Mémoire

Auteur : Dierick, Antoine
Promoteur(s) : Habraken, Serge
Faculté : Faculté des Sciences
Diplôme : Master en sciences spatiales, à finalité spécialisée
Année académique : 2023-2024
URI/URL : http://hdl.handle.net/2268.2/21630

Faculty of Sciences

Department of Astrophysics, Geophysics and Oceanography

A thesis presented for the completion of the Master of Space Sciences degree, under the professional focus specialization.

Coding schemes and applications for quantum key distribution

Author: Antoine Dierick Academic Advisor: Serge Habraken

Comittee members: Alain Carapelle, Lionel Clermont, François Damanet

Academic year 2023-2024

Acknowledgements

I would like to express my gratitude to my academic supervisor, Professor Serge Habraken, for his continuous support and guidance throughout the creation of this manuscript. His feedback and corrections were crucial in shaping the work to its present state.

I would also like to thank my reading committee composed of Prof. Alain Carapelle, Prof. Lionel Clermont, and Prof. François Damanet, for dedicating a part of your time to read my thesis.

Additionally, I am grateful to my office mates Antoine and Sélim for their presence, their valuable advice, and for taking the time to help correct various parts of this work.

Finally, I would like to thank all my loved ones for their support during the writing of this work. In particular, I want to express my gratitude to Camille and Marcel for their advice and willingness to help. I also extend my thanks to Zoé, Arnaud, Pamella, Elliot, Caroline, Elias and Kenza for their unwavering support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Our current telecommunications networks allow two parties to communicate almost instantaneously from nearly anywhere on Earth and even beyond. This achievement has been made possible thanks to the development of telecommunications, which is itself the result of advancements in mathematical and physical sciences. Efforts have been made to secure these telecommunications, leading to the development of cryptography. In the modern world, digital management encompasses nearly everything, from the internet and communications to banking transactions. Data security is therefore vital for the smooth operation of our society. However, traditional cryptographic protocols rely on computational complexity and do not provide unconditional security. This means that it is theoretically possible for a malicious third party to intercept and decrypt these exchanges, provided that they has sufficient computational power. Presently, only one theoretical method is known to achieve unconditional security. This method is named Vernam encryption, after Gilbert Vernam, who had invented it near the end of World War I. However, implementing this method raises seemingly insurmountable problems, which quantum communications are able to solve.

This first chapter will explore why classical cryptography cannot be directly used to implement Vernam encryption, and the implications of this limitation will also be discussed. The second chapter will cover the fundamentals of quantum information theory, which is crucial for understanding quantum cryptographic systems, particularly quantum key distribution (QKD). The third chapter will delve into the principles of QKD, detailing the main protocols and discussing potential security issues due to imperfect implementations. The fourth chapter will explore alternative coding schemes that may offer advantages in specific scenarios. Chapter five is dedicated to the characterization of the various components of a QKD link and will address the specific needs associated with various QKD implementations. Finally, the sixth chapter will review major practical implementations in QKD, demonstrating how the technology's maturity enables its integration into real-world applications.

1.1 Limitations of classical cryptography

The issue that cryptography addresses can be succinctly stated as: how to send information to a legitimate recipient while ensuring it remains entirely incomprehensible to others. If Alice wants to remotely share a secret message with Bob, she will use a method to scramble her message without destroying the information. She will then send this message to Bob, ensuring that her encryption method is robust enough so that no one except Bob can decrypt the message. Over time, the ways of telecommunication have evolved, and cryptographic methods have had to keep up.

Today's information world is digital and its language is binary. In this framework, there is an amazingly simple method to perfectly scramble a message. Formalized by Gilbert Vernam in 1917, it is known as the Vernam cipher or "one-time pad" (OTP) protocol. The process involves adding a secret random

binary key to the message twice: the first addition results in an encrypted message whose information can only be extracted by adding the key a second time. This is because applying the binary addition, also called the XOR operation, twice with the same key effectively leaves the message unchanged (refer to Table 1.1 for clarity). Thus, Alice encrypts her message by XORing it with the key and sends it to Bob, who can decrypt the message by XORing again the encrypted message with the key. In 1949, Shannon showed that the Vernam cipher enables unconditional security if the key satisfies the following three conditions [23]:

- the key must be at least as long as the message to be encrypted,
- the key must be random,
- each key must be used only once.

Message	Key	Encrypted message (Message $\oplus$ Key)	Decrypted Message (Encrypted Message $\oplus$ Key)
000000	101001	101001	000000
011001	101001	110000	011001

Table 1.1: The message (column 1) is encrypted with the key (column 2) via a XOR operation resulting in an encrypted message (column 3). It can be decrypted by XORing it again with the key (column 4).

The problem with this theoretically perfect method arises when trying to implement it in practice. How can Alice and Bob, and only they, access such a key? If they could exchange it beforehand, couldn't they exchange the message directly? One can imagine scenarios where this method is still useful, such as if Alice and Bob know they will need to exchange secrets but don't know what they will be. In this case, they can exchange the key beforehand and communicate securely, provided the key meets the three above conditions. However, Shannon's third condition implies that each message must be encoded with a unique key, limiting the number of messages that can be securely exchanged if a finite key is shared beforehand. Imposing such conditions clearly does not meet most of today's communications needs.

For this reason, practical cryptographic schemes do not use the OTP scheme but instead rely on asymmetric protocols. The idea is to use a particular key pair: a public key for encryption (EK) and a private key for decryption (DK). The particularity of this pair is that it is extremely complicated to decrypt a message encrypted with EK without knowing DK. Alice sends EK to Bob, who uses it to encrypt his message. Only Alice, who knows DK, can decrypt it. This one-way exchange makes these protocols "asymmetric". To enable two-way communication, Bob can generate a key, encrypt it with EK, and send it to Alice. This key, accessible exclusively to Alice and Bob, can be employed in the OTP scheme.
In practice, asymmetric protocols leverage trapdoor functions, which are challenging to reverse without additional information. One of the most commonly used protocols today is the Rivest-Shamir-Adleman (RSA) protocol, which secures much of the internet traffic. RSA relies on functions based on the computational difficulty of prime factorization of large integers.

The notion of difficulty mentioned above should be understood in the context of algorithmic complexity, indicating that the number of operations needed to break a code increases exponentially with the key size. Therefore, securing an information exchange simply requires using an encryption key large enough such that, given current computational capabilities, decrypting the message within a reasonable time is impossible. The main difference between OTP and current cryptosystems is that the former provides unconditional security, while the latter relies on the ever-evolving limits of human knowledge.

Until now, breaking RSA-like protocols with classical attacks seemed hypothetical because it requires computing power well beyond what is available today or in the near future. Nevertheless, advances in quantum computing has led to some important results and some quantum algorithms have been shown to be more efficient for specific tasks than classical ones. In particular, Shor's algorithm [24] that efficiently prime factors large numbers, could potentially be used to decrypt RSA. While reaching such a quantum supremacy is henceforth theoretically possible, implementation of physical quantum systems to operate

quantum algorithms is still a challenging task nowadays.
Finding an appropriate solution to overcome this threat before quantum computers become a mature technology is one of the crucial challenges in telecommunications.

Quantum key distribution could address this need. It is a technique based on the principles of quantum mechanics, particularly the uncertainty principle, which implies that a single quantum state cannot be cloned. This was demonstrated by W.K. Wootters and W.H. Zurek four decades ago [25]. This finding can be utilized to securely share a cryptographic key. Combined with the OTP encryption scheme, this enables information-theoretic security for communications, meaning that this method is robust against any adversary's computational power.

In the next chapter, the tools required to moove from classical information theory to quantum information theory will be introduced. This foundation will then allow for a detailed explanation of the working principles of QKD.

Chapter 2

Basics in quantum information

Quantum bits, or qubits, serve as the fundamental units of quantum information, much like bits are central in classical information theory. This chapter will focus on describing the fundamental properties of qubits and their physical realisation.

2.1 From classical to quantum information

Information can be reduced to its most elementary form, basically yes or no. Following this idea, it may be implemented very naturally by binary digits, or bits, 1 and 0. These are the building blocks of classical information theory, whose foundations were laid by Shannon in 1948 [26]. Ultimately, information is represented by physical systems and for this reason, information theory is intimately linked to physics. This connection becomes evident when considering how to process information: what physical systems allow us to store and communicate information? Naturally, the physical systems used to address these issues were based on the knowledge and technical means available at the time, which allowed for their control. Magnetic polarisation or electric charge are widely used for storing the bits while electric current, voltage or light intensity are often used for transmitting the information. These processes underpin a multitude of technologies used today.

In the seventies, Stephen Wiesner realized that quantum systems could be used in communications, providing unique properties that offer capabilities unattainable by classical systems. In a paper published in 1983, he presented two concrete applications based on the polarization of light for transmitting information securely [27]. The "polarized light" or "spin-1/2 particles" he used in his paper are in fact the qubits at the heart of quantum information theory.

2.2 Qubits

Similarly to classical information, quantum information is based on quantum bits, or "qubits". The quantum properties of these entail a new mathematical framework, specific to quantum physics, and offer new potential beyond what classical information theory allows.

A qubit is a two-levels system that may be represented by the set of two orthogonal quantum states denoted by:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.1}$$

it is possible to describe these quantum states in a bidimensional Hilbert space.

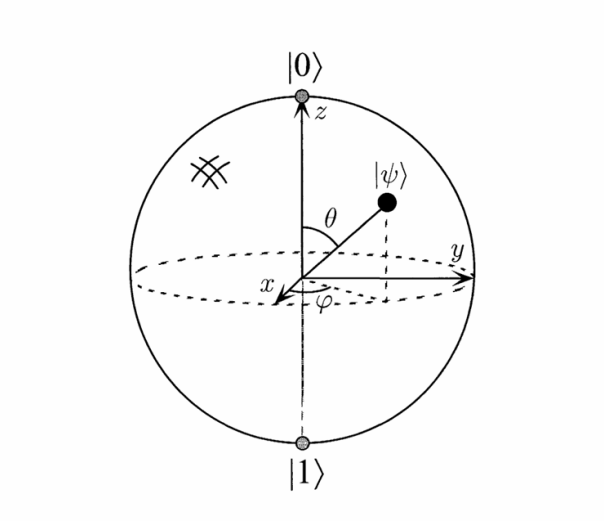

Figure 2.1: The Bloch sphere with X, Y and Z basis. Figure from Ref.[1].

The main difference between classical and quantum information is that a qubit can also be in a superposition of the previous states (2.1), i.e.:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2}$$

where α and β are complex numbers. This means that qubits are living in a continuum, α and β can take an infinite number of values. Nevertheless, they are still two-levels systems because performing a measurement on the state (2.2) will only give one of the two outcomes $|0\rangle$ or $|1\rangle$ with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively. Requiring $|\alpha|^2 + |\beta|^2 = 1$ ensures that the probabilities sum to 1. This condition also ensures that any state with the form of (2.2) is pure, i.e. its norm is equal to 1. With this condition, the states can be rewritten as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = e^{i\gamma}\big(cos(\theta/2)\,|0\rangle + e^{i\phi}sin(\theta/2)\,|1\rangle\,\big) \tag{2.3}$$

with $\theta \in (0,\pi)$, γ, $\phi \in (0,2\pi)$ and i the imaginary unit. The first exponential has no observable effect and can therefore be removed from the equation giving:

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi}sin(\theta/2)\,|1\rangle \tag{2.4}$$

The above equation suggests a geometrical view: pure states are located on the unit three-dimensional sphere. This sphere is represented in Figure 2.1 and is known as the "Bloch sphere". The cosine and sine coefficients of (2.4) determine the position on the sphere, or said differently, the respective probabilities of observing the system in the states $|0\rangle$ or $|1\rangle$. The exponential factor carries the information about the phase.

A qubit may also be represented by a statistical combination of several pure states. Such a combination is called a mixed state. To describe mixed states, it is convenient to use the density formalism by writing a generic state as:

$$\rho = \sum_i p_i\,|\psi_i\rangle\,\langle\psi_i| \tag{2.5}$$

where ρ is a density matrix and p_i are the probabilities associated to the states $|\psi_i\rangle$. While pure states are located on the surface of the Bloch sphere and have a unitary trace, i.e. $Tr(\rho^2) = 1$, mixed states are inside the Bloch sphere and have a trace inferior to 1.

As mentioned earlier, a qubit is represented by a quantum state in a bidimensional Hilbert space. A convenient choice is to align the z axis with the two states outlined in Eq.(2.1). For this reason, the $|0\rangle$ and $|1\rangle$ states are also denoted respectively by $|+_z\rangle$ and $|-_z\rangle$ and form the Z basis. This choice

simplifies the calculations, which is why the Z basis is often referred to as the "computational basis". The expression of the superposed state Eq.(2.2) in this basis is then simply denoted by:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2.6}$$

Other usual choices are to consider the X basis, also called the Hadamard basis, comprising the two following states:

$$|+_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-_x\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{2.7}$$

or the Y basis which is composed of the two states:

$$|+_y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad |-_y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}. \tag{2.8}$$

The expressions of the X basis vectors in terms of the two states of the computational basis are:

$$|+_x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-_x\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{2.9}$$

Likewise, for the Y basis:

$$|+_y\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}, \qquad |-_y\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}. \tag{2.10}$$

Note that the X, Y and Z form a set of mutually unbiased bases (MUBs). Two orthogonal basis $\{|\psi_i\rangle, ..., |\psi_d\rangle\}$ and $\{|\phi_i\rangle, ..., |\phi_d\rangle\}$ of a d-dimensional Hilbert space are said mutually unbiased if $| < \psi_i|\phi_j > |^2 = \frac{1}{d}$ for any i, j. Measuring a state from one of these basis in another would produce either one of the eigenstates with equal probability. Therefore measuring a state from one basis in another would not provide any information. This is a key feature exploited in cryptographic quantum schemes. Note also that it has been shown in Ref.[28] that complete sets of MUBs exist for prime power dimensions and that the maximum number of MUBs in a complete set for a space of dimension d is $d+1$. Specifically, for qubits, which are 2-dimensional quantum systems, the set formed by the X, Y and Z MUBs is complete. This is significant for QKD protocols since it poses the limit on the number of MUBs that can be used for measurements.

So far we have considered the description of a single qubit. A system composed of two qubits may be represented by the following state in the computational basis:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{2.11}$$

with the normalization condition on the coefficients: $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$.

Generalisation to n-qubits systems is possible by a similar superposition of computational basis states having the form: $|x_1x_2...x_n\rangle$ with $x_i \in \{0,1\}$ for $i = 1, ..., n$.

2.2.1 Operations on qubits

As for classical information, the operations on qubits are represented by logical gates and quantum information processing can be schematized by quantum circuits (for an example of such a quantum circuit, see Figure 2.2). The mathematical framework defined by the description of qubits does not impose specific constraints on the operations that can be performed. However, to ensure that the normalization condition is always satisfied after the gate, the transformation must be unitary.

For single-qubit systems, the set of possible operations is represented by the set of 2x2 unitary matrices U, i.e. matrices that fulfill $U^\dagger U = I$. Since the set is infinite, there exists an infinite number of single qubit gates. In fact, it is possible to decompose any arbitrary single qubit gate into a sequence of rotations and a global phase shift, which takes the form of a constant factor $e^{i\alpha}$. In addition, through

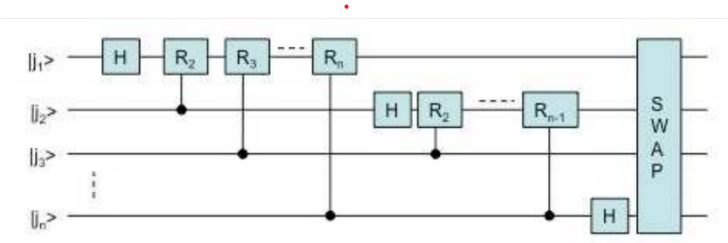

Figure 2.2: Example of a quantum circuit implementing a Quantum Fourier Transform. The H gates are Hadamard gates, and the R gates are single-qubit gates defined by $R_k := \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$. The SWAP gate reverses the sequence of qubits, mapping each basis vector $|i_1 i_2 ... i_n\rangle$ to $|i_n ... i_2 i_1\rangle$. Figure from Ref.[2].

the use of the appropriate finite set of parameters for rotations and the phase shift, any single-qubit gate can be approximated to an arbitrary degree of accuracy [1].
This is a crucial result for anyone developing a physical system for quantum information, as it means only a finite set of gates needs to be implemented to perform any operation on single-qubit system.

A rotation of any angle φ around any axis $\vec{n}$ is represented by a unitary operator defined as follows:

$$R_{\hat{n}}(\varphi) = e^{-i\varphi\vec{n}.\vec{J}} \tag{2.12}$$

$$= cos(\frac{\varphi}{2})I - i(\vec{n}.\vec{\sigma})sin(\frac{\varphi}{2}) \tag{2.13}$$

with

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.14}$$

the Pauli matrices and $J_k = \frac{1}{2}\sigma_k$.

The operation to perform to go from the Z to the X basis is a rotation of angle $\varphi = \frac{\pi}{2}$ around the y axis, it is clear by looking at the Bloch sphere (Figure 2.1).

$$R_{\hat{y}}(\frac{\pi}{2})\,|+_z\rangle = \frac{1}{\sqrt{2}}(I - i\sigma_y)\,|+_z\rangle \tag{2.15}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}|+_z\rangle \tag{2.16}$$

$$= |+_x\rangle\,. \tag{2.17}$$

Similarly, switching from the X to the Y basis is achieved by a rotation of angle $\varphi = \frac{\pi}{2}$ around the z axis.

As stated earlier, quantum gates are always unitary and thus invertible. Conversely, some classical gates are not invertible and therefore have no quantum analogue. This is the case for the NAND (NOT-AND) gate among others. In classical information, the NAND gate is universal, meaning any operation can be achieved through a composition of NAND gates. Now the question is: is there a quantum universal gate? The answer is yes; any operation on a multi-qubit system can be achieved through a composition of cNOT (controlled-NOT) gates and single-qubit gates [29].

In a system of two qubits, the cNOT gate retains one qubit (called the "control qubit") on one branch of the circuit and conducts binary addition between the two qubits on the second branch. The matrix representation of the cNOT gate in the computational basis is determined by examining its action on the basis vectors: $|00\rangle$ and $|01\rangle$ are sent over itself because the control qubit is $|0\rangle$ while $|10\rangle$ and $|11\rangle$ are respectively sent towards $|11\rangle$ and $|10\rangle$ as the control qubit is now $|1\rangle$. Therefore, the cNOT gate is

represented by the following matrix in the computational basis:

$$U_{cNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.18}$$

and the associated truth table outlined below.

Input		Output	
x	y	x	x+y
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Table 2.1: Truth table of the cNOT gate. Note that it has the same form as the truth table of the classical XOR operation.

2.2.2 Physical realisation

In 2000, David DiVicenzo summarized the requirements that a physical system must meet in order to enable quantum information processing [30]. These are the following:

1. The system must be scalable and made up of well characterized qubits.

2. The system must provide the ability to initialize the state of the qubits to a simple fiducial state, such as $|000...i\rangle$.

3. The system needs a universal set of efficiently controllable quantum gates.

4. Decoherence time should be long compared to the average operation time.

5. The state of the system must be measurable efficiently to read the qubits.

If the system satisfies the above requirements, quantum computation becomes feasible. The list can be expanded by two additional requirements for enabling quantum communications:

6. The system must be able to interconvert stationary and flying qubits.

7. The system must be able to transmit flying qubits between specified locations.

The whole set of constraints on the system is now referred to as the DiVicenzo criteria and has established a framework for the pursuit of hardware for quantum information. The principles of quantum computing are posed using the most fundamental properties of quantum mechanics. Therefore, the implementation of quantum information may be done in varied fields of physics that exhibits these properties. That is, "stationary qubits", used for information storage and processing, can be realized notably in the fields of atomic physics or condensed matter.

One of the earliest methods came from another branch of physics, one of the oldest areas in quantum physics: liquid state nuclear magnetic resonance (NMR). The principle involves encoding each qubit through the nuclear spins of a molecule. Qubit control is obtained by manipulating the nuclear spins

with a controlled magnetic field, i.e. by applying radio-frequency pulses on the sample. The duration of the magnetic field application allows for spin state manipulation, enabling to perform operations on a qubit. The technique is detailed in [31] and more recently in [32], where some major experiments in the field are provided. When encoding qubits via this method, two major difficulties arise. The first is the initialization phase, which requires ultra-low temperatures; otherwise, the system's energy exceeds typical spin flip energies, causing the spins to become randomly oriented and violating the second condition of DiVicenzo's criteria. The scalability of this method also poses a significant challenge [2]. Indeed, to perform individual operations on each qubit in the system, one must select molecules whose nuclei have varying properties, thereby rapidly constraining the system's size. Other solutions exist, which might better meet these expectations, notably ion traps [33, 34], quantum dots or superconducting qubits [35].

Building a system that allows for the control of numerous qubits is still very challenging today. The development era of these systems was termed the "Noisy Intermediate-Scale Quantum (NISQ) era" by Preskill in 2018 [36], marked by the limited size of quantum circuits that can be executed reliably. More recently, in early 2024, two quantum processors, from Atom Computing's [37] and IBM [38], have passed the 1000 qubits mark. The first one is based on nuclear spin qubits realized on individually trapped neutral atoms [39]. These atoms are arranged in an organized grid using optical tweezers and transformed into qubits using laser pulses which adjust the nuclear spin of the atoms (see Figure 2.3). Even if today's qubit counts are theoretically sufficient to solve certain real-world problems, the error rates remain too high for the results of any computation to be useful. A significant advancement for quantum computing will be the advent of fault-tolerant quantum computing (FTQC). Achieving FTQC could require millions of qubits, but efforts in quantum error correction codes could drastically lower this number [40].

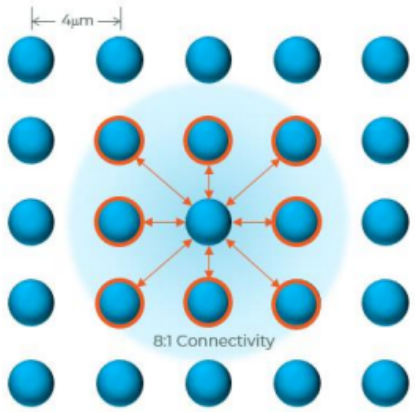

Figure 2.3: Atomic array technology at the core of Atom Computing's first generation platform, named "Phoenix". Single-qubit and two-qubit gates can be implemented using laser pulses. Figure from Ref.[3].

For the "flying qubits", intended to be exchanged between two correspondents and thus enabling quantum communications, the challenge is quite different. While stationary qubits require reliable computation, flying qubits must be capable of reliable transmission over macroscopic distances. Since they meet different needs, it is likely that stationary and flying qubits will be based on different physical principle or design.

Due to their ease of manipulation and transmission over long distances, photons are frequently used to encode flying qubits. However, other methods exist, including the use of electrons [41]. The Hilbert space for a single polarized photon is bidimensional and makes it particularly convenient for the qubits encoding. A correspondence can be made between the Bloch formalism, utilized to describe qubits, and the Poincaré formalism, used for describing the polarization state of a photon. Indeed, one can associate the MUBs X, Y, and Z defined in Section 2.2 with the diagonal, circular, and rectilinear polarization bases of the photon, respectively. In his seminal paper [27], Wiesner suggested using a sequence of pho-

tons randomly polarized in two complementary bases, the rectilinear and circular bases, to transmit a sequence of bits. Each bit value, 0 or 1, matches a specific polarization direction in these bases. For instance, 0 could be linked to vertical and right-hand circular polarization, while 1 could be linked to horizontal and left-hand circular polarization (refer to Table 2.2 for clarity).

0	$\|\uparrow\rangle$ or $\|\circlearrowright\rangle$
1	$\|\rightarrow\rangle$ or $\|\circlearrowleft\rangle$

Table 2.2: Correspondence between the values of the bits and the polarization states. The choice of the used polarization basis is random.

The polarization bases used can be described by quantum states and are mutually unbiased bases, as defined in Section 2.2. Therefore, according to the uncertainty principle, measuring a photon in the wrong basis provides random results, making it impossible to retrieve information without the correct encoding basis. This concept underpins the earliest quantum cryptography protocols, which will be discussed in the following chapter. More complex encoding schemes exist, notably the time-bin encoding [7] or via the orbital angular momentum [42] and will be discussed later in Chapter 4.

