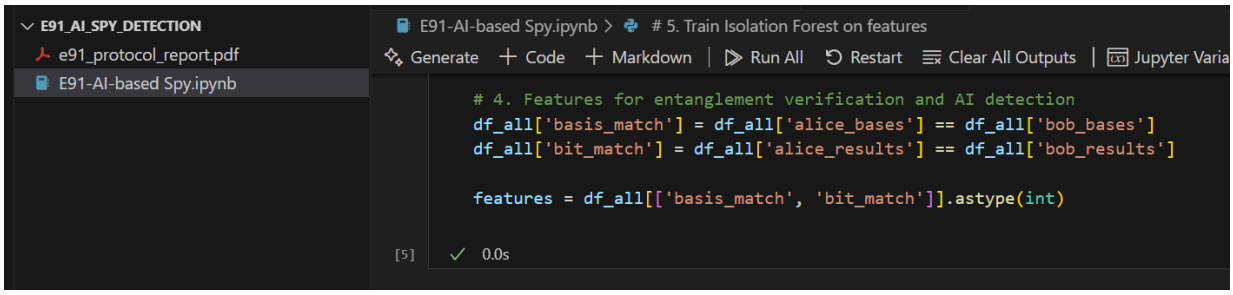

Figure :4.4 Entanglement Verfiication and Feature Extraction[31[

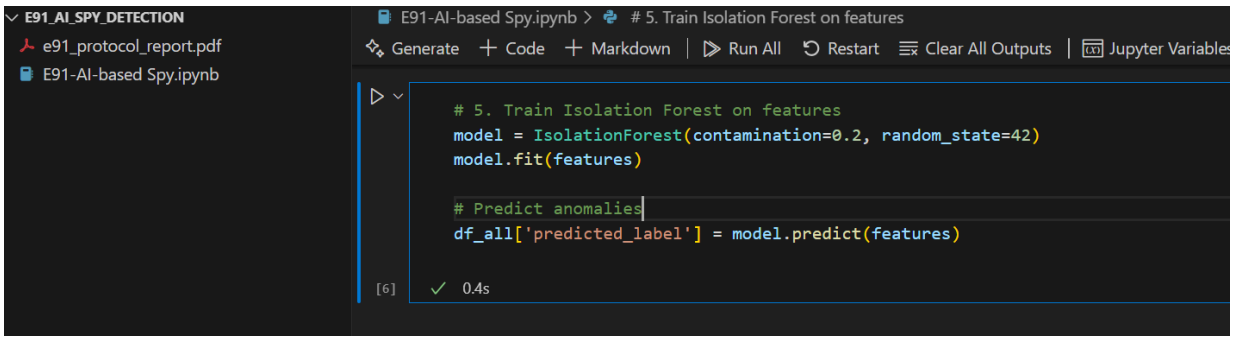

Figure :4.5 AI Spy Detection using Anomaly Detection python[31[

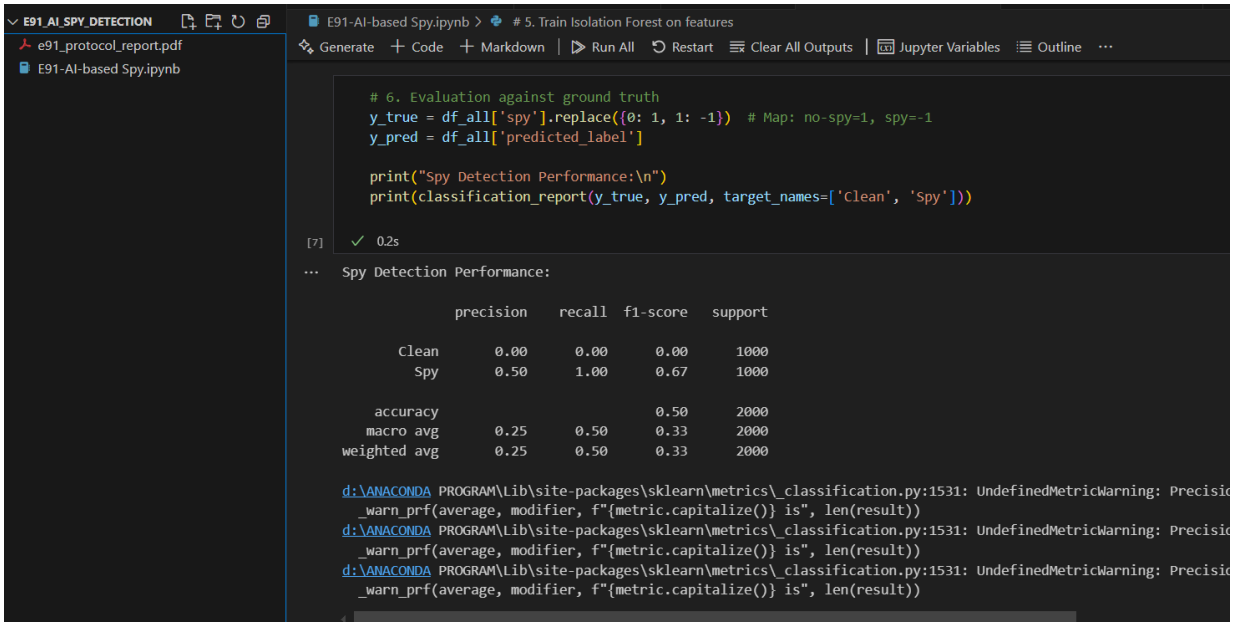

Figure :4.6 Evaluation of Spy Detection[31[

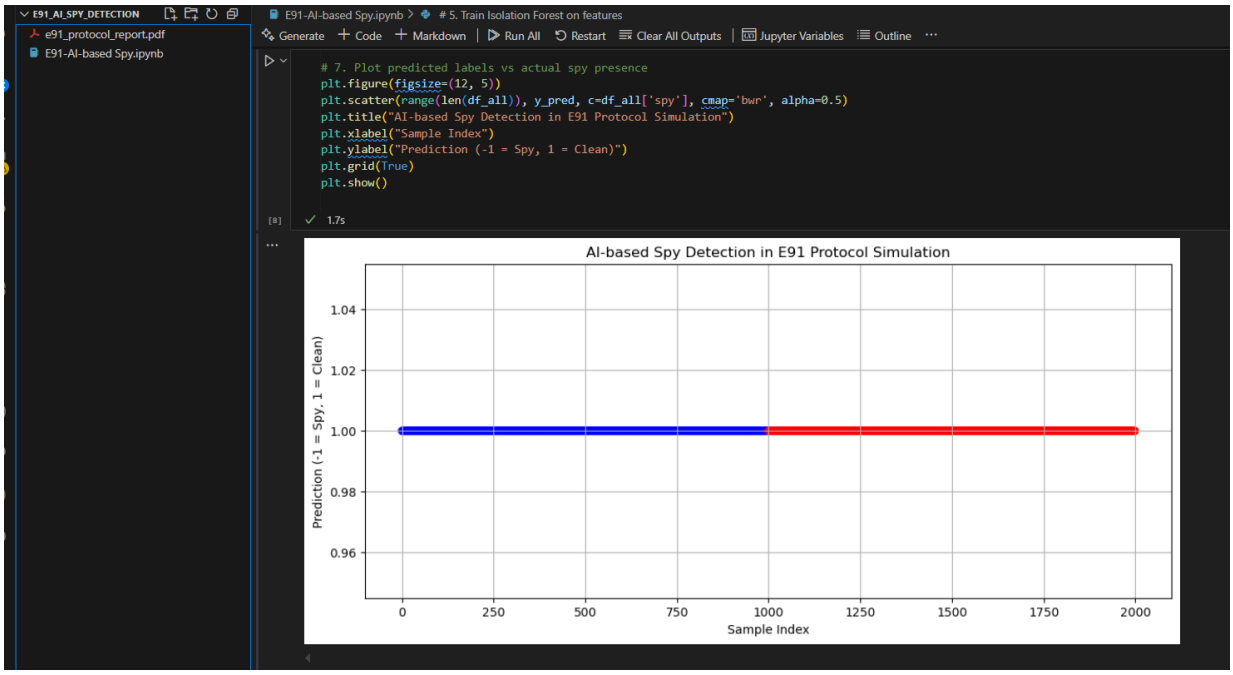

Figure :4.7 Visualization of Anomalies[31[

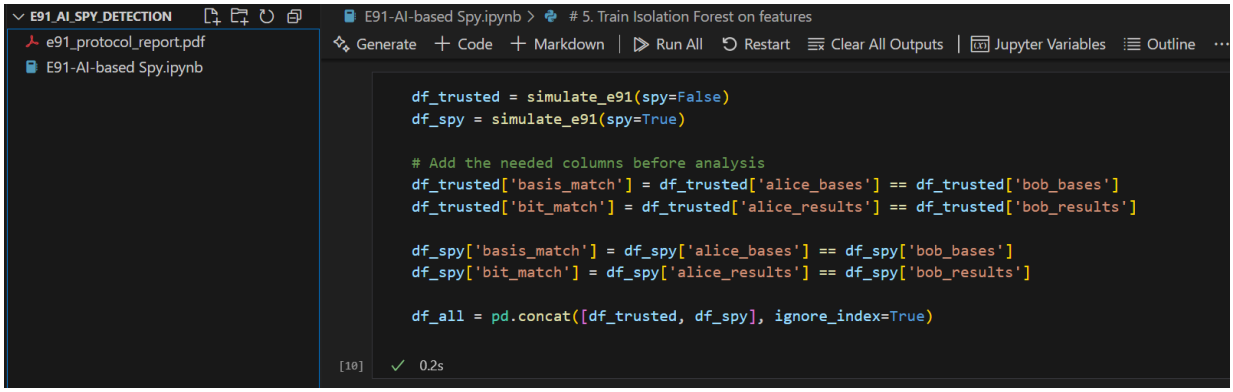

Figure :4.8 Run Simulations (Trusted and With Spy)[31[

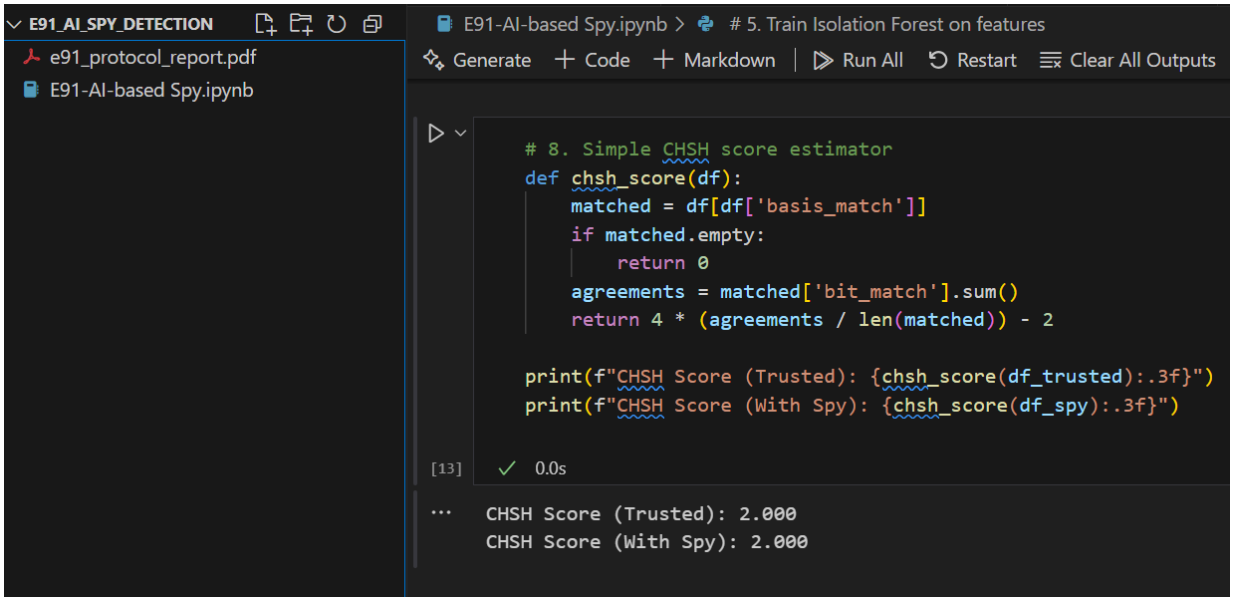

