Umons University

Computer Science department

Master thesis

Quantum Key Distribution Protocols

Author:
Gregory Cuozzo

Director:
Dr. BUYS Alain

Year 2025-2026

I, Gregory Cuozzo , certify that I have complied with the applicable ethical standards, including the University's charter regarding the use of Artificial Intelligence.

Generative Artificial Intelligence tools were used during the preparation of this thesis as assistive tools for linguistic revision and preliminary exploration of scientific concepts related to Quantum Key Distribution.

I reviewed, corrected, verified, and analyzed the generated content before its integration into this report.

I remain responsible for the scientific accuracy, interpretation, structure, and originality of the master thesis.

Contents

List of Figures

List of Algorithms

Acknowledgements

Completing this thesis represented a significant academic and personal challenge, particularly in the context of balancing full-time professional responsibilities with evening higher education studies over more than seven years. The final years of this journey were especially demanding and were accompanied by periods of fatigue and uncertainty. Nevertheless, this experience became a meaningful lesson in perseverance, discipline, resilience, and intellectual curiosity. Beyond the scientific and technical knowledge acquired throughout these years, this journey ultimately strengthened my ability to overcome challenges and maintain long-term commitment despite adversity.

I would like to sincerely thank my classmates Rachel Lefebvre , Diego Anselmo, and Arnaud Malhaize with whom I shared memorable experiences throughout these years of study and with whom meaningful bonds were built over time.

My sincere gratitude also goes to professors Tom Mens and Stephane Dupont for the programming skills, technical knowledge and software engineering they helped me develop during this academic journey.

Also, I would like to thank professors Véronique Bruyere and Gwenael Joret for providing valuable conceptual insights and for contributing to the development of my scientific rigor and analytical reasoning.

I am deeply grateful to Cassandra Cuozzo, Dylan Cuozzo, Malika Khelfi and Gabriel Huygebaert for their moral support, encouragement, and assistance throughout my university journey and academic endeavors.

Finally, I would like to thank my thesis supervisor, professor Alain Buys, for offering me the opportunity to work on a topic relying on computer and physical sciences. This work allowed me to combine my scientific interests with my academic background and contributed to my intellectual improvement.

Abstract

Keywords: Quantum Key Distribution (QKD), quantum cryptography, quantum communication, cybersecurity, Shor's algorithm, RSA, quantum-secure communications.

This master thesis investigates the cybersecurity challenges arising from the rapid evolution of quantum technologies and their implications for conventional cryptographic systems. In particular, the work highlights the vulnerability of widely deployed public-key cryptographic schemes, such as RSA, against quantum algorithms including Shor's algorithm. To illustrate these limitations, a numerical example demonstrating the theoretical compromise of RSA encryption is presented.

In order to provide the necessary scientific background, the thesis first introduces the fundamental concepts of quantum mechanics required to understand Quantum Key Distribution (QKD). The study then presents a global overview of QKD, including its classification, physical implementation layer, as well as the main notions related to security and reliability in practical systems.

Then, representative QKD protocols is analyzed.
Indeed, rather than reviewing all existing protocols, the thesis focuses on four protocols chosen which represent and illustrate the principal operating paradigms encountered in QKD. This approach avoids redundancy while providing a comprehensive understanding of QKD.

Finally, the thesis discusses the current state of QKD deployment, including existing infrastructures, emerging industrial applications. The thesis concludes with a summary of the presented concepts and a discussion concerning the future perspectives of quantum-secure communications.

1 Introduction

1.1. Context and Motivation

Nowadays, most information is exchanged via computerized devices. Some of this information can be confidential and critical. This is where the notion of "cybersecurity" comes in.

Cybersecurity is defined as all the practices and technologies used to secure a computer system. It enables the implementation of defensive measures designed to guarantee four essential elements : [6] [31]

1. **Authentication:**

   This element makes it possible to identify the actors (sender and receiver) during a network communication.
2. **Confidentiality:**

   Confidentiality ensures that information is not divulged outside the identified actors. This is where the concept of encryption comes in.
3. **Integrity:**

   The aim is to ensure that the message is not modified, thereby avoid loss of information.
4. **Availability:**

   This last element ensures that the communication service is available in all circumstances.

To ensure secured communication, a variety of protocols and paradigms co-exist.
The following is an example of two types of encryption: [6] [31]

1. **Symmetric encryptions** :

   Symmetric encryptions use a shared same secret key between communicating parties.This key is used for encryption and decryption.

   The following are some examples of symmetric encryptions:

   (a) AES;
   (b) 3DES.

2. **Asymmetric encryptions**:

   Asymmetric encryptions rely on mathematical problems assumed to be " hard " and use two keys (a private key for decryption and a public key for encryption)

   The following are some examples of asymmetric encryptions:

   (a) RSA, relying on the integer factorization: [1]
   (b) ElGamal;

As technology evolves, the quantum computer appears. The computer security currently available is at risk.
Take, for example, the RSA encryption principle. The principle is based on the difficulty of factoring a large number into two prime numbers. The factoring time required to break the key is in the order of several thousand years for conventional computers.

Quantum computers, on the other hand, could theoretically solve this problem much more efficiently by using Shor's algorithm. However, this remains a theoretical threat at present: current quantum computers are not yet capable of breaking real-world RSA keys, since this would require a large-scale fault-tolerant quantum computer with a sufficient number of reliable qubits. The vulnerability of RSA must be understood as a long-term cryptographic risk rather than as an immediate practical break.

[1] The difficulty of factoring a large number into two prime numbers will be discussed later on in RSA section.

To prepare for tomorrow's computer security, new encryption methods are being researched. These are known as quantum cryptography [2] [15] and post-quantum cryptography. [9]

Quantum Cryptography uses the quantum property of the matter(Quantum Mechanics). This method guarantees an alert in case an unauthorized access or interference occurs in the communication channel. There are variety of protocols included in quantum cryptography.
The following are some examples :

1. **Quantum key Distribution (QKD) :**

   These protocols allow two parties to securely generate a shared key using quantum properties of the matter. They are based on the no-cloning theorem. The former states that quantum states cannot be copied without disturbing the system (the state itself).

2. **Position-based Quantum cryptography:**

   This protocol authenticates a user based on their geographical location. It highlights the fact that quantum information cannot be copied and transmitted faster than light. To do so, the sender sends a quantum challenge; the receiver is led to respond within a specific time frame from their communicated position.

3. **Device-Independent Quantum Cryptography:**

   These protocols guarantee security even if the devices are untrusted. They are based on Bell Inequalities.[3]

Post-Quantum Cryptography (PQC) [4] refers to cryptographic algorithms designed to remain secure against adversaries equipped with quantum computers. Unlike quantum key distribution, these schemes can be deployed over classical communication channels without requiring quantum infrastructure.

[2]Note that this is a misnomer. Quantum cryptography does not encrypt messages, but rather constructs the encryption key based on the physical properties of matter.

[3]Bell Inequalities will be discussed later on in the section Quantum Information Principles

[4]An in-depth treatment of this subject is omitted in this thesis for the sake of conciseness. The reader may refer to [9] for further information.

The National Institute of Standards and Technology (NIST) has initiated a standardization process to identify and approve quantum-resistant algorithms.

The selected schemes can be categorized as follows:

1. **Key establishment (confidentiality):**
   - Module-lattice-based key encapsulation mechanisms (e.g., CRYSTALS-Kyber, standardized as ML-KEM)
2. **Digital signatures (authentication and integrity):**
   - Module-lattice-based signature schemes (e.g., CRYSTALS-Dilithium, standardized as ML-DSA)
   - Hash-based signature schemes (e.g., SPHINCS+)

Although Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) are both motivated by the emergence of quantum computers, they rely on fundamentally different security paradigms. QKD is based on the physical transmission of quantum states in order to establish secret keys between two parties, whereas PQC consists of classical cryptographic algorithms designed to resist attacks performed by quantum computers.

This work deliberately restricts its scope to Quantum Key Distribution. Although Post-Quantum Cryptography is part of the quantum-safe cryptography, it is not considered as a central object of study in this thesis. The analysis is focused on the foundations of QKD, its operational mechanisms, its security assumptions, and the constraints associated with its deployment.

1.2. Research Question and Methodology

This thesis adopts an exploratory perspective. Its purpose is to build a clear understanding of how QKD works and why it represents a different approach to key establishment compared with classical cryptography.

The question of this work can be formulated as follows: how can the principles of quantum mechanics make it possible to establish a secret cryptographic key between two distant parties, and what theoretical and practical difficulties must be considered when such a system is implemented? To answer this question, this thesis is based on a review of the scientific literature and on a conceptual analysis of several representative QKD protocols.

The objective is to understand the main mechanisms that make quantum key distribution possible. For this reason, the work first introduces the necessary foundations in classical cryptography and quantum physics. It examines both discrete-variable and continuous-variable approaches. Protocols such as BB84, E91, and GG02 are used as reference examples because they illustrate different ways in which quantum properties can be exploited to distribute a secret key, while also highlighting their respective assumptions, operational steps, and security principles.

2 Cryptographic Limitations and Quantum Threats

This section introduces the stake brought by the evolution of quantum technologies.
Indeed, nowadays, cybersecurity mainly relies on mathematical problems assumed to be impossible to solve in a short time with classical computation. As already mentioned, factoring a large number into two prime numbers takes several thousand years with conventional computers.
RSA uses this fact and is currently widely used.

From now on, a quantum algorithm known as Shor's algorithm is able to solve RSA's core problem ; the time to solve the problem of factoring a large number into two prime numbers is reduced from several thousand years to a few minutes. Note that it is purely theoretical. The practical execution of Shor's algorithm at a scale relevant to real-world RSA parameters requires a large number of high-quality qubits. As mentioned before, the current problem lies in the decoherence of the quantum computers. Calculation carried out has a margin of error.

At this point, it is relevant to describe RSA, Shor's algorithm and see how Shor's algorithm is capable of breaking RSA [1] with a considered smaller key than the real-world one.

2.1. Breaking RSA

2.1.1 RSA Algorithm

RSA [6] [31] [20] [39] (Rivest , Shamir , Adleman) encryption is today's best-known security protocol, part of the so-called "asymmetric" encryption. It is based on the difficulty of factoring a large integer into its prime factors.

Let the public and private keys be respectively (n, e) and (p, q, d). RSA algorithm allows to determine each of the parameters n, e, p, q and d. Once the public and private keys constructed, the message sent from the sender Bob to the receiver Alice can be encrypted using the public key of Alice and decrypted by the private key of Alice as illustrated in the RSA Illustrated figure 2.1

[1] This RSA-breaking example is not intended to provide a complete treatment of quantum algorithms. Its purpose is to illustrate why alternative key-establishment mechanisms are investigated in the context of quantum threats.

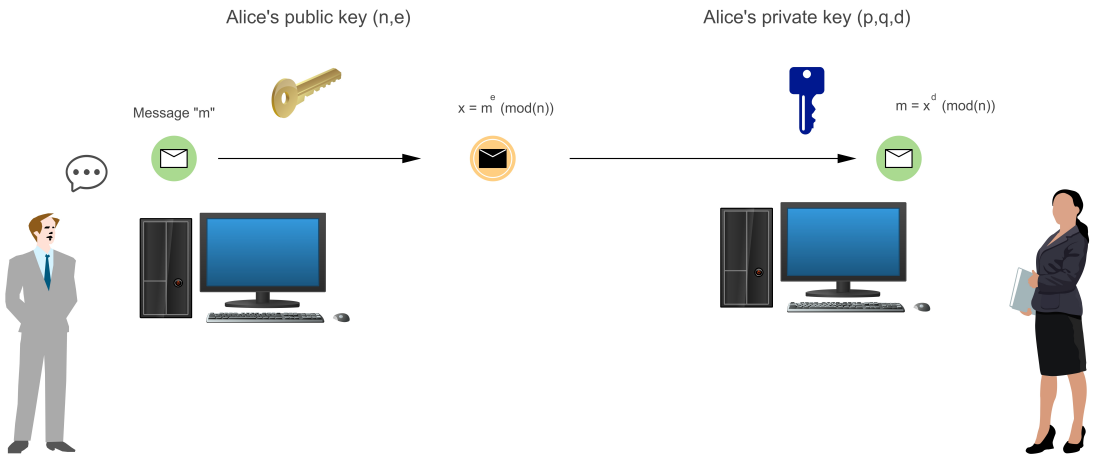

Figure 2.1: RSA Illustrated

Algorithm 1 RSA Algorithm

1: Choose two large prime numbers p and q
2: Compute $n \leftarrow p \times q$
3: Compute the Euler totient function $\varphi(n) \leftarrow (p-1)(q-1)$
4: Choose e such that $\gcd(\varphi(n), e) = 1$
5: Compute $d \leftarrow e^{-1} \mod \varphi(n)$
6: **return** Public key (e, n) and private key (p, q, d)

RSA application example

1. Let's define two prime numbers p and q respectively 11 and 13;
2. n is determined such that $n = p \cdot q$

   $n = 11 \cdot 13 = 143$
3. $\varphi(n)$ is determined such that $\varphi(n) = (p-1) \cdot (q-1)$

   $\varphi(n) = (11-1) \cdot (13-1) = 120$
4. e is determined such that $GCD(\varphi(n), e) = 1$

   let $e = 7$. We have $GCD(120, 7) = 1$
5. The private key d is determined as follows : $d = e^{-1} mod \varphi(n)$

   In order to determine d, we need to find the inverse of 7 with $\varphi(n)$. To do so, the Extended Euclidean Algorithm is used. After execution $d = 103$

   It can be verified as follows :

   $e \cdot d = 1 mod \varphi(n) \Leftrightarrow 7 \cdot 103 = 721 = 1 mod 120$

As a result , the public and private keys are respectively $(143, 7)$ and $(11, 13, 103)$

2.1.2 Shor's Algorithm

As mentioned before, Shor's algorithm [20] [34] is theoretically able to solve RSA's core problem.

Shor's algorithm consists of two main parts:

1. A classical reduction of the prime factor problem to a group's order finding problem;
2. A quantum algorithm used to solve the order finding problem.

Let's give an example of Shor's algorithm application and let's break RSA.
The RSA application example, as seen before, used $n = 143$.
Let's factorise this number n so we can determine the private key which is supposed to be kept secret.

Algorithm 2 Shor's Algorithm

Require: Integer n which as to be factorised.