Chapter 3

Working Principles of QKD

Section 1.1 of this work emphasized the failure of classical systems to achieve unconditional security. The limitations of current encryption methods, reliant on algorithmic complexity, were underscored. In Paragraph 2.2.2, we noted that while hardware advancements have yet to provide a quantum advantage, progress is rapid. In reality, a secure communication system needs to be implemented before current methods become obsolete, as classified data often requires long-term confidentiality. Even if a third party cannot decrypt the data at the time of interception, they might store it until decryption technology becomes available. If the required secrecy period for the data is longer than the time it takes for such technology to be developed, then confidentiality cannot be assured during that period. This risk is known as the "store now and decrypt later" threat.

Quantum key distribution is a technique that enables the remote transmission of a key with total security. This security is guaranteed by the laws of physics, representing a significant paradigm shift from current methods, which rely on computational complexity. Combined with the one-time pad, QKD achieves unconditional security for telecommunications.

QKD protocols can be divided into two main categories: prepare-and-measure protocols and entanglement-based protocols. Both types are introduced below, with the seminal protocol for each category detailed to illustrate the concepts.

3.1 Prepare-and-measure protocols

Prepare-and-measure protocols benefit from the intrinsic randomness of quantum mechanics, articulated through the uncertainty principle. This fundamentally implies that one cannot clone or measure an arbitrary quantum state without modifying it [25].

In these protocols, the first step is to select a set of MUBs for qubit encoding. The subsequent physical realization of qubits was discussed in the Section 2.2.2. Each qubit is randomly encoded in one of the MUBs and then sent to the legitimate recipient via a quantum channel. The randomness of the MUBs selection prevents any eavesdropper from intercepting the qubit without detection, as measuring in a different basis results in a random outcome and wave function collapse, irreversibly altering the state. Once the qubits reach the recipient, each state is randomly measured in one of the MUBs.

After this quantum transmission, a classical channel is used for the sifting procedure: the sender reveals the basis choice for each qubit, enabling the recipient to determine if the measurement was performed in the correct basis. When the sender's and recipient's basis choices align, the measured qubit must match the sent qubit (assuming a perfect channel). To verify the security of the quantum channel, they compare a subset of the qubits with matching bases. The detection of errors indicates the presence of an

eavesdropper, prompting correspondents to abort the process.
If no errors are found, the channel was secure, and both participants share a symmetric key from the untested qubits. This key can be used in the OTP scheme to securely communicate. The basic architecture of prepare-and-measure protocols is shown in Figure 3.1.

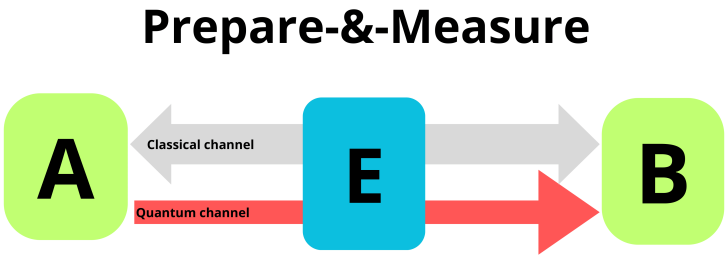

Figure 3.1: Basic architecture of prepare-and-measure protocols. Alice (A) encodes the qubits and sends them to Bob (B) through the quantum channel. Alice and Bob have also access to a classical channel. Eve (E) is assumed to have total control over the quantum channel while she only has passive control over the classical channel.

3.1.1 BB84

Inspired by the work of Wiesner [27], Charles Bennett and Henri Brassard designed the first quantum communication protocol in 1984 [43]. This protocol paved the way for a series of protocols based on the same method, known as prepare-and-measure protocols, whose general principle was explained earlier. The various steps of this protocol are detailed below. In their paper, Bennett and Brassard propose that the realization of the MUBs representing the qubits are two complementary polarization bases.

Qubits preparation:
Alice produces randomly two tuples of length $4n$: $a = (a_1,a_2,...,a_{4n})$ and $b = (b_1,b_2,...,b_{4n})$ where each elements of a and b can take on values of either 1 or 0. Each element of the first tuple determines the basis that Alice will use to encode the corresponding qubit. To do so, she has to choose between two MUBs. A common approach is to select the Hadamard (X, formed by the vectors $|\pm_x\rangle$) and the computational basis (Z, formed by the vectors $|\pm_z\rangle$): 0 represents the Z basis and 1 represents the X basis. The physical realization of these bases can be achieved by using complementary polarization bases, for instance, matching the computational basis with the rectilinear polarization basis (formed by the states $|H\rangle$ and $|V\rangle$) and the Hadamard basis with the diagonal polarization basis (formed by the states $|D\rangle$ and $|A\rangle$). The second tuple contains the bits forming the key to send, and the two possible values, 0 and 1, can be associated with one of the vectors from either basis. For instance, the value 0 can be assigned to the states $|+_x\rangle$ and $|+_z\rangle$, and the value 1 to the states $|-_x\rangle$ et $|-_z\rangle$.
Thanks to these two tuples and the correspondence between binary values and quantum states to be transmitted, Alice knows which states to send to Bob, forming a block of $4n$ qubits :

$$|\psi\rangle_A = \bigotimes_{i=1}^{4n} |\psi_{a_i b_i}\rangle_A \tag{3.1}$$

where all the individual qubits are in one of the four states :

$$|\psi_{00}\rangle_A = |+_z\rangle_A \tag{3.2}$$
$$|\psi_{01}\rangle_A = |-_z\rangle_A \tag{3.3}$$
$$|\psi_{10}\rangle_A = |+_x\rangle_A \tag{3.4}$$
$$|\psi_{11}\rangle_A = |-_x\rangle_A \,. \tag{3.5}$$

These states are not all mutually orthogonal and so there is no measurement that allows to perfectly distinguish between all of the states with certainty.

Qubits transmission:
The transmission process can be influenced by the characteristics of the quantum channel, which can be either optical fiber or free space. Additionally, there exists a risk of interference from a third party, whom we will refer to as Eve, attempting to eavesdrop on the communication. As a result, Bob will receive a state $|\psi\rangle_B = \mathcal{E}(|\psi\rangle_A)$ where $\mathcal{E}$ represents both the effect of the quantum channel and the eventual Eve's interaction with the state.

Qubits measurement:
Bob measures each qubit rather in the computational basis or in the Hadamard basis at random. As a result, he now holds two strings of length $4n$: a' where his choice of basis is stored an b' that represents the decoded bit values.

Post-processing:
Now Alice and Bob have their own keys, respectively b and b'. The quantum communication is over. The differences between these keys arise from imperfections in the channel and instruments, as well as potential interaction by Eve. In order to share a symmetric key, it is necessary to make them identical. To do so, they proceed first the so-called sifting process. It functions as follows: Alice announces a through a classical public channel. All the pair of bits for which $a_i \neq a_i^{'}$ are discarded, so in the ideal case the remaining strings of Alice and Bob are the same, i.e. $b_i = b_i^{'}$, consituting the so-called sifted key. The length of these string must be about $2n$ since the probability that Bob chose the same basis for the measurement is $\frac{1}{2}$.

In reality, the sifted keys still contain differences due to the presence of noise or eavesdropping in the channel, resulting in a certain error rate, commonly referred to as the Quantum Bit Error Rate (QBER). To determine if the QBER is abnormally high, the quantum channel needs to be characterized. This can be achieved through parameter estimation, typically using half of the string. Consequently, Alice and Bob are left with a string of length n. After characterizing the quantum channel, Alice and Bob can continue the process as long as the number of errors among the remaining n bits is below a threshold value. They can then move on to the rest of the post-processing procedure to extract a secret key from the remaining data. The post-processing involves privacy amplification and error correction, transforming the partially secret key into a secure key of length $m < n$.

3.1.2 Discussion

Although theoretically unconditionally secure, as shown by Preskill and Shor in Ref.[44], the practical implementation of the BB84 protocol often deviates from the theoretical framework. This can make it vulnerable to side-channel attacks. One way to protect against these attacks is to require device independence [45]. In practice, this is too constraining, resulting in extremely low key rates [46] and a more pragmatic approach is to resort to measurement device independence [47]. These security aspects will be developed in Section 3.3.

The intensive study of QKD has led to numerous variations that address practical imperfections causing security issues or that improve performance. Nevertheless, almost all implementations are subject to problems related to imperfections in the channel and the single-photon source. Proposed solutions to these challenges are outlined below.

- Practical imperfections:

Imperfect channel:
In practice, perfect channels do not exist, and there will be noise even if the channel used by Alice and Bob is not being eavesdropped. It has been explained that Eve's presence would add additional noise to the channel. However, assuming Eve has active control over the channel, she could replace the imperfect channel with a better one. In this way, she could then extract information without Alice and Bob noticing an increase in the QBER. One way to defend against such attacks is to assume that all noise is caused by Eve. The question then becomes not whether the line is being eavesdropped, but whether it is still possible

to transmit information securely. In other words, given the observed QBER on the channel, is it possible to perform privacy amplification and transmit a private key? The amount of privacy amplification needed, and thus the answer to this question, naturally depends on the observed QBER. Shor and Preskill have shown [44] that this is indeed possible as long as the QBER is below approximately 11% (in the most general case of a coherent attack,detailed in Paragraph 3.3.3). This establishes an acceptable security threshold for the amount of QBER that a channel can support within the framework of the BB84 protocol.

Imperfect source:
BB84 relies on the ability to send single photons. However, current single-photon sources are imperfect. Indeed, the sources often used for implementing BB84 are weak coherent lasers. There is a non-zero probability that such a source emits multiple photons with identical encodings during a given execution of the QKD protocol. Considering a source of intensity μ, the probability for a pulse to contain a number n of photons is given by [6]:

$$P_n = \frac{\mu^n}{n!}\, e^{-\mu}. \tag{3.6}$$

The raw detection rate is defined as the probability that Bob detects a photon per pulse sent by Alice. In absence of Eve and for an imperfect setup where the source has intensity μ, the channel has attenuation η_δ, and the detector has a quantum efficiency η_δ, it is given by:

$$R_{raw}(\delta) = \sum_{n\geq 1} P_n[1-(1-\eta_{det}\eta_\delta)^n] \simeq \eta_{det}\eta_\delta\mu. \tag{3.7}$$

This equation is valid for $\eta_{det}\eta_\delta P_n n << 1$ which is always true for weak pulses.

For an imperfect photon source, Gottesman, Lo, Lutkenhaus, and Preskill (GLLP) in Ref. [48] derived an expression for the secure key generation rate, defined as the ratio of the secure key length to the total number of signals sent by Alice:

$$K \geq Q_\mu \{-H_2(E_\mu) + Q_1[1-H_2(e_1)]\} \tag{3.8}$$

where Q_μ is the gain of the signal state, which is the number of Bob's detection events when his choice of basis is the same as Alice, E_μ is the QBER of the signal state, Q_1 is the gain of single photon pulses, e_1 is the QBER of detection events by Bob that have originated from single-photon signal emitted by Alice and finally H_2 is the binary Shannon entropy defined by $H_2(x) = -x\, log_2 x - (1-x) log_2(1-x)$.

Q_μ and E_μ can be measured directly from experiments but obtaining a reliable lower bound on Q_1 and an accurate upper bound on e_1 is very challenging. The first method to tackle this issue involved assuming that all multi-photon signals sent by Alice are received by Bob. This assumption is not realistic and cannot be met by practical setups. For this reason, the unconditional security of a practical implementation using weak coherent pulses of the BB84 protocol cannot be assured if no measures are taken.

Indeed, this discrepancy between theoretical and experimental frameworks can be exploited as a security breach by Eve through the so-called "photon number splitting attack" (PNS) [49]. Lets assume that she has access to unlimited technology, being solely restricted by the laws of physics. The idea is that she can perform a non-destructive measurement to count the number of photons in a pulse emitted by the source. If the pulse contain a unique photon, she would just block it. If more than one photon are emitted, Eve could theoretically store one of them and send the others to Bob, through a perfect channel. She would then wait for Alice to announce her choice of bases to measure the stored qubit in the appropriate basis, without any risk of detection. In this way, Eve can have perfect knowledge of the multi-photon qubits without being detected.

In order to remain undetected, Eve must ensure that the raw detection rate Eq.(3.7) of Bob is not modified. Therefore, she may perform PNS attacks on all multi-photons pulses only if the expected losses in the channel due to its attenuation are equal to those introduced by her attack. This is the case if the attenuation in the channel is larger than a critical value δ_c^{BB84} defined by:

$$R_{raw}(\delta_c^{BB84}) = \sum_{n\geq 2} P_n[1-(1-\eta_{det})^{n-1}] \simeq \eta_{det} P_2. \tag{3.9}$$

For a typical intensity $\mu = 0.1$, $\delta_c^{BB84} = 13$ dB, meaning that for attenuation larger than 13 dB, the weak-pulse implementation of BB84 becomes insecure, even for a null QBER [50].

One way to foil the PNS threat is provided by the so-called "decoy-sates" strategy introduced in 2005 by Hwang [51]. The idea is that in addition to the signal state with an average photon number μ, Alice randomly blends some decoy states with other average photon numbers μ'. After Bob's reception of the signals, Alice announces which pulses are signals and which are decoy states. Alice and Bob are then able to compare detection rates between low-intensity and high-intensity states, thereby revealing any attempt by Eve to exploit multi-photon states.

The implementation of decoy-state technique is typically achieved using sources that produce phase-randomized weak coherent state pulses (WCPs). The coherent states from a laser, which are written as:

$$|\mu\rangle = e^{-\frac{|\mu|^2}{2}} \sum_{n=0}^{\infty} \frac{\mu^n}{\sqrt{n!}} |n\rangle \tag{3.10}$$

are subjected to variable optical attenuators, which adjust the amplitude μ to μ' such that $|\mu'| << |\mu|$, ensuring the average photon number is low (typically around 0.1). These variable attenuators enable different μ values for each individual state.

Phase randomization involves adding a random phase to each coherent pulse. It can be accomplished by placing an electro-optic phase modulator (PM) in the laser's optical path. This device modulates the phase of the light passing through it according to an applied electrical signal. This signal can be controlled by a random number generator (RNG) to generate a random phase. After phase randomization, the state becomes $\left|\mu e^{i\theta}\right\rangle$, where θ is a random phase uniformly distributed over [0,2π]. Therefore, phase randomization converts a coherent state into a statistical mixture of coherent states with various phases. The probability distribution for the number of photons in the signal state follows a Poisson distribution, i.e., the probability of obtaining n photons is given by $P(n) = \frac{\mu^n e^{-\mu}}{n!}$.

By following this process, Alice can generate any Poissonian mixture of photon number states and can vary the parameter μ for each individual signal. This allows the implementation of the decoy states technique [52], the concept of which is described above.

Another strategy to be robust against PNS attacks was proposed by Scarani *et al.* in Ref.[50]. The quantum aspect of the exchange is not altered: Alice randomly selects between the X and Y bases for qubit encoding, and Bob performs the measurement randomly in one of these two bases. Only the classical sifting procedure needs to be adjusted: instead of revealing the basis, Alice announces publicly one of the four pairs of nonorthogonal states $\mathcal{A}_{\omega,\omega'} = \{|\omega x\rangle, |\omega' z\rangle\}$ with ω,$\omega' \in \{+,-\}$. To obtain a conclusive result that allows him to unambiguously determine which state Alice sent among the two announced, Bob must have chosen the wrong basis and obtained the wrong result, which happens with a probability of 1/4. In this case, he can add the appropriate bit to his key.

To clarify the ideas, consider the case when Alice has sent $|+x\rangle$ and announced the set $\mathcal{A}_{++}$. The only scenario that allows Bob to unambiguously know the state sent by Alice is if he measured in the Z basis and obtained the result 1 (corresponding to the state $|-_z\rangle$). In this case, he is certain that Alice sent the state $|+_x\rangle$ and can add a 0 to his key. If, instead, Bob had obtained the result 0 (corresponding to the state $|+_z\rangle$) after his measurement, he would not have been able to conclude the state sent by Alice, as this result corresponds to both $|+_x\rangle$ and $|+_z\rangle$, the two states announced by Alice. If Bob had measured in the X basis, he would had obtained 0 with certainty and would have to reject the qubit.

This variant of BB84 is called the SARG04 protocol, named after its authors. Compared to BB84, it permits a higher attenuation threshold for security against PNS attacks but comes at the cost of a greater reduction in the size of the raw key during the sifting procedure; only a quarter of the bits can be retained compared to half in the original BB84 protocol. More precisely, the critical attenuation with this approach is determined by P_3 instead of P_2 in Eq.(3.9), leading to a increased tolerance of $\delta_c^{SARG04} - \delta_c^{BB84} \simeq 10$ dB for typical values. Security aspects for different QBERs are discussed in the

original paper [50].

- Performance:

More states:
Theoretically, it is possible to enhance the key generation rate and noise tolerance of the BB84 protocol by using six states in three MUBs [53]. In this scenario, Alice randomly selects between three pairs of MUBs. Typically, the eigenstates of the Y measurement operator are used in addition to the two bases typically employed in the BB84 protocol. These eigenstates are:

$$|+_y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}, \qquad |-_y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -i\end{pmatrix}.$$

The physical realization of these states can be performed using the circular polarization base.
For a given QBER, the key rates achieved by the six-states protocol are higher than those of the BB84 protocol. This is due to the fact that despite the number of discarded bits during the sifting process is higher, i.e. approximately $\frac{2n}{3}$ in place of $\frac{n}{2}$, the eavesdropper also has to choose between three different basis and this relaxes the constraints for the privacy amplification process [54].

Care must be taken with the following point: while the six-state protocol theoretically achieves higher key rates, adding bases necessitates additional lossy optical components for its physical implementation. This increase in equipment, apart from complicating the setup, inevitably adds noise. Hence, choosing a protocol should go beyond theoretical aspects and also consider its physical implementation to optimize parameters.

Higher dimension:
The BB84 protocol can be generalized to higher-dimensional quantum systems, transitioning from two-level quantum states to N-level quantum systems, known as qudits or qu$N$its [55]. One advantage of using a larger alphabet is the potential for increased noise tolerance [56], surpassing the 11% limit of the original two-level protocol. Implementing such protocols with higher-dimensional quantum systems is complex, leading to the emergence of a dedicated subfield in QKD, known as High Dimensional (HD) QKD, discussed in Section 4.4.

3.2 Entanglement based protocols

One of the major differences between classical and quantum bits is that these can be in a superposed state like (2.2). Another property specific to quantum systems is the entanglement between particles. Entanglement is a fundamental property of quantum systems wherein the quantum states of multiple particles become intertwined in such a way that the individual states can no longer be described independently. Mathematically, this is expressed as follows: an entangled state $|\psi\rangle \in \mathcal{H}^k$ in a Hilbert space of dimension k cannot be factorized, i.e., there are no $|\psi_i\rangle \in \mathcal{H}^{m_i}$ such as $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$ with $k = \sum_{i=1}^{n} m_i$. As a consequence, the measurement of one of the particles instantly affects the overall state of the system, so the other entangled particles. Moreover, measurement of physical properties performed on entangled particles can be correlated, regardless of the spatial distance between those particles.

Bell states are maximally entangled states that are notable for their relative ease of implementation

(see Section 5.1) and their simple representation (in the computational basis):

$$|\psi\rangle^{+}_{AB} = \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}} \tag{3.11}$$

$$|\psi\rangle^{-}_{AB} = \frac{|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B}{\sqrt{2}} \tag{3.12}$$

$$|\phi\rangle^{+}_{AB} = \frac{|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B}{\sqrt{2}} \tag{3.13}$$

$$|\phi\rangle^{-}_{AB} = \frac{|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B}{\sqrt{2}} \tag{3.14}$$

If the system is described by one of the $|\psi\rangle$ states, and if a measurement is performed on qubit A, then a measurement of qubit B would give the identical result with certainty. In other words, by performing a measurement on one qubit of the entangled pair, the state of the second qubit is instantaneously modified. For the $|\psi\rangle$ states, the results of the measurements would give perfectly anti-correlated results.

An essential point to highlight is that it is possible to determine the degree of entanglement between particles by evaluating the correlations between measurements of physical quantities using the CHSH inequality. This inequality was formulated in 1969 by John Clauser, Michael Horne, Abner Shimony, and Richard Holt [57]. The inequality is derived by considering four random variables A_1, A_2, B_1 and B_2 allowed to take only -1 or +1 as value. Then, taking the expectation value over N assignments gives:

$$|\,\langle (A_1(B_3 + B_2) + A_2(B_3 - B_2)\rangle\,| \leq 2. \tag{3.15}$$

Using the fact that taking the expectation value of a random variable is a linear operation, rewriting of equation (3.15) allows to obtain the CHSH inequality :

$$S := |\,\langle A_1 B_3\rangle + \langle A_1 B_2\rangle + \langle A_2 B_3\rangle - \langle A_2 B_2\rangle\,| \leq 2 \tag{3.16}$$

where $\langle A_i B_j\rangle = \sum A_i^{\nu} B_j^{\nu}$ with A_i^{ν} and B_j^{ν} the assigned values ν to the random variables A_i and B_j. The parameter S, known as the Bell factor, satisfies $S \leq 2$ for all local realistic models. However, entangled quantum systems can violate the CHSH inequality, demonstrating values of S greater than 2. The maximal value for this violation is $S_q = 2\sqrt{2}$.

A source of entangled photons can be utilized to transmit a secret key between two correspondents. This concept is central to entanglement-based protocols, which were first introduced by Ekert in 1991 with the E91 protocol [58]. This protocol is detailed below. The idea involves using a source of entangled qubits, which are transmitted to the correspondents via a quantum channel. Entanglement ensures that the measurement results of the correspondents are correlated, allowing them to share a secret key. The confidentiality is derived from the monogamy of entanglement [59], ensuring no other quantum system can be entangled with maximally entangled states without reducing their entanglement degree. An eavesdropper would decrease the degree of entanglement, leading to reduced correlation between the measurements of the correspondents. To ensure the channel's security, the correspondents communicate (via a classical channel) part of their measurements to verify their correlation degree by verifying the violation of the CHSH inequality. It is not necessary for the source to be a trusted device as the quantum correlations between the two photons measured by the communication partners cannot be emulated or faked by a malicious adversary.

The basic architecture of such protocols is shown in Figure 3.2.

3.2.1 E91

In the E91 protocol introduced by Artur Ekert in 1991 [58], the physical realization of the qubits can be achieved by using polarized light, similar to the BB84 protocol. As usual, the X (Hadamard) and Z (computational) basis are represented by the diagonal and rectilinear polarization basis, respectively. The different steps of the protocol are detailed below.

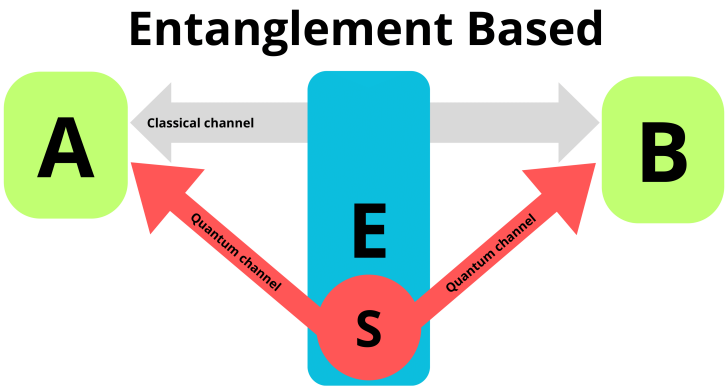

Figure 3.2: Basic architecture of entanglement based protocols. A source (S) delivers entangled qubits to Alice (A) and Bob (B) via quantum channels. Additionally, Alice and Bob have a classical channel at their disposal. Eve (E) is assumed to have full control over the quantum channels and the source but is limited to passive control over the classical channel.

Qubit preparation:
A source generates maximally entangled pairs of qubits among them, for instance the Bell state $|\phi\rangle^-_{AB}$ of Eq.(3.14).