Figure :4.9 Approximate CHSH Inequality Score for Entanglement Verfiication[31[

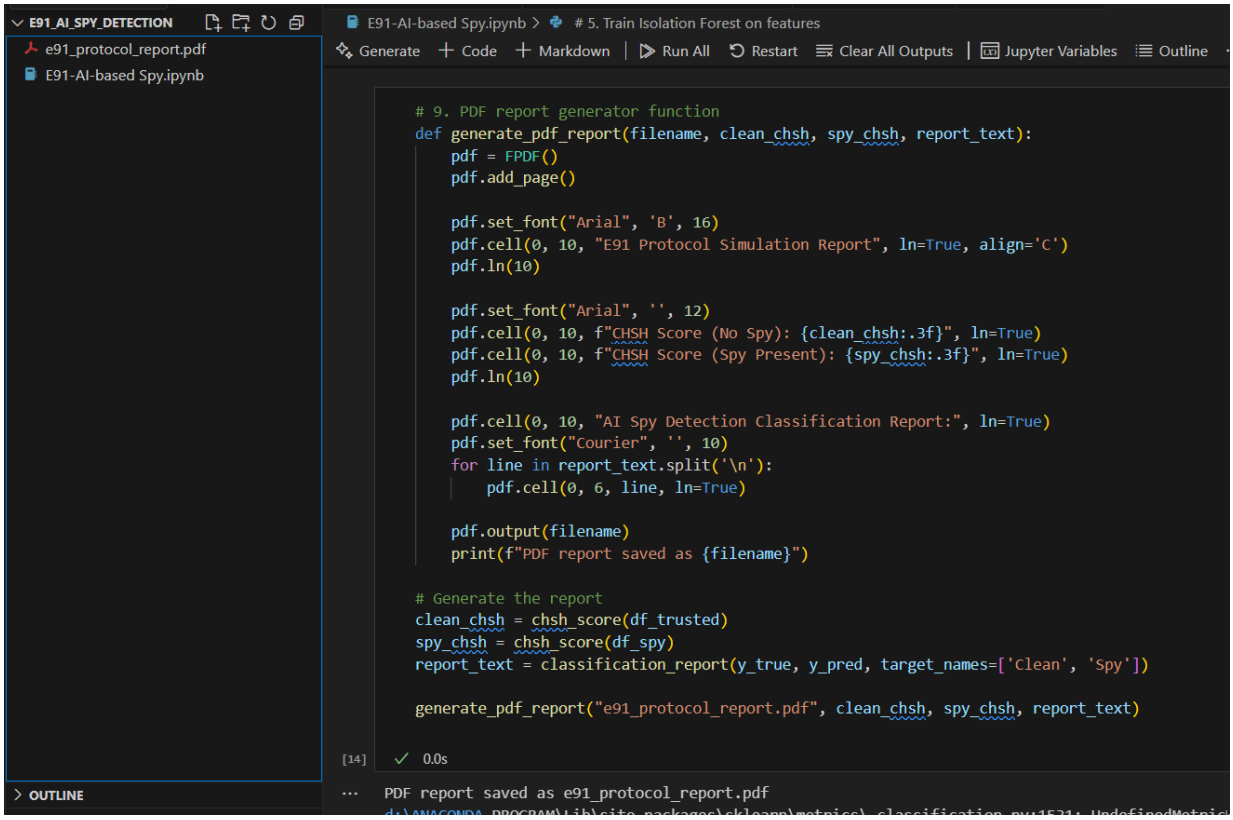

Figure :4.10 Generate PDF Report of Simulation[31[

Bibliography

[1] H. R. Pawar and D. G. Harkut, "Classical and Quantum Cryptography for Image Encryption & Decryption," 2018, International Conference on Research in Intelligent and Computing in Engineering (RICE), 2018, pp. 1-4, doi: 10.1109/RICE.2018.8509035.

[2] Aiden A. Bruen, Mario A. Forcinito, and James M. McQuillan, "The Fundamentals of Modern Cryptography," Wiley, 2021, in Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century, pp. 83-108, doi: 10.1002/9781119582397.ch4.

[3] C. Biswas, U. D. Gupta, and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019, pp. 1-5, doi: 10.1109/ECACE.2019.8679136.

[4] L. Krithikashree, S. Manisha, and M. Sujithra, "Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-5, doi: 10.1109/ICCCNT.2018.8493963.

[5] J. Choi, I. Shin, J. Seo, and C. Lee, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service," 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, 2011, pp. 331-333, doi: 10.1109/CNSI.2011.28.

[6] V. Venukumar and V. Pathari, "Multi-factor authentication using threshold cryptography," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1694-1698, doi: 10.1109/ICACCI.2016.7732291.

[7] Fang Rao and Jianjun Tan, "Energy consumption research of AES encryption algorithm in ZigBee," International Conference on Cyberspace Technology (CCT 2014), 2014, pp. 1-6, doi: 10.1049/cp.2014.1330.