1: $a \leftarrow$ random number such as $1 < a < n$.
2: $k \leftarrow GCD(a, n)$
3: **if** $k \neq 1$ **then**
4: $factor1 \leftarrow k$
$factor2 \leftarrow \frac{n}{k}$
5: **else**
6: Reduce the prime factor problem to a group's order r finding problem
7: **if** r is odd **then**
8: Go back step 1
9: **else**
10: $factor1 \leftarrow GCD(a^{\frac{r}{2}} + 1, n)$
$factor2 \leftarrow GCD(a^{\frac{r}{2}} - 1, n)$
11: **end if**
12: **end if**
13: **return** $factor1$, $factor2$

Shor's algorithm application example

1. let $a = 2$. Note that $1 < (a = 2) < (n = 143)$
2. compute $k = GCD(2, 143)$. As a result we obtain $k = 1$
3. as $k = 1$, the prime factor problem is reduced to a group's order finding problem
   The objective is to determine r the smallest integer such that :

$$a^r \equiv 1 \cdot (mod 143)$$

   For this example, as $a = 2$, we have :

$$2^r \equiv 1 \cdot (mod 143)$$

   Let $2^r \equiv x \cdot (mod 143)$
   The objective is to determine x for each value of r incrementing progressively. The order is found when $x = 1$

Order	x value
2^1	2
2^2	4
2^3	8
$\vdots$	$\vdots$
2^5	32
2^{10}	23
2^{15}	21
$\vdots$	$\vdots$
2^{60}	1

According to the computation, as a result, we have $r = 60$

4. As $r = 60$ is even , the factorisation is processed as follows :

   Factor 1 : $GCD(2^{\frac{60}{2}} - 1, n) = 11$
   Factor 2 : $GCD(2^{\frac{60}{2}} + 1, n) = 13$

As a result, $n = 143$ can be factored as $n = p \cdot q = 11 \cdot 13$. The Euler totient function is therefore given by:

$$\varphi(n) = (p-1)(q-1) = 10 \cdot 12 = 120.$$

The private exponent d is defined as the modular inverse of e modulo $\varphi(n)$:

$$d \equiv e^{-1} \pmod{\varphi(n)}.$$

For $e = 7$, we obtain:

$$d = 103,$$

since:

$$7 \cdot 103 = 721 \equiv 1 \pmod{120}.$$

The private key is therefore given by $(p, q, d) = (11, 13, 103)$.

2.2. Limitations of Classical Security

Shor's algorithm is theoretically efficient to break RSA easily and so today's communication security. The challenge is its implementation. It requires a large number of Qubits. Because of Qubits's decoherence and error correction operations requirement, quantum computers are not able to solve RSA's core problem using large keys without having a margin of error.

To prepare the tomorrow's computer security, researches are being done relying, for instance, on Quantum Key Distribution (QKD).
Indeed, QKD create symmetric key using the quantum properties of matter, such light. Devices continually and randomly generate private keys that both parties share. These keys are generally constructed according to the photon's polarisation. The advantage of polarisation is that it is well conserved in the course of light propagation through the atmosphere and allows a transmission distance of more and less 1200 km (for instance, from a satellite to the ground station)

Although Shor's algorithm represents a major theoretical threat to RSA, the practical realization of a large-scale fault-tolerant quantum computer remains an important technological challenge. Consequently, the urgency of migration toward quantum-resistant cryptographic solutions is still subject to debate within the cybersecurity community.

Before introducing QKD protocols themselves, several notions from quantum mechanics must first be clarified.

3 Quantum Mechanics Fundamentals

3.1. Light Properties

Light is an electromagnetic radiation that propagates through space and carries energy [19]. The electromagnetic spectrum spans a wide range of wavelengths, from gamma rays to radio waves. Visible light corresponds to the portion of this spectrum that can be detected by the human eye.

One of the properties of light is its polarization. Polarization is defined as the orientation and temporal evolution of the electric field vector in the plane perpendicular to the direction of propagation. This property plays a role in discrete-variable quantum key distribution (DV-QKD) protocols such as BB84.

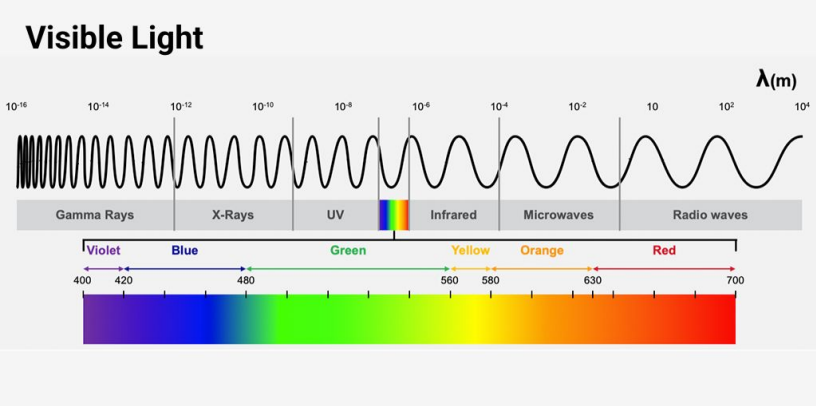

Figure 3.1: Radiative Spectrum
[10]

Relying on the polarization of light, two main categories can be distinguished: unpolarized light and polarized light.

Définition 1 (Unpolarized Light)**.** *Unpolarized light is defined as an electric field vector that exhibits random temporal variations in all directions perpendicular to the direction of propagation.*

Définition 2 (Polarized Light)**.** *Polarized light refers to electromagnetic waves in which the electric field vector has a well-defined orientation or evolution over time. Three main types of polarization can be distinguished:*

1. *Linear polarization*
2. *Elliptical polarization*
3. *Circular polarization*

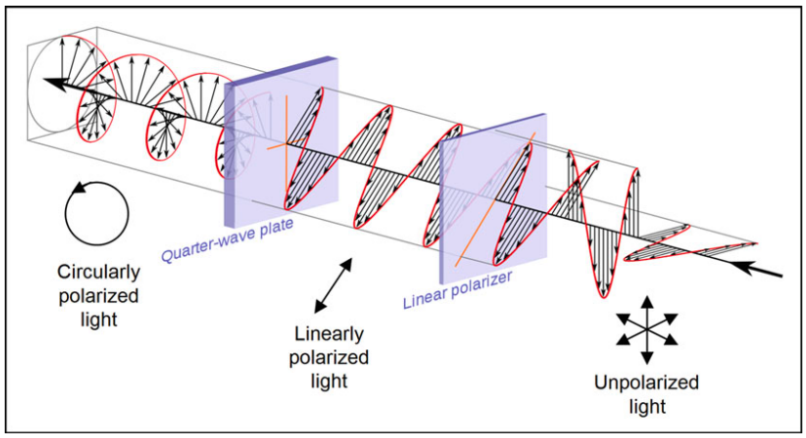

Figure 3.2: Polarisation State of Light
[30]

In Continuous-Variables Quantum Key Distribution (CV-QKD) such as GG02, information is encoded using the quadratures of the electromagnetic wave [25] [32] ; the amplitude and phase components. Therefore, before introducing the GG02 protocol, it is necessary to formalize the concept of quadratures.
In the GG02 protocol, information is transmitted using coherent optical states generated by a laser source. These states correspond to optical modes described through their quadratures.

Définition 3 (Optical Mode)**.** *An optical mode is a configuration of the electromagnetic field characterized by a specific spatial profile, frequency, polarization, and phase. It can be described using two real-valued orthogonal components known as quadratures. These two components play a role analogous to Cartesian coordinates in a phase space and provide a complete description of the electromagnetic field state.*

Définition 4 (Monochromatic Field)**.** *A monochromatic field is an electromagnetic field oscillating at a single, well-defined frequency. Its temporal evolution is typically described by a sinusoidal function with constant amplitude and phase. The temporal evolution of a monochromatic electromagnetic field is mathematically analogous to that of a classical harmonic oscillator.*

Définition 5 (Classical Harmonic Oscillator)**.** *A classical harmonic oscillator is a dynamical system in which a particle of mass m is subject to a restoring force proportional to its displacement x from an equilibrium position.*

The restoring force is described by Hooke's law:

$$F = -kx, \tag{3.1}$$

where $k > 0$ is the stiffness (spring constant) of the system.

The motion of the system is governed by Newton's second law, leading to the differential equation:

$$m\frac{d^2x}{dt^2} + kx = 0. \tag{3.2}$$

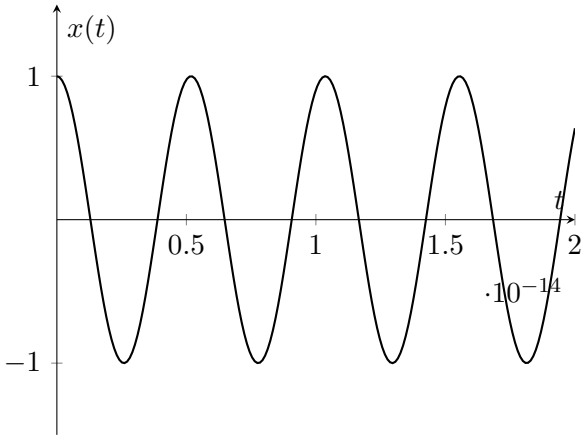

Figure 3.3: Sinusoidal Oscillation $x(t) = A\cos(\omega t + \phi)$

The general solution of this equation is a sinusoidal oscillation illustrated in the figure 3.3 :

$$x(t) = A\cos(\omega t + \phi), \tag{3.3}$$

where:

- $x(t)$ is the value of the electromagnetic field at time t,
- A is the amplitude of the field,
- ω is the angular frequency (in rad/s),
- t is time,
- ϕ is the initial phase.

The angular frequency is related to the frequency f by:

$$\omega = 2\pi f \tag{3.4}$$

In the case of monochromatic electric field, the Equation (3.3) can equivalently be represented as a linear combination of two phase-orthogonal quadratures:

$$E(t) = X\cos(\omega t) + P\sin(\omega t), \tag{3.5}$$

where:

- X is the in-phase quadrature
- P is the quadrature component shifted by $\frac{\pi}{2}$ in phase.

Consequently, any optical signal can be represented as a point (X, P) in phase space. The two quadratures therefore define orthogonal axes that fully characterize the state of the field and encode the following information:

1. **The total amplitude of the field;**

   The total amplitude A of the field is given by

   $$A = \sqrt{X^2 + P^2}. \tag{3.6}$$

2. **The phase of the field;**

   The phase φ is given by:

   $$\varphi = \arctan\left(\frac{P}{X}\right). \tag{3.7}$$

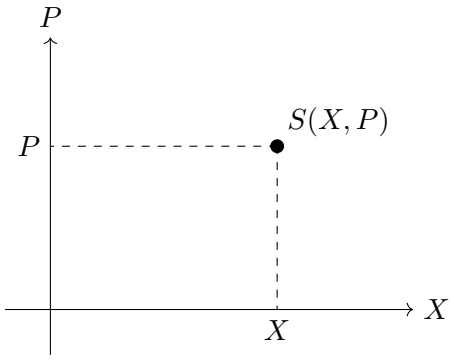

Figure 3.4: Signal $S(X, P)$ in Phase Space.

These quadratures (X and P) are used in Continuous-Variable Quantum Key Distribution (CV-QKD) protocols, such as GG02. The quadratures are treated as quantum observables associated with a quantized optical mode. They are analogous to position and momentum variables of a harmonic oscillator.

3.2. Superposition

In the purpose to explain what the superposition [40] [2] [20]is about, a quantum state and a Qubit are to be defined.

Définition 6 (Quantum State)**.** *A quantum state is a mathematical object that contains all the information required to predict the probabilities of measurement outcomes for a quantum system. Mathematically, a quantum state can be described as a linear combination of states.*

Définition 7 (Qubit)**.** *A Qubit is the fundamental unit of quantum information used by QKD, analogous to a bit in classical computing and can be represented by the Bloch Sphere*

When measured in the computational basis, a qubit yields one of two possible outcomes, 0 or 1. Before measurement, however, its state may be any superposition of the two basis states :

$$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle \tag{3.8}$$

where:

- $|\alpha|^2$ is the probability of measuring the state $|0\rangle$
- $|\beta|^2$, is the probability of measuring the state $|1\rangle$

Note that $\alpha, \beta \in \mathbb{C}$ and satisfy the condition as follows :

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3.9}$$

This normalization ensures that the total probability of finding the qubit in either state is one.

Note that this notation is difficult to visualize. In order to provide a more intuitive geometrical interpretation of a Qubit, the Bloch sphere representation is used.

Définition 8 (Bloch Sphere)**.** *The Bloch sphere [20] [36] is a three-dimensional unit sphere allowing any pure qubit state to be represented as a point located on its surface.*

Using this representation, the general qubit state can be rewritten as:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{3.10}$$

where:

- $\theta \in [0, \pi]$ determines the position of the quantum state between the north and south poles of the Bloch sphere,
- $\phi \in [0, 2\pi]$ represents the relative phase between the two computational basis states.

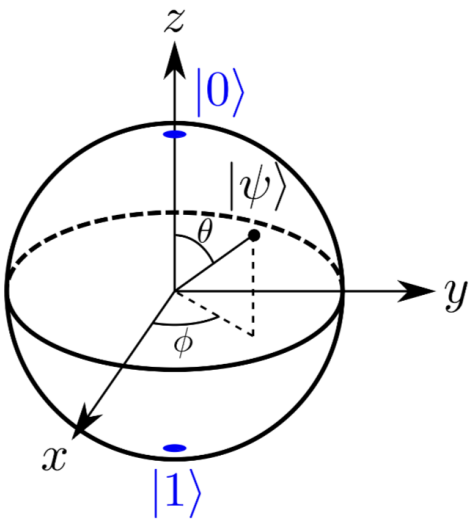

Figure 3.5: Bloch Sphere Representation
[36]

3.3. Measurement

As described in the subsection "superposition" , before measurement the quantum state of a Qubit is written as follows:

$$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle \tag{3.11}$$

Measurement alters the quantum state and results in probabilistic outcome. [2] After measurement, the quantum state of the Qubit collapses in order to give a certain outcome (specific state: either $|0\rangle$ or $|1\rangle$) according to the probability of observing one of the states mentioned in the linear combination equation (3.8). Note that quantum measurement is irreversible.

3.4. Heisenberg Uncertainty Principle

The Heisenberg Uncertainty Principle [13] [17] states that it is impossible to know everything about Quantum properties of an object. In particular, two complementary observables cannot be measured simultaneously with precision. Indeed, measuring one of these observable destroys the information of the other. Consequently, it limits the amount of information that can be obtained about quantum physical properties of the matter. Measurement implies system perturbation.

As an exemple, if a mass m is moving along a trajectory with velocity v, it is impossible to know exactly and simultaneously its position and its momentum $p = m \cdot v$
Let Δx, the uncertainty in position x and Δp, the uncertainty in momentum p, we have :

$$\Delta x \cdot \Delta p \geq \frac{h}{4\pi}. \tag{3.12}$$

with $h = 6,626 \cdot 10^{-34} J \cdot s$ denoting the Planck constant.
Since the momentum can be expressed as $p = mv$, it follows that $\Delta p = m \cdot \Delta v$. Therefore, the inequality can also be written as:

$$\Delta x \cdot \Delta v \geq \frac{h}{4\pi m} \tag{3.13}$$

In BB84, the relevant principle is not primarily the position-momentum uncertainty relation, but the impossibility of perfectly distinguishing non-orthogonal quantum states and the disturbance induced by measurements performed in an incompatible basis. Consequently, an eavesdropper who measures photons in an inappropriate basis introduces detectable errors in the sifted key, which can be revealed through the estimation of the Quantum Bit Error Rate (QBER)[1].

[1]QBER will be discussed later on with the section 5.3 QKD Security and Reliability

4 Quantum Information Principles

4.1. The No-Cloning Theorem

The no-cloning theorem is one of the central principles of quantum information theory. It states that an arbitrary unknown quantum state cannot be copied perfectly.