Qubit transmission:
Each pair of entangled photons is distributed such that one photon goes to Alice and the other to Bob. The effect of a non-ideal channel is to replace the initial entangled state $|\psi\rangle$ with an isotropic mixed state with probability p. This effect can be modeled as follows:

$$\rho_\psi = p\,|\psi\rangle\langle\psi| + (1-p)\mathbb{I}/4. \tag{3.17}$$

Here, ρ represents the resultant state of the system after considering the impact of the non-ideal channel, $|\psi\rangle\langle\psi|$ is the pure entangled state, and $\mathbb{I}$ is the identity matrix in the four-dimensional space, signifying a completely mixed state.
The specific instance of an ideal channel corresponds to the choice $p = 1$.

Qubit measurement:
To measure the entanglement degree of their qubits according to the experiment described in [57], Alice and Bob are required to use specific polarization bases for their measurements. There are optimal basis choices that maximize the violation of the CHSH inequality. For example, for the bipartite states $|\psi\rangle^-_{AB}$, Alice and Bob can randomly select a measurement basis A_i and B_i with i = 1,2,3 from the following set:

$$A_1 = Z, \qquad B_1 = Z, \tag{3.18}$$

$$A_2 = X, \qquad B_2 = \frac{1}{\sqrt{2}}(Z - X), \tag{3.19}$$

$$A_3 = \frac{1}{\sqrt{2}}(Z + X), \qquad B_3 = \frac{1}{\sqrt{2}}(Z + X). \tag{3.20}$$

The angles of the polarization analyser used for the measurement in these basis are respectively $a_1 = 0$, $a_2 = \pi/2$, and $a_3 = \pi/4$ for Alice and $b_1 = 0$, $b_2 = 3\pi/4$, and $b_3 = \pi/4$ for Bob. The meaning of the equalities $A_1 = B_1$ and $A_3 = B_3$ is that it corresponds to situations where the measurement directions chosen by Alice and Bob are the same. The table below outlines the possible scenarios:

CHSH game:
Alice and Bob publicly (via the classical channel) announce the directions they chose for each measurement. For those pairs where the directions match, i.e. the pairs (A_1,B_1) or (A_3,B_3) they get completely anti-correlated results. Thus they can get the sifted key by one party inverting all its bits. For the other

	B_1	B_2	B_3
A_1	k	c	c
A_2	c	c	c
A_3	c	c	k

Table 3.1: In the E91 protocol, $\frac{2}{9}$ of the transmitted qubits are used to generate key bits (the entries of the table containing a k), while the remaining qubits are utilized to verify the violation of the CHSH inequality (the entries of the table containing a c).

pairs, measurements are used to estimate how much information an eavesdropper has about the key. This is done by checking the CHSH inequality. Consider A_1, A_2, B_1 and B_2 of the (3.16) to be the quantum observables as defined in the protocol. It is possible to evaluate their expectation values with respect to the state $\rho = |\psi^-\rangle\langle\psi^-|$ using that their products is then given by $\langle A_i B_j\rangle = Tr(A_i \otimes B_j \rho)$. For instance, if we consider the measurement directions A_1 and B_3, their expected value is then given by

$$\langle A_1 B_3\rangle = \langle\psi^-| \left(Z \otimes \frac{1}{\sqrt{2}}(Z+X)\right) |\psi^-\rangle = -\frac{1}{\sqrt{2}}. \tag{3.21}$$

Using this it is possible to compute all the terms of (3.16) with the polarization directions as defined in the protocol. If Alice and Bob are sharing a maximally entangled state, this would give the following value for the Bell factor:

$$S_q = 2\sqrt{2} \tag{3.22}$$

which is a maximal violation of (3.16). It means that a third party cannot get any information since a maximally entangled bipartite state cannot be entangled with a third party.

Post-processing:
The CHSH inequality violation factor can be defined as the ratio of its quantum value to its classical value:

$$v = \frac{S_q}{S} \tag{3.23}$$

where $S = 2$ is the maximal value for the Bell factor under local realistic assumptions.

If $v > 1$, then Alice and Bob can obtain the final secret key by applying error correction and privacy amplification on the sifted key. If $v \leq 1$ then the sifted key may be compromised, and the protocol must be restarted. With the optimal choice of measurement bases proposed in the protocol, the maximal value for the violation factor is $v = \sqrt{2} \simeq 1.414 > 1$.

3.2.2 Discussion

- Practical implementation:

Practical implementations of the E91 protocol will be discussed later in Chapter 6. However, it is already worth noting that the protocol does not specify the location of the source. It might be more convenient for the source to be with one of the parties, allowing one photon of the pair to be measured locally while the other is sent to the other party. Nevertheless, to cover greater distances, the source can be placed between the two parties, so that each channel has a shorter distance than the separation between the parties (for example, see the experiments conducted by Peng *et al.* discussed later in Paragraph 6.2.1).

- Practical imperfection:

Imperfect channel:
The effect of a non-ideal channel is modeled by Eq.(3.17). This modeling allows to establish a threshold

marking the limit on the acceptable amount of noise in the channel. Indeed, the presence of noise decreases the violation factor down to $(1-p)v$; values of p greater than:

$$p_{max} = 1 - \frac{1}{v} \tag{3.24}$$

imply $v \leq 1$ and it becomes impossible for the CHSH inequality to be violated. The maximum QBER that allows the protocol to remain unconditionally secure is approximately 14.64% [60]. It can already be stated that this result is superior to that of the original BB84 protocol.

Imperfect source:
It is possible for a source of entangled photons to generate multiple pairs of entangled photons in one single pulse. From these pairs, a maximally entangled three-qubit state can be observed. Such a state is known as a Greenberger-Horne-Zeilinger (GHZ) state and is represented as

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{3.25}$$

Observation of GHZ states is outlined in Ref.[61]. Consequently, the protocol is susceptible to PNS attacks similarly to the BB84 protocol. Nonetheless, the decoy-state method can be employed in practical implementation as an efficient countermeasure.

- Performance:

It has been demonstrated that the violation of local realism is more pronounced in entangled quantum systems with qu$N$its [62]. To achieve this, the CHSH inequality for qubits must be generalized to N dimensions, referred to as the commonly CGLMP inequality [63]. In particular, the generalization of the E91 protocol to "qutrits," which are three-level quantum systems, has been proven to be more robust and safer compared to its two-dimensional version [64, 65]. In Ref.[60], the E91 protocol was generalized to N-level quantum systems, resulting in the N-dimensional Entanglement Based (N-DEB) protocol. In their paper [60], Durt *et al.* showed that the security of the protocol is higher for higher dimensional systems. A more general discussion on the security of QKD will be provided in Section 3.3.

- Alternative for the verification entanglement's degree:

Alternative basis choice:
Another optimal choice for verifying the CHSH inequality involves selecting polarizer angles at $\phi_A = 0°$, $\phi'_A = 45°$ for Alice and $\phi_B = 22.5°$, $\phi'_B = 67.5°$ for Bob. The polarization coefficient is then define as:

$$E(\phi_A,\phi_B) = \frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}} \tag{3.26}$$

where $N_{ij}(\phi_A,\phi_B)$ are the coincidences i channel of the polarizer of Alice set at angle ϕ_A and the j channel of the polarizer of Bob set at angle ϕ_B. These angles provide a maximal theoretical violation of the CHSH inequality for entangled states, as they allow for the highest possible correlation differences between the measurement outcomes, which cannot be explained by local realism. Quantum mechanics predicts a sinusoidal dependence for $N_{ij} \propto sin^2(\phi_A - \phi_B)$.

The CHSH inequality Eq.(3.16) can be written as:

$$S = |E(\phi_A,\phi_B) - E(\phi_A,\phi'_B) + E(\phi'_A,\phi_B) + E(\phi'_A,\phi'_B)|. \tag{3.27}$$

Visibility of an entangled pair:
For polarization-entangled photons, they are measured by independently adjustable polarization analyzers. Strong correlation, or anti-correlation depending on the prepared quantum state, is observed when the analyzers are aligned. By adjusting the analyzer angles, a sinusoidal variation in joint detection probability, known as interference fringes, emerges. These fringes, which directly result from the quantum

states superposition, demonstrate maxima when states are perfectly aligned and minima when opposed. These fringes reveal the correlation between the polarization states of the photons, thereby serving as a means to quantify the degree of entanglement. In practice, the visibility V of an entangled photon pair can be used as an indicator of the degree of entanglement. It is defined by the contrast in the interference fringes observed when measuring the correlations between the two photons:

$$V = \frac{C_{max} - C_{min}}{C_{max} + C_{min}} \tag{3.28}$$

where C_{max} and C_{min} represent the maximum and minimum coincidence rates observed during the measurement of correlations between the two photons, respectively. A visibility of 100% indicates perfect entanglement, with no decoherence or noise, while a visibility of 0% indicates the absence of entanglement. The assessment fort

The Bell parameter S_q is proportional to V according to the relation $2\sqrt{2}V$. To observe a violation of the CHSH inequality, the visibility must therefore exceed $\frac{1}{\sqrt{2}}$, which corresponds to 70.7%.

- Link between Prepare-and-measure and Entanglement based protocols:

There exists an entanglement-based version of the BB84 protocol, known as BBM92, described by Bennett *et al.* in Ref.[66]. Similar to E91, a Bell state $|\psi\rangle^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ is prepared by a source, and one qubit of this pair is transmitted to Alice and Bob. For each qubit they receive, Alice and Bob perform measurements randomly in one of the same MUBs as in the BB84 protocol, i.e., the X and Z bases, represented by diagonal and rectilinear polarization bases, respectively. They then proceed to the sifting procedure, publicly announcing their basis choices. When their basis choices match, Alice and Bob are expected to have correlated results, with discrepancies indicating the presence of an eavesdropper. Therefore, they discard a portion of their bits to compare them and ensure that there is no eavesdropper on the channel. Here, there is no need to perform a Bell inequality test.

In fact, any prepare-and-measure protocol can be directly converted into an entanglement-based scheme [5]. Indeed, first Alice can prepare the entangled state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d_n}} \sum_{\mathcal{S}_n} |\mathcal{S}_n\rangle_A \otimes |\psi(\mathcal{S}_n)\rangle_B \tag{3.29}$$

where d_n represents the number of possible $\mathcal{S}_n$ sequences and the $|\mathcal{S}_n\rangle_A$ constitute an orthogonal basis. Then, Alice measures it in this orthogonal basis. In doing so, she identifies one $\mathcal{S}_n$ and prepares the corresponding $|\psi(\mathcal{S}_n)\rangle$ on the subsystem sent to Bob. From Bob's point of view, this procedure is indistinguishable from a prepare-and-measure protocol. This implies that the security proofs for the prepare-and-measure protocol translates immediately to the corresponding entangled protocol and vice versa (more about security proofs in the next Section). Caution is advised; even though the theoretical security proofs may be equivalent, the experimental verification of channel security differs between prepare-and-measure protocols and the ones based on entanglement-based. In the former, one checks the QBER using samples from the sifted key, whereas for entanglement-based schemes the parties assess the degree of correlation using a part of the raw key through the CHSH inequality.

- Benefits of Entanglement based protocols:

One notable benefit of entangled versions of the protocols is that the source does not need to be situated at Alice's location; instead, it can be placed between the communicating parties, thus shortening the distance that needs to be covered on a single channel. Moreover, a trusted source is not required since the quantum correlations between the two photons, recorded by the communication partners, are immune to imitation or falsification by any malicious entity.

Another advantage of entanglement-based protocols is that they do not require a random number generator at the source, unlike prepare-and-measure protocols where Alice randomly selects between MUBs

for encoding her qubit. Consequently, no information about the individual photon states exists prior to measurement.

Finally, it has been emphasized [67] that entanglement-based QKD systems can tolerate higher channel losses than systems based on weak coherent laser pulses (WCP), in particular, when the source is located symmetrically between the two communicating parties, Alice and Bob.

3.3 Security of QKD

The claim of QKD is to achieve unconditional security for telecommunications. This section aims to provide tools for understanding how to evaluate the security level of a protocol and the related issues.

3.3.1 Notions of security

In this paragraph, the security of QKD protocols will be discussed. To do so, it is important to bring a quantifiable aspect to the notions of security. Therefore, the initial step is to rigorously define these concepts.

- Security:

Following Scarani *et al.* [5], the ϵ-security of a key can be defined by its deviation ϵ from a perfect key, which is a list of perfectly correlated symbols shared exclusively between the legitimate correspondents. This deviation is measured using the trace distance D [1]: if $\sigma^I_{S_A S_B E}$ and $\sigma^R_{S_A S_B E}$ are respectively the outputs of the ideal and of the real protocol, then it is ϵ-secure if

$$D(\sigma^I_{S_A S_B E}, \sigma^R_{S_A S_B E}) \leq \epsilon. \tag{3.30}$$

- Composability:

The concept of composability enables the quantification of the security level when combining several cryptographic tasks. When an ϵ-secure key is used in an ϵ'-secure task, composability guarantees that the overall process is at least $(\epsilon + \epsilon')$-secure.

These notions form the foundation for deriving security proofs of different quantum cryptography protocols.

3.3.2 Tradeoffs

The security of a protocol is directly linked to the achievable key rates; the more bits from the raw key used during post-processing, the fewer errors are present in the final key and the more secure it is. Indeed, there are two tradeoffs during post-processing.

First, verifying successful error correction involves Alice and Bob using hash functions f with two properties: 1) it is impossible to infer x from the output $f(x)$; 2) if the outputs are equal, $f(x) = f(y)$, there is a high probability p that the inputs are equal, $x = y$. Decreasing p requires more raw key bits, reducing the final key size. Hence, there is a tradeoff between the key amount and error probability.

Second, during privacy amplification, compressing error-corrected bit strings reduce Eve's information. More compression means less information for Eve, resulting in a tradeoff between key length and secrecy.

On the other hand, increasing the security of a QKD protocol, i.e., reducing ϵ^{QKD}, decreases the risk of a security breach. In Ref.[4], this is described in terms of the cost for insurance that would cover the damage caused by a security breach. Reasoning in these terms, the situation can be illustrated as shown in Figure 3.3.

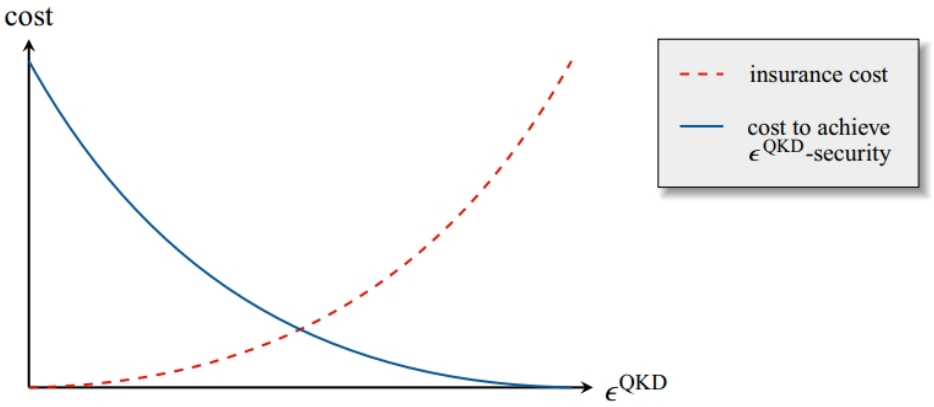

Figure 3.3: Schematic depiction of the tradeoff betwen security and insurance cost. Increasing the security level, i.e. lowering ϵ^{QKD}, requires higher implementation costs. On the other hand, the insurance cost are lower when the level of security is higher. Figure from Ref.[4].

3.3.3 Different attack strategies

By classifying different attack strategies, it becomes easier to identify which protocols are robust against particular types of attacks. This paragraph will therefore be dedicated to such a classification.

- Theoretical framework:

A preliminary assessment of protocol robustness can be made without considering its physical implementation—or, put another way, assuming a perfect experimental setup. Security is then assessed in terms of the resources available to Eve. In addition to the basic Intercept-Resend strategy, three scenarios can be considered.

Intercept-Resend strategy:
In Intercept-Resend attacks, Eve intercepts each qubit intended for Bob and measures it in a random basis. When her basis matches Alice's choice, she can obtain all the information and transmit the qubit to Bob without him detecting any disturbance. When Alice's and Eve's bases do not match, Eve gets no information, and the qubit she sends to Bob is inevitably disturbed.

Individual attacks:
In the scenario of individual attacks, it is assumed that Eve can only target each qubit separately, applying the same attack strategy uniformly across all qubits. This implies that Eve will use a fresh ancilla to interact with each qubit and then measure each resulting ancillary system individually. Eve might however have access to a quantum memory, enabling her to store the intercepted states and delay her measurement until after the basis revelation phase, allowing her to optimize her measurement choices.

Collective attacks:
In collective attacks Eve uses again a fresh ancilla for each signal but each output is then stored in a quantum memory, allowing her to perform a collective measure at the end of the protocol on all the stored qubits in her quantum memory.

Coherent attacks:
Coherent attacks represent the most general form of attack, limited only by the laws of physics. In these scenarios, Eve can exploit the entire quantum state, potentially gaining more information by analyzing the correlations between different qubits. In particular, Eve's ancilla and the signals may be subjected to a joint unitary interaction, and the outputs are stored in a quantum memory for measurement after the classical communication between the parties [6].

- Practical considerations:

The physical implementation of a protocol rarely aligns exactly with its theoretical framework, which assumes perfect devices for the source, classical and quantum channels, as well as detectors. Imperfections in the setup can be exploited as security loopholes by malicious third parties. Such attacks that exploit features not modeled in the security proof are known as side-channel attacks. A particularly significant example is the PNS attack mentioned in Section 3.1.2.

Upon discovery, side-channel attacks can be addressed with countermeasures like the decoy-state protocol, specifically designed to combat PNS attacks. However, the reliability of mitigating such attacks hinges on their discovery. Certification of components via Device-Independence (DI) [45] is an approach that enhances trust in QKD systems. DI protocols are not susceptible to side-channel attacks because they make no assumptions about how devices are utilized. Therefore, there is no need for a mathematical model to characterize the behavior of a device; these devices are treated as black boxes that receive inputs and produce outputs. Security is ensured by testing these inputs/outputs using CHSH inequality tests, which verify the presence of quantum correlations and confirm device behavior aligns with expected models.

Implementing DI-QKD protocols is significantly more challenging than deploying ordinary QKD. The main difference lies in the fact that in a device-dependent protocol, failed detection events merely slow down key generation. In contrast, these events completely hinder the successful execution of a device-independent protocol because they prevent the CHSH inequality test. Therefore, DI-QKD requires detectors to operate with near-unity efficiency; otherwise, these protocols cannot be realized. This makes DI-QKD protocols very difficult to implement in practice and the achieved key rates are extremely low, of the order of 10^{-10} bits per pulse [46].

MDI-QKD [47] offers a particularly promising alternative by utilizing untrusted measurement devices. This method eliminates all detector side channels, the most critical part of the implementation, transferring these vulnerabilities to the source instead. Alice and Bob have better control over their sources, with the signals being attenuated laser pulses that can be prepared and potentially verified by themselves. Removing the constraints on detectors allows for the use of superconducting nanowire single-photon detector (SNSPDs), which exhibit remarkable efficiencies, achieving key rates comparable to those of decoy-state protocols.

Another difference between the theoretical framework and the physical implementation that can impact the security proof of a protocol is the common assumption that the parties exchange a number $n \to \infty$. In reality, this number is finite, and finite-size effects can become significant, necessitating consideration in the establishment of the security proof. Quantitative considerations about such effects are available in Ref.[6].

3.3.4 Security proofs

In the previous paragraphs, the main aspects to consider in order to establish the security proof of a protocol have been mentioned. The role of a security proof, beyond providing a quantitative estimation of the security of a protocol, is to offer an explicit expression for the achievable secret key rates. Practically, this involves linking the ϵ-security criterion (3.30) to the length l of the secret key that can be extracted from a given amount of sent signals.

The first strategy to establish such a connection was based on the principle of uncertainty [68]. Another effective approach for establishing the unconditional security of a QKD protocol is to reduce it to an entanglement distillation protocol (EDP). Such a protocol enhances the degree of entanglement of a set of non-maximally entangled pairs at the cost of reducing the number of entangled pairs. Such an "entanglement-purification" can be achieved using only local operations and classical communication through quantum error correction codes, specifically the Calderbank-Shor-Steane (CSS) code [1]. This approach was used by Shor and Preskill [44] to establish the security proof of BB84 (in the ideal case of a noiseless channel). The techniques developped by Shor and Preskill to remove the use of quantum

computation using CSS codes have been generalized to apply in the case of imperfect devices [48, 69]. In particular, in Ref. [48], the authors considered the security loopholes that emerge from imperfect implementations and establish the upper bound for the fraction of tagged bits (raw bits generated by multi-photon pulses) below which it is still possible to transmit a secure final key, giving rise to an expression for the secure key generation rate Eq.(3.8).

For entanglement-based protocols, the lower bound required for the key generation rate was established in Ref.[67] by applying Koashi and Preskill's security proof for entanglement-based protocol [70]. It is given by:

$$K \geq q \left\{ Q \left[1 - f(E) H_2(E) - H_2(E) \right] \right\} \tag{3.31}$$

where q is the basis reconciliation factor, Q is the gain factor, E is the QBER, $f(x)$ is the error correction efficiency and $H_2(x)$ is the binary entropy function.

Chapter 4

Alternative coding schemes

In the last four decades, QKD has undergone intensive research, resulting in many approaches designed to address particular requirements and adapt to technological progress, giving rise to multiple QKD subfields.

4.1 Continuous variable QKD

It is possible to encode information using continuous variables (CV) rather than discrete variables (DV). The quantum systems of interest for representing these variables are then described in an infinite-dimensional Hilbert space [71]. Essentially, there are four types of CV QKD, based on the signal states (squeezed or coherent) and the detection method (homodyne or heterodyne).

The physical observables used to realize such variables can be the quadratures $\hat{q}$ and $\hat{p}$ of the electromagnetic field. For each bosonic mode $k = 1,...,n$, the quadratures $\hat{q}_k$ and $\hat{p}_k$ are defined. The quantization of the electromagnetic field implies that quadrature components cannot be measured simultaneously with infinite precision, as their fluctuations adhere to the Heisenberg inequality [72]. For a specific mode, several classes of quantum states can be considered, notably coherent and squeezed states, which are important for QKD. Coherent states have minimal, symmetrically distributed vacuum noise in the two quadratures. Squeezed states exhibit reduced noise in one quadrature and increased noise in the other [6].

CV QKD enables homodyne detection, unlike DV QKD which requires single-photon detection. Homodyne detection involves coupling the optical signal with the beam from a local oscillator (LO) of the same frequency. The LO acts as a phase reference, allowing the selection of which field quadrature to measure. The beams are superimposed at a balanced beam splitter and the intensity of the resulting beam is measured by two proportional detectors. Depending on the phase difference between the signal and the LO, the difference in photocurrents produced in the detectors will be proportional to one of the two field quadratures, enabling its measurement.

As the homodyne detection discriminates between field quadratures, information can be transmitted using a single-mode beam that is randomly squeezed in one of the quadrature directions [73]. Heterodyne detection allows to simultaneously measure both quadratures by splitting the incoming signal and performing two homodyne measurements with LO phases differing by $\pi/2$ [74].