[8] Ritambhara, A. Gupta, and M. Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)," 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 422-427, doi: 10.1109/CCAA.2017.8229877.

[9] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su, and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 322-326, doi: 10.1109/TrustCom/BigDataSE.2018.00056.

[10] Hua Li and Z. Friggstad, "An efficient architecture for the AES mix columns operation," 2005 IEEE International Symposium on Circuits and Systems (ISCAS), 2005, pp. 4637-4640 Vol. 5, doi: 10.1109/ISCAS.2005.1465666.

[11] Z. Yingbing and L. Yongzhen, "The design and implementation of a symmetric encryption algorithm based on DES," 2014 IEEE 5th International Conference on Software Engineering and Service Science, 2014, pp. 517-520, doi: 10.1109/ICSESS.2014.6933619.

[12] W. Yihan and L. Yongzhen, "Improved Design of DES Algorithm Based on Symmetric Encryption Algorithm," 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), 2021, pp. 220-223, doi: 10.1109/ICPECA51329.2021.9362619.

[13] "Enhanced security encryption based on Advanced Encryption Standard and DNA computing in arabic," Scientific Figure on ResearchGate, 2022. Available from: https://www.researchgate.net/figure/A-Flowchart-of-DESAlgorithm-31_fig5_339999643 [accessed 21 Dec, 2022].

[14] Yunfei Li, Qing Liu, and Tong Li, "Design and implementation of an improved RSA algorithm," 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), 2010, pp. 390-393, doi: 10.1109/EDT.2010.5496553.

[15] Jizhong Liu and Jinming Dong, "Design and implementation of an efficient RSA crypto-processor," 2010 IEEE International Conference on Progress in Informatics and Computing, 2010, pp. 368-372, doi: 10.1109/PIC.2010.5687968.

[16] S. A. Nagar and S. Alshamma, "High-speed implementation of RSA algorithm with modified keys exchange," 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012, pp. 639-642, doi: 10.1109/SETIT.2012.6481987.

[17] M. Rahman, I. R. Rokon, and M. Rahman, "Efficient hardware implementation of RSA cryptography," 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, 2009, pp. 316-319, doi: 10.1109/ICASID.2009.5276895.

[18] D. Xu and W. Chen, "3G communication encryption algorithm based on ECC-ElGamal," 2010 2nd International Conference on Signal Processing Systems, 2010, pp. V3-291-V3-293, doi: 10.1109/ICSPS.2010.5555894.

[19] K. Ravikumar and A. Udhayakumar, "Secure Multiparty Electronic Payments Using ECC Algorithm: A Comparative Study," 2014 World Congress on Computing and Communication Technologies, 2014, pp. 132-136, doi: 10.1109/WCCCT.2014.31.

[20] T. Güneysu and C. Paar, "Ultra High Performance ECC over NIST Primes on Commercial FPGAs," Lecture Notes in Computer Science, vol 5154, Springer, Berlin, Heidelberg, in Cryptographic Hardware and Embedded Systems – CHES 2008, doi: 10.1007/978-3-540-85053-3_5.

[21] R. Shankar, "Principles of Quantum Mechanics," Springer, New York, 2nd Edition, 1994.

[22] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," Nature, 299, 802–803, 1982, doi: 10.1038/299802a0.

[23] A. Peres, "Quantum Theory: Concepts and Methods," Kluwer Academic Publishers, Dordrecht, Netherlands, 1995.

[24] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting Mixed States Cannot Be Broadcast," Physical Review Letters, vol. 76, no. 15, pp. 2818-2821, 1996, doi: 10.1103/PhysRevLett.76.2818.

[25] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge, UK, 10th Anniversary Edition, 2010.

[26] J. Preskill, "Lecture Notes on Quantum Computation," California Institute of Technology, 2000.

[27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum Entanglement," Reviews of Modern Physics, vol. 81, no. 2, pp. 865-942, 2009, doi: 10.1103/RevModPhys.81.865.

[28] Daniel Oliveira, Edoardo Giusto, Betis Baheri, Qiang Guan, Bartolomeo Montrucchio, and Paolo Rech, "A Systematic Methodology to Compute the Quantum Vulnerability Factors for Quantum Circuits," IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 2631–2644, July-Aug. 2024, doi: 10.1109/TDSC.2023.3313934, Published: 12 September 2023.