More formally, there exists no universal unitary operation U such that, for any arbitrary quantum state $|\psi\rangle$ and a fixed initial blank state $|0\rangle$, the following transformation holds:

$$U\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{4.1}$$

The implications of the no-cloning theorem are particularly significant in the context of Quantum Key Distribution (QKD). Any attempt by an eavesdropper to duplicate a transmitted quantum state inevitably introduces disturbances due to the measurement process, thereby altering the state. As a consequence, legitimate parties can detect the presence of an adversary.

4.2. Entanglement

Quantum entanglement [40] [38] is a phenomenon observed in quantum mechanics in which the quantum state of two objects must be described globally.
When quantum objects are placed in an entangled state, correlations exist between the observed physical properties of these objects. Thus, although the entangled objects O_1 and O_2 are separated by large spatial distances, they are not independent, and the system $\{O_1, O_2\}$ must be considered as a single physical system.

The simplest set of maximally entangled states of two Qubit is the Bell states [35]. The former constitute one of the most fundamental objects in quantum information theory and are denoted as follows :

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \end{aligned} \tag{4.2}$$

Measuring the first Qubit implies knowledge about the second Qubit.

As an example, let's consider the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

1. If the measurement outcome is 0, the second Qubit is also 0;
2. If the measurement outcome is 1, the second Qubit is also 1.

Quantum entanglement has significant applications in Quantum Key distribution entanglement-based protocols.

Concerning entangled states, a fundamental concept is based on Bell inequalities. These inequalities must be satisfied by any local hidden variable theory. As seen before, the outcomes of quantum measurements are probabilistic. However, quantum entanglement gives rise to strong correlations between measurement outcomes of two intricated objects O_1 and O_2, which cannot be explained by classical local models.

Two main classes of interpretations have been proposed:

- **Non-local theories.**

  These approaches allow for correlations that cannot be explained by local mechanisms. These correlations do not imply the existence of any faster-than-light signaling.

- **Hidden variable theories.**

  These theories assume that quantum mechanics is incomplete and that additional variables determine measurement outcomes. Bell inequalities specifically rule out local hidden variable theories, although certain non-local hidden variable models remain theoretically possible.

Bell inequalities provide a mathematical framework to test these hypotheses through statistical correlations between measurement outcomes. Their experimental violation demonstrates that nature cannot be described by any local hidden variable theory. The most commonly used formulation of Bell inequalities in experimental contexts is the Clauser–Horne–Shimony–Holt (CHSH) inequality. It is expressed as:

$$|S| = \left|E(a,b) + E(a,b') + E(a',b) - E(a',b')\right| \leq 2 \tag{4.3}$$

where:

- a, a' denote the measurement settings chosen by the first observer (Alice),
- b, b' denote the measurement settings chosen by the second observer (Bob),
- $E(a,b)$ represents the correlation coefficient between the measurement outcomes, taking values in the interval $[-1,1]$.

In any local hidden variable theory, the CHSH parameter satisfies the bound:

$$|S| \leq 2 \tag{4.4}$$

A value of $S > 2$ therefore indicates a violation of Bell inequalities and demonstrates that the observed correlations cannot be explained by any local classical model.
Entanglement-based protocols such as E91 use the degree of violation of the CHSH inequality as a test of security.

5 Quantum Key Distribution

5.1. Overview of Quantum Key Distribution

5.1.1 Generalities

Quantum Key Distribution (QKD) provides a mechanism for establishing a secure cryptographic key between two parties. It enables the generation of symmetric key material [1]by using quantum properties of light, as well as modern optical technologies such as fiber optics and free-space transmission systems.
In most implementations, the information is encoded either in the polarization states or in the relative phase of photons.

One of the advantages of polarization-based encoding is its robustness during propagation through the atmosphere. This allows for long-distance transmission, reaching approximately 1200 km in satellite-to-ground communication scenarios.

Quantum cryptography relies on two distinct communication channels [2] [38]:

1. **Quantum channel:**

   This channel is used to transmit quantum states (typically photons) that carry information according to the laws of quantum mechanics and corresponds to the first stage of QKD protocols.
   The objective of the first stage is for two parties, commonly denoted as Alice (A) and Bob (B), to establish a *raw key*, denoted K_A and K_B, respectively. At this stage, the generated key is only partially secure and may contain errors due to noise in the quantum channel and imperfections in the physical devices.

[1]QKD systems continuously and randomly generate new private keys, which are automatically shared between the communicating parties.

2. **Classical channel:**

   This channel is used for classical communication between the parties and correspond to the second stage of QKD protocols.
   It is used for:

   (a) Authentication procedures

   (b) Classical cryptographic protocols

   (c) Post-processing steps [2]such as :

      i. sifting and error Estimation in order to extract a consistent subset of the raw key. for each transmission round, Alice and Bob publicly disclose the basis used for state preparation and measurement.

         - If their bases differ, the corresponding bit is discarded.
         - If their bases match, the resulting bit is kept and appended to their respective raw keys.

      ii. Error Correction in order for Alice (A) and Bob (B) to agree on a single final key

      iii. Privacy amplification in order to minimise eavesdropper's information

In order to better understand the diversity of existing QKD schemes, the next section presents a general classification of QKD protocols.

5.1.2 QKD Classifications

QKD protocols can be classified [40] [38] [8] into two types :

1. **Discrete-Variable QKD (DV-QKD)**

   In DV-QKD protocols, information is encoded in discrete quantum states, typically using single photons.

2. **Continuous-Variable QKD (CV-QKD)**

   In CV-QKD protocols, information is encoded using quadratures of the electromagnetic field.

Two approaches in QKD co-exist: [44].

1. **The prepare-and-measure protocols**

Prepare-and-measure protocols is a class of quantum key distribution schemes in which one legitimate party (Alice) prepares quantum states encoding classical information and transmits them to another party (Bob) through a quantum channel. Bob performs measurements on the received states using randomly chosen measurement settings. The correlations between the prepared and measured data are then processed via classical post-processing steps (sifting, error correction, and privacy amplification) to extract a shared secret key.

From a theoretical point of view , the security of prepare-and-measure protocols relies on fundamental quantum properties such as the no-cloning theorem and the disturbance induced by measurement. Any eavesdropping attempt inevitably introduces detectable errors in the transmitted quantum states, allowing the legitimate parties to estimate the level of information leakage.

2. **The Entanglement-based protocols**

Entanglement-based protocols form another class of QKD protocols in which the secret key is generated from measurements performed on entangled quantum systems.
Indeed, a source emits pairs of entangled particles and distributes one particle to Alice and the other one to Bob. Each party then performs local measurements on their own subsystem, using measurement bases that are chosen independently.

The interest of this approach lies in the fact that the measurement outcomes can exhibit correlations. These correlations can be exploited to establish a shared secret key between Alice and Bob.

From a security point of view, entanglement plays a central role because the violation of Bell inequalities can reveal whether the observed correlations are compatible with genuine quantum behaviour. If an eavesdropper interacts with the quantum systems, these correlations may be disturbed, which can make the intrusion detectable.

The following table [8] highlights typical QKD protocols.

Table 5.1: Summary of Typical QKD Protocols

Protocol	Type	Approach	Year
BB84	DV	Prepare-and-measure	1984
E91	DV	Entanglement-based	1991
BBM92	DV	Entanglement-based	1992
GG02	CV	Prepare-and-measure	2002
DPS	DV	Prepare-and-measure	2002
Decoy-state	DV	Prepare-and-measure	2003–2005
SARG04	DV	Prepare-and-measure	2004
COW	DV	Prepare-and-measure	2005
MDI	DV/CV	Prepare-and-measure	2012
TF	DV	Prepare-and-measure	2018
PM	DV	Prepare-and-measure	2018

As we can see from the table 5.1, BB84 can be considered the starting point of modern QKD, as many later protocols either extend or adapt its original security principles.

5.2. Physical Layer of a QKD System

5.2.1 Photon Sources and Photon Detection

As the prepare-and-measure protocol such as BB84 uses photons as information vector, it is relevant to discuss the photon source and the photon detector.

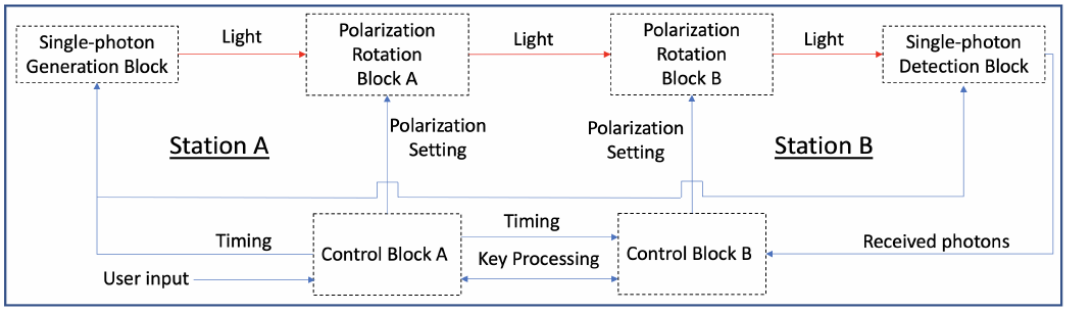

Figure 5.1: Functional Organization of a QKD Demonstration Apparatus [7]

The figure (5.1) presents the functional organization of a QKD demonstration apparatus [7]. The system is divided into two main stations:

1. **Station A** performing photon generation and state preparation
2. **Station B** performing photon reception, measurement, and detection.

The purpose of this section is not to describe the complete QKD protocol, but to illustrate the physical layer involved in photon generation and photon detection. For this reason, the discussion focuses on the Single-Photon Generation Block and the Single-Photon Detection Block.

1. **Single-Photon Generation Block.**

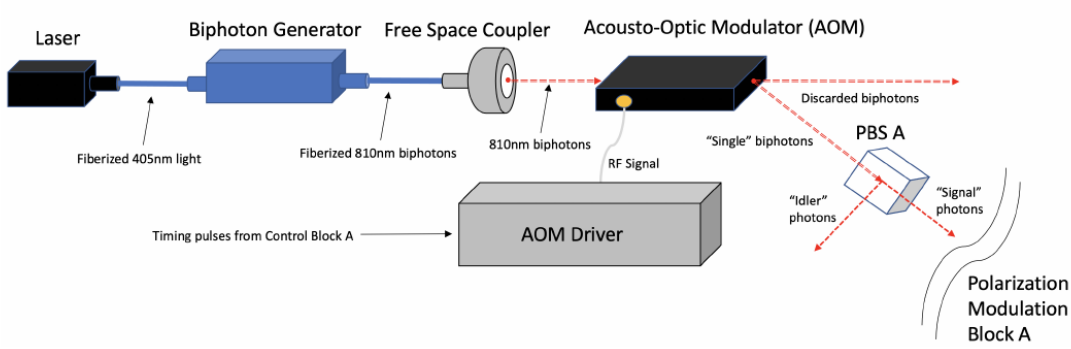

Figure 5.2: Single-Photon Generation Block
[7]

The Single-Photon Generation Block is the starting point of the apparatus. Its role is to provide the photons used during the key generation process. This block contains a laser and a biphoton generator that produce a continuous stream of biphotons.

Laser. The laser provides the 405 nm optical pump used to feed the biphoton generator.

Biphoton generator. The biphoton generator converts part of the incident pump light into 810 nm biphotons, which are subsequently routed toward the rest of the optical setup.

Acousto-optic modulator. (AOM) The acousto-optic modulator acts as a fast optical shutter, selecting photons during controlled time windows defined by the control electronics.

Polarizing beam splitter. PBS A acts as a polarization-selective optical element. It transmits the horizontal polarization component and reflects the vertical polarization component. Consequently, when a degenerate biphoton pair arrives at PBS A, the two photons are separated according to their orthogonal polarization states. Only one photon is retained in the useful optical path, while the other is discarded. The retained photon therefore constitutes the single polarized photon delivered by the Single-photon Generation Block before entering Polarization Rotation Block A

2. **Single-Photon Detection Block.**

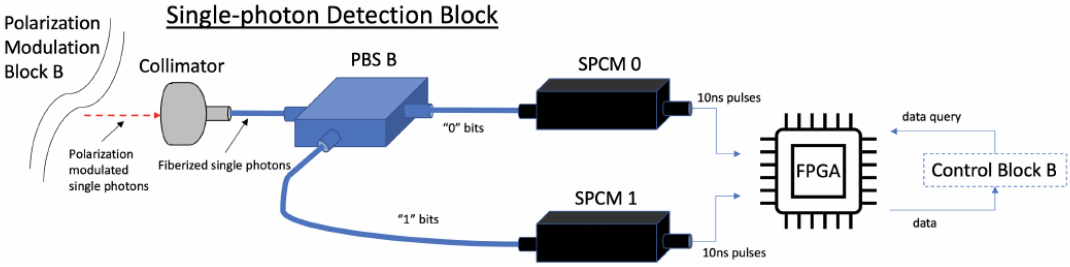

Figure 5.3: Single-Photon Detection Block
[7]

The **Single-Photon Detection Block** converts the incoming optical information into detection data. This block consists of a beam collimator, PBS B, SPCMs 0 and 1 and an FPGA. Photons entering this block are first coupled into a single-mode optical fiber, which directs them to a fiberized polarizing beam splitter. Let's have a closer look at the components in order to understand how it works.

Collimator The Collimator converts the diverging optical beam into a nearly parallel beam.

PBS B The PBS separates photons according to their polarization. Photons aligned with the pump-laser axis are transmitted toward one detector, whereas orthogonally polarized photons are reflected toward the other detector. Photons with intermediate polarization angles are distributed according to the corresponding weighting factor.

SPCMs These components are the photon-counting detectors. This is a silicon-based avalanche photodiode detectors. Their role is to generate an electrical signal when a photon is detected. This allows the optical event to be converted into an electronic event that can be processed by the control system.

FPGA receives the electrical pulses generated by the SPCMs. Its utility is to detect and record the short pulses coming from the detectors during the relevant control window. Particularly, It allows the data acquisition.

5.2.2 Coherent Optical State Source And Detection

As prepare-and-measure protocols such as GG02 encode information into the continuous quadratures of coherent optical states, it is relevant to discuss the generation and detection of these optical properties.