The security of CV QKD relies on the properties of the quadrature measurements and the impossibility of simultaneously measuring $\hat{q}$ and $\hat{p}$ with infinite precision due to Heisenberg's uncertainty principle. The security proofs of CV QKD protocols demonstrate that any attempt by an eavesdropper to gain information about the key will introduce detectable noise or disturbances in the quadrature measurements [75, 76]. The practical security of CV-QKD involves handling the finite number of data points collected

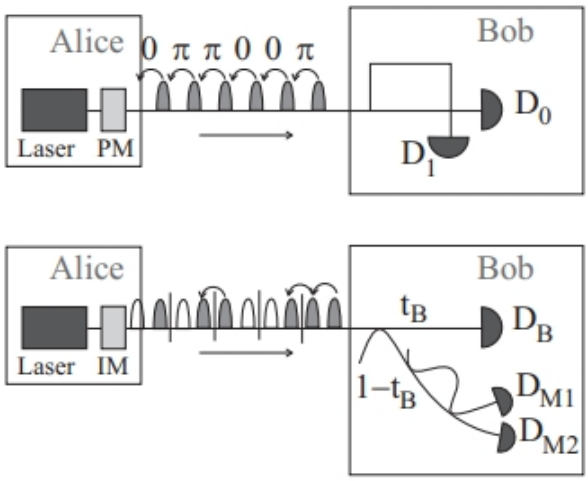

Figure 4.1: Schematic view of the two DPR protocols. DPS (on top) is based on phase modulation (PM). Measuring the phase differential requires between two subsequent pulses requires to make them interact necessitating a device such as an unbalanced MZI, which introduces an optical path difference between the two pulses. COW (on bottom) relies on intensity modulation (IM), using temporal differences between pulse detections to establish the secret key. A single detector (D_B) suffices ideally. In practice, the measurement of the phase differences between successive pulses support channel estimation and PNS attack detection. This measurement is achievable through an unbalanced MZI with outputs read by two detectors (D_{M1} and D_{M2}). Figure from Ref.[5].

during experimental implementation, finite-size effects must therefore be taken into account [77].

4.2 Distributed-phase-reference QKD

Distributed-phase-reference (DPR) protocols are characterized by encoding information through the phase or intensity differences between subsequent pulses rather than in each pulse separately. Protocols that use phase modulation are called differential phase shift protocols, while those that use intensity modulation are known as coherent-one-way protocols [5].

While DPR QKD protocols are relatively easy to implement, their security proofs are challenging to establish. The complexity stems from extracting the secret key from the relative phases of adjacent pulses, with all pulses being interconnected, thus necessitating the consideration of an extensive Hilbert space. Current security proofs assume ideal conditions for Bob's measurement unit [78]. The two protocols are illustrated by Figure 4.1.

4.2.1 Differential Phase Shift

The concept behind Differential Phase Shift (DPS) QKD involves encoding information through the phase difference between successive signals. The main advantage of this technique is its relative ease of implementation: a coherent laser is attenuated, and the phase differential can be introduced by an electro-optic modulator controlled by a random number generator (RNG) placed in the optical path of the beam. The decoy-states strategy is not required as the PNS attacks are no longer zero-error attacks for DPS, enabling higher key rates [79]. Alice therefore send a sequence of coherent states of same intensity:

$$|\psi(\mathcal{S}_n)\rangle = ... \left|e^{i\phi_{k-1}}\sqrt{\mu}\right\rangle \left|e^{i\phi_k}\sqrt{\mu}\right\rangle \left|e^{i\phi_{k+1}}\sqrt{\mu}\right\rangle \tag{4.1}$$

with each phase set at $\phi = 0$ or $\phi = \pi$. The bits are encoded in the phase difference of subsequent pulses: $b_k = 0$ if $e^{i\phi_k} = e^{i\phi_{k+1}}$ and $b_k = 1$ otherwise. At the receiver, an unbalanced Mach-Zehnder interferometer (MZI) combined with two detectors allows the determination of the phase difference between successive pulses.

4.2.2 Coherent-One-Way

For Coherent-One-Way (COW) protocols, the bits are coded using sequences of empty and non-empty pulse:

$$|0\rangle_k = |\sqrt{\mu}\rangle_{2k-1} |0\rangle_{2k}, \qquad |1\rangle_k = |0\rangle_{2k-1} |\sqrt{\mu}\rangle_{2k} \tag{4.2}$$

Channel estimation can be achieved by measuring the phase difference between two specifically generated coherent states, called decoy-states. To perform this phase measurement it is necessary to make interact the two coherent states using, for example, an unbalanced (MZI). This also allows for the detection of PNS attacks [6], hence the term "decoy states" for this sequence of coherent states.

The main advantage of this method is that, apart from measurements made on the decoy states, it is sufficient to measure the arrival times of the pulses to distinguish the two states and derive the secret key.

4.3 MDI QKD

As explained in section 3.3.3, MDI QKD is a method that requires no assumptions about how measurements are performed; only the inputs and outputs matter. This means that the measurements can be monitored or even controlled by Eve, and yet, Alice and Bob will still be able to exchange a secret key. The principle of MDI QKD is based on the distribution and measurement of a maximally entangled photon pair. Its security is based on the time-reversed version of entanglement-based QKD protocols. An example of its operation is described in [80]: Alice and Bob randomly and independently prepare single photons in one of the four BB84 qubit states, i.e., $|\pm_z\rangle$ or $|\pm_x\rangle$. These qubits are then sent to the measurement unit, assumed to be under Eve's control. Eve performs a Bell state measurement (BSM) [81], projecting the joint state of the photons onto the 4-dimensional Hilbert space spanned by the four Bell states:

$$|\psi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B) \tag{4.3}$$

$$|\phi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B). \tag{4.4}$$

Eve announces the instances where the measurement resulted in a projection onto $|\phi\rangle^-$. For these instances, Alice and Bob publicly announce the bases in which they prepared their photons. They then keep only the instances where they chose the same basis. In these cases, the state $|\phi\rangle^-$ could only have been obtained with different basis states. Thus, Alice and Bob end up with perfectly anti-correlated keys (in the ideal case), and one party only needs to flip all its bits. They can then disclose a sample of the keys to evaluate the error rate, which is used to bound the information Eve might have acquired during photon transmission. Finally, they perform error correction and privacy amplification.

4.4 High dimensional QKD

High-dimensional (HD) QKD leverages the capability to transmit more than one bit per signal by utilizing quantum systems with N dimensions. These are known as qudits or qu$N$its and allow to transmit $log_2 N$ bits of information per photon but the information density per mode is decreased as $\frac{log_2 N}{N}$ [6].

When transmitting a given amount of information, HD QKD requires fewer photons compared to basic QKD. This is especially useful when Alice's emission rate is lower than Bob's detection rate or in the reverse situation. Typically, Alice uses an attenuated laser source, making the emission rate non-critical. Bob, however, reaches saturation when his detection rate, limited by the dead time of his detectors, is below the incoming signal flux, corresponding to Regime I in Figure 4.2. In this case, HD QKD is advantageous as it allows sending fewer photons, just below Bob's detection threshold, while still conveying the same amount of information [6].

Another advantage of HD QKD is that it exploits the increased robustness to noise with higher dimensions N of qudits [56], making it a viable alternative in noisy environments.

However, HD QKD has its drawbacks. It can be more complex to implement, particularly since detection methods require a number of single-photon detectors (SPDs) that scale with the dimensionality N, quickly making practical deployment infeasible. Furthermore, adding devices such as SPDs not only complicates the experimental setup but also introduces additional noise into the protocol. This results in a situation where a method theoretically more tolerant to noise is only implementable at higher noise levels. Some solutions have been proposed to address this issue [82], but no security proofs have been provided. Additionally, since HD QKD relies on single-photon transmission, decoy state techniques are necessary to counter PNS attacks.

A physical observable investigated for implementing HD QKD is the orbital angular momentum (OAM) of photons [83]. The computational basis eigenvectors are realized by single-photon quantum states corresponding to elementary excitations of Laguerre-Gauss modes (LG_l) carrying an OAM value of $l\hbar$. This enables the realization of qu$N$its of dimension $N \geq 2$. For instance, in the case of $N = 3$, the states of the computational base are realized by the LG_l modes of a photon with OAM values $l = -1, 0, 1$:

$$\left\{ |-1\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |0\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}. \tag{4.5}$$

The matrix representations of the three remaining MUBs expressed in the computational basis are:

$$\frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega \\ 1 & \omega & 1 \\ \omega & 1 & 1 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \\ \omega^2 & 1 & 1 \end{pmatrix} \tag{4.6}$$

where each column represents the vectors of the corresponding MUB and ω represents a primitive third root of unity, i.e. $\omega = e^{2\pi i}/3$ satisfying $\omega^3 = 1$.

A generic prepare-and-measure OAM protocol consists of Alice preparing her qu$N$its randomly in one of the $(N + 1)$ MUBs and Bob measuring the incoming signals randomly in the same set of MUBs. The subsequent post-processing is similar to BB84, comprising the steps of sifting, parameter estimation, error correction, and finally privacy amplification.

Other encoding modes are possible for HD QKD, such as time-bin coding (see next Paragraph).

4.5 Time-bin coding

The principle of time-bin QKD is to encode information in the temporal position of photons. In the first proposal [7], it was suggested to use two time intervals. The state $|0\rangle$ of the computational basis corresponds to a photon arriving in the first time interval, denoted as $|short\rangle$, and the state $|1\rangle$ corresponds to a photon arriving in the second time interval, denoted as $|long\rangle$. The general expression of a qubit is thus a superposition similar to Eq.(2.2):

$$|\psi\rangle = \alpha\,|short\rangle + \beta\,|long\rangle\,. \tag{4.7}$$

For a two-qubit system, the four Bell states are written as:

$$|\psi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|short\rangle_A\,|short\rangle_B \pm |long\rangle_A\,|long\rangle_B) \tag{4.8}$$

$$|\phi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|short\rangle_A\,|long\rangle_B \pm |long\rangle_A\,|short\rangle_B). \tag{4.9}$$

The physical realization of the superposed state (2.2) can be achieved using a simple setup like the one illustrated in Figure 4.3: A single photon pulse is sent through an unbalanced MZI, resulting in the two well separated pulses $|short\rangle$ and $|long\rangle$ (the arm length difference of the MZI needs to be long in regard

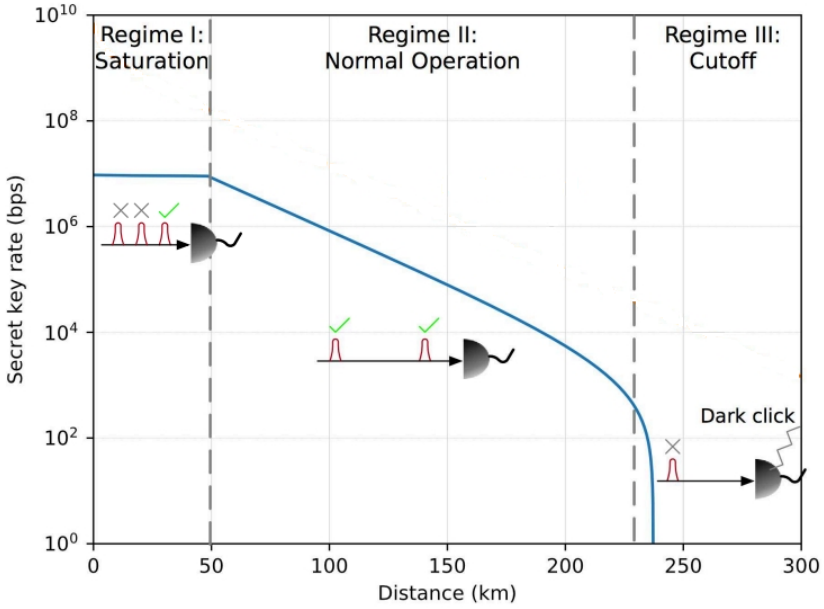

Figure 4.2: The typical secret key rate versus distance for a generic DV QKD protocol using currently achievable device parameters (1 GHz clock rate, 93% detector efficiency, 1000 cps dark count rate, 100 ns detector dead time). Figure from Ref.[6].

to the pulse duration). An optical switch is then used to recombine the pulses without losses (this can be replaced by a passive 50-50 PBS at the cost of 50% losses).

The same device can be used for measurement in a reverse configuration: the switch is synchronized so that when $|short\rangle$ and $|long\rangle$ enter the device, $|short\rangle$ takes the long path through the MZI while $|long\rangle$ takes the short path. At the output of the interferometer, both pulses interfere either constructively or destructively depending on the phase shift.

The Bell states of Eq.(4.9) can be obtained through spontaneous parametric downconversion (SPDC). A pump laser creates the superposed state of the form of Eq.(4.7) (as detailed earlier) and passes it through a nonlinear crystal. The downconversion process in the crystal transforms this state into:

$$|\psi\rangle^{+} = \alpha\,|short\rangle\,|short\rangle + \beta\,|long\rangle\,|long\rangle\,. \tag{4.10}$$

The SPDC process is explained in more details in Paragraph 5.1.2.

Compared to other encoding methods, the main advantage of the time-bin scheme is that the entangled state is not influenced by the inevitable polarization fluctuations and depolarization in optical fibers.

It is possible to generalize time-bin encoding to HD QKD by using more than two time intervals, provided that the pulse duration remains much shorter than the bins.

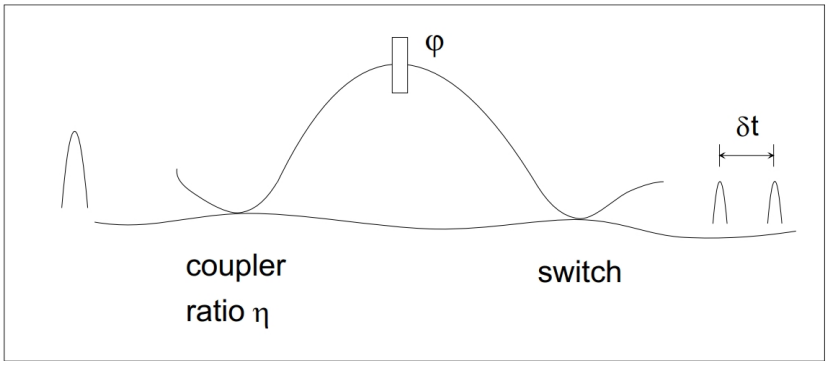

Figure 4.3: Set up to produce (left to right configuration) or analyze (right to left configuration) time-bins qubit. The coupling ratio η of the coupler and the phase φ of the phase shifter are tunable to produce any superposition of the basis states $|short\rangle$ and $|long\rangle$. The optical switch allows to couple or separate the basic states $|short\rangle$ and $|long\rangle$ without losses. Figure from Ref.[7].

Chapter 5

Characterization of the various components of a QKD link

This section will focus on characterizing the various components of the transmission chain, including the source, the detection system, and the quantum channel necessary for implementing a quantum communication link.

5.1 Sources

Prepare-and-measure protocols are typically implemented using phase-randomized weak coherent state (WCP) pulses. On the other hand, the most advanced technique for the generation of entangled photons is to use the spontaneous parametric downconversion (SPDC) process (different designs of entangled photon sources are outlined in Ref.[84]).

5.1.1 Weak coherent pulses

The coherent pulses of a laser are attenuated by filters to reach low photons numbers per pulse, typically on the order of 0.1. Phase randomization involves adding a random phase to each coherent pulse, creating a statistical mixture of Fock states (states with a variable photon number) following a Poisson distribution, allowing the use of decoy states, a crucial countermeasure against PNS attacks.

Early implementations of the BB84 scheme used active polarization control, which limited the key generation rate. One way to overcome this is by using four laser diodes in a single transmitter, each corresponding to a unique polarization. However, this method is not ideal due to spectral differences providing a potential side-channel for eavesdroppers. A better approach is coupling a single laser diode to four waveguides, each rotating polarization by a fixed amount. The waveguides are then recombined to result in a single-mode output with four possible polarization states. This is possible within a compact design suitable for both ground and satellite transmitters [14].

5.1.2 Spontaneous parametric downconversion

SPDC is a nonlinear process in which a photon, called the pump photon, is used to generate two other photons, called signal and idler photons. It was first proposed as a direct source of polarization-entangled photon pairs in Ref.[8]. This process, described in details in Ref.[85], is governed by energy conservation, i.e. $\omega_p = \omega_V + \omega_H$ and by phase matching condition: $\vec{k_p} \simeq \vec{k_V} + \vec{k_H}$. This latter condition expresses the fact that the pump beam must stay in phase with the signal and idler beams in order for the signal power to constructively interfere throughout the crystal. In particular, type II SPDC refers to the specific case where two photons are generated with orthogonal polarizations and in symmetrical directions relative to

the incident pump beam. Therefore, the entangled photon pairs are emitted in distinct directions and can be isolated using spatial filters. More precisely, the two down-converted photons are emitted into two cones. For a specific angle θ_p between the crystal optic axis and the pump photon, the configuration is referred to as collinear: the two cones are tangent to one another, with their intersection aligning with the pump beam direction. If the angle θ_p decreases, the two cones become disjoint. Conversely, if θ_p increases, the two cones converge, intersecting along two distinct directions (see Figure 5.1). Along these directions, the light can be described by the entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_1 |V\rangle_2 + e^{i\alpha} |V\rangle_1 |H\rangle_2 \right) \tag{5.1}$$

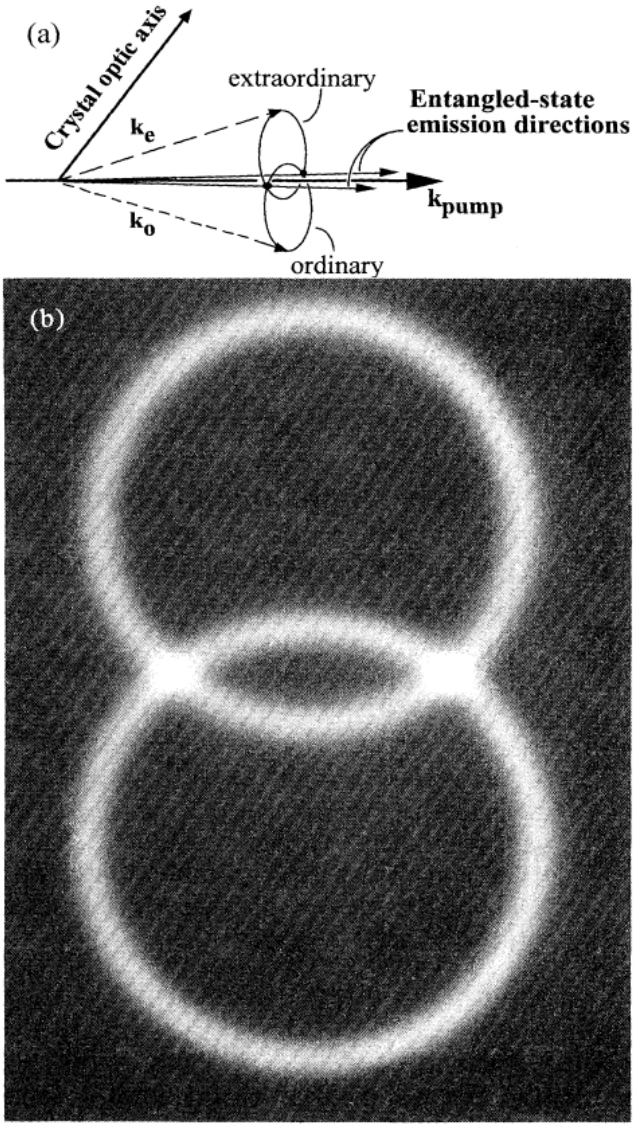

Figure 5.1: (a) The ordinary SPDC cone corresponds to the direction along which vertically polarized photons are emitted, while the extraordinary one corresponds to horizontally polarized photons. At their intersections, the light is described by Eq.(5.1), corresponding to entangled states. (b) A photograph of the down-conversion photons, through an interference filter at 702 nm (5 nm FWHM). The infrared film was located 11 cm from the crystal, with no imaging lens (Photograph by M. Reck). Figure from Ref.[8].

The birefringent nature of down-conversion crystals causes photons with different polarization to travel with different velocities inside the crystal and propagate along different directions. This results in a

walk-off which is maximal for pairs created near the entrance face. For a crystal of length L, it is given by: $\delta T = L(\frac{1}{v_V} - \frac{1}{v_H})$ with v_V and v_H the velocities of the vertically and horizontally polarized photons, respectively. This walk-off is responsible for the relative phase α of Eq.(5.1). It can be fine-tuned, for example by using an extra birefringent phase shifter, enabling any value to be assigned to it, especially 0 or π. On the other hand, implementing a half-wave plate in one path can convert horizontal polarization to vertical and vice versa. The combined effect of these two techniques enables the easy generation of any of the four Bell states:

$$|\psi\rangle^{\pm} = \frac{1}{\sqrt{2}} \left(|H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2 \right) \tag{5.2}$$

$$|\phi\rangle^{\pm} = \frac{1}{\sqrt{2}} \left(|H\rangle_1 |V\rangle_2 \pm |V\rangle_2 |H\rangle_2 \right) \tag{5.3}$$

Two types of crystals commonly used as SPDC sources are periodically-poled potassium titanyl phosphate (PPKTP) and single-domain crystals like beta barium borate (BBO). PPKTP offers higher $\chi^{(2)}$ non-linearity, while BBO is more temperature-tolerant. Larger apertures are possible for single-domain crystals, making optical alignment easier, whereas periodically poled materials are limited to apertures of 2 mm or less due to the challenge of maintaining regular poling across the crystal [14].

Pulsed lasers are commonly used to pump crystals, as they have been well-modeled since 2007 in Ref.[67]. However, a recent model of entanglement-based QKD using continuous-wave (CW) pump lasers has been introduced by Ref.[86]. CW pumping offers several benefits over pulsed-pumping. First, the down-converted photons have a narrower spectrum, thus lessening chromatic dispersion which occurs in optical fibers. Second, pulsed laser setups require precise synchronization between the sender and receiver to correctly identify and match corresponding photon pairs. Any time discrepancy could lead to errors or data loss. On the other hand, when using CW lasers, the photons are emitted continuously rather than in distinct pulses. A delay histogram records the time differences between detection events, allowing to identify correlated photon pairs even without exact timing alignment. The histogram helps in determining the coincidence window within which the photons were detected, thereby establishing the temporal correlation necessary for secure key generation. By relying on delay histograms, CW-pumped QKD systems can simplify their design by not requiring extremely precise timing mechanisms, as the temporal correlations can still be accurately assessed and utilized for secure communication. Finally, using CW pumping allows for the avoidance of high-intensity pulses, which can potentially damage optical components.

5.2 Detectors

Putting DV QKD into practice requires single photons detectors after the optical processing of the signals. Achieving high key rates requires minimizing dead times, a crucial factor for low-distance links. The efficiency of the detectors sets also a limit on the achievable performance. For long distance transmissions, low dark count rates are necessary. Another factor to consider is detection jitter, which refers to the variance introduced by the detector in measuring the arrival time of a photon. Jitter becomes particularly problematic for high key rates [87] and it should be small, to ensure good timing resolution. There are basically two technology of detectors suitable for QKD applications: avalanche photodiodes single photon detectors (APSPDs) and superconducting nanowire single photon detectors (SNSPDs).

CV QKD is a more flexible approach regarding detection, allowing for both homodyne and heterodyne detection. This flexibility enables the use of technologies similar to existing fiber optical technology.

5.2.1 APSPD

In an APSPD, the incoming photon is absorbed through in the depletion region (a region where mobile charge carriers, free electrons and holes, are depleted) of a semi-conductor material. A strong electric field is applied across the depletion region. This field accelerates the generated electron and hole, causing them to gain enough kinetic energy. As the accelerated carriers move through the depletion region they create additional electron-hole pairs through impact ionization. This process of impact ionization and

subsequent generation of more carriers leads to an avalanche effect, amplifying the initial signal.

On one hand, the high dark count rates (typically 100 cps) of APSPD limit the maximal distance for the communication. Indeed, When the detection rate approaches the dark count rate, discrimination between signal and noise becomes impossible, effectively halting communication. On the other hand, their relatively large dead times (10-100 ns) at telecom wavelengths [88] pose a limit on the achievable key rates. Their quantum efficiencies are typically around 50%. Their key benefit lies in their operation capability at near-ambient temperatures (220-250K).

5.2.2 SNSPD

Superconducting Nanowire Single-Photon Detectors (SNSPDs) are composed of nanowires arranged in a meander structure on a chip. An incident photon breaks a Cooper pair in the nanowire, reducing the superconducting critical current below the bias current, resulting in a measurable voltage pulse (see Figure 5.2).