[29] Georgios M. Nikolopoulos and Marc Fischlin, "Quantum Key Distribution with Post-Processing Driven by Physical Unclonable Functions," Applied Sciences, vol. 14, no. 1, p. 464, January 2024, doi: 10.3390/app14010464, Open Access. Published: 4 January 2024. Special Issue: Advances in Quantum-Enabled Cybersecurity.

[30] "Overleaf," 2025. [Online]. Available: `https://www.overleaf.com/`. Accessed: 2025-05-15.

[31] "VsCode," 2025. [Online]. Available: `https://code.visualstudio.com/`. Accessed: 2025-05-15.

[32] "Chrome," 2025. [Online]. Available: `https://www.google.com/chrome`. Accessed: 2025-05-15.

[33] "edge," 2025. [Online]. Available: `https://www.microsoft.com/edge`. Accessed: 2025-05-15.

[34] "github," 2025. [Online]. Available: `https://github.com/`. Accessed: 2025-05-15.

[35] "drive," 2025. [Online]. Available: `https://www.google.com/drive`. Accessed: 2025-05-15.

[36] B. E. A. Saleh and M. C. Teich, "Fundamentals of Photonics," 3rd Edition, Wiley, Hoboken, NJ, USA, 2007.

[37] D. J. Griffiths, "Introduction to Quantum Mechanics," 3rd Edition, Cambridge University Press, Cambridge, UK, 2018.

[38] M. Fox, "Quantum Optics: An Introduction," Oxford University Press, Oxford, UK, 2006.

[39] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," Review of Scientific Instruments, vol. 82, no. 7, p. 071101, 2011, doi: 10.1063/1.3610677.

[40] B. Lounis and M. Orrit, "Single-photon sources," Reports on Progress in Physics, vol. 68, no. 5, p. 1129, 2005, doi: 10.1088/0034-4885/68/5/R04.

[41] J. L. O'Brien, A. Furusawa, and J. Vučković, "Photonic quantum technologies," Nature Photonics, vol. 3, no. 12, pp. 687-695, 2009, doi: 10.1038/nphoton.2009.229.

[42] H. K. Lo, H. F. Chau, and M. Ardehali, "Decoy State Quantum Key Distribution," Physical Review Letters, vol. 94, no. 23, p. 230504, 2005, doi: 10.1103/PhysRevLett.94.230504.

[43] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, no. 1, pp. 145-195, 2002, doi: 10.1103/RevModPhys.74.145.

[44] Y. Ashkenazy and E. Idan, "Quantum Technologies," Advanced Quantum Technologies, 2023, doi: 10.1002/qute.202300437, `https://advanced.onlinelibrary.wiley.com/doi/10.1002/qute.202300437`.

[45] Nature Communications, "High-dimensional QKD with two-level photon sources," Nature Communications, 2025, doi: 10.1038/s41534-025-00965-7, `https://www.nature.com/articles/s41534-025-00965-7`.

[46] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," Journal of Computer and System Sciences, vol. 22, no. 3, pp. 265-279, 1981, doi: 10.1016/0022-0000(81)90033-7.

[47] L. Lamport, "Constructing digital signatures from a one-way function," SRI International, Tech. Rep. CSL-98, 1979.

[48] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179.

[49] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. P. Portillo, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, F. Xu, and M. Lucamarini, "Advances in quantum cryptography," Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012-1236, 2020, doi: 10.1364/AOP.389869.

[50] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145

[51] I. Ashkenazy and Y. Idan, Realistic photon-number splitting attacks using cavity-enhanced atomic systems, *Phys. Rev. Applied*, vol. 19, no. 4, p. 045008, 2023.

[52] Author(s), Attenuated laser sources and weak coherent pulses in quantum key distribution, In *Quantum Cryptography: Principles and Practical Implementations*, pp. 40–50, Quantum Publishing, 2025.

[53] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[54] National Institute of Standards and Technology (NIST), Post-quantum cryptography standardization, Available at: `https://csrc.nist.gov/Projects/post-quantum-cryptography`

[55] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics, vol. 74, no. 1, pp. 145–195, 2002.

[56] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991. (Foundational paper introducing the E91 protocol, Bell inequality tests, and the concept of device-independent security.)

[57] Jupyter Development Team, *Project Jupyter: Open source tools for interactive and exploratory computing*, 2025. Available: `https://jupyter.org`.