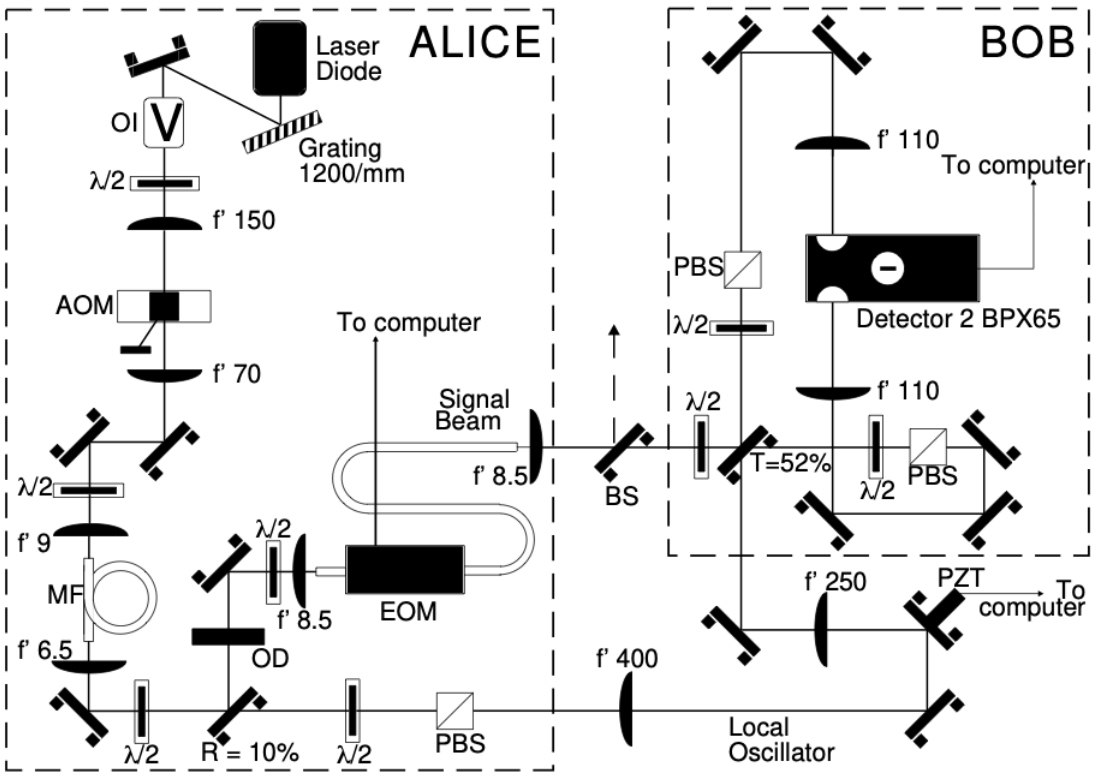

Figure 5.4: Generator And Detector Of Coherent Optical State apparatus [18]

1. **Generator**

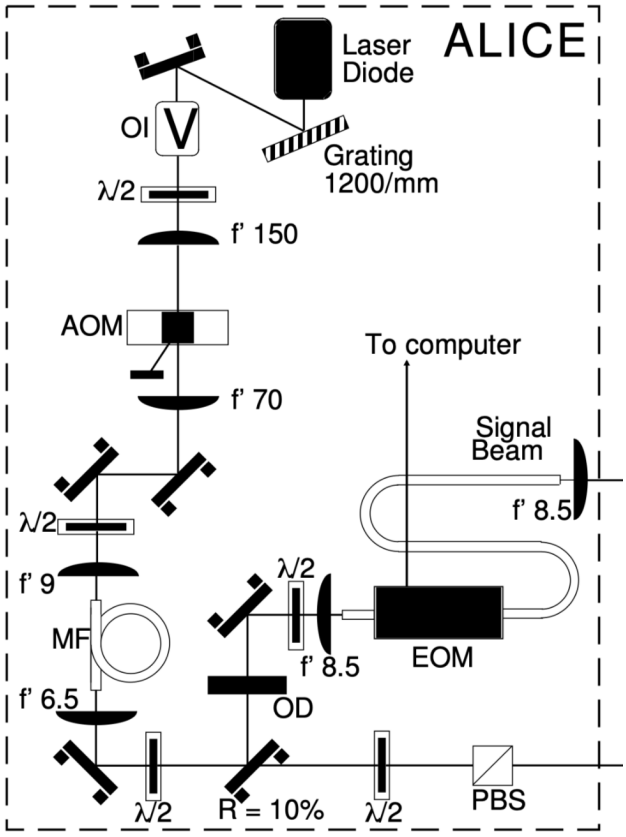

Figure 5.5: GG02 State Preparation Apparatus
[18]

Let's have a closer look at the components highlighted in the Figure 5.5 representing the state preparation apparatus.

The optical field is first generated by a continuous-wave laser diode.
The grating-extended cavity contributes to improving the spectral stability of the source
The optical isolator prevents back-reflections from reaching the laser diode.
The acousto-optic modulator (AOM) is used to carve the continuous beam into optical pulses.

After spatial filtering through a single-mode fibre, the optical beam is divided into two paths.

(a) the first path contains the signal beam. This is where the information encoded by Alice is ;

(b) The second path contains the local oscillator

The electro-optic modulator (EOM) In the GG02 protocol, Alice generates two random variables, denoted x_A and p_A, according to a centred Gaussian distribution with variance $V_A N_0$:

$$x_A, p_A \sim \mathcal{N}(0, V_A N_0), \tag{5.1}$$

where:

- V_A is the modulation variance
- N_0 denotes the shot-noise variance.

These two variables are associated with the two field quadratures. The value x_A corresponds to the in-phase quadrature, while p_A corresponds to the phase quadrature.
The electro-optic modulator is used to modulate the optical pulses according to these Gaussian variables. In this way, Alice prepares a coherent state of the form:

$$|x_A + ip_A\rangle \,. \tag{5.2}$$

The lenses denoted by their focal lengths f', allow the beam to be focused, collimated or mode-matched through the different optical components.

The half-wave plates $\lambda/2$ adjust the linear polarization of the field, ensuring proper alignment with the polarizing elements and with the modulation apparatus.

The prepared Gaussian-modulated coherent pulses are then transmitted through the quantum channel toward Bob.

2. **Detector**

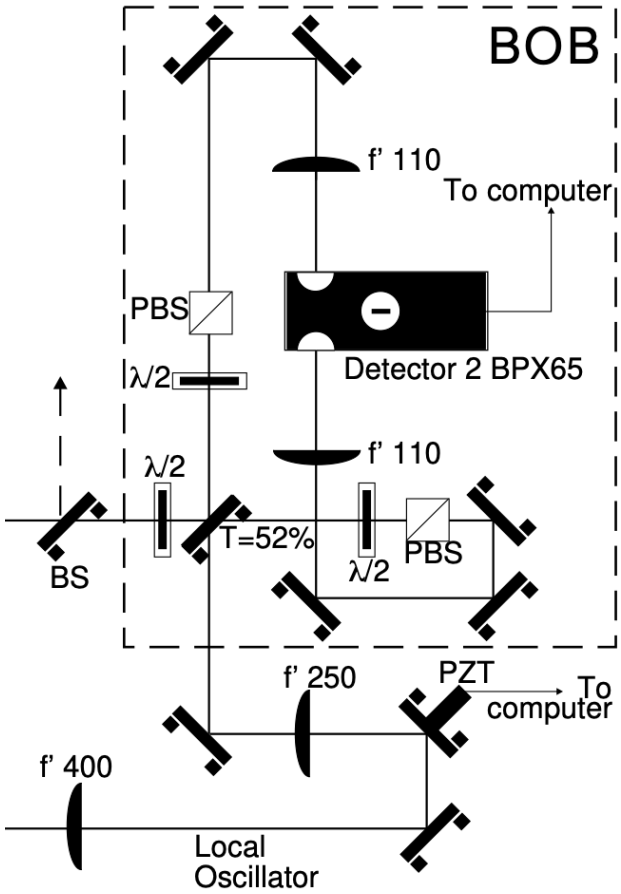

Figure 5.6: GG02 State Detection Apparatus
[18]

For each received state, Bob randomly measures one of the two quadratures and records the corresponding measurement result.To do so, Bob uses the Homodyne Detetector apparatus. The Figure 5.6 represents a setup for homodyne detection.

The incoming quantum signal is combined with a strong Local Oscillator (LO) using a beam splitter. The interference between the signal and the LO allows the extraction of quadrature information from the optical field.

Several polarization control components are used in the setup.

Let's have a look at the components.
Polarizing Beam Splitters (PBS) separate orthogonal polarization components.

Half-wave plates ($\lambda/2$) rotate the polarization state in order to maximize interference visibility and optimize alignment conditions.

A piezoelectric transducer (PZT) is employed to precisely control the optical phase difference between the signal and the local oscillator. This phase stabilization is essential because the measured quadrature depends directly on the relative phase between both optical fields.

BPX65 photodiodes The optical signal is detected using photodetection. The photodiodes measure the optical intensities associated with the two output ports. The corresponding photocurrents are electronically amplified and subtracted, leading to a balanced detection scheme. The differential photocurrent is given by:

$$I_- = I_t - I_r \tag{5.3}$$

This subtraction suppresses common classical noise contributions originating from the laser source and isolates the interference term between the signal and the local oscillator.
Assuming that the local oscillator intensity is much larger than the signal intensity, the differential signal becomes proportional to the field quadrature:

$$I_- \propto |\alpha_{LO}| X_\phi \tag{5.4}$$

Where

- $|\alpha_{LO}|$ is the amplitude of the local oscillator
- $X_\phi = X\cos\phi + P\sin\phi$ is the generalized field quadrature. The phase ϕ imposed by the PZT determines which quadrature is measured. For instance:

$$\phi = 0 \Rightarrow X_\phi = X \tag{5.5}$$

$$\phi = \frac{\pi}{2} \Rightarrow X_\phi = P \tag{5.6}$$

5.2.3 Quantum Transmission Medium

A QKD link [8] relies on two communication channels:

1. A quantum channel, used to transmit quantum states,
2. A classical channel, used for public information exchange during the protocol.

Both channels may be publicly accessible, but their communications must be authenticated in order to prevent impersonation or man-in-the-middle attacks.

In practice, quantum signals are significantly more fragile than classical optical signals. Indeed, they are affected by propagation impairments such as :

1. attenuation,
2. scattering,
3. noise in optical fibers,
4. atmospheric turbulence in the case of free-space links.

Unlike classical signals, quantum states cannot be straightforwardly amplified, since amplification would require extracting information about the state (measurement) and effectively copying it. Let's remember, measurement make the quantum state collapse and copying a quantum state is forbidden by the no-cloning theorem as seen before.

At this point, it is relevant to discuss about the two existing QKD links.

5.2.3.1 Optical-Fiber QKD

Optical fibers is the most mature transmission medium for QKD. Their relatively low attenuation and high stability make them suitable for controlled point-to-point quantum communication. Experimental demonstrations have progressively increased both the achievable transmission distance and the secret-key rate. Fiber-based QKD has reached secret-key rates in the Mbps range over metropolitan distances, while long-distance demonstrations have extended the range to several hundred kilometres.

An advantage of fiber-based QKD is its compatibility with existing telecommunication infrastructures, which facilitates practical deployment and reduces implementation costs. Commercial QKD systems based on optical fiber are already available. However, the distance of point-to-point fiber QKD remains fundamentally constrained by optical loss and noise accumulation. Moreover, fiber deployment may be difficult or economically impractical across geographical obstacles such as rivers, mountains, or remote areas.

5.2.3.2 Free-Space QKD

Free-space QKD offers complementary advantages, notably large coverage, flexible link reconfiguration, and the possibility of satellite-based distribution. Experimental results have demonstrated QKD through atmospheric channels, including aircraft-to-ground, satellite-to-ground, daylight free-space transmission, and even underwater or air-water quantum communication scenarios.

One of the main reasons for considering free-space QKD is that the limitations of the transmission channel are different from those encountered in optical fibers.
Indeed, in a fiber-based link, attenuation increases very rapidly with distance, which makes long-distance QKD difficult without trusted nodes or additional technological solutions. In free space, the situation is different: the losses are mainly caused by beam divergence, atmospheric perturbations, and imperfect alignment. When the transmission takes place above the atmosphere, for example in a satellite link, absorption and scattering can be significantly reduced. This explains why satellite-assisted QKD is often presented as a promising path toward long-distance, and potentially global, quantum-secure communication.

5.2.3.3 Conlusion

Fiber-based QKD currently provides the most mature and deployable solution for short- and medium-distance applications, whereas free-space QKD offers a promising route toward wide-area and global quantum networks. The integration of both media is therefore a plausible architecture for future large-scale QKD infrastructures.

The following table [8] allows the reader to have a comparison between the optical-fiber QKD and free-space QKD:

Table 5.2: Optical Fiber vs. Free Space for QKD

	Optical fiber	**Free space**
Stability	High	Low
Flexibility	Low	High
Maturity	High	Low
Cost	Low	High
Commercialization	Available	Unavailable
Achievable distance without relaying	605 km (104.8 dB)	1,200 km (<33 dB)
Future direction	Complement each other towards a global network	

5.3. QKD Security and Reliability

5.3.1 Generalities

The security of Quantum Key Distribution (QKD) [2] is fundamentally based on the laws of quantum mechanics rather than on computational assumptions. In contrast to classical cryptographic systems, whose security relies on the presumed hardness of mathematical problems, QKD guarantees security against adversaries limited only by the laws of physics.

A fundamental property of QKD is its ability to detect any eavesdropping attempt by an adversary. Indeed, due to the principles of quantum mechanics, any measurement performed on the quantum states disturbs them, thereby revealing the presence of an interceptor. The more information an adversary attempts to extract, the higher the induced noise, increasing the probability of detection.

During the post-processing phase of QKD, error correction and parameter estimation are essential steps to ensure the reliability and security of the generated key. A subset of size m of the raw key is randomly selected and publicly disclosed by one of the parties. This subset is used to perform *parameter estimation*, allowing both parties to evaluate the noise characteristics of the quantum channel. By comparing their measurement outcomes, Alice and Bob establish statistical properties of the channel. In particular, they estimate the probability that a quantum state prepared in a given basis is incorrectly measured, which is interpreted as noise.

5.3.2 Assumptions and Limitations of QKD

Although Quantum Key Distribution is presented as a cryptographic approach that reduces the dependence on computational hardness assumptions, it does not provide security without any assumptions [3]. Its security relies on several physical, theoretical and implementation-related hypotheses. These assumptions vary depending on the protocol considered. Some of them can be discussed independently of a specific QKD scheme.

1. **Validity of quantum theory.**

   QKD security is fundamentally based on the assumption that quantum theory correctly describes the behaviour of physical systems involved in the protocol. It is assumed that the mathematical structure of quantum mechanics accurately predicts the outcome of quantum measurements. This assumption is supported by a large number of experimental results.

2. **Completeness of quantum theory.**

   Completeness means that there is no deeper physical theory that would allow an adversary to predict measurement outcomes more accurately than quantum mechanics permits.

3. **Absence of unintended information leakage.**

   Practical QKD implementations also require the assumption that the devices used by Alice and Bob do not leak relevant secret information outside the intended protocol operations. This concerns several components, including single-photon detectors, quantum random number generators, optical modulators, lasers, control electronics and the classical computer used to store or process the raw key.

   For instance, if the raw key stored on a classical computer were unintentionally leaked through an implementation flaw or a side channel, the theoretical security of the QKD protocol would no longer be sufficient. In practice, this requires appropriate hardware protection, shielding and careful implementation.

4. **Existence of an authenticated classical channel.**

   A fundamental requirement is the existence of an authenticated classical communication channel.
   Indeed, after the quantum transmission phase, Alice and Bob must exchange classical information in order to perform basis reconciliation, error estimation, error correction and privacy amplification. If this classical channel is not authenticated, an adversary could perform a man-in-the-middle attack by impersonating Alice to Bob and Bob to Alice.

5. **Correctness of the protocol implementation.**

   The validity of a QKD security proof depends on how closely the real implementation follows the assumptions of the theoretical model.
   If some devices behave differently from what is assumed, for example if detectors do not have identical efficiencies, the proof may no longer fully apply. Such imperfections can create exploitable side channels.
   Therefore, the security of a QKD system depends not only on the protocol itself, but also on the correctness and reliability of its practical implementation.