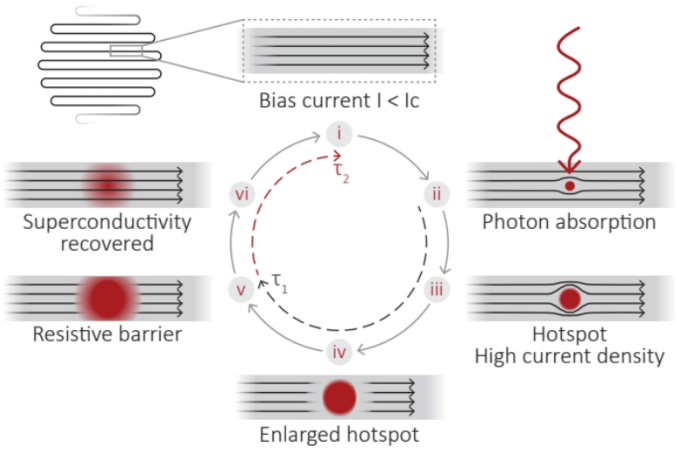

Figure 5.2: Illustrative representation of the detection mechanism in SNSPD. (i) The superconducting nanowire is maintened well below the critical temperature, leading to a bias current I just below the critical current I_C (at which the superconductivity property is lost). (ii) The absorption of a photon creates a small resistive hotspot. (iii) The flow of supercurrent is deviated by the resistive hotspot. The current density arround the hotspot increases, exceeding the superconducting critical current density. (iv) This results in a resistive barrier across the width of the nanowire. (v) Growth of the resistive barrier along the axis of the nanowire due to Joule heating until the current flow is blocked. (vi) The bias current is shunted by the external circuit, allowing the resistive region to subside and the nanowire becomes superconducting again. The bias current is then reset to the original value, restoring the situation (i) and a new event can be detected. Figure adapted from Ref.[9].

SNSPDs offer significantly better performance compared to APSPDs. Their dark count rates can be as low as 0.02 cps, they have low jitter (around $<$26 ps), and their quantum efficiency can reach up to 98% [89]. The drawback of SNSPDs is that they require extremely low operating temperatures, typically around 0.8K [6].

5.2.3 Homodyne detection

The principle of homodyne detection was discussed in Paragraph 4.1. The intensities are measured by Positive Intrinsic Negative (PIN) diodes [90] which provide high detection efficiency (typically 80%) and relatively low noise. Therefore homodyne detection could in principle operate at GHz repetition rates.

5.3 Quantum channel

The optical links that connect the correspondents of a quantum communication consist of optical fiber or free space. Both of these mediums are characterized by a non-unity transmittivity η, restricting the maximal distance for point-to-point link QKD, that only quantum repeaters [91] can surpass. The secret-key capacity of a lossy channel, defined as the maximal achievable rate by any optical implementation of QKD, was determmined in Ref.[92] and is given by:

$$K = -log_2(1-\eta). \tag{5.4}$$

At long distance, $\eta \simeq 0$ and the optimal rate-loss scaling is given by $K \simeq 1.44\eta$. This fundamental limit is known as the PLOB bound, named after the authors of Ref.[92].

For current optical fiber, with typical attenuation around 0.18 dB/km [93], practical key rates are achievable only for distances under 100 km [14]. Similarly, free-space links on ground are limited by atmospheric attenuation and turbulence, as well as by Earth's curvature.

Quantum repeaters

As previously mentioned, the secret key capacities for a pure-loss point-to-point link are constrained by the PLOB bound Eq.(5.4). However, the distance between two end users can be increased by employing quantum repeaters, which act as middle nodes between Alice and Bob, effectively dividing the original quantum channel into sub-channels [6]. The achievable secret key capacities for chains of repeaters have been determined in Ref.[94]. For a chain of repeaters connected by pure loss channels with transmissivities $\{\eta_i\}$, the bound is given by [6]:

$$K_{loss} = -log_2(1 - min\,\{\eta_i\}) \tag{5.5}$$

which is completely determined by the minimum transmissivity in the chain. A particularly interesting scenario involves an optical fiber with transmissivity η splitted into $N+1$ segments by inserting N equidistant quantum repeaters. Each part has then a transmissivity $\eta^{1/(N+1)}$ and the secret key capacity of the channel is given by [6]:

$$K_{loss}(\eta,N) = -log_2(1-\eta^{1/(N+1)}) \tag{5.6}$$

Unlike classical repeaters, which can simply amplify and resend signals, quantum repeaters need to preserve the delicate quantum states of the information they handle.

One approach to deploying quantum repeaters involves using them as intermediary nodes for entanglement distribution. One approach to deploying quantum repeaters involves using them as intermediary nodes for entanglement distribution. For instance, when distributing entangled photon pairs to Alice (A) and Bob (B), repeaters M and N are employed to generate entangled pairs over shorter segments: A-M, M-N and N-B. Once the entangled pairs are established between neighboring nodes, the repeaters perform a process called entanglement swapping. This involves a Bell-state measurement at the intermediate nodes which, when combined with classical communication of the measurement results, effectively entangles the end nodes directly, even though they never interacted directly. The critical aspect of quantum repeaters is the use of quantum memory, which temporarily stores the quantum state of photons or qubits.

Another approach is to utilize quantum error correction techniques to mitigate losses and operational errors. This concept is akin to data communication networks, where redundancy is added to messages to correct errors introduced by the channel. Implementing this method would necessitate the use of advanced quantum computing modules [6].

Both methods require advanced hardware that is not yet available, making the near-term implementation of quantum repeaters unlikely.

5.3.1 Optical fiber

Optical fiber is a relatively stable medium compared to free space, but it requires installation between each communication node and subsequent maintenance.Light propagation along the z-axis within the

fiber is determined by the refractive index profile $n(x,y)$ across the cross-section of the fibers. Under the usual slowly varying envelope approximation, this propagation is governed by an equation identical to the Schrodinger equation, with $V(x,y) = -n(x,y)$. A positive bump in the refractive index corresponds to a potential well. The region of the well is called the fiber core. When this core is large compared to the considered wavelength, multiple bound modes can exist, leading to the presence of numerous guided modes within the fiber. These are referred to as multimode fibers. In multimode fibers, mode coupling occurs easily, causing the qubit to behave as if it were in a nonisolated environment, rendering these fibers unsuitable for quantum channels. On the other hand, when the core is small, with a diameter comparable to a few wavelengths, it supports only a single spatial mode, forming single-mode fibers that are optimal for transmitting single quanta and thus well-suited for quantum telecommunications [95].

The losses arise from imperfect fiber structure and phenomena such as Rayleigh scattering and absorption. If the core-cladding interface is not smooth or the fiber contains impurities, light will scatter, causing losses. These losses are material-dependent and vary with wavelength. In particular, Rayleigh scattering is inversely proportional to the fourth power of the wavelength, and is therefore significantly reduced at long wavelengths. Additional losses come from imperfect connections between fiber segments, microbending, compression, and stretching of the fiber [96].

In addition to the losses affecting the maximum communication distance, the effects of decoherence should be carefully studied. Two primary effects need to be considered.

Firstly, chromatic dispersion, which arises because different wavelengths travel at different velocities, results in an incoherent temporal spread of light pulses. This can become problematic when subsequent pulses begin to overlap. Therefore, this issue particularly concerns time-bin encodings, which may use narrower time windows. However, chromatic dispersion is a fixed quantity for a given fiber, and solutions exist, such as dispersion compensation or spectral filtering [97].

Secondly, polarization mode dispersion (PMD) which is a birefringent effect that creates fast and slow polarization modes orthogonal to each other, causing any pulse to split into two components. This results in pulse depolarization. Birefringence can vary over time due to environmental factors, meaning it cannot be compensated for statically. PMD induces decoherence in polarization coding and can be problematic for implementations requiring polarization control. The severity of these effects depends on the specific fibers and sources employed [50].

In order to avoid additional losses, it is necessary to ensure an effective coupling between the fiber and the other components of the system, whether during emission or detection. The fiber's acceptance cone, characterized by its half-angle θ_{max} (see Figure 5.3), plays a crucial role. This angle is directly related to the fiber's numerical aperture, $NA = n \sin \theta_{max}$, where n is the refractive index of the medium the light passes through before entering the fiber. The numerical aperture depends on the refractive indices of the core and cladding: $NA = \sqrt{n_{core}^2 - n_{cladding}^2}$. Incident beams within the acceptance cone undergo total internal reflection, minimizing refraction losses. The numerical aperture of the fiber similarly defines the exit cone, thereby affecting both the input and output couplings of the fiber. For QKD applications, the numerical aperture of fibers typically ranges from 0.05 to 0.40 [10].

5.3.2 Free space

Decoherence effects due to traversing the atmosphere are negligible [98, 99]. The main issues of free space links stem from losses, which are generally divided into geometric and atmospheric categories.

Atmospheric losses arise from scattering and scintillation, and they vary significantly with changing weather conditions. Scattering effects can be summarized in terms of atmospheric transmittance as a function of wavelength. Within the 700-10,000 nm wavelength range, there are several atmospheric transmission windows, such as 780-850 nm and 1520-1600 nm, which support wavelenghts of commercial laser diodes and which have attenuation $\alpha < 0.1$ dB/km in clear weather (see Figure 5.4) [50]. Scintillation is due to atmospheric turbulence and adaptive optics may be used to reduce the losses.

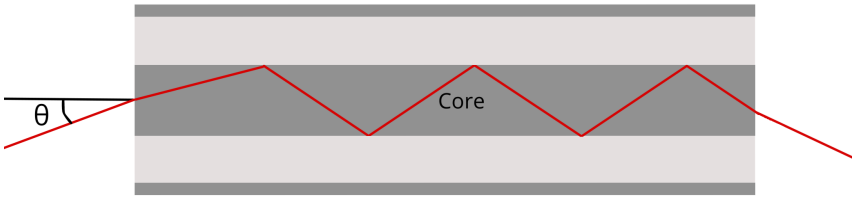

Figure 5.3: Total internal reflection regime for an incident light beam inside the acceptance cone of the fiber, defined by its half-angle θ_{max}. This regime is reached for incident angle satisfying $\theta \leq \theta_{max}$. Figure adapted from Ref.[10].

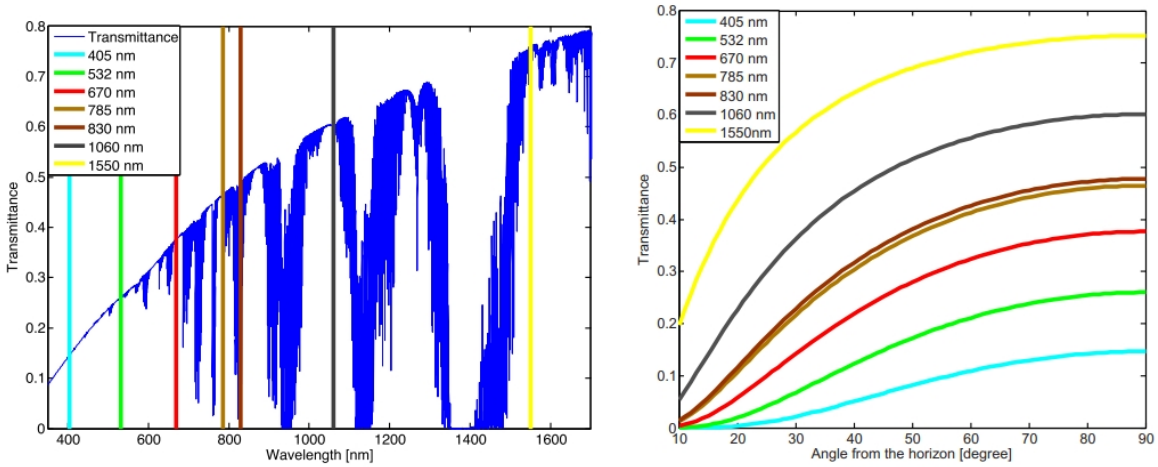

Figure 5.4: Atmospheric transmittance versus wavelength (left). Atmospheric transmittance versus Angle from the horizon (right). Coloured lines represent wavelengths of commercially available laser systems. Figure from Ref.[11]. The authors modeled the atmospheric transmittance of a rural sea-level location with a visibility of 5 km using MODTRAN 5.

Geometric losses are due to the diffraction of the beam, making its transverse area quadratically increase with distance. This directly reduces the amount of information per unit area, as the same number of photons is spread over a larger surface. If, upon arrival, the beam is wider than the aperture of the receiving telescope, a portion of the information is irretrievably lost.

The broadening of a Gaussian beam is characterized by the Rayleigh length, defined from the minimal waist as the distance after which the beam radius has increased by a factor of $\sqrt{2}$, effectively doubling its area (see Figure 5.5).

The focusing limit of a light beam is determined by the diffraction limit:

$$sin(\theta) = 1.22\frac{\lambda}{D} \tag{5.7}$$

where θ represents the divergence angle resulting from diffraction, D denotes the diameter of the telescope, and λ is the wavelength.

5.3.3 Noise

In classical telecommunications, the quality of a signal is measured by the signal-to-noise ratio. It is possible to improve signal quality by increasing its power or reducing noise. However, in quantum communications, where single photons are used to transmit a qubit, the signal quality cannot be enhanced

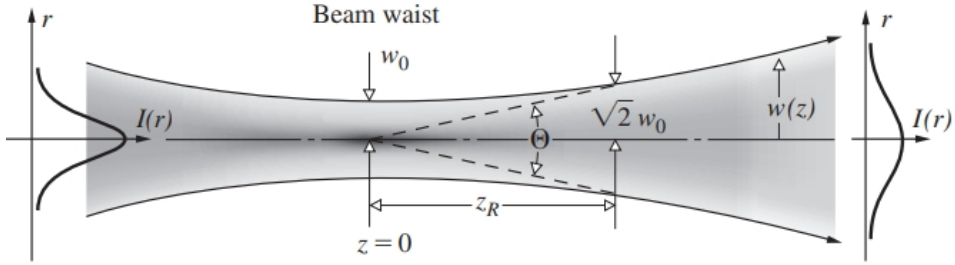

Figure 5.5: The geometry of a gaussian beam is determined by the beam waist w_0, the Rayleigh length Z_R and the total diffraction angle Θ. Figure from Ref.[12].

by increasing power. Instead, the quality is expressed using the Quantum Bit Error Rate (QBER), which corresponds to the error rate in the sifted key. This QBER can originate from two different sources: technical QBER, which refers to errors due to imperfections in the devices used, particularly the dark count of detectors, and noise from stray light, consisting of background photon detections.

To minimize background noise as much as possible, filtering is performed at three levels: spatial, spectral, and temporal.

Temporal filtering involves limiting detection windows to specific time intervals when a useful signal is expected. The single-photon detector remains off except during these narrow windows when the arrival of a signal photon is probable. This approach requires precise knowledge of the signal's arrival time, necessitating accurate synchronization between the transmitter and receiver.

To achieve this, it is possible to use a software-controlled phase-locked loop driven by the incoming photons, allowing synchronization with subnanosecond precision [100]. An alternative approach is to use a bright pulse of a different wavelength to lock the timing, which involves matching the repetition rates of both the bright and dim pulses. This method requires addressing wavelength-dependent factors such as the Doppler effect, which can gradually shift the repetition frequency and thus must be monitored and corrected.

Spatial filtering techniques involve selecting only the optical path used by the useful signals. This is achieved through the use of baffling and optical blacking, as well as by focusing the incident beam through a pinhole (see Figure 5.6).

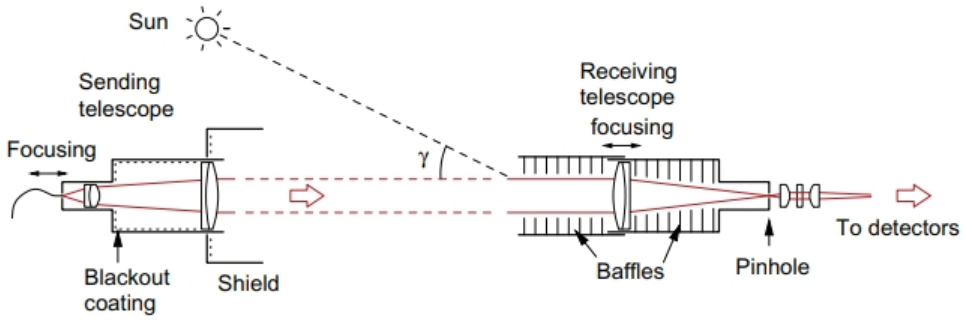

Figure 5.6: Schematic view of the components used for spatial filtering. Figure from Ref.[13].

Finally, spectral filters are used to transmit only the narrow bandwidth corresponding to the source's emission frequency. There are three types of filters: interference, birefringence, and atomic filters. The

latter are the most effective, with a bandwidth of 0.01 nm and a transmittance above 90%. However, spectral filtering must account for the Doppler effect caused by the relative motion between the source and the receiver [15].

5.4 Satellite QKD

The different losses associated with the free-space channel were discussed earlier. In addition to addressing these, several additional challenges arise when considering satellite QKD, part of them were discussed in [101]. Prepare-&-measure and entanglement-based protocols for satellite QKD are illustrated in Figure 5.7.

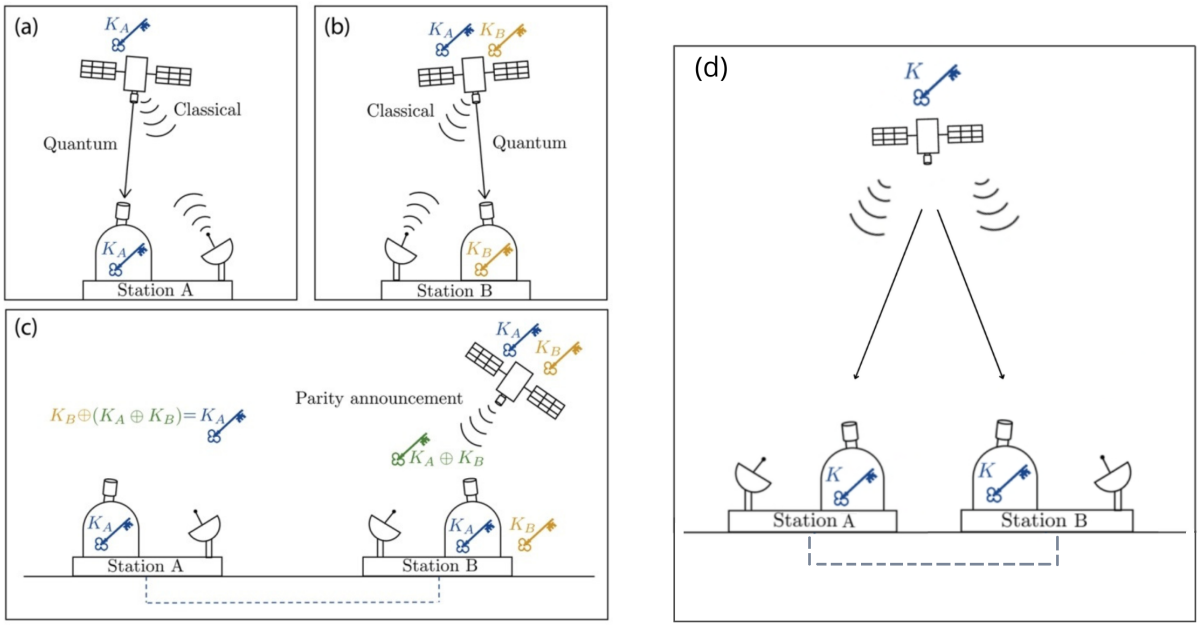

Figure 5.7: Left: The Prepare-and-Measure protocol is conducted using a satellite as intermediate trusted node in a downlink configuration. (a) When the satellite comes into view of ground station (GS) A (Alice), quantum states generated and encoded to form a string of qubits onboard the satellite are transmitted to the GS through the quantum channel. After post-processing, including sifting, error correction, and privacy amplification, both the satellite and Alice share the secure key K_A. For a Low Earth Orbit (LEO), the transmission typically lasts a few minutes. (b) When the satellite passes over the second ground station, GS B (Bob), the same process is repeated to share a key K_B with this station. (c) Prior to exiting GS B's line of sight, the satellite will transmit the parity $K_A \oplus K_B$ over a classical channel. Using this information, Bob can recover the key K_A through straightforward binary addition $K_A = K_B \oplus (K_A \oplus K_B)$. Alice and Bob are now sharing a secure key via the satellite, without any specific constraints regarding the distance between GS A and B. Right: Satellite entanglement distribution. (d) The onboard entangled photon source directly distributes the entangled photons to the two ground stations. Subsequent post-processing is conducted over a classical channel between the ground stations. The quantum transmission remains feasible as long as both GS are within the satellite's line of sight. Figure adpated from Ref.[14].

5.4.1 Configuration

Atmospheric turbulence, particularly prevalent in the first 20 kilometers [102], causes fluctuations in atmospheric properties such as temperature and composition. This leads to variations in the refractive index, which exacerbate the angular spread of a beam traversing the atmosphere. The passage through the atmosphere is particularly detrimental in an uplink configuration. Here, the beam traverses the atmosphere at the start of its transmission path, and the angular spread caused by atmospheric turbulence results in significant beam widening over the remaining distance, leading to a very broad beam at the

receiver. The difference between the link attenuation at 800 nm for downlink and uplink scenarios are shown in Table 5.1.

Additional differences between uplink and downlink configurations are discussed below.

	1 m ground receiver	30 cm LEO receiver	30 cm GEO receiver
1 m ground transmitter		27.4 dB (500 km)	64.5 dB (36 000 km)
30 cm LEO transmitter	6.4 dB (500 km)	28.5 dB (2 000 km)	52.9 dB (35 000 km)
30 cm GEO transmitter	43.6 dB (36 000 km)	52.9 dB (35 000 km)	64.5 dB (40 000 km)

Table 5.1: The simulation of link attenuation at 800 nm for ground-to-space station links shows that uplink configurations to both LEO (500 km) and GEO (36,000 km) suffer more than 20 dB higher attenuation than downlink configurations. Table adapted from Ref.[14].

- Uplink:

Having the source on the ground enables better pointing accuracy compared to an onboard system, which is limited by the constraints of space deployment and operation (see Figure 5.9, where the excess loss due to pointing error for both configurations was simulated for a 600 km orbit altitude).

Moreover, on a ground station, it is relatively easy to use larger telescopes to mitigate the beam diffraction (which is inversely proportional to the diameter of the telescope as outlined by Eq.(5.7)). However, the total beam size at the receiver results from the combination of diffraction and turbulence. The impact of turbulence is independent of the transmitter aperture size, and can only be mitigated using adaptive optics. The simulation conducted by Bedington *et al.* in Ref.[14] shows that a satellite in Low Earth Orbit (LEO) at 500 km altitude faces an additional 20 dB of attenuation in an uplink configuration compared to a downlink. A downlink configuration is usually chosen to prevent this level of attenuation.

A simple model to quantify the amount of background noise for both downlink and uplink configurations is presented in Ref.[103].

In an uplink configuration and during daytime operations, the primary noise source is sunlight reflected by the Earth. Assuming Lambertian scattering (isotropic radiance), the number of background photons collected by the optical system, which has an aperture radius R and an instantaneous field-of-view (IFOV), at a distance L from the Earth's surface per unit time and wavelength can be expressed as:

$$N_{day} = \frac{1}{\pi} a_E H_{Sun} \Sigma \Omega = a_E r^2 (IFOV)^2 H_{Sun} \tag{5.8}$$

where a_E is the Earth albedo, H_{Sun} is the solar spectral irradiance at one astronomical unit, $\Sigma = (IFOV)^2 L^2$ is the emitting area seen by the telescope and $\Omega = \frac{\pi R^2}{L^2}$ is the solid angle from which the telescope on the satellite can be seen from Earth.

During night-time operations, three main sources contribute to background noise: moonlight reflected off the Earth, the Earth's black-body radiation, and scattered light from human activities. For the Moon reflection, the number of photons collected per unit time and wavelength can be expressed as:

$$N_{night} = \alpha N_{day} \tag{5.9}$$

with $\alpha = a_M \left(\frac{R_M}{d_E M}\right)^2$ where a_M is the Moon albedo, R_M is the Moon radius and $d_E M$ is the Earth-Moon distance. Assuming $a_M \simeq 0.12$ for the Moon albedo gives $\alpha \simeq 10^{-6}$, meaning that the amount of background noise is reduced by six orders of magnitudes.

The number of photons radiated by the Earth towards the telescope is given by:

$$N_{Black-body} = N_0 \Sigma \Omega \Delta \lambda \tag{5.10}$$

where N_0 is the spectral radiance of the Earth, according to Planck law's for black-body's radiation, per unit time, area, bandwidth and solid angle:

$$N_0(\lambda) = \frac{2c}{\lambda^4} \frac{1}{e^{hc/\lambda kT} - 1}. \tag{5.11}$$

For a telescope of radius $r = 15$ cm and FOV of 15 μrad, $N_{Black-body} \simeq 10^{-12}$, which is three orders of magnitude less than the Moon's contribution to background noise [103].

Light pollution from human activities significantly varies depending on the ground station's location, and its effect on the number of photons collected by the satellite must be evaluated individually.

- Downlink:

As previously noted, the attenuation in downlink configurations is significantly lower compared to uplink configurations. Here, the main source of loss is beam diffraction. The broadening effect caused by atmospheric turbulence happens near the end of the transmission path, thus having a negligible impact.

Another significant advantage of downlink configurations is the ability to use directly the satellite as an untrusted node for entanglement distribution between two ground stations (see Figure 5.7).

Lastly, this configuration, with the detector on the ground and the source in space, offers a dual advantage. First, the performance of QKD systems is often constrained by the quality of the detectors. Downlink setups enable the use of high-performance detectors, which are easier to deploy on the ground compared to in space. Additionally, placing the source on a satellite makes it less vulnerable to certain attacks, thus facilitating the implementation of MDI QKD protocols, where the source must be part of a trusted node, but the detector does not have to be.

The amount of background noise can be determined based on the brightness of the sky and the telescope's specifications. The power received by the telescope, P_B can be expressed as follows [15]:

$$P_b = H_b \Omega_{FOV} \pi R^2 B \tag{5.12}$$

where H_b is the brightness of the sky background (in $Wm^{-2}sr^{-1}\mu m^{-1}$), Ω_{FOV} is solid angle corresponding to the FOV of the telescope, R is its radius, finally B is the spectral filter's bandwidth. The quantity of background photons detected is highly dependent on weather conditions, with typical values illustrated in Figure 5.8.

5.4.2 Orbit

The proximity of Low Earth Orbits (LEO), at altitudes below 2,000 km, helps to minimize losses due to diffraction. This makes LEOs the optimal choice since diffraction is the primary source of loss for downlink configurations. LEOs also offer additional benefits: they are more accessible and have lower exposure to ionizing radiation. Moreover, selecting the orbital inclination allows for global coverage within a few hours or maintaining a consistent relative position to the sun (Sun Synchronous Orbit).

On the downside, LEO satellites have a high relative speed to the surface, leading to several negative impacts. Indeed, accurate pointing becomes more challenging, transmission duration is limited due to short overflight times, and Doppler shifts must be managed. Additionally, the spacecraft's temperature varies significantly with eclipse cycles, necessitating thermal control or robustness in the optical setup to prevent performance degradation.

Medium Earth Orbits (MEO), ranging from 2,000 to 36,000 km, and Geostationary Orbits (GEO), situated at 36,000 km above the equator, offer significantly longer link durations (with GEO providing permanent coverage) at the expense of much higher losses and greater exposure to ionizing radiation.

Conditions	Cloudy daytime	Hazy daytime	Clear daytime	Full moon clear night	New moon clear night	Moonless clear night
Relative brightness	1.0	10^{-1}	10^{-2}	10^{-5}	10^{-6}	10^{-7}
Typical brightness ($W\,m^{-2}\,Sr\,\mu m$)	150	15	1.5	1.5×10^{-3}	1.5×10^{-4}	1.5×10^{-5}
Photons $pulse^{-1}$						
$\theta = 100\,\mu rad$ $B = 0.2\,nm$ $t = 3\,ns$	7.4	7.4×10^{-1}	7.4×10^{-2}	7.4×10^{-5}	7.4×10^{-6}	7.4×10^{-7} $+7.4 \times 10^{-7}$
$\theta = 100\,\mu rad$ $B = 0.2\,nm$ $t = 1\,ns$	2.5	2.5×10^{-1}	2.5×10^{-2}	2.5×10^{-5}	2.5×10^{-6}	2.5×10^{-7} $+2.5 \times 10^{-7}$
$\theta = 100\,\mu rad$ $B = 0.01\,nm$ $t = 1\,ns$	1.3×10^{-1}	1.3×10^{-2}	1.3×10^{-3}	7.4×10^{-6} $+1.3 \times 10^{-8}$	1.3×10^{-7} $+1.3 \times 10^{-8}$	1.3×10^{-8} $+1.3 \times 10^{-8}$
$\theta = 10\,\mu rad$ $B = 0.2\,nm$ $t = 3\,ns$	7.4×10^{-2}	7.4×10^{-3}	7.4×10^{-4}	7.4×10^{-7} $+7.4 \times 10^{-9}$	7.4×10^{-8} $+7.4 \times 10^{-9}$	7.4×10^{-9} $+7.4 \times 10^{-9}$
$\theta = 10\,\mu rad$ $B = 0.2\,nm$ $t = 1\,ns$	2.5×10^{-2}	2.5×10^{-3}	2.5×10^{-4}	2.5×10^{-7} $+2.5 \times 10^{-9}$	2.5×10^{-8} $+2.5 \times 10^{-9}$	2.5×10^{-9} $+2.5 \times 10^{-9}$
$\theta = 10\,\mu rad$ $B = 0.01\,nm$ $t = 3\,ns$	3.7×10^{-3}	3.7×10^{-4}	3.7×10^{-5}	3.7×10^{-8} $+3.7 \times 10^{-10}$	3.7×10^{-9} $+3.7 \times 10^{-10}$	3.7×10^{-10} $+3.7 \times 10^{-10}$
$\theta = 10\,\mu rad$ $B = 0.01\,nm$ $t = 1\,ns$	1.3×10^{-3}	1.3×10^{-4}	1.3×10^{-5}	1.3×10^{-8} $+1.3 \times 10^{-10}$	1.3×10^{-9} $+1.3 \times 10^{-10}$	1.3×10^{-10} $+1.3 \times 10^{-10}$

Figure 5.8: This table lists the number of background photons for different optical configurations and under several weather conditions. In certain entries, an additional term accounts for noise photons caused by satellite reflections. If not specified, this term is considered negligible. Table from [15].

5.4.3 Telescope design

Reflective telescopes can be preferred over transmissive ones since reflective mirrors can be larger, which minimizes beam divergence. However, depolarization effects need to be considered for polarization based QKD. To achieve the optimal beam waist, the curvatures of the lenses or mirrors of the telescope are carefully selected. However, care must be taken in the optical design for polarization-based schemes because curved optics in an off-axis configuration may introduce some spatially dependent polarization effects [103] . Bourgoin *et al.* in Ref.[11] established that for SPDC sources, the optimal losses occur when the full-width at half maximum (FWHM) beam waist is equal to half the diameter of the transmitter. On one hand if the beam is too small, diffraction increases. On the other hand if it is too large, it is clipped by the transmitter telescope. For WCP sources, optimal losses are reached for any FWHM beam waist greater than the transmitter telescope diameter, as clipping losses at the telescope can be compensated by increasing the source intensity to maintain the average photon number per pulse.

5.4.4 Attitude

Pointing errors lead to excess losses. In the uplink configuration, the beam divergence is primarily caused by the initial atmospheric traversal. This means that the influence of the transmitter size on the beam width at the receiver is negligible, and also results in a larger beam width compared to the downlink configuration. Consequently, for a given pointing accuracy, the excess losses due to pointing errors are more pronounced in the downlink configuration. These effects are depicted in the graphs shown in Figure 5.9.

Note that the relative motion between the ground station and the satellite induce a time-dependent rotation of the polarization states of the signal photons. For polarization based scheme, this is the most important source of perturbation as shown in [98], the authors also provide ideas for the implementation of an active compensation system.

One possible solution is to use a reference beam with a different wavelength from the signal photons. At the ground station, polarization analysis of the reference beam can be performed to evaluate the transformation it underwent, followed by applying the inverse transformation to the polarization states of the signal photons. However, this solution is not perfect as the modification of the polarization states is wavelength-dependent.

Another option is to use the same wavelength for the reference beam and the signal photons in a time-multiplexing configuration. This approach requires a high rate for the transmission and analysis of the reference beam to match the temporal variations in the polarization states. While this would allow for better compensation, it comes at the cost of reduced key rates.

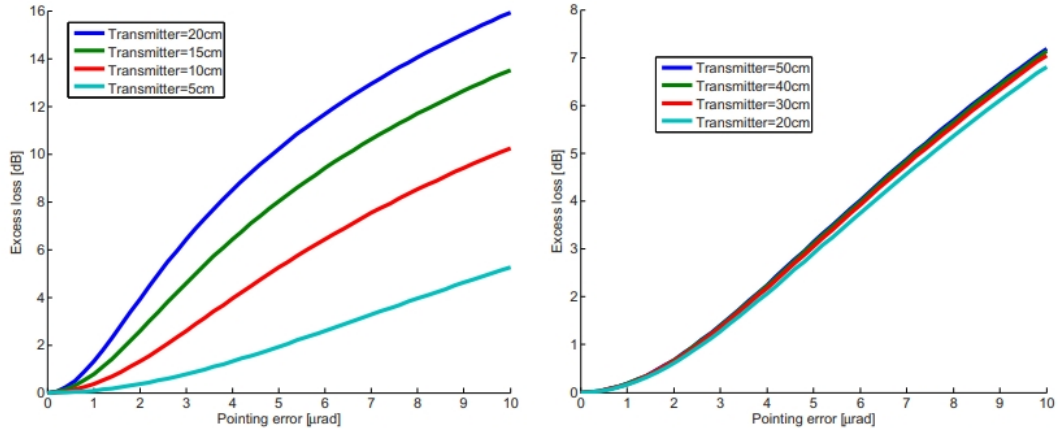

Figure 5.9: Excess loss due to systematic pointing error of the transmitter for various transmitter sizes at 40° from zenith in a downlink (left) and in an uplink (right) assuming a two-dimensional Gaussian distribution of the pointing error. In the case of the uplink, the four curves are confused, indicating that the transmitter size's influence on the beam width at the receiver negligible. For downlink: wavelength, 670 nm; ground receiver diameter, 50 cm. For uplink: wavelength, 785 nm; satellite receiver, 30 cm. In both cases, the orbit altitude is 600 km and the atmosphere is rural sea level. Figure from Ref.[11].

Chapter 6

Practical implementations of QKD

6.1 Prepare-&-Measure

6.1.1 BB84: First Implementation

The first implementation of BB84 was performed by Bennett *et al.* in 1992 [16]. This experimental setup successfully demonstrated the practical feasibility of QKD, paving the way for further implementations. However, it was vulnerable to many attacks and not optimal. An original picture of the apparatus is provided by Figure 6.1. The quantum channel itself is a free air optical path of approximately 32 cm.

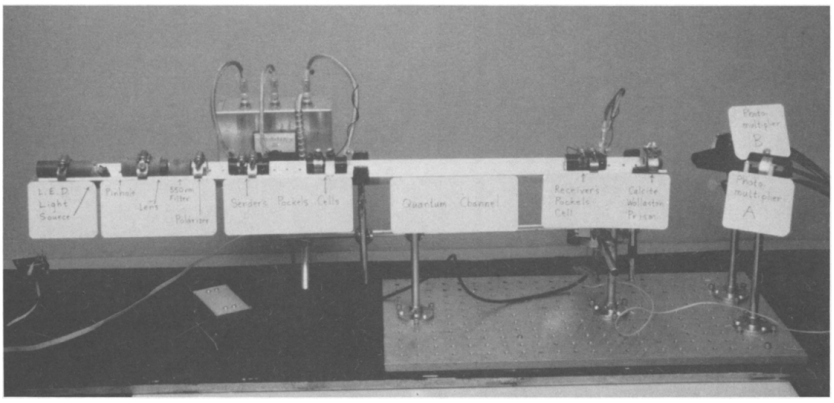

Figure 6.1: Original photograph of the apparatus used by Bennett *et al.* to implement the BB84 protocol. Image from Ref.[16].

Emitter

The light source was a green LED, emitted through a 25 μm pinhole and then passed through a 25 mm focal length lens to form a collimated beam. This beam was then filtered with a 550±20 nm interference filter to reduce the light's intensity and spectral width. The wavelength was chosen to fit the spectrum at which the photomultipliers have relatively high quantum efficiency. Finally, the beam passed through a dichroic sheet polarizer to select horizontal polarization. At the end of the path, the intensity was about 0.1 photons per pulse, with half of the photons emitted during the first 500 ns.

The four polarization states required in the BB84 scheme are made possible by using Pockels cells. These are birefringent crystals whose refractive index varies linearly with the intensity of the applied

electric field. Consequently, these cells can act as electro-optic devices to modulate polarization. These cells are described in [104]. When the Pockels cells are operated at the quarter-wave voltage, defined as the applied voltage that induces a phase shift of $\frac{\pi}{2}$, which corresponds to a 45-degree rotation of the light's polarization, it allows selection between the four polarization states: horizontal, vertical, left-circular, or right-circular. Pockels cells enable polarization modulation up to GHz rates [105].

Receiver

The detection unit is composed of a Pockels cell followed by a polarizing beamsplitter (PBS) oriented so as to split the beam into vertically and horizontally polarized beams which are directed into two photomultiplier tubes. The Pockells cell is also operated at quarter-wave voltage in order to enable rectilinear and circular polarization measurement with the same PBS, depending on whether the voltage is off or on. The quantum efficiency of the photomultipliers was about 9% with dark counts of about 10^{-4} per 500 ns time window.

Performance

With a source producing an average of 0.1 photons per pulse and a 500 ns window passing half of them, the dark count of the detectors should have resulted in a 2% bit error rate. The actual error rate was approximately 4%, which the authors explained as due to the misalignment of the Pockels cells. Simple measures like better optical alignment and cooling the detectors to reduce their dark counts could significantly reduce the error rate.

6.1.2 BB84: outside the lab

The first transmission of qubits outside the lab was achieved by Jacobs and Franson in 1996 [17]. This demonstrated the feasibility of QKD in an uncontrolled environment, with the quantum channel extending over a 75m distance outside the lab in daylight, providing a foundation for considering a global system for quantum cryptography based on a network of ground stations and satellites. A schematic view of the setup is provided by Figure 6.2.

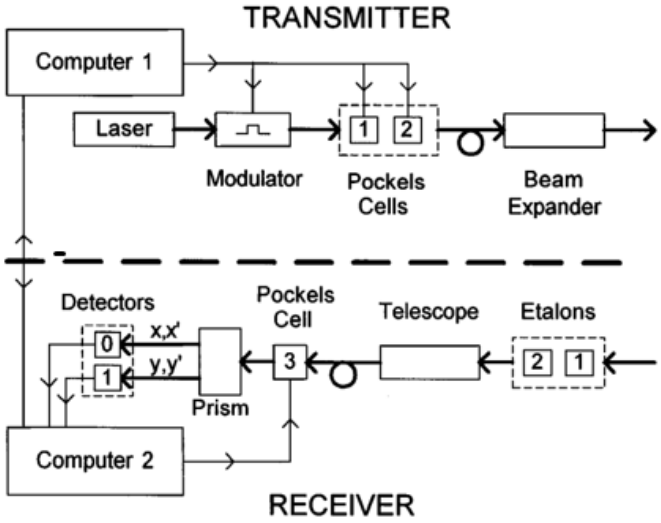

Figure 6.2: Schematic view of the setup used by Jacobs and Franson to implement the BB84 protocol. Image from Ref.[17].

Emitter

The light source is a 633 nm coherent laser producing 0.1 μs pulses. In addition to the signal photons, two etalons are used for background rejection. Neutral-density filters are used to attenuate the pulses,

reducing the probabilty of multi-photons emission to about 2%. As for the previous experimental setup, the four polarizations states are realized using two Pockels cells. The first one, oriented at an angle of 45° to the x axis, allows to convert an arbitrary amount of x polarization into a y polarization depending on the applied voltage. The second Pockels cell is used to switch between x and y polarization. Optical fibers are used to propagate the photon to the transmission optics where the beam diameter is expanded to 1 cm.

Receiver

Reception optics are similar to transmission one, it focuses the beam back into an optical fiber. The background is passively reduced by using small core diameter fiber optics (3 μm), limiting the acceptance angle. It is further reduced by the use of a narrow-band (1 nm) interference filter and two Fabry-Perot etalons with FWHM transmission peaks of 0.5 and 10 GHz. The detection unit is composed by a PBS preceded by a Pockels cell. The detectors are two silicon avalanche photodiodes with efficiency near 50%.

Performance

The raw transmission rate was 2%, mainly influenced by an abnormally high dark count (600 cps) in one of the detectors, whereas the single-channel rate for the other detector was 0.7%. The secret key generation rate was 1kHz. It is noteworthy that the team conducted the experiment again with the same setup, substituting the free-space channel with polarization-preserving optical fiber. In the fiber setup, the error rate remained comparable to the free-space scenario, but the secret key rate was five times greater. The authors attribute this difference primarily to losses caused by the efficiency of coupling into the return fiber, along with diffraction and atmospheric refraction effects.

Utilizing narrow time windows, enabled by the high modulation rate of Pockels cells, has allowed for a reduction in background noise by a factor of 10^2. Spectral filtering, achieved through the use of filters and etalons, reduced background noise by a factor of 10^5. Furthermore, the small size of the fiber's acceptance cone further reduced background noise by a factor of 10^{10} compared to an acceptance angle of 4π.

6.2 Entanglement-based

6.2.1 E91: Beyond the atmosphere thickness

In an experiment conducted by Peng *et al.* in 2005, entangled photons were successfully distributed over a distance of 10.5 km, surpassing the effective thickness of the entire atmosphere (corresponding to 5-10km of ground atmosphere). This milestone is significant because atmospheric attenuation is a major challenge in free-space QKD. The source was located 7.7 km from Alice and 5.3 km from Bob, who were separated by 10.5 km (see Figure 6.3).

A second experiment implementing the BBM92 protocol was conducted. This experiment did not require any additional equipment to the experimental setup.

Emitter

An argon ion laser is utilized to pump a BBO crystal, producing polarization-entangled photons with a wavelength of 702 nm through type II parametric down conversion. The generated states can be described as:

$$|\phi\rangle^- = \frac{1}{\sqrt{2}} \left(|H_A\rangle |V_B\rangle - |V_A\rangle |H_B\rangle \right) \tag{6.1}$$

For a power of 300 mW, the setup locally detects 10,000 pairs of entangled photons per second using narrow bandwidth filters of 2.8 nm. The local visibility at the sender is about 98% at the sender for the rectilinear basis while for the diagonal basis it is 94%. The entangled photons are captured into two single-mode fibers linked to the sending telescopes. The chosen transmissive telescopes offer a transmission rate exceeding 70% and expand the beam diameter to 12 cm.

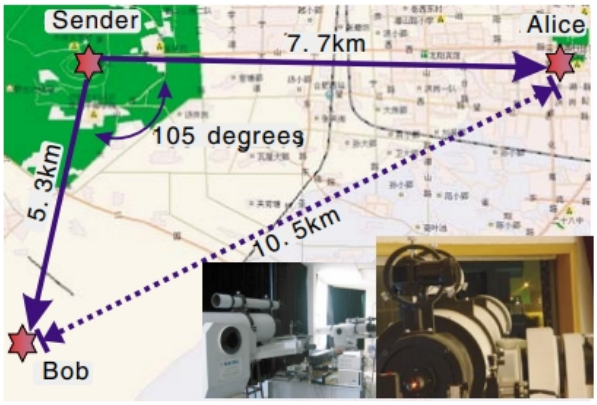

Figure 6.3: Schematic view of the positions of the sender between Alice and Bob. The transmitted photons traverse a noisy city environment (up to 30 000 cps of background noise at night without interference filters). Image from Ref.[18].

Receiver

Alice and Bob each have telescopes similar to those used for sending the photons. At their arrival, the signal photons are separated from the synchronization pulses by a dichroic mirror. A balanced beam splitter provides a random choice between the rectilinear and diagonal polarization bases. The photons then pass through a polarization beam splitter and are coupled into 62.5 μm fibers connected to single-photon detectors (SPD). Due to the different distances of Alice and Bob from the source, the entangled photons will arrive with a certain delay. This delay is subject to random variations caused by atmospheric turbulence, resulting in a time difference fluctuation ΔT. Thus, the coincidence time window needs to be larger than ΔT. However, if ΔT is set too high, it increases the accidental coincidence count rate, thereby reducing visibility. In their experiment, the authors opted for a coincidence time window of 20 ns.

Synchronization between the two receivers is achieved using a 532 nm laser. The beam, emitted from the source, is divided and directed towards the receivers, traversing the same optical path as the entangled photons. At each receiver, the time difference between the single-photon event signal and the associated synchronous laser pulse is recorded, allowing for coincidence determination via a classical communication link. A dichroic mirror is employed to separate the signal pulses from the synchronization pulses.

Interference filters are used to minimize the background count rate to 400 cps. Under ideal weather condition the total count rate is about 40 000 cps at Bob and about 18 000 cps at Alice and the coincident rate is about 300 cps when the visibility is high (>15km) and for normal visibility (10 km) the coincident count rate is about 150 cps.

Performance

The observed visibilities are 94% in the rectilinear basis and 89% in the diagonal basis which is above the 70.7% required for the violation of the CHSH inequality. The degree of entanglement was further assessed by calculating the Bell factor S_q defined by Eq.(3.27) using specific polarizer settings: 0° and 45° for Alice and 22.5° and 67.5° for Bob. These settings are optimal for testing the CHSH inequality and the obtained results for the correlation coefficient in these settings are reported in Table 6.1, resulting in a Bell factor $S_q = 2.45 \pm 0.09$. The violation of the CHSH inequality by 5 standard deviations confirms the entanglement between the distributed photons.

BBM92

From 15,308 transferred bits of raw key, the reconciliation of bases yielded 7,956 bits of sifted key with a QBER of 5.83%. After error correction, 4,869 bits of key remained, with the QBER reduced to 1.46%. The final step of privacy amplification resulted in 2,435 bits of secure key. The BBM92 protocol was performed during four minutes, and the key distribution rate is therefore of 10 bits per second. This achievement

$E(\phi_A,\phi_B)$	(0°, 22.5°)	(0°, 67.5°)	(45°, 22.5°)	(45°, 67.5°)
Value	-0.681	0.764	-0.421	-0.581
Deviation	0.040	0.036	0.052	0.046

Table 6.1: Measured correlation coefficient at specific angles of the polarization analyzers of Alice and Bob. These angles maximize the violation of the CHSH inequality. Table from Ref.[18].

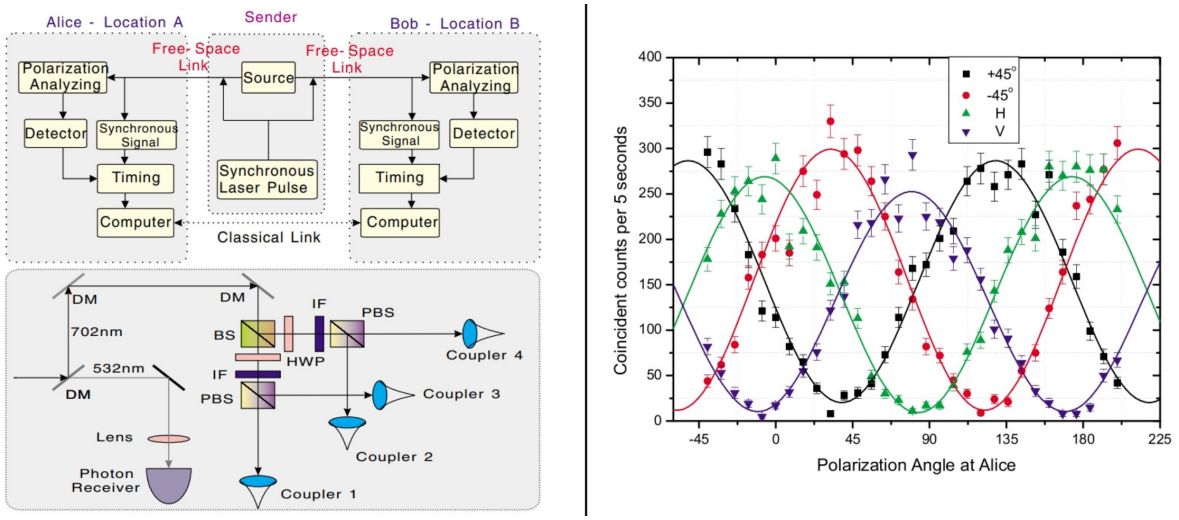

Figure 6.4: Block diagram of the experiment and optical setup at the receivers. Image from Ref.[18].

demonstrated the feasibility of exchanging entangled photons in a noisy atmospheric environment. The modest final key rate could be easily improved, potentially reaching several hundred key bits per second, with the use of a more intense source and couplers with higher collecting efficiency.