6. **Technological assumptions for long-distance communication.**

   Long-distance QKD is limited by the attenuation and noise affecting quantum signals in optical fibres or free-space channels. To extend the transmission range, approaches such as quantum repeaters and trusted nodes can be considered. Quantum repeaters would preserve the quantum nature of the communication, but they remain technologically difficult to deploy at large scale. Trusted nodes are more mature in practice, but they introduce an additional security assumption, since the intermediate nodes must be trusted.

In conclusion , QKD should be understood as a cryptographic paradigm whose security is theoretically strong, but whose practical reliability depends on well-identified physical and engineering conditions.

5.3.3 The Quantum Bit Error Rate (QBER)

Security and reliability leads to the definition of the Quantum Bit Error Rate (QBER).

Définition 9. *The QBER is defined as the probability that a quantum state prepared in a given basis and measured in the same basis yields a different outcome than the one initially encoded.*

$$\text{QBER} = \Pr(\text{measured bit} \neq \text{sent bit})$$

A high QBER indicates either the presence of noise in the quantum channel or a potential eavesdropping attempt. The acceptable QBER threshold depends on the specific QKD protocol and its implementation.
if the estimated noise level remains below the acceptable threshold, Alice and Bob proceed with an error correction phase in order to reconcile their raw keys.

For instance, in the BB84 protocol, the tolerable QBER is typically around 11%, although under certain conditions it may reach values close to 20%. Under a simplified noise model, the QBER can be expressed as [16] [28]:

$$e_{84} = \frac{c\, p_{\text{signal}} + \frac{1}{2}\left(p_{\text{dark}} + p_{\text{stray}}\right)}{p_{\text{click}}}. \tag{5.7}$$

Where

- c represents intrinsic optical or alignment error coefficient. It accounts for errors affecting genuine signal photons, for example due to imperfect polarization preparation, imperfect basis alignment, optical misalignment, or detector imperfections.
- p_{signal} denotes the probability that a detector click is caused by a genuine signal photon sent by Alice and received by Bob.
- p_{dark} denotes the probability of a dark-count event, i.e. a detector click occurring in the absence of an incident signal photon due to detector noise.
- p_{stray} denotes the probability of a detector click caused by stray light or background photons not originating from the intended quantum signal.
- p_{click} concerns the total probability that Bob's detector registers a click. It includes clicks caused by the intended signal as well as clicks caused by noise sources such as dark counts and stray light.

In order to minise the amount of information the eavesdropper would have , a privacy amplification is executed. The resulting key is shorter than the original raw key, as part of the information must be sacrificed to guarantee security.

5.3.4 QKD Attacks Overview

Considering the security analysis of QKD, there are three main classes of attacks as follows : [2]:

- **Individual attacks:** The adversary interacts independently with each quantum signal and measures immediately after the interaction.
- **Collective attacks:** The adversary interacts independently with each signal but may delay measurements and perform a collective quantum measurement at a later stage.
- **Coherent attacks:** The most general and powerful class of attacks, where the adversary performs a joint operation on all transmitted quantum systems simultaneously, exploiting the full power of quantum mechanics.

Here is a list of attacks' examples [14] [26]:

1. **Intercept-Resend Attack**

   The intercept-resend attack consists of an adversary, Eve, intercepting the photons transmitted by Alice, measuring them in a basis of her choice, and then sending newly prepared photons to Bob according to her measurement results. In the BB84 protocol, Eve does not know in advance which basis Alice used to prepare each quantum state. Consequently, Eve's measurement basis is chosen probabilistically.

   When Eve selects the wrong basis, her measurement disturbs the original quantum state and may introduce errors into the sifted key shared by Alice and Bob. These errors can be detected statistically by comparing a subset of the key or by estimating the quantum bit error rate. This attack illustrates a central feature of QKD: an unauthorized measurement of an unknown quantum state generally modifies the transmitted information and can therefore reveal the presence of eavesdropping.

2. **Faked State Attack** [11]

   The faked-state attack uses imperfections in the physical implementation of BB84 systems, particularly the avalanche photodiode (APD) detectors used by the receiver.
   Indeed, the attack relies on manipulating the APD detectors used by Bob.
   Under normal operating conditions, these detectors require a short recovery time before they are able to detect another photon. However, it was shown that continuous illumination can prevent the detector from properly recharging, causing it to behave as a classical photodiode rather than as a quantum detector. In this state, the detector may either be blinded or forced to produce detection events under the control of the attacker.

   In the faked-state attack, Eve first intercepts the photon transmitted by Alice and performs her own measurement. She then prepares and sends a so-called "faked state"[2] to Bob. Indeed, the attack strategy consists in preparing the opposite bit value in the opposite measurement basis with respect to Eve's own measurement result.

[2]The term "faked" refers to the fact that Eve does not transmit a genuine quantum state, but instead manipulates Bob's detection apparatus so that it behaves as if a valid quantum state had been received.

For instance, if Eve measures bit 0 in the X basis, she prepares bit 1 in the Z basis before sending the signal to Bob. Simultaneously, Eve blinds selected detectors in Bob's apparatus. As a result, if Bob measures in the same basis as Eve, he may detect the bit chosen by Eve or obtain no detection event. Conversely, if Bob measures in a different basis, no valid detection occurs.

3. **Man-in-the-Middle Attack**

   A man-in-the-middle attack becomes possible when the QKD communication process is not properly authenticated. Without authentication, Alice and Bob cannot reliably verify whether they are communicating with each other or with an adversary positioned between them. Eve may therefore impersonate Bob when communicating with Alice and impersonate Alice when communicating with Bob.

   This attack demonstrates that QKD cannot be considered secure if the classical communication channel is unauthenticated.

4. **Photon Number Splitting Attack**

   The photon number splitting attack arises from the difficulty of producing ideal single-photon sources.
   Indeed, in practical QKD systems, weak coherent pulses are frequently used instead of true single-photon emitters. The number of photons contained in each pulse follows a probabilistic distribution, which means that some pulses may contain more than one photon.

   In practical, when a multi-photon pulse is emitted, Eve can intercept one photon while the remaining photons continues toward Bob. These remaining photons carry the same quantum information as the stolen one. She can store the intercepted photon until Alice and Bob publicly disclose their basis choices. Once this information is available, Eve can measure her photon in the correct basis and obtain information about the key without introducing detectable errors.

5.3.5 Attack Prevention

As in any branch of cryptography, attacks and countermeasures are closely related in Quantum Key Distribution [14] [26] . Over the last decades, the QKD community has investigated attacks, vulnerabilities, imperfections, and the corresponding strategies intended to prevent them or mitigate their consequences. In some cases, a given countermeasure does not only address a single attack, but can protect an entire class of QKD protocols or implementations.

Several practical attacks against QKD systems rely on the use of bright light pulses by an eavesdropper. For this reason, modifications at the level of the physical apparatus may be required. In the case of photon-number-splitting attacks, the use of a true single-photon source is preferable to an attenuated laser source.

To mitigate the **PNS attack**, the decoy-state method was introduced as an efficient countermeasure. The main idea consists in randomly varying the intensity of the emitted optical pulses during the quantum transmission phase. In addition to the standard signal states used to generate the secret key, the transmitter also sends decoy states with different average photon numbers.

These decoy states are prepared such that they are indistinguishable from the signal states in every aspect except their photon-number statistics.

Since an eavesdropper cannot determine whether a given pulse corresponds to a signal state or to a decoy state, any selective attack targeting multi-photon pulses inevitably modifies the statistical behavior of the transmitted signals. After the quantum transmission, the transmitter publicly reveals which pulses corresponded to decoy states. Using the observed detection and error rates associated with the different pulse intensities, the legitimate users can estimate the behavior of single-photon events and detect inconsistencies caused by a potential PNS attack.

The decoy-state method does not physically block an eavesdropper from interacting with the quantum channel. Its role is rather to make certain attacks statistically visible by comparing the behaviour of signal and decoy pulses. If the observed transmission rates are inconsistent with the expected behaviour, Alice and Bob can suspect a manipulation of the channel. For this reason, decoy states are widely used as a practical security enhancement in modern DV-QKD systems.

Another important family of countermeasures is based on interference-based QKD [26] . Here comes the Measurement-Device-Independent Quantum Key Distribution [3] (MDI-QKD) which allows to mitigate the **faked state attack**.
In these schemes, quantum-optical interference is central to the distribution of quantum correlations over long distances. Quantum signals are prepared by two QKD transmitters and sent through quantum channels to a relay station that contains the measurement apparatus. A major advantage of this approach is that the security of the protocol does not rely on trust assumptions concerning the measurement devices, especially the detectors. The relay station itself may even be entirely controlled by an eavesdropper without compromising the security framework of the protocol. Consequently, attacks targeting imperfections in the detection system, such as the faked-state attack presented previously, do not provide a practical advantage to Eve in these implementations.

Post-processing countermeasures are also essential. Privacy amplification can be used to remove information that may have leaked to Eve. This process reduces the length of the key available for encryption, but ensures that Eve has no information about the final key. In practical QKD, this is important because it takes into account deviations between theoretical security assumptions and real implementations.

In addition to these countermeasures, practical QKD security also requires taking into account the finite amount of data available during a real protocol execution.
Indeed, in practical QKD systems, the number of exchanged quantum signals is finite. Therefore, channel parameters such as QBER, transmission, or excess noise cannot be estimated with perfect precision. Finite-key analysis accounts for statistical fluctuations due to limited sample sizes and adjusts the final key length accordingly. This aspect is essential in practical security proofs, although a detailed mathematical treatment is beyond the scope of this exploratory thesis.

It is important to note that the classical communication channel used in QKD must be authenticated. Although the quantum channel allows the detection of eavesdropping attempts through measurement-induced disturbances, it does not guarantee the identity of the communicating parties. Without authentication, an adversary could perform a man-in-the-middle attack by

[3] Measurement-Device-Independent Quantum Key Distribution will be discussed later on with the section QKD main protocols

impersonating each party to the other. Therefore, QKD establishes secret key material only under the assumption that the classical channel is authenticated.

5.4. Quantum Key Distribution Protocols

From now on, four selected illustrative QKD protocols will be discussed. These protocols are selected because of their representativeness and their ability to illustrate the principal operating paradigm encountered in QKD.

5.4.1 BB84

The BB84 [5] [27] [37] [23]protocol was introduced in 1984 by Bennett and Brassard. BB84 is considered the first practical Quantum Key Distribution (QKD) protocol. Its objective is to allow two distant parties, traditionally called Alice and Bob, to establish a shared secret cryptographic key while being able to detect the presence of an eavesdropper. The protocol relies on fundamental principles of quantum mechanics, especially the impossibility of perfectly measuring or copying an unknown quantum state without disturbing it.

In the BB84 protocol, information is encoded onto single photons using two conjugate polarization bases. The first basis is the rectilinear basis, represented by the states :

$$|0\rangle, |1\rangle \tag{5.8}$$

while the second one is the diagonal basis, represented by

$$|+\rangle,\ |-\rangle \tag{5.9}$$

Where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},\ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

In practical polarization-based implementations, these quantum states correspond to different photon polarizations. The states $|0\rangle$ and $|1\rangle$ are usually associated with horizontal and vertical polarizations, whereas $|+\rangle$ and $|-\rangle$ correspond to $+45°$ and $-45°$ diagonal polarizations.

The operation of the BB84 protocol can be divided into two main stages:

1. **Stage 1**

   This stage corresponds to the quantum communication channel.

   (a) **Alice's side**

   Alice first generates a random binary sequence. For each bit, she randomly chooses one of the two polarization bases and prepares the corresponding quantum state. The prepared photons are then transmitted one by one through a quantum channel toward Bob.

(b) **Bob's side**

Upon reception, Bob independently and randomly chooses a measurement basis for each incoming photon. If Bob selects the same basis as Alice, the transmitted bit can be recovered correctly. However, if Bob measures the photon using the wrong basis, quantum mechanics predicts that the measurement outcome becomes completely random.

2. **Stage 2**

This stage corresponds to the classical communication channel.

(a) **Sifting process**

Bob announces the measurement basis used for each received photon, while Alice indicates which basis choices were correct. The bit values themselves are never revealed during this discussion.
Both parties then discard all events for which different bases were used. The remaining correlated bits form the so-called sifted key.

(b) **Error estimation**

Alice and Bob compare a small subset of their sifted key, this is where the quantum bit error rate (QBER) is computed. If the error rate exceeds a predefined threshold, the communication is considered insecure and the key is discarded.

(c) **Reconciliation**

The purpose of reconciliation is to transform Alice's and Bob's sifted keys into identical bit strings while minimizing the amount of information revealed over the authenticated classical channel. Since transmission noise, detector imperfections, or potential eavesdropping may introduce discrepancies between the two sifted keys, an error-correction procedure is required before generating the final secret key.

One of the most widely known reconciliation procedures used in Quantum Key Distribution is the Cascade protocol [41]. Cascade is an error-correction protocol based on parity comparisons and iterative binary searches. Although it is considered simple and efficient, its principal limitation lies in the large amount of classical communication required between Alice and Bob. Consequently, modern QKD implementations often favor LDPC [4]-based reconciliation schemes , which reduce the communication.

Cascade relies on a subprotocol called *BINARY*, whose objective is to localize a single erroneous bit inside a block containing an odd number of errors. Alice and Bob first divide their respective bit strings into smaller sub-blocks and compare the associated parity values over the authenticated public channel. Whenever two parities differ, this

[4]Low Density Parity Check. Although LDPC codes play an important role during the reconciliation phase of practical QKD systems, an in-depth analysis of their foundations would considerably extend the scope of this work. For further information the reader may refer to [29]

indicates the presence of an odd number of errors inside the considered sub-block. The same operation is recursively repeated until the erroneous bit is isolated and corrected.

The complete Cascade protocol is performed over several successive passes. During the first pass, Alice and Bob divide their sifted keys into blocks of predefined size and publicly exchange the parity associated with each block. For every block presenting different parity values, the BINARY procedure is executed in order to identify and correct one error.

Note that the recursive divisions performed during the BINARY procedure should not be confused with the successive passes of the Cascade protocol. The BINARY subprotocol is used locally to isolate an erroneous bit inside a given block, whereas a new pass corresponds to a global reshuffling of the sifted key into newly generated blocks in order to reveal previously undetected errors.

Although Cascade publicly reveals parity information, the actual values of the secret bits are never directly disclosed. Consequently, an eavesdropper only gains limited partial information regarding the reconciled key.

(d) **Amplification**

Privacy amplification [1] is then applied to reduce Eve's possible information about the reconciled key. Alice and Bob process the corrected key with a suitable hashing procedure, which compresses the bit string into a shorter one. Privacy amplification generally relies on hash functions, which map large input domains into smaller output domains. In practical QKD systems, families of Universal_2 hash functions are commonly employed. Instead of using a single deterministic hash function, one function is randomly selected from a predefined collection of hash functions. When properly designed, Universal_2[5] hash families provide strong security guarantees and ensure that any partial information potentially obtained by Eve becomes negligible after the compression process.