6.2.2 E91: long distance transmission

After demonstrating the feasibility of free-space entanglement-based QKD through the atmosphere, the next milestone before considering satellite QKD was to prove its viability over long distances. This was achieved in 2007 by Ursin *et al.*, who implemented the E91 protocol between the Canary Islands of La Palma and Tenerife via a 144 kilometers optical free-space link using the Optical Ground Station (OGS) of the European Space Agency (ESA) [19].

An illustration of the experimental setup is provided by Figure 6.5.

Emitter

A 355 nm pulsed Nd:Vanadate laser is used to pump a BBO crystal generating 710 nm polarization-entangled photons through type II parametric down conversion. The entangled photons are described by:

$$|\phi\rangle^- = \frac{1}{\sqrt{2}} \left(|H_A\rangle |V_B\rangle - |V_A\rangle |H_B\rangle \right). \tag{6.2}$$

After passing through the crystal, the photons are coupled into a single-mode optical fiber, which selects photons within a wavelength band of 710 ± 3, nm. For a power of 150 mW, 1 Mcps individual events, including 145,000 coincidence events, are locally observed. The local visibilities are 98% and 96% for the rectilinear and diagonal bases, respectively.

One photon from each entangled pair is measured locally while the second photon is sent via a single mode fibre to a transmitter telescope (150 mm diameter, 400 mm focal length, f/2.7). In the diffraction limited case, the transmitter telescope is designed to produce a beam of 1.5 m in diameter a the OGS.

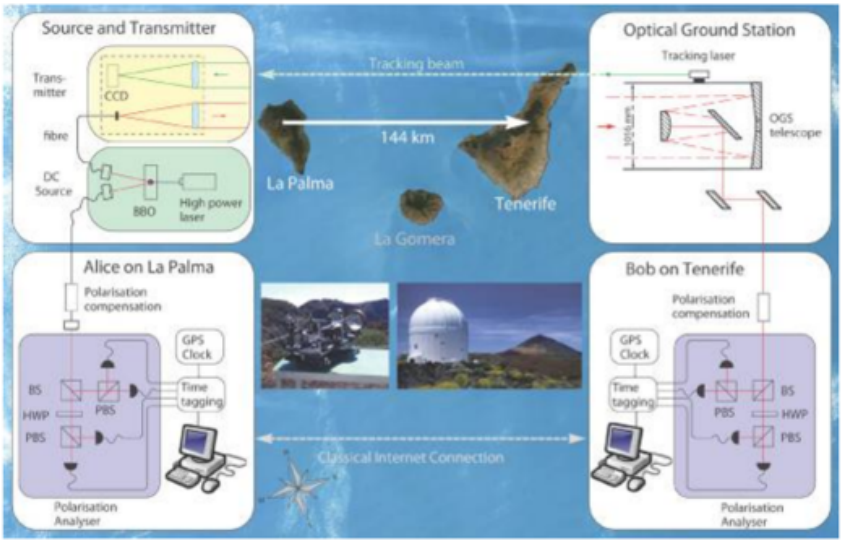

Figure 6.5: Illustration of the experimental setup employed by Ursin *et al.* to implement the E91 protocol between the Canary Islands of La Palma and Tenerife. Image from Ref.[19].

The effective beam diameters vary from 3.6 to 20 m depending on weather conditions. To mitigate the effects of atmospheric turbulence, the transmitter telescope alignment is automatically adjusted by a closed-loop tracking system. This system employs a 532 nm beacon laser, which is directed from the OGS to the single-photon transmitter.

Receiver

The OGS features a 1-meter Ritchey-Chrétien/Coudé telescope with an effective focal length of 39 meters (f/39) and a FOV of 8 arcseconds. To mitigate atmospheric turbulence, an additional f = 400 mm lens was incorporated to reduce beam wandering at the receiver. The single-photon beam is then focused using an f = 50 mm lens onto the polarization analysis unit, identical to the one used at the emitter. This unit consists of a balanced BS, allowing for random measurements in either the rectilinear or diagonal basis by directing the beam to one of the two corresponding PBS. Each photon is subsequently directed to one of the two couplers connected to the SPADs, depending on its polarization (see Figure 6.5).

Performance

Total losses in the optical link were generally around -25 to -30 dB. The main factor was beam divergence, causing a loss of -10 to -16 dB as the beam spread wider than the receiver telescope's aperture. Atmospheric conditions contributed another -8 to -12 dB to the loss. Finally, losses attributed to optical components and detector were about -8 dB.

During nighttime operations, the total count rate recorded at the OGS is 1500 cps. For each of the four detectors, 120 cps are attributed to the source, while 50 cps are from background detections. The majority of cps come from the detector's dark noise, which accounts for about 200 cps.

Each event is tagged with the detector channel and the detection time (with a 156 ps resolution using 10 MHz local oscillators, directly disciplined by the Global Positioning System (GPS), maintaining a relative drift of less than 10^{-11} over 100 seconds). Alice and Bob's time reference is synchronized via a 1 Hz GPS signal. The Network Timing Protocol (NTP) is employed to initialize time tagging within 500 ms for both parties. Coincidence between events is determined by cross-correlating the two sets of time tags, which identifies the offset (487 µs) and drift between the two timescales. Within a coincidence window of approximately 1 ns, the average coincidence count rate is 20-40 cps, depending on atmospheric conditions.

Over a period of 221 seconds, various configurations of polarization analyzer angles were applied to

determine the correlation coefficients, with 7058 coincidence events recorded. These coefficients, listed in Table 6.2, were used to calculate the Bell factor, resulting in a value of $S_q = 2.508 \pm 0.037$. This corresponds to a violation of the CHSH inequality (Eq.3.27) by 13 standard deviations.

$E(\phi_A,\phi_B)$	(0°, 22.5°)	(0°, 67.5°)	(45°, 22.5°)	(45°, 67.5°)
Value	-0.775	0.486	-0.435	-0.812
Deviation	0.015	0.020	0.023	0.014

Table 6.2: Measured correlation coefficient at specific angles of the polarization analyzers of Alice (local measurement) and Bob (at the OGS). These angles maximize the violation of the CHSH inequality. Datas from Ref.[19].

The setup was used to execute the E91 protocol over a 75-second duration, during which 789 coincidence events were recorded. From these, 417 raw key bits were generated, including 20 erroneous bits, yielding a QBER of $4.8\% \pm 1\%$. Following error correction and privacy amplification, the final secure key comprised 178 bits.

6.3 Satellite QKD

6.3.1 QUESS

The most significant satellite QKD project completed to date is the Chinese research initiative known as the Quantum Experiment at Space Scale (QUESS). This project notably included the deployment of the first satellite dedicated to quantum communications, named Micius and launched on 16 August 2016.

(i) Decoy-states BB84

Micius's first mission, described in Ref.[20], involved executing a three-level Decoy-state BB84 protocol in a downlink configuration. Each night, the satellite, orbiting in a 500 km Sun-synchronous trajectory, passes over the Xinglong ground station at around 00:50 local time for approximately 5 minutes. About 10 min before the satellite enters the shadow zone, its attitude is adjusted changing from a geocentric to a ground station centric pointing mode. When the satellite exceeds an elevation angle of 5° from the horizon plane of the ground station, a pointing accuracy of better than 0.5° is achieved. At 10° above the horizon, the APT systems are activated, starting bidirectional tracking and pointing to guarantee that the transmitter and receiver are robustly locked throughout the orbit. This enables a tracking accuracy of approximately 1.2 μrad, significantly smaller than the beam divergence.

From an elevation angle of about 15°, the QKD transmission begins, signal and decoy photons are emitted by the satellite together with the beacon laser for timing synchronization, which are received and detected by the ground station. The transmission concludes when the satellite's elevation angle decreases to 10° during its descent.

Emitter

A sketch of bot the encoding and decoding BB84 modules is presented in Figure 6.6. Three levels of intensity are used (they are optimized by performing simulations to maximize the secret bit rate for the satellite-to-ground channel): μ_s (high), μ_0 (vacuum) and μ_1 (moderate) with probability 0.5, 0.25 and 0.25 respectively.

Eight fibre-based laser diodes (four used as signal with intensity μ_s and four used as decoy states with intensities μ_0 and μ_1) emit 0.2 nm pulses with wavelength 848.6 nm with a repetition rate of 100 MHz. In-orbit measurements ensure that the eight lasers match their wavelengths within 0.006 nm, which is much smaller than their intrinsic bandwidth (0.1 nm). Moreover, they are synchronized to be within 10 ps, which is much smaller than their pulse duration of around 200 ps. A physical thermal noise device generates a 4-bit random number for each run that drives the eight lasers and determines the intensity

levels. The average photon number in the output of the telescope are obtained through a careful adjustement of the attenuation, with the following values: $\mu_s = 0.8$, $\mu_0 = 0$ and $\mu_1 = 0.1$.

The encoding module includes B84-encoding module consisting of a half-wave plate, two PBS and a BS, which randomly prepares the emitted photons in one of the four BB84 polarization states. A 300 mm Cassegrain telescope onboard is employed to transmit the light beam, which has a near-diffraction-limited far-field divergence of about 10 µrad, resulting in a beam diameter of approximately 12 meters after traveling 1200 km.

Receiver

A 1-meter Ritchey–Chrétien telescope, featuring a 10-meter focal length, is employed to collect the photons. The decoding system, which is similar to the encoding system, includes a BS, two PBS, and four SPD that boast 50% efficiency, dark counts under 25 cps, and a timing jitter of approximately 350 ps. The overall optical efficiency, including the receiving telescope and the fibre coupling on the ground station, is approximately 16%. Synchronization is achieved using a beacon laser with a 0.9 ns pulse width and a repetition rate of 10 kHz. A dichroic mirror at the receiver separates the beacon laser, extracting the timing information needed. This setup enables a synchronization jitter of 0.5 ns, which is used to tag the received signal photons within a 2-ns time window, and filter out the background noise.

Attitude control

To maintain a stable link with the satellite, which travels at a speed of approximately 7.6 km/s, an efficient APT system is essential. The APT systems for both the receiver and transmitter are illustrated in Figure 6.7.

The initial telescope alignment relies on the satellite's predicted position with an accuracy of within 200 meters. The ground station is equipped with a coarse pointing system that uses a two-axis gimbal mirror, achieving a pointing precision of around 0.5°. When the satellite reaches an elevation of 10°, a 671 nm beacon laser with a 0.9 mrad divergence is directed towards it. Once the optical transmitter's coarse-tracking CMOS camera, which has a wide FOV of 2.3°x2.3°, detects the ground beacon laser, the onboard APT system begins to accurately track it. Fine pointing is then carried out using a fast-steering mirror driven by piezo ceramics, with a tracking range of 1.6 mrad, and a camera with a narrower FOV of 0.64mrad×0.64mrad.

Meanwhile, the 532 nm beacon laser of the optical transmitter, with a divergence of 1.25 mrad, is targeted at the ground station. Upon the ground station's detection of the transmitter's beacon, the APT system begins precise tracking of the satellite's beacon laser, achieving secure bidirectional locking between the transmitter and receiver.

Using closed-loop feedback, the APT systems enable a tracking accuracy of approximately 1.2 μrad.

Another effect to consider is the time-dependent rotation of photon polarization due to the relative motion between the satellite and the ground station. Without compensation, this would theoretically degrade the polarization contrast ratio from 150:1 to zero over the course of an orbit. To counteract this, a motorized half-wave plate is used for dynamic polarization compensation, increasing the average polarization contrast ratio to 280:1.

Noise filtering

The detections are restricted to 2 ns time windows set by the synchronization system with beacon lasers, allowing for temporal filtering. Spectral filtering involves using interference filters that permit only photons within the 0.1 nm bandwidth of the laser diodes, thereby minimizing background noise. Note also that all the operations are performed during night time to avoid sunlight.

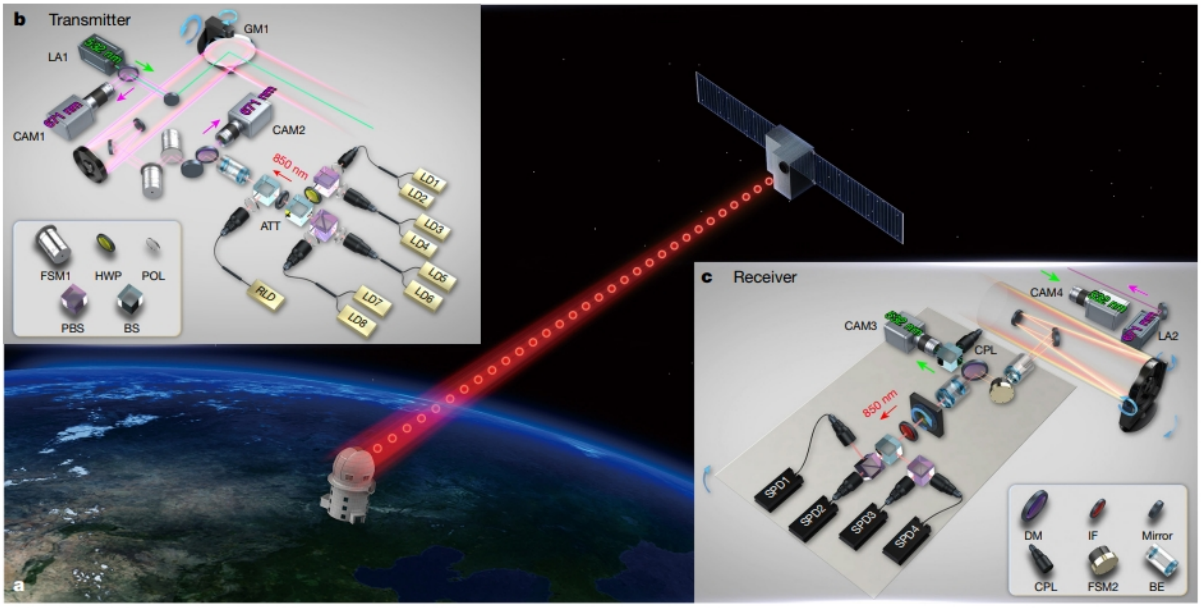

Figure 6.6: Illustration of the experimental setup employed by Liao *et al.* to implement the Decoy states BB84 protocol between the Micius satellite and the Xinglong ground station. **a:** General overview. **b:** Schematic view of the transmitter: the photons are collected by a 1-meter Ritchey–Chrétien telescope. The laser pulses of wavelength 850 nm are emitted from eight separate laser diodes (LD1-LD8) pass through a BB84 encoding module consisting of two polarizing beam splitters (PBSs), a half-wave plate (HWP) and a beam splitter (BS) and finally pass through an intensity attenuator (ATT). Another laser beam (LA1) with wavelength 532 nm is emitted for the tracking and the synchronization processes. Both are sent by a 300 mm Cassegrain telescope. Another laser is used as a polarization reference (RLD). A two-axis gimbal mirror (GM1) and a large FOV camera (CAM1) are used to drive the coarse tracking loop, while the fine tracking is achieved thanks to two fast steering mirrors (FSM1s) and a fast camera (CAM2). **c:** Schematic view of the receiver: the 532 nm beacon laser beam is separated in two paths; one is imaged by a camera (CAM3) for tracking while the other is imaged by a camera (CAM4) for time synchronization. The 850 nm decoy-state photons pass through interference filters (IF) for noise cancelling and are analysed by a BB84 decoder, which consists of a BS and two PBS, and are finally detected by four single-photon detectors (SPD1–SPD4). A 671 nm laser (LA2) is directed towards the satellite for system tracking. Image from Ref.[20].

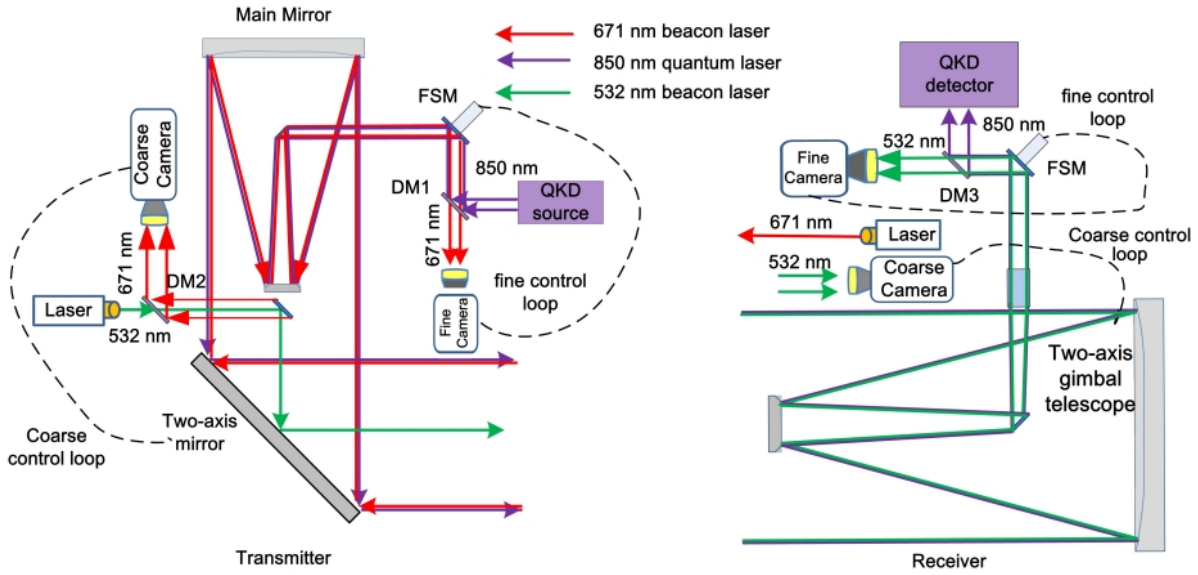

Figure 6.7: Schematic view of the APT systems on the satellite and at the ground station. Image from Ref.[20].

Performance

The loss budget estimated for a 1200 km distance includes a diffraction loss of approximately -22 dB, atmospheric absorption and turbulence losses ranging from -3 to -8 dB, and a pointing error contributing less than -3 dB. In the worst-case scenario, this results in a total attenuation of around 33 dB.

The minimum distance between the satellite and the ground station is determined by the highest elevation angle of the day, varying from 507.0 km at 85.7° to 1,034.7 km at 25.0°. The sifted key rate fluctuates with this distance, peaking at 40.2 kbits/s at 530 km and dropping to 1.2 kbits/s at 1,034.7 km, depending on both distance and weather conditions. The QBER observed ranges between 1% and 3%.

(ii) E91

The second mission of Micius, desribed in Ref.[21] was to distribute entangled photons between a ground station located in Delingha and two distant stations located in Nanshan and Lijiang, situated 1120 kilometers and 1203 kilometers away, respectively. In its sun-synchronous orbit at about 500 km altitude, the satellite passes into the field of view of the ground stations at approximately 1:30 AM local time, staying within sight for around 275 seconds. The satellite's distance from these stations varied between 500 and 2000 kilometers. The APT systems are started when the satellite reaches a 5° elevation angle, and the quantum transmission begins when it reaches a 10° elevation angle.

Emitter

A 405 nm continuous-wave laser is employed to pump a 15 mm long PPKTP crystal. The issue of the phase difference between the two superimposed states in the entangled state Eq.(5.1) can be addressed using a specific optical setup known as a Sagnac interferometer (see Figure 6.8). After passing through a PBS, the photons randomly follow either a clockwise or counterclockwise path in the Sagnac loop. As they traverse the PPKTP crystal, they generate 810 nm polarization-entangled photon pairs via the SPDC type II process. The direction in which these entangled photons travel matches that of the pump photon that produced them. This configuration allows for the generation of the Bell state $\phi^+ = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2)$ with the photons being separated by the PBS at the loop's exit and distributed to Alice and Bob. For a power of 30 mW, the source emits 5.9 million pairs of entangled photons per second.

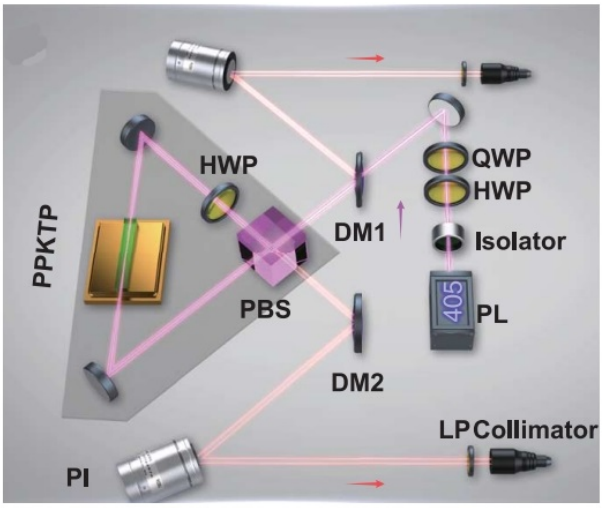

Figure 6.8: Schematic view of the spaceborne entangled photon source. A PBS oriented at 45° relative to the polarization plane of the photons generated by the 405 nm pump laser causes the path direction within the Sagnac loop to be randomized, the wave function describing a pump photon then splits into two components. When a pump photon passes through the crystal, it generates a pair of polarization-entangled photons via the type II SPDC process. These entangled photons, which have orthogonal polarizations, will be separated upon passing through the PBS at the output of the loop. A half-wave plate (HWP) is introduced into one of the branches such that the system is described by the Bell state $|\phi^+\rangle$ after the recombination of the wavefunctions for both traversal directions. Image from Ref.[21].

Two Cassegrain telescopes with apertures of 300 mm (the same as the one used for the decoy-states transmission) and 180 mm are utilized to establish the satellite-to-ground links. These telescopes, which emit beams with a near-diffraction-limited divergence of approximately 10 mrad, have been specifically optimized to reduce chromatic and spherical aberrations at 810 nm. They have optical efficiencies of about 45 to 55%.

The entangled photon source is housed within a 430 mm x 355 mm x 150 mm enclosure. The optical components are mounted and adhered to both sides of a base board that is 40 mm thick. The base board is made from titanium alloy, chosen for its favorable combination of rigidity, thermal expansion properties, and density.

Receiver

The receiving telescopes at the Delingha, Lijiang, and Nanshan stations have diameters of 1200 mm, 1800 mm, and 1200 mm, respectively. The link efficiency with the Lijiang station is enhanced due to its larger aperture size. The decoding module consists of a Pockels cell controlled by random numbers, allowing for the switch between rectilinear and diagonal measurement bases, followed by a PBS that directs the outputs to two couplers connected to the SPDs with dark counts below 100 Hz (see Figure 6.9B).

Attitude control

The APT systems are similar to those used for the decoy-states transmission, described above. They are illustrated in Figure 6.9.