Algorithm 3 BB84 Protocol Quantum Communication

Input: Number of transmitted qubits n
Output: A sifted secret key shared between Alice and Bob
Alice generates a random bit sequence $A = (a_1, a_2, \ldots, a_n)$
Alice generates a random basis sequence $B_A = (b_1^A, b_2^A, \ldots, b_n^A)$
Bob generates a random basis sequence $B_B = (b_1^B, b_2^B, \ldots, b_n^B)$
for $i = 1$ to n **do**
    Alice prepares a quantum state $|\psi_i\rangle$ according to bit a_i and basis b_i^A
    Alice sends $|\psi_i\rangle$ to Bob through the quantum channel
    Bob measures the received quantum state using basis b_i^B
    Bob stores the measurement result as r_i
end for
Execute Phase 2 described in Algorithm 4

[5]Foundations underlying Universal_2 hash functions are not developed in detail in this thesis in order to preserve conciseness and maintain the focus on the overall operation of the BB84 protocol and its processing phases. For further information the reader may refer to [21]

Algorithm 4 BB84 Protocol Classical Communication

Input: basis sequence of Alice $B_A = (b_1^A, b_2^A, \ldots, b_n^A)$
Input: basis sequence of Bob $B_B = (b_1^B, b_2^B, \ldots, b_n^B)$
Bob publicly announces the basis sequence B_B
Alice publicly indicates the positions where $b_i^A = b_i^B$
Alice and Bob discard all positions where $b_i^A \neq b_i^B$
The remaining bits form the sifted key K_{sifted}
Alice and Bob publicly compare a small subset of K_{sifted}
They estimate the quantum bit error rate $QBER$
if $QBER$ is above the accepted threshold **then**
    Abort the protocol
else
    Keep the remaining bits as the shared key material
    Alice and Bob execute the reconciliation phase
    Alice and Bob executed the privacy amplification
end if

Algorithm 5 Cascade Reconciliation Protocol

Input: Alice's sifted key K_A, Bob's sifted key K_B, number of passes r
Output: Bob's corrected key $K_B^{corrected}$
for $i = 1$ to r **do**
    Choose a block size k_i
    Randomly permute the positions of K_A and K_B
    Divide K_A and K_B into blocks of size k_i
    for each block B_j **do**
        Alice computes the parity $P_A(B_j)$
        Bob computes the parity $P_B(B_j)$
        Alice and Bob publicly compare $P_A(B_j)$ and $P_B(B_j)$
        if $P_A(B_j) \neq P_B(B_j)$ **then**
            execute algorithm 6
        end if
    end for
end for
return $K_B^{corrected}$

Algorithm 6 BINARY Subprotocol

Input: A block B for which Alice's and Bob's parities differ
Output: Location and correction of one erroneous bit
while the size of B is greater than 1 **do**
  Divide B into two sub-blocks B_L and B_R
  Alice and Bob compare the parity of B_L
  if the parities of B_L differ **then**
    $B \leftarrow B_L$
  else
    $B \leftarrow B_R$
  end if
end while
Bob flips the remaining bit in B
return corrected bit

The BB84 protocol was selected for the detailed numerical illustration because it introduces the essential principles underlying most QKD protocols. Since many protocols rely on similar key distribution concepts while introducing more advanced implementation or security mechanisms.

BB84 protocol Application Example

Here is an example of BB84 application

Table 5.3: Results of a BB84 Application Example

	1	2	3	4	5	6	7
Quantum Communication							
Alice's transmission	−	|	\	/	\	−	/
Alice's bits	0	1	0	1	0	0	1
Bob's bases	+	+	×	×	×	+	×
Bob's measurement	−	|	\	/	\	−	\
Bob's bit	0	1	0	1	0	0	0
Sifted key after basis comparison							
Alice's key	0	1	0	1	0	0	1
Bob's key	0	1	0	1	0	0	0
Error estimation							
Publicly compared bits	0	1	0	1	0	0	1/0
Detected error							Yes
Reconciliation							
Bob's corrected key	0	1	0	1	0	0	1
Privacy amplification							
Final key	101						

1. **Quantum communication**

   This step corresponds to the first stage of the BB84 protocol.
   Alice first generates a random binary sequence and encodes each bit into a quantum state using one of the two polarization bases chosen at random. Bob then measures each received qubit using his own randomly selected measurement basis.

2. **Sifted key After basis comparison**

Alice and Bob publicly compare their measurement bases without revealing the bit values. Only the positions where both parties used compatible bases are retained. The sifted keys are:

$$K_A = 0101001$$

$$K_B = 0101000.$$

3. **Error estimation**

Alice and Bob then compare a subset of their sifted keys over the authenticated public channel in order to estimate the Quantum Bit Error Rate. In this illustrative example, the whole sifted key is compared to make the calculation explicit. There is one mismatch between Alice's and Bob's keys, located at the last bit:

$$K_A = 0101001$$

$$K_B = 0101000.$$

The number of compared bits being $n_{compared} = 7$ and the number of detected errors being $n_{errors} = 1$, the Quantum Bit Error Rate is:

$$QBER_{calculated} = \frac{n_{\text{errors}}}{n_{\text{compared}}} = \frac{1}{7} \simeq 0.1429 = 14.29\%.$$

Let's suppose this BB84 protocol application example's QBER thresholds is $QBER_{max} = 20\%$.

$14.29\% \leq 20\%$ implies the execution of the next steps of the protocol

4. **Reconciliation**

Consider the following sifted keys obtained by Alice and Bob :

$$K_A = 0101001$$

$$K_B = 0101000$$

The two keys differ by one bit located at the seventh position. The Cascade protocol is then used in order to identify and correct this discrepancy.

First phase :

Alice and Bob first choose a block size $k = 4$ and divide their sifted keys into two blocks.

$$\underbrace{0101}_{B_1}\ \underbrace{001}_{B_2}$$

$$\underbrace{0101}_{B_1}\ \underbrace{000}_{B_2}$$

They then compute and compare the parity associated with each block.
For the first block:

$$P_A(B_1) = 0 \oplus 1 \oplus 0 \oplus 1 = 0$$

$$P_B(B_1) = 0 \oplus 1 \oplus 0 \oplus 1 = 0$$

Since the parity values are identical, Alice and Bob conclude that no odd number of errors is present in the first block.

For the second block:

$$P_A(B_2) = 0 \oplus 0 \oplus 1 = 1$$

$$P_B(B_2) = 0 \oplus 0 \oplus 0 = 0$$

The parity values are different:

$$P_A(B_2) \neq P_B(B_2)$$

which indicates the presence of an odd number of errors inside the second block.

BINARY Procedure on the first phase :

Alice and Bob then execute the BINARY subprotocol on the second block:

001

000

The block is divided into two parts:

$$00 \mid 1$$

$$00 \mid 0$$

The parity of the first sub-block is computed:

$$0 \oplus 0 = 0$$

For both Alice and Bob, since the parity values are identical, the error is not located inside the first sub-block. Consequently, the erroneous bit is located in the second sub-block corresponding to the seventh position.
Bob therefore corrects his bit:

$$0 \to 1$$

After correction, Bob obtains:

$$K_B^{corrected} = 0101001$$

Thus:

$$K_A = K_B^{corrected}$$

5. **Privacy amplification**

Even after reconciliation, some information may have been revealed during the public discussion. Privacy amplification therefore compresses [a] the reconciled key into a shorter final key. In the example, the reconciled key contains: $n_{\text{rec}} = 7$ bits. It is compressed into a final key of length $n_{\text{final}} = 3$.
The compression ratio is therefore:

$$r = \frac{n_{\text{final}}}{n_{\text{rec}}} = \frac{3}{7} \simeq 0.4286 = 42.86\%.$$

Thus, about 57.14% of the reconciled key is discarded during privacy amplification:

$$1 - r = 1 - \frac{3}{7} = \frac{4}{7} \simeq 57.14\%.$$

For instance, the reconciled key:

$$0101001$$

may be compressed into the final secret key:

$$K_{\text{final}} = 101.$$

This final key is shorter, but it is more secure because the compression reduces the amount of information that a potential eavesdropper could have retained.

[a] Note that, in practical QKD implementations, this compression step is generally achieved using Universal$_2$ hash functions. However, the mathematical foundations of these hashing techniques are outside the scope of this thesis and only the conceptual principle of key compression is illustrated here.

BB84 protocol Application Example with Eve's intervention

Table 5.4: Example of BB84 transmission with Eve's intervention

The following example illustrates the impact of an intercept-resend attack on the BB84 protocol. Rather than reintroducing the complete protocol procedure, this example focuses on the disturbances generated by Eve's measurements and their consequences on the sifted keys shared between Alice and Bob.

Position i	1	2	3	4	5	6	7	8
Alice bit	0	1	0	1	1	0	1	0
Alice basis	+	+	×	×	+	×	+	×
Alice state	−	|	\	/	|	\	|	\
Eve basis	+	×	×	+	×	×	+	+
Eve bit	0	0	0	0	0	0	1	1
Bob basis	+	+	×	×	+	+	+	×
Bob bit	0	0	0	0	0	1	1	0
Kept after sifting?	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Alice sifted key	0	1	0	1	1	–	1	0
Bob sifted key	0	0	0	0	0	–	1	0

As shown in the table 5.4, Eve occasionally measures photons using a basis different from Alice's preparation basis. Due to the no-cloning principle and the probabilistic nature of quantum measurements, the original quantum state may be disturbed during this interception process. Consequently, even when Bob later measures the photon using the same basis as Alice, incorrect bits can appear in the sifted key.

The highlighted positions illustrate situations where Eve's intervention introduced discrepancies between Alice's and Bob's sifted keys. Such disturbances increase the Quantum Bit Error Rate (QBER), allowing Alice and Bob to statistically detect the potential presence of an eavesdropper.

5.4.2 GG02

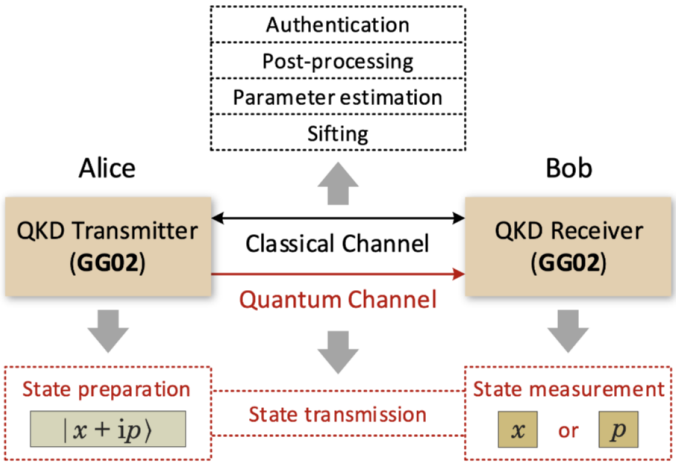

Figure 5.7: GG02 Protocol Illustrated
[8]

The GG02 [8] protocol, introduced by Grosshans and Grangier in 2002, is one of the most widely adopted Continuous-Variable Quantum Key Distribution (CV-QKD) protocols. Unlike the BB84 protocol, which relies on discrete quantum states such as photon polarizations, GG02 encodes information into continuous properties of coherent optical states using Quadratures of light.

1. **Stage 1 :**

   Alice generates coherent quantum states [18] represented by $|x + ip\rangle$, where x and p correspond to the two quadratures of the electromagnetic field. These coherent states are transmitted through the quantum channel toward Bob.

2. **Stage 2 :**

   (a) **Sifting:**

   Bob publicly announces which quadrature was measured for each transmitted state. Based on this information, Alice discards the irrelevant data associated with incompatible quadratures. After this phase, Alice and Bob share correlated Gaussian variables.
   Note that the measured values themselves are not publicly disclosed.

(b) **Post-processing:** [4] [43] [45]

Since the exchanged information consists of continuous variables, the measured data are first discretized before reconciliation can be applied. The method is called slice reconciliation.
Indeed, the data obtained after the quantum transmission are not binary. As discussed before, Alice chooses continuous Gaussian variables to modulate the quadratures of coherent states, while Bob obtains continuous measurement results that are correlated with Alice's values but not strictly identical because of channel losses, excess noise, and detection imperfections.
Consequently, before a cryptographic key can be extracted, these data must be converted into binary sequences during the slice reconciliation phase. This method discretizes the real line into several regions. Each region is associated with a binary label, so that a continuous quadrature value can be mapped onto one or several bits.

Slice Reconciliation Application Example

As an example of slice reconciliation application, let's consider a simplified quantization rule based on four intervals:

$$x < -1 \to 00, \qquad -1 \leq x < 0 \to 01, \qquad 0 \leq x < 1 \to 10, \qquad x \geq 1 \to 11.$$

If Bob measures the value $x_B = 0.62$, this value belongs to the interval $[0, 1[$, and is therefore associated with the binary label 10.

If Alice's correlated value is $x_A = 0.55$, she will also assign the same label 10.

However, if Bob obtains $x_B = 0.08$ while Alice has $x_A = -0.04$, the two values are close from a physical point of view, but they fall on different sides of the quantization boundary. Bob would assign the label 10, whereas Alice would assign 01. This illustrates why a reconciliation procedure is required after discretization: small differences between correlated continuous values may result in different binary labels.

Before generating the final secret key, Alice and Bob must also estimate the quality of the quantum channel. For this purpose, a randomly selected subset of their data is publicly disclosed and compared. This parameter estimation step allows them to evaluate relevant channel properties, such as transmission, excess noise, and the strength of their correlations. These quantities are then used to estimate the mutual information shared by Alice and Bob, denoted by I_{AB}, as well as the information potentially available to an eavesdropper.

The reconciliation phase is subsequently applied in order to transform Alice's and Bob's correlated data into a common bit string. Its objective is to correct discrepancies between their data while revealing as little information as possible through the public classical channel.

Two main reconciliation strategies can be distinguished:

i. **Direct reconciliation**

Alice's data are taken as the reference. Alice sends classical side information to Bob, allowing him to correct his data so that they agree with Alice's values. The actual identification and correction of discrepancies are performed by a practical error-correction algorithm, such as Cascade or LDPC codes. In a simplified information-theoretic picture, a secret key can be extracted only if Alice and Bob have an information advantage over Eve ;

$$I_{AB} - I_{AE} > 0,$$

where I_{AE} [6] denotes Eve's information about Alice's data.

ii. **Reverse reconciliation**

Bob's measurement results are used as the reference values. Bob sends classical side information to Alice, allowing her to correct her data so that they agree with Bob's values. As in the Direct reconciliation, the actual identification and correction of discrepancies are performed by a practical error-correction algorithm, such as Cascade or LDPC codes. In this case, the final key is constructed from Bob's data rather than from Alice's initially prepared variables. In a simplified formulation, the corresponding security condition becomes

$$I_{AB} - I_{BE} > 0,$$

where I_{BE} [6] represents Eve's information about Bob's data.

These quantities are obtained from the parameter estimation step rather than assumed a priori. The mutual information I_{AB} is estimated from the statistical correlations between Alice's and Bob's data, whereas Eve's information is bounded from the observed channel parameters, including channel losses and excess noise, according to the adopted security model.

After reconciliation, Alice and Bob apply privacy amplification. This last post-processing step reduces the length of the reconciled key in order to remove the residual information that Eve may have obtained during the quantum transmission and classical communication phases. The resulting key is shorter, but can be considered secret if the estimated security conditions are satisfied.

Note that, as in the BB84 protocol, privacy amplification in GG02-type CV-QKD protocols can be implemented using universal hash functions.

[6]The value is estimated from the statistical correlations between Alice's and Bob's data. For conciseness, the detailed derivation of the value is not reproduced here, since the purpose of this section is to provide a conceptual overview of the GG02 post-processing procedure. The interested reader is referred to [22, 42] for a more complete treatment of CV-QKD security analysis.

(c) **Authentication:**

The classical communication channel must be authenticated in order to guarantee the origin and integrity of the exchanged messages and to prevent man-in-the-middle attacks during the QKD session.

The GG02 protocol can be summarized at a conceptual level as a sequence of Gaussian modulation, coherent-state transmission, quadrature measurement, parameter estimation, information reconciliation, and privacy amplification. Algorithms 7 8 provide a simplified pseudo-code representation of these main steps.

Algorithm 7 GG02 Protocol Quantum Communication

Input: Number of signals N, modulation variance V_A
Output: Secret key K
for $i \leftarrow 1$ to N **do**
    Alice draws two Gaussian random variables:

$$x_i, p_i \sim \mathcal{N}(0, V_A)$$

    Alice prepares the coherent state:

$$|\alpha_i\rangle, \qquad \alpha_i = x_i + ip_i$$

    Alice sends $|\alpha_i\rangle$ to Bob through the quantum channel.
    Bob randomly selects one quadrature:

$$q_i \in \{X, P\}$$

    Bob measures the selected quadrature using homodyne detection.
end for
return GG02 Protocol Classical Communication 8

Algorithm 8 GG02 Protocol Classical Communication

Bob announces the measured quadrature for each signal.
Alice keeps the modulation values corresponding to Bob's measured quadratures.
Alice and Bob estimate the channel parameters, including transmittance and excess noise.
if the estimated secret key rate is not positive **then**
    Abort the protocol.
end if
Alice and Bob perform information reconciliation to correct discrepancies.
Alice and Bob apply privacy amplification to reduce Eve's residual information.
return final secret key K

5.4.3 E91

The E91 [12,33] protocol was introduced by Artur Ekert in 1991 and is part of the entanglement-based quantum key distribution protocol. Its objective is to allow two legitimate parties, Alice and Bob, to establish a shared encryption key that can be used to secure their communication over a public channel. Unlike protocols based on individually prepared quantum states, E91 relies on a source emitting pairs of photons whose polarizations are maximally entangled. Each emitted pair forms a Bell pair: one photon is sent to Alice, while the other one is sent to Bob.

For each received photon, Alice and Bob independently and randomly select a measurement basis. According to the notation used in the protocol, Alice chooses one basis among the set $\{a, b, a'\}$, whereas Bob chooses one basis among $\{b, a', b'\}$.

The two parties therefore share two common bases, namely b and a'. After all measurements have been performed, Alice and Bob publicly announce the bases they used for each photon. The measurement outcomes are denoted by $+1$ or -1. When Alice and Bob have measured their respective photons using the same basis, the corresponding results are retained to form the raw encryption key. The other relevant measurement outcomes are not used directly for key generation, but rather for testing the security of the quantum correlations.

A characteristic of the E91 protocol is that its security is assessed through the violation of Bell inequalities, more specifically through the CHSH inequality. In this context, Alice and Bob reveal and compare the measurement results associated with the following combinations of bases:

$$(a, b), \quad (a', b), \quad (a, b'), \quad (a', b').$$

For each pair of results, Alice and Bob compute the product

$$m_A m_B,$$

where m_A and m_B denote the measurement outcomes obtained by Alice and Bob, respectively. The average value of these products is then computed for each combination of measurement bases in order to estimate the corresponding correlation term, such as $E(a, b)$.

The CHSH test is based on a parameter S constructed from these correlation terms. In a classical framework, this parameter is bounded by the value 2. However, when the measurements are performed on maximally entangled photons, the expected quantum value tends toward

$$2\sqrt{2} \approx 2.83.$$

Thus, if the source of entangled photon pairs is reliable and if the quantum channel is not significantly affected by noise or by an eavesdropping attempt, Alice and Bob should observe a value of S approaching $2\sqrt{2}$ as the number of measured photon pairs increases. Conversely, if the observed value remains below 2, the generated key cannot be considered trustworthy and should not be used.

It is important to emphasize the statistical nature of this verification step. Since the correlations are estimated from average values, a sufficiently large number of photon pairs is required to draw meaningful conclusions. With too few samples, statistical fluctuations may lead to misleading observations. Finally, some combinations of bases are not exploited in the E91 protocol. In particular, the combinations

$$(a, a'), \quad (b, b'), \quad (b, a')$$

are discarded and do not contribute either to key generation or to the CHSH security test.

Algorithm 9 E91 Protocol Quantum Communication

Input: A source producing maximally entangled photon pairs.
Output: A raw secret key shared by Alice and Bob.
The source generates a sequence of maximally entangled photon pairs.
For each pair, one photon is sent to Alice and the other photon is sent to Bob.
for each entangled photon pair **do**
    Alice randomly chooses a measurement basis from $\{a, b, a'\}$.
    Bob randomly chooses a measurement basis from $\{b, a', b'\}$.
    Alice measures her photon and obtains an outcome $m_A \in \{+1, -1\}$.
    Bob measures his photon and obtains an outcome $m_B \in \{+1, -1\}$.
    Alice and Bob store their chosen bases and their measurement outcomes.
end for

Algorithm 10 E91 Protocol Classical Communication

Alice and Bob publicly announce the measurement bases used for each photon pair.
for each recorded photon pair **do**
    if Alice and Bob used the same basis b or a' **then**
        The corresponding outcomes are retained for raw key generation.
    else if the basis pair is (a, b), (a', b), (a, b'), or (a', b') **then**
        Alice and Bob reveal the corresponding outcomes.
        They compute the product $m_A m_B$.
        The product is used to estimate the corresponding correlation term.
    else
        The corresponding results are discarded.
    end if
end for
Alice and Bob estimate the correlation values $E(a, b)$, $E(a', b)$, $E(a, b')$, and $E(a', b')$.
Alice and Bob compute the CHSH parameter:
$S = E(a, b) - E(a, b') + E(a', b) + E(a', b')$.
if S is compatible with a violation of the classical CHSH bound **then**
    The quantum correlations are considered valid.
    The retained outcomes are used as the raw secret key.
else
    The generated key is rejected.
end if
return the raw secret key if the CHSH test is successful.

E91's CHSH Test Application Example

In order to better understand how the CHSH test is used in the E91 protocol, it is useful to consider a simple numerical example. In this protocol, Alice and Bob obtain measurement outcomes denoted by $+1$ or -1.
For each pair of measurement bases, a correlation coefficient $E(x, y)$ can be estimated from the observed joint outcomes, where x denotes Alice's measurement basis and y denotes Bob's measurement basis.
For a given pair of bases (a, b), the correlation coefficient is defined as :

$$E(a,b) = P_{++}(a,b) + P_{--}(a,b) - P_{+-}(a,b) - P_{-+}(a,b),$$

where

- $P_{++}(a,b)$ is the probability that Alice and Bob both obtain $+1$,
- $P_{--}(a,b)$ is the probability that they both obtain -1,
- $P_{+-}(a,b)$ is the probability that Alice obtains $+1$ while Bob obtains -1,
- $P_{-+}(a,b)$ is the probability that Alice obtains -1 while Bob obtains $+1$.

This expression is equivalent to computing the average value of the product $m_A m_B$, where m_A and m_B are the respective outcomes obtained by Alice and Bob. Identical outcomes contribute positively to the correlation, whereas opposite outcomes contribute negatively.
As an illustrative example, suppose that Alice and Bob obtain 1000 valid measurements for the pair of bases (a, b). The observed joint outcomes are assumed to be distributed as follows:

Joint outcome	Number of occurrences	Estimated probability
$++$	75	0.075
$--$	75	0.075
$+-$	425	0.425
$-+$	425	0.425
Total	1000	1.000

The corresponding correlation coefficient is therefore

$$E(a,b) = 0.075 + 0.075 - 0.425 - 0.425.$$

Hence,

$$E(a,b) = 0.15 - 0.85 = -0.70.$$

This negative value means that, for this pair of measurement bases, Alice and Bob obtain opposite outcomes more frequently than identical outcomes.

The same procedure is applied to the other combinations of measurement bases. Let's suppose that Alice and Bob estimate the following four correlation coefficients:

$$E(a,b) = -0.70, \qquad E(a,b') = 0.71, \qquad E(a',b) = -0.69, \qquad E(a',b') = -0.72.$$

The CHSH parameter is then computed as

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b').$$

we obtain,

$$S = -0.70 - 0.71 - 0.69 - 0.72.$$

Thus,

$$S = -2.82.$$

Using the absolute value convention commonly adopted when discussing the CHSH inequality, this corresponds to

$$|S| = 2.82.$$

This value is greater than the classical CHSH bound,

$$|S| \leq 2,$$

and is close to the ideal quantum prediction

$$2\sqrt{2} \approx 2.83.$$

The estimated value of $|S|$ violates the classical bound. Alice and Bob can conclude that the observed correlations are compatible with quantum entanglement. The corresponding key can be considered suitable for the next step.

5.4.4 MDI-protocol

After presenting BB84, GG02 and E91, it is useful to briefly introduce Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) as an opening toward more implementation-secure QKD architectures. The purpose of this subsection is not to analyze MDI-QKD with the same level of detail as the previous representative protocols, but to show how QKD research addresses practical vulnerabilities arising from imperfect measurement devices.

Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) was proposed by Lo, Curty and Qi as a practical solution to remove detector side-channel vulnerabilities in quantum key distribution systems. The central motivation is that, although QKD is theoretically secure, real implementations may deviate from idealized security models, especially because of imperfections in single-photon detectors. Several attacks have exploited such detector imperfections in practical QKD systems, which shows that the measurement apparatus represents one of the most critical security loopholes in realistic implementations [24].

The fundamental idea of MDI-QKD is to remove the need to trust the measurement device. Indeed, Alice and Bob independently prepare phase-randomized weak coherent pulses in one of the four BB84 polarization states and send them to an untrusted relay ;Charlie. Charlie performs a Bell State Measurement (BSM) on the incoming signals and publicly announces whether the measurement was successful, as well as the corresponding Bell-state outcome [24]. The essential security advantage is that Charlie's detection system can be arbitrarily flawed or even controlled by Eve without compromising the security of the final key.

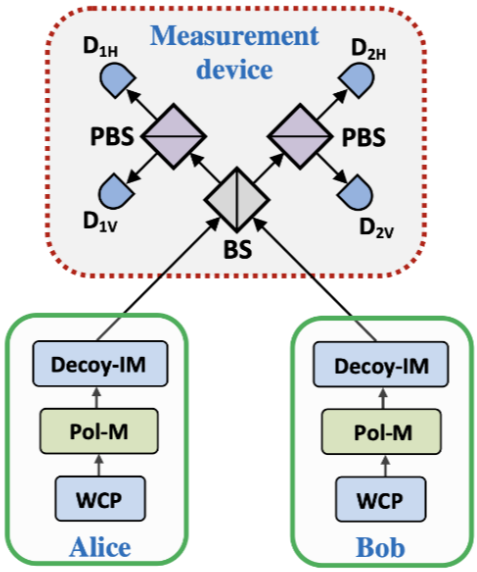

Figure 5.8: Basic implementation of MDI-QKD [24]

In the basic implementation, Alice and Bob use weak coherent pulses generated by conventional laser sources. Polarization modulators are used to select the BB84 polarization states, while intensity modulators are used to generate decoy states. Inside the measurement device, the optical signals from Alice and Bob interfere at a $50 : 50$ beam splitter. The outputs are then directed toward polarizing beam splitters and single-photon detectors. A successful Bell State Measurement corresponds to the simultaneous triggering of two detectors associated with orthogonal polarization components.

MDI-QKD is particularly interesting because it addresses an important weakness of practical QKD systems: the trust placed in the measurement device. By moving the measurement step to an untrusted relay, detector-side attacks are no longer part of Alice's and Bob's trusted implementation. However, MDI-QKD is not fully device-independent, since the state-preparation devices used by Alice and Bob must still be properly characterized. In this thesis, MDI-QKD is therefore presented as a practical evolution of QKD architectures, rather than as a protocol studied in full technical detail.

5.5. Summary of Representative Quantum Key Distribution Protocols

The protocols discussed in this thesis were selected in order to represent the main paradigms encountered in Quantum Key Distribution rather than to provide an exhaustive survey of all existing schemes. BB84 was chosen because it constitutes the historical and conceptual foundation of QKD. GG02 was included to illustrate the continuous-variable approach, in which information is encoded in the quadratures of coherent optical states. E91 was selected to represent entanglement-based QKD and to highlight the role of Bell-inequality violations as a security test. Finally, MDI-QKD was considered because it addresses practical detector-side-channel vulnerabilities, which represent an important concern in real-world QKD implementations.

This selection gives a structured view of the main mechanisms used in QKD. Table 5.5 compares BB84, GG02, E91, and MDI-QKD according to their variable type, operational logic, physical resource, security principle, and main practical limitation. The purpose of this comparison is to show that these protocols pursue the same objective, the establishment of a secret key, while relying on different physical assumptions and implementation choices.

From this comparison, BB84 appears as the pedagogical reference protocol because it introduces the basic prepare-and-measure mechanism using discrete quantum states. GG02 extends this perspective to continuous variables and coherent optical states, thereby connecting QKD with standard optical communication technologies. E91 introduces a distinct security perspective based on entanglement and non-classical correlations, while MDI-QKD illustrates how more recent protocols attempt to mitigate implementation vulnerabilities, especially those affecting measurement devices. Consequently, the four selected protocols are complementary rather than redundant, since each one emphasizes a different theoretical or practical dimension of QKD.

Table 5.5: Comparative summary of representative QKD protocols

Protocol	**Variable type**	**Approach**	**Main resource**	**Security principle**	**Practical limitation**
BB84	DV	Prepare-and-measure	Single photons or weak coherent pulses	No-cloning theorem and measurement disturbance	Photon loss and photon-number-splitting attacks
GG02	CV	Prepare-and-measure	Coherent optical states	Quadrature correlations and noise estimation	Excess noise and reconciliation efficiency
E91	DV	Entanglement-based	Entangled photon pairs	Bell inequality violation	Complexity of entangled-photon sources
MDI-QKD	DV/CV	Measurement-device-independent	Bell-state measurement	Removal of detector side-channel vulnerabilities	Lower key rates and complex synchronization

6 Deployment Areas of QKD Network

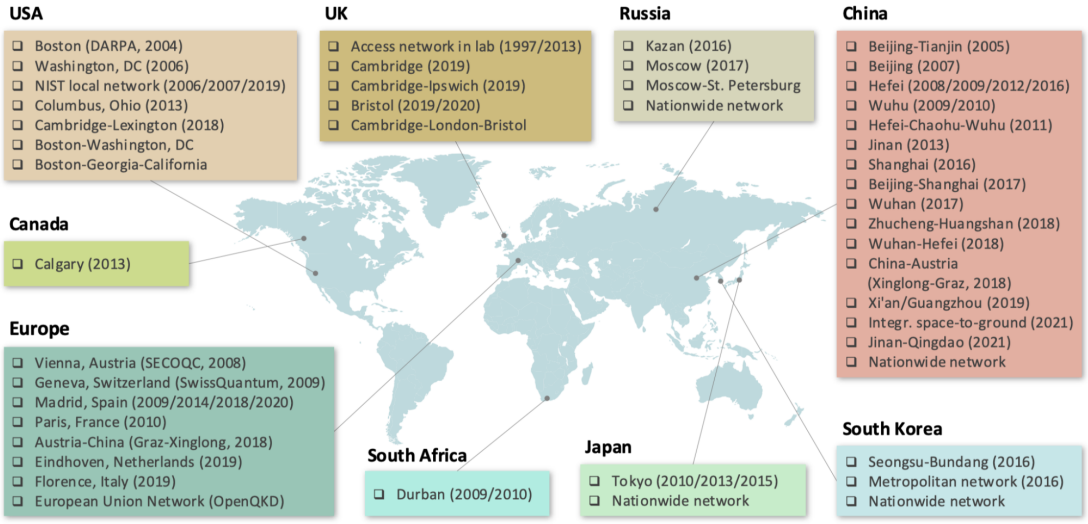

Figure 6.1: QKD Deployment
[8]

Quantum Key Distribution (QKD) is no longer limited to laboratory demonstrations. QKD networks [8] have progressively moved from academic research toward preliminary real-world applications, especially through optical-fiber and free-space communication infrastructures. This evolution shows that QKD is increasingly considered as a practical technology for securing sensitive communications requiring long-term confidentiality.

Several field deployments have already been reported worldwide. the DARPA network in the United States, the SECOQC network in Austria, the Tokyo QKD network in Japan, the SwissQuantum network in Switzerland, the Beijing–Shanghai network in China, and the Cambridge QKD network in the United Kingdom.
These examples illustrate that QKD has been tested and deployed at different geographical scales,

ranging from local and metropolitan networks to long-distance backbone infrastructures.

From a network perspective, QKD deployments can be grouped into three main categories.

1. **Short-range QKD networks** designed for local or access environments, where multiple users may be connected within a restricted area
2. **Metropolitan QKD networks** are deployed at city scale and may interconnect institutions, companies, or public infrastructures
3. **Long-haul QKD networks** aim to connect distant regions through backbone infrastructures, often relying on trusted relay nodes or hybrid architectures

While optical-fiber QKD is more mature and easier to integrate into existing telecommunication infrastructures, free-space QKD offers greater flexibility and may support longer-distance links. In particular, satellite-based QKD is presented as a promising approach for intercontinental secure communication and for the future construction of a global QKD network

In terms of application domains, QKD networks are mainly relevant for sectors where the confidentiality of information must be preserved over long periods such as

1. Finance and banking,
2. Government and defense,
3. Cloud and data centers,
4. Critical infrastructure,
5. Healthcare systems.

Overall, QKD networks seem to be progressing from experimental demonstrations toward more operational communication infrastructures. Current deployments are still limited, but they show that QKD can be integrated into existing optical networks and extended through space-to-ground links. This evolution suggests that QKD may become one component of future quantum-safe communication systems, rather than a complete solution on its own.

7 Discussion and Critical Analysis

An important observation emerging from this study is that Quantum Key Distribution provides a fundamentally different approach to secure communications compared to classical cryptographic systems, the practical deployment of QKD technologies still raises several scientific, technological, and industrial challenges.

One of the principal strengths of QKD lies in the fact that its security does not rely on computational complexity assumptions, but rather on the laws of quantum mechanics themselves. In theory, any eavesdropping attempt inevitably disturbs the transmitted quantum states and can therefore be detected through the Quantum Bit Error Rate (QBER). This represents a major conceptual advantage compared to conventional public-key cryptography, whose security depends on mathematical problems that may become tractable with the evolution of computational capabilities and quantum algorithms such as Shor's algorithm.

However, an important distinction must be made between theoretical security and practical security. Most security proofs rely on idealized assumptions concerning the physical devices used in QKD implementations.In practice, imperfections affecting photon sources, optical components, transmission channels, and detectors may introduce exploitable vulnerabilities. As seen before, attacks such as photon-number-splitting attacks or faked-state attacks use precisely these implementation imperfections rather than the theoretical weaknesses of quantum mechanics itself. Consequently, practical QKD security strongly depends on the quality, calibration, and reliability of the physical apparatus. This highlights an important limitation of real-world QKD systems: although the theoretical framework may provide unconditional security, the implementation layer remains vulnerable to engineering imperfections and side-channel attacks.

Another important limitation concerns the deployment constraints associated with QKD infrastructures.
Indeed, unlike post-quantum cryptographic algorithms, which can generally be implemented using existing classical communication infrastructures and software-based approaches, QKD requires dedicated optical hardware, specialized detectors, and, in some cases, optical-fiber infrastructures or free-space optical links. Such requirements significantly increase deployment complexity and operational costs. Moreover, the achievable transmission distance remains constrained by attenuation, noise accumulation, detector efficiency, and the impossibility of directly amplifying unknown quantum states due to the no-cloning theorem. Although satellite-based QKD and free-space implementations provide promising perspectives for long-distance quantum communications, these

technologies still face important technical challenges including atmospheric turbulence, alignment precision, environmental perturbations.

Another important point is that QKD protocols have evolved with practical security concerns. While early protocols such as BB84 mainly illustrate the fundamental principles of quantum-secure communication, more recent approaches such as MDI-QKD directly address implementation weaknesses, especially detector-side attacks. This shows that QKD research has progressively moved from idealized security models toward architectures designed for more realistic experimental conditions.

Finally, despite the remaining challenges, Quantum Key Distribution remains one of the most fascinating applications of quantum mechanics in modern cybersecurity. The field combines concepts originating from computer science, cryptography, optical engineering, quantum optics, and information theory. Future developments involving quantum repeaters, satellite quantum communications, and hybrid cryptographic infrastructures may progressively contribute to the emergence of large-scale quantum-secure communication networks.

Therefore, although QKD cannot yet be considered a universal replacement for classical cryptographic systems, it nevertheless represents a major scientific and technological advance toward the development of future quantum-secure communication infrastructures.

8 Conclusion

This thesis has explored Quantum Key Distribution as a promising approach for securing cryptographic key exchange by relying on the fundamental principles of quantum mechanics rather than on computational hardness assumptions. The main objective was not only to describe QKD as a theoretical concept, but also to understand how its security properties emerge from physical phenomena such as quantum measurement, basis incompatibility, the no-cloning theorem, and the disturbance introduced by an eavesdropper.

A first important result of this work is that QKD must be understood as a hybrid security mechanism. The quantum channel does not directly transmit a secret message, but allows two legitimate users to establish correlated raw data whose security can then be evaluated and improved through classical post-processing. In this sense, phases such as error estimation, information reconciliation, and privacy amplification are not secondary details, but essential components of the protocol. They transform imperfect experimental data into a shorter but more secure final key.

The analysis of BB84 shows why it remains a central reference in QKD. Its relative simplicity makes it a useful starting point for understanding the main steps of quantum key distribution: state preparation, basis selection, sifting, error estimation, and key distillation. However, the protocol also illustrates the gap between the ideal theoretical model and practical implementations. In real systems, sources, optical components, channels, and detectors can introduce losses, noise, imperfections, or vulnerabilities that must be included in any realistic security analysis.

Another important observation is that the security of QKD is not absolute in a naive practical sense. While the theoretical framework provides strong guarantees under well-defined assumptions, real devices may deviate from the ideal models used in security proofs. Attacks such as photon-number-splitting attacks, detector-related attacks or faked-state attacks illustrate that implementation security is a fundamental issue. Consequently, countermeasures such as decoy states, improved detector monitoring, optical isolation, and measurement-device-independent approaches are necessary to bridge the gap between theory and practice.

This thesis also shows that QKD is not limited to a single protocol or mechanism. Prepare-and-measure schemes, entanglement-based protocols, continuous-variable approaches, and MDI-QKD architectures each exploit quantum phenomena in a different way to establish a secret key. Taken together, these approaches illustrate that QKD is a broad interdisciplinary field, at the intersection of quantum physics, optical engineering, information theory, and cybersecurity.

From a critical perspective, QKD should not be presented as a universal replacement for classical cryptography. Its deployment requires specific hardware, controlled optical links, synchronization mechanisms, and careful integration with classical authentication methods. Moreover, distance limitations, losses, cost, and infrastructure constraints remain important practical challenges. Nevertheless, QKD provides a distinctive security model: it offers a way to detect the presence of an eavesdropper and to quantify the amount of information that may have leaked during transmission.

In conclusion, this work shows that Quantum Key Distribution is both a scientifically rich and technologically demanding domain. Its interest lies in the fact that it connects abstract quantum principles with concrete security applications. Although practical QKD systems still face several limitations, they represent a significant evolution in the way secure communication can be conceived. Future progress will likely depend on the development of more robust components, better integration into existing network infrastructures, and continued work on protocols that reduce implementation assumptions. Therefore, QKD should be considered not as a complete solution by itself, but as an important component of the broader evolution toward quantum-safe communication systems.

Bibliography

[1] Ahmed Mahmoud Abbas, Amr Goneid, and Sherif El-Kassas. Privacy amplification in quantum cryptography bb84 using combined universal$_2$-truly random hashing. *International Journal of Information and Network Security (IJINS)*, 3(2):98–115, 2014.

[2] Omar Amer, Vaibhav Garg, and Walter O. Krawec. An introduction to practical quantum key distribution. April 2020.

[3] Nick Aquina, Bruno Cimoli, Soumya Das, Kathrin Hövelmanns, Fiona-Johanna Weber, Chigo Okonkwo, Simon Rommel, Boris Škorić, Idelfonso Tafur Monroy, and Sebastian Verschoor. A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography. *arXiv:2502.04009V2 [cs.CR]*, 2025.

[4] Gilles Van Assche, Jean Cardinal, and Nicolas J. Cerf. Reconciliation of a quantum-distributed gaussian key. *arXiv:cs/0107030V3*, 2002.

[5] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014.

[6] Matt Bishop. *Computer Security: Art and Science*. Addison-Wesley, 2 edition, 2018.

[7] Jack R. Brault. *Quantum Key Distribution Laboratory Demonstration*. Master thesis, Naval Postgraduate School, Monterey California, 2021.

[8] Yuan Cao, Yongli Zhao, Qin Wang, Jie Zhang, Soon Xin Ng, and Lajos Hanzo. The evolution of quantum key distribution networks: On the road to the qinternet.

[9] CLOUDFLARE. https://www.cloudflare.com/en-gb/learning/ssl/quantum/what-is-post-quantum-cryptography/.

[10] Datacolor. Visible light. https://www.datacolor.com/wp-content/uploads/2024/01/electromagnetic-spectrum.jpg.

[11] Travis Denny. Faked states attack and quantum cryptography protocols. *Oklahoma State University*, November 2024.

[12] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6), 1991.

[13] Rouquérol Françoise, Gilberte Chambaud, Roland Lissillour, and Abdou Boucekkine. *Chimie Générale : les cours de Paul Arnaud*. Dunod, Paris, 2013.

[14] Vimal Gaur, Devika Mehra, Anchit Aggarwal, Raveena Kumari, and Srishti Rawat. Quantum key distribution : Attacks and solutions. *3rd International Conference on Innovative Computing and Communication*, pages 3–5, 2020.

[15] Hrant Gharibyan. https://www.bluequbit.io/blog/quantum-cryptography.

[16] Nicolas gisin, Gregoire Ribordy, Wolfgang tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, pages 22–23, 2008.

[17] Frédéric Grosshans. La cryptographie quantique : l'incertitude quantique au service de la confidentialité. May 2014.

[18] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421:238–241, 2003.

[19] Eugene Hecht. *Physique*. De Boeck Supérieur, Bruxelles, 2004.

[20] Julien Ladeuze, Maxime Bazin, and Kacem Barkanis. Quantum computing. Document revised by V.Bruyere and S.Dynerowicz Umons University, 2024.

[21] Carter Larry and Wegman Mark. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[22] Fabian Laudenback and al. Continuous-variable quantum key distibution with gaussian modulation - the theory of practical implementations. *arXiv:1703.09278V3 [quant-ph]*, 2018.

[23] Erik Lidbjörk and Rasmus Söderström Nylander. *Cost and Efficiency Comparison of Quantum Key Distribution Schemes*. PhD thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2023.

[24] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108, 2012.

[25] Rob Malaney. Quantum communications tutorial for engineers. Washington, DC, USA, 2016. UNSW Engineering.

[26] Christoph Marquardt and al. Implementation attacks against qkd systems. Technical report, Federal Office for Information Security, 2023.

[27] Kabeya Mpinda. Experimental realization of quantum key distribution. Master of science thesis, University of KwaZulu-Natal, Durban South Africa, 2009.

[28] Muskan, Ramniwas Meena, and Subhashish Banerjee. Performance analysis of satellite-based qkd protocols. *arXiv preprint arXiv:2308.01036*, pages 6–8, 2025.

[29] Maki Ohata and Kanta Matsuura. Constructing css codes with ldpc codes for the bb84 quantum key distribution protocol. *arXiv preprint arXiv:quant-ph/0702184*, 2007.

[30] Radek Pelc, Wolfgang Walz, and J. Ronald Doucette, editors. *Neurohistology and Imaging Techniques*, volume 153 of *Neuromethods*. Springer, New York, 2017.

[31] Jean-François Pillou and Jean-Philippe Bay. *Tout sur la sécurité informatique*. CommentçaMarche.net. Dunod, Paris, 4 edition, 2019.

[32] QOSST. https://phys.libretexts.org/bookshelves/university-physics/university-physics-(openstax)/university-physics-ii—optics-and-modern-physics-(openstax)/07

[33] Institut Quantique. https://www.quantumcrypto.app/e91.

[34] QuEra. https://www.quera.com/glossary/shors-algorithm.

[35] Osama M. Raisuddin and Suvranu De. *Quantum Computing for Engineers*. Springer, 2021.

[36] Benjamin Rousseaux. *Control For Quantum Technologies at the Nanoscale*. PhD thesis, Université de Bourgogne Franche-Comté, November 2016.

[37] Davide Rusca and Nicolas Gisin. Quantum cryptography: an overview of quantum key distribution. University of Vigo and University of Geneva.

[38] Hitesh Singh, D. L. Gupta, and A. K. Singh. Quantum key distribution protocols: A review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(2):01–09, March – April 2014.

[39] Barry Steyn. https://doctrina.org/how-rsa-works-with-examples.html.

[40] Anastasija Trizna and Andris Ozols. An overview of quantum key distribution protocols. *Information Technology and Management Science*, 21:37 – 44, December 2018.

[41] Devashish Tupkary and Norbert Lutkenhaus. Using cascade in quantum key distribution. *arXiv preprint arXiv:2312.00576*, 2023.

[42] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J.cer, and al. Gaussian quantum information. *arXiv:1110.3234V1 [quant-ph]*, 2011.

[43] Xuan Wen, Qiong Li, Haokun Mao, Xiaojun Wen, and Nan Chen. An improved slice reconciliation protocol for continuous-variable quantum key distribution. *Entropy*, 2021.

[44] Wikipedia. https://en.wikipedia.org/wiki/quantum-key-distribution.

[45] Shenshen Yang, Zhilei Yan, Hongzhao Yang andQing Lu, Zhenguo Lu, Liuyong Cheng, Xiangyang Miao, and Yongmin Li. Information reconciliation of continous-variables quantum key distribution: principles, implementations and applications. *EPJ Quantum Technology*, 2023.