At the emitter, the signal photon beam is combined with an infrared laser at 850 nm for synchronization and with a green laser at 532 nm for the tracking process. The synchronization laser is a 100 kHz pulsed laser, allowing for a synchronization jitter of 0.77 ns. Dynamic polarization compensation is managed

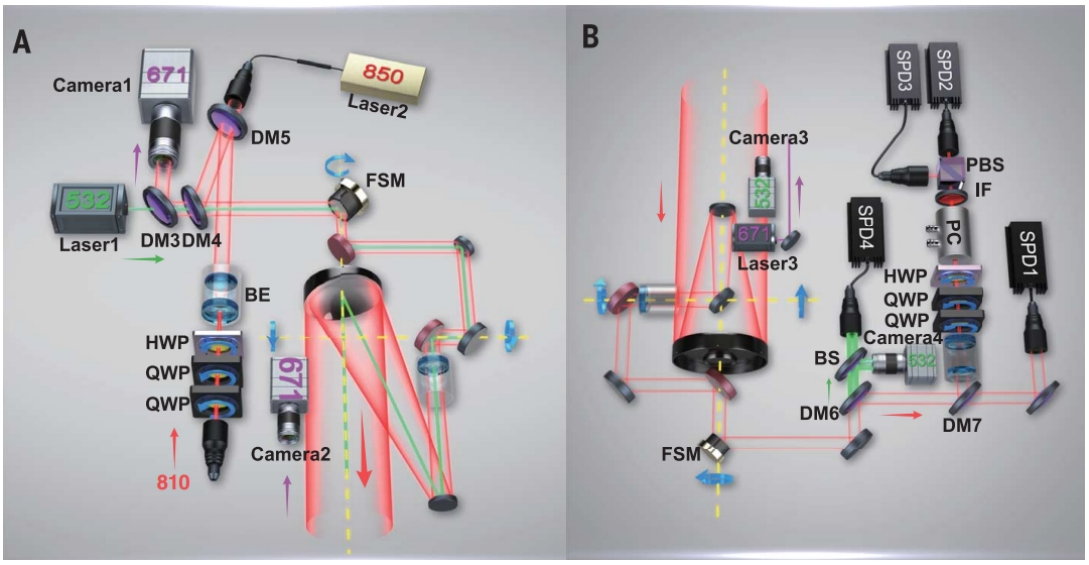

Figure 6.9: Schematic view of the optical setups: in the emitter (**A**) and in the receiver (**B**). Image from Ref.[21].

using two motorized quarter-wave plates and a half-wave plate, all remotely controlled. The tracking process is performed by finely imaging the incoming 671 nm laser beacon emitted by the ground stations. More precisely, coarse tracking is achieved using a two-axis turntable combined with a wide-field-of-view camera, allowing for a precision better than 50 μrad. Fine tracking is handled by a fast steering mirror paired with a high-speed camera. Together, these closed-loop feedback systems lock the ground stations with an accuracy of 0.41 μrad, which is much smaller than the beam divergence.

At the receiver, the 671 nm laser beacon is directed towards the satellite. The APT and polarization compensation systems are similar to those employed by the satellite. The synchronization and tracking beams are separated from the signal beam using dichroic mirrors.

Noise filtering

Temporal filtering is achieved through coincidence detection within a 2.5 ns time window, while spectral filtering is implemented by using 20 nm bandwidth interference filters in the receiving telescopes. The background noise, influenced by the Moon's position, varied between 500 and 2000 cps per detector. A reference laser on the satellite was employed to measure the real-time overall attenuation of the two-downlink channels, which varied between 64 and 82 dB.

Performance

A space-to-ground two-downlink channel was successfully established between the satellite and the Delingha and Lijiang stations. To confirm the presence of entanglement, correlation coefficients were calculated for different polarization analyzer angles at Alice's (Delingha station) and Bob's (Lijiang station) locations. During an effective period of 1159 seconds, 1167 coincidence events were recorded. The results, showed in Figure 6.10, revealed a Bell parameter $S_q = 2.37 \pm 0.09$, indicating a violation of the CHSH inequality by four standard deviations.

6.3.2 Other initiatives

The success of Micius' operations has significantly heightened interest in satellite QKD. The European Space Agency (ESA) intends to take this step forward by developing the Eagle-1 satellite in partnership with European space companies. This satellite is designed to pave the way for an ultra-secure network based on QKD and is part of the broader effort to develop the European Quantum Communication Infrastructure (EuroQCI) within the ScyLight (SeCure and Laser communication Technology) programme.

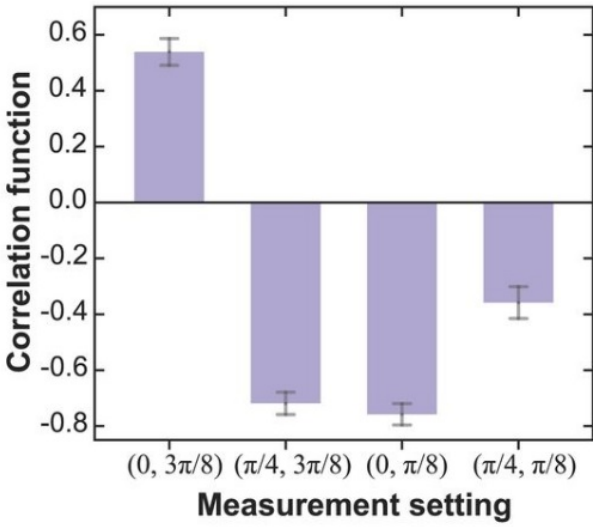

Figure 6.10: Diagram showing the correlation coefficients measured in various polarization measurement configurations. The data facilitated the calculation of the CHSH inequality, whose violation signifies the persistent entanglement between the photons pair. Image from Ref.[21].

Initially, the system will rely on an upgraded optical ground terminal from the German Aerospace Centre (DLR) in conjunction with a new optical ground terminal developed by a team from the Netherlands. The Eagle-1 satellite platform, constructed by the Italian company Sitael, will host a quantum-key payload developed by Tesat Spacecom of Germany, with operations managed by SES, headquartered in Luxembourg.

The Eagle-1 satellite is slated for launch between late 2025 and early 2026 and will undergo three years of in-orbit validation, supported by the European Commission [106].

6.4 QKD networks

QKD allows the establishment of a secure link between two parties, suitable for initiating a secure communication session or for the direct exchange of encrypted data. The range of point-to-point QKD is restricted by the PLOB bound (Eq.(5.4)), and fiber-based systems are limited to metropolitan areas, covering a few kilometers only.

Metropolitan QKD networks are established by linking several trusted nodes, which allows for multi-user capabilities and broadens the range of applications. This provides a secure communication alternative for critical infrastructures, such as hospital networks that manage patient sensitive data, as well as banking systems that facilitate interbank financial transactions.

Within the network, trusted nodes can be utilized as quantum relays to extend communication distances, as shown in Figure 6.11. This method is feasible for densely connected networks, ensuring that there are always intermediate nodes available for key exchange. However, the network should be geographically limited to avoid passing through too many intermediate nodes, which would significantly reduce the effective key rate between the end nodes. Moreover, each intermediary node holds the key information K_A, necessitating that it be trusted. This marks a significant difference from quantum repeaters, which enable end nodes to exchange a key without requiring access to the key material.

Ref.[107] proposed architecture designs for both trusted and untrusted intermediate nodes, aiming to integrate QKD technology into the broader, well-established internet security framework. The proposed untrusted setup is based on all-optical paths through the network mesh of fibres, switches and endpoints. Therefore, it can not be used to extend the distance of the QKD link between two end-users.

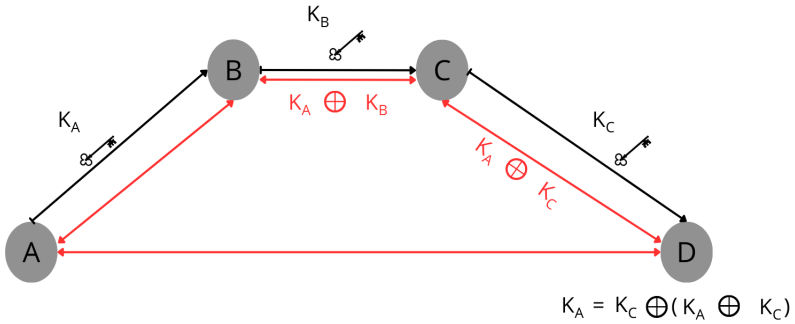

Figure 6.11: Schematic view of trusted nodes serving as quantum relays. If the distance between two network nodes A and D is too great, a cryptographic key K_A can still be exchanged with the help of intermediary trusted nodes B and C. These intermediary nodes hold the key information K_A, allowing them to decrypt the transmission, and must therefore be trusted.

In 2002, the Defense Advanced Research Projects Agency (DARPA) employed the trusted nodes approach to integrate four distinct types of QKD hardware into its network, thereby creating the world's first quantum network [108]. Since then, other networks following the same approach have emerged, including the Tokyo QKD network as one of the largest metropolitan QKD network [109].

As highlighted in Ref.[110], a star-topology MDI-QKD network, with only one intermediary node between any two users, can ensure secure communication without the need for a trusted relay. Field tests conducted in 2015 [111] showed that the key rates achieved were lower compared to the standard BB84 protocol using trusted relays under similar conditions. The authors suggest combining MDI-QKD over untrusted metropolitan networks with BB84 for the trusted backbone to achieve both practicality and security in wide-area QKD networks.

The largest quantum network to date spans over 4,600 kilometers and is detailed in Ref.[22]. This network comprises four metropolitan networks in a star topology linked by a 2,000 km backbone fiber connection. The network includes three types of nodes: user nodes, optical switches, and trusted relays. Additionally, two space-to-ground links connect two ground stations separated by over 2,600 km.

The fiber network utilized the decoy BB84 protocol with commercial devices, operating at 40 MHz in the metropolitan network and 625 MHz in the backbone network, resulting in secret key rates of 5 kbps and 80 kbps, respectively. This setup supports various services, such as text and file transmission, as well as audio and video calls. While the key rate isn't sufficient for one-time pad encryption, the secure key is used in combination with AES-128 encryption, with the key being regularly updated to ensure secure communication as long as the shared key remains undisclosed. For instance, if each pair of users consumes a 128-bit key per minute, the typical key rate of the backbone network can accommodate approximately $80 \times 10^3 \times 60/128 \simeq 37\,500$ users.

Future plans include constructing another backbone from Beijing to Shanghai, forming a large circular backbone QKD network. This design will allow the network to maintain functionality even if a trusted relay in the backbone encounters a failure. Moreover, with advancements in high-rate networks, one-time pad encryption could be employed to achieve information-theoretical security for data exchange, ensuring the highest level of security. On the other hand, when the technology reaches sufficient maturity, MDI-QKD protocols could serve as a compelling alternative to the decoy BB84 protocol. This approach could potentially eliminate the need for trusted relays, especially given the star topology of metropolitan networks.

The satellite-to-ground communication is based on a decoy-state BB84 protocol between Micius and the two ground stations of Xinglong and Nanshan. The total magnification of the 1.2m receiving telescope is reduced to increase its FOV. Consequently, the decoding module is modified to match the expanded

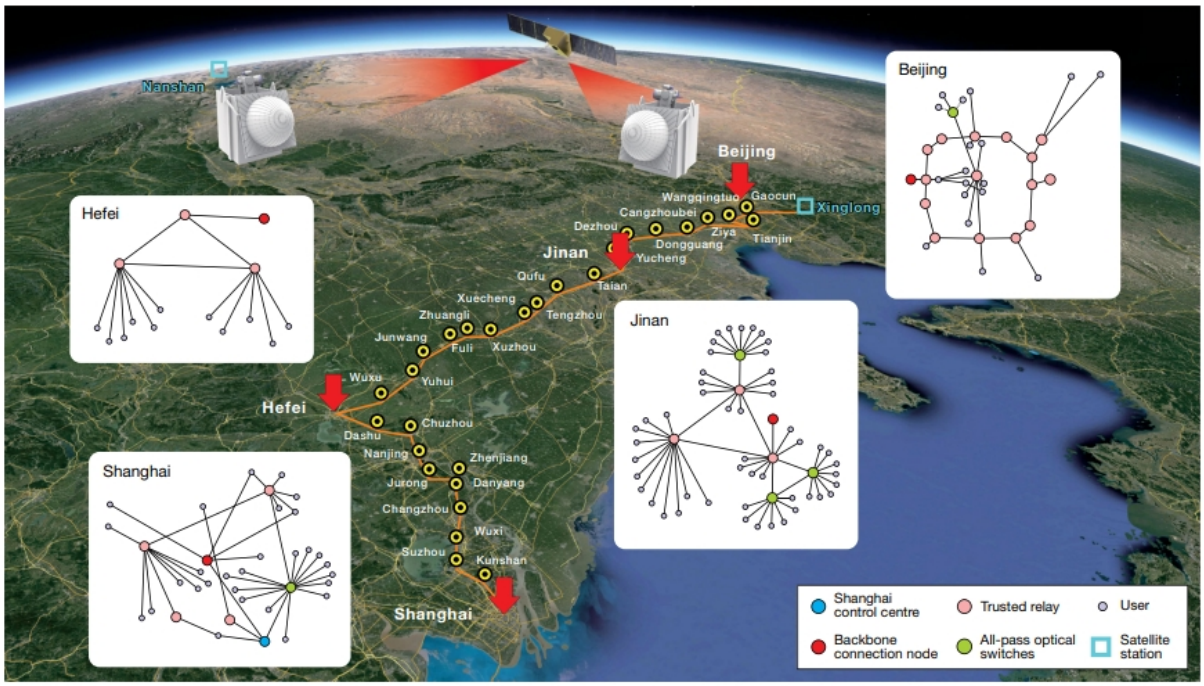

Figure 6.12: Illustration of the Chinese quantum networks shows a backbone fiber link extending over 2,000 km and a satellite link connecting the Xinglong and Nanshan ground stations, which are 2,600 km apart. This network, covering a total distance of over 4,600 km and serving four metropolitan networks, is currently the largest telecommunication network in existence. Image from Ref.[22].

beam waist size at its entrance, increasing from 0.8 mm to 2.7 mm. The duration link is restricted by the brief overpass duration of the satellite, lasting about 8 minutes. The prolonged period is made possible by an adaptive algorithm that dynamically adjusts the tracking cameras' sample rate and exposure time on the satellite, with these settings being actively controlled by the operator for the ground station cameras. This improvement allows establishing a connection at an elevation angle of approximately 5°, rather than the previous 10°. Furthermore, the quantum communication is dependent on the weather conditions, and transmission is not possible in rain, fog, or haze. A narrower 5 nm spectral filter is also used in place of the 10 nm one to suppress the background noise further.

Thanks to all these improvements, the highest sifted key rate reaches up to 462 kbps at the central points of the orbit with an average QBER of 0.50%. At the 5° minimum elevation angle, the satellite's distance from the ground station exceeds 2,000 kilometers, resulting in a sifted key rate reduction to 2 kbps and a QBER of approximately 2.5%. Typically, the satellite-to-ground communication channel generates a total secret key size of around 36 Mbit per week. When combined with AES-128 encryption, this can allow a pair of satellite users to update their secret keys by 8 Kbit every 10 days. In this mode, the secret key provided by the satellite can support approximately 6,000 users.

A satellite constellation might eventually remove the limitations due to satellite passing time. This possibility is analyzed in Ref.[112], and in Ref.[113] with a focus on a cost-effective constellation enabled by the use of low-cost cubesats. Addressing this challenge seems to be the next critical and perhaps final milestone in achieving a truly efficient global-scale QKD network.

Chapter 7

Conclusion

This work aims to provide the reader with an understanding of the mechanisms and stakes involved in quantum communication. Over the past 40 years since Bennett and Brassard developed the first QKD protocol, a range of coding schemes has emerged, with the best option being determined by factors such as environmental conditions, security requirements, and available resources. Several communication networks are already operational and offer services, but their geographic coverage and achievable key rates are still limited. However, their existence demonstrates the feasibility of a global-scale QKD network, making it reasonable to expect that a Quantum Internet, where data exchange is secure, will be achievable in the coming years. Reaching this objective requires optimizing the technologies used in QKD, and numerous research teams are dedicated to this effort. Satellite availability for QKD applications is a crucial factor for enabling the geographic expansion of quantum communication networks.

In addition to commercial systems, QKD is being explored by standardization bodies like the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). ETSI's efforts focus on QKD systems tailored for large-scale secure networks, exemplified by the work of the ETSI Industry Specification Group on Quantum Key Distribution for Users (ISG-QKD). This standardization process is essential for uniting global efforts, which will accelerate the development of QKD technologies and reduce costs through mass production of components. Lower costs will, in turn, facilitate the wider adoption of QKD networks. In the same spirit of cost reduction, QKD systems should be designed to integrate as seamlessly as possible with the already widely deployed traditional telecommunication networks.

Bibliography

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[2] Y. Leroyer and G. Sénizergues. *Introduction à l'information quantique*. ENSEIRB-MATMECA, 2017.

[3] Atom Computing. White paper: Highly scalable quantum computing with atomic arrays. Technical report, Atom Computing, 918 Parker St. Suite A-13, Berkeley CA 94710, 2022.

[4] Renato Renner and Ramona Wolf. Quantum advantage in cryptography. *AIAA Journal*, 61(5):1895–1910, May 2023.

[5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[6] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[7] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Phys. Rev. Lett.*, 82:2594–2597, Mar 1999.

[8] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4341, Dec 1995.

[9] Chandra Natarajan, Michael Tanner, and Robert Hadfield. Superconducting nanowire single-photon detectors: Physics and applications. *Superconductor Science Technology - SUPERCONDUCT SCI TECHNOL*, 25, 04 2012.

[10] R. Paschotta. Numerical aperture. RP Photonics Encyclopedia.

[11] J-P Bourgoin, E Meyer-Scott, B L Higgins, B Helou, C Erven, H Hübel, B Kumar, D Hudson, I DSouza, R Girard, R Laflamme, and T Jennewein. Corrigendum: A comprehensive design and performance analysis of low earth orbit satellite quantum communication (2013 new j. phys. 15 023006). *New Journal of Physics*, 16(6):069502, jun 2014.

[12] E. Hecht. *Optics*. Pearson Education, Incorporated, 2017.

[13] Matthew P Peloso, Ilja Gerhardt, Caleb Ho, Antía Lamas-Linares, and Christian Kurtsiefer. Daylight operation of a free space, entanglement-based quantum key distribution system. *New Journal of Physics*, 11(4):045007, apr 2009.

[14] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, Aug 2017.

[15] Miao Er-long, Han Zheng-fu, Gong Shun-sheng, Zhang Tao, Diao Da-sheng, and Guo Guang-can. Background noise of satellite-to-ground quantum key distribution. *New Journal of Physics*, 7(1):215, oct 2005.

[16] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, Jan 1992.

[17] B. C. Jacobs and J. D. Franson. Quantum cryptography in free space. *Opt. Lett.*, 21(22):1854–1856, Nov 1996.

[18] Cheng-Zhi Peng, Tao Yang, Xiao-Hui Bao, Jun Zhang, Xian-Min Jin, Fa-Yong Feng, Bin Yang, Jian Yang, Juan Yin, Qiang Zhang, Nan Li, Bao-Li Tian, and Jian-Wei Pan. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94:150501, Apr 2005.

[19] Rupert Ursin, Felix Tiefenbacher, T. Schmitt-Manderbach, Henning Weier, Thomas Scheidl, M. Lindenthal, Bibiane Blauensteiner, Thomas Jennewein, J. Perdigues, Pavel Trojek, B. [Ouml]|mer, M. F|[uuml]|rst, M. Meyenburg, Rarity JG, Zoran Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481–486, 06 2007.

[20] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, Sep 2017.

[21] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[22] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, Sheng-Long Han, Qing Yu, Ken Liang, Fei Zhou, Xiao Yuan, Mei-Sheng Zhao, Tian-Yin Wang, Xiao Jiang, Liang Zhang, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Chao-Yang Lu, Rong Shu, Jian-Yu Wang, Li Li, Nai-Le Liu, Feihu Xu, Xiang-Bin Wang, Cheng-Zhi Peng, and Jian-Wei Pan. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, Jan 2021.

[23] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[24] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[25] W. K. Wootters and W.H. Zurek. A single quantum can not bey copied. *Nature*, 299:802–803, Oct 1982.

[26] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[27] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, jan 1983.

[28] William K Wootters and Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[29] M. N. Vyalyi A. Yu. Kitaev, A. H. Shen. *Classical and Quantum Computation*. Graduate Studies in Mathematics. Amer Mathematical Society, 2002.

[30] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9–11):771–783, September 2000.

[31] L. M. K. Vandersypen and I. L. Chuang. Nmr techniques for quantum control and computation. *Reviews of Modern Physics*, 76(4):1037–1069, January 2005.

[32] Dawei Lu, Aharon Brodutch, Jihyun Park, Hemant Katiyar, Tomas Jochym-O'Connor, and Raymond Laflamme. Nmr quantum information processing, 2015.

[33] J. F. Poyatos, J. I. Cirac, R. Blatt, and P. Zoller. Trapped ions in the strong-excitation regime: Ion interferometry and nonclassical states. *Physical Review A*, 54(2):1532–1540, August 1996.

[34] D. J. Wineland, D. Leibfried, M. D. Barrett, A. Ben-Kish, J. C. Bergquist, R. B. Blakestad, J. J. Bollinger, J. Britton, J. Chiaverini, B. Demarco, D. Hume, W. M. Itano, M. Jensen, J. D. Jost, E. Knill, J. Koelemeij, C. Langer, W. Oskay, R. Ozeri, R. Reichle, T. Rosenband, T. Schaetz, P. O. Schmidt, and S. Seidelin. Quantum control, quantum information processing, and quantum-limited metrology with trapped ions. In *Laser Spectroscopy*. World Scientific, December 2005.

[35] He-Liang Huang, Dachao Wu, Daojin Fan, and Xiaobo Zhu. Superconducting quantum computing: a review. *Science China Information Sciences*, 63(8), July 2020.

[36] John Preskill. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, August 2018.

[37] A. Wilkins. Newscientist, 2023. Accessed on 07 02, 2024.

[38] J. Gambetta. Ibm, 2023. Accessed on 07 02, 2024.

[39] K. Barnes. Assembly and coherent control of a register of nuclear spin qubits. *Nature Communications*, 13(1):2779, May 2022.

[40] R. Mandelbaum, M. Steffen, and A. Cross. Ibm, 2023. Accessed on 07 02, 2024.

[41] H Edlbauer. Semiconductor-based electron flying qubits: review on recent progress accelerated by numerical modelling. *EPJ Quantum Technology*, 9(1):21, Aug 2022.

[42] Zhongqi Sun, Yue Li, and Haiqiang Ma. Experimental high-dimensional quantum key distribution with orbital angular momentum. *J. Opt. Soc. Am. B*, 41(2):351–355, Feb 2024.

[43] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 1984.

[44] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[45] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23), June 2007.

[46] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical Review Letters*, 105(7), August 2010.

[47] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), March 2012.

[48] D. Gottesman, Hoi-Kwong Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, 4:325–360, 09 2004.

[49] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5), April 2000.

[50] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[51] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters*, 94:230503, 07 2005.

[52] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[53] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, October 1998.

[54] Ramona Wolf. *Quantum Key Distribution*. 0075-8450. Springer Cham, 2021.

[55] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.

[56] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[57] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[58] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[59] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000.

[60] Thomas Durt, Dagomir Kaszlikowski, Jing-Ling Chen, and L. C. Kwek. Security of quantum key distributions with entangled qudits. *Phys. Rev. A*, 69:032313, Mar 2004.

[61] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Observation of three-photon greenberger-horne-zeilinger entanglement. *Phys. Rev. Lett.*, 82:1345–1349, Feb 1999.

[62] Dagomir Kaszlikowski, Piotr Gnaciński, Marek Żukowski, Wieslaw Miklaszewski, and Anton Zeilinger. Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85:4418–4421, Nov 2000.

[63] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Physical review letters*, 88:040404, 02 2002.

[64] Dagomir Kaszlikowski, Kelken Chang, Daniel Kuan Li Oi, Leong Chuan Kwek, and C. H. Oh. Quantum cryptography based on bell inequalities for three-dimensional system. *arXiv: Quantum Physics*, 2002.

[65] Thomas Durt, Nicolas J. Cerf, Nicolas Gisin, and Marek Żukowski. Security of quantum key distribution with entangled qutrits. *Phys. Rev. A*, 67:012311, Jan 2003.

[66] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[67] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, Jul 2007.

[68] Dominic Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, may 2001.

[69] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D*, 41(3):599–627, January 2007.

[70] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.*, 90:057902, Feb 2003.

[71] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, Jun 2005.

[72] Giacobino, É. Effets non linéaires et fluctuations quantiques. *Collection de la Société Française d'Optique*, 6:185–201, 1998.

[73] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000.

[74] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, Oct 2004.

[75] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. *Phys.*

Rev. A, 63:022309, Jan 2001.

[76] Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Physical Review Letters*, 101(20), November 2008.

[77] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[78] Akihiro Mizutani, Masanori Terashita, Junya Matsubayashi, Shogo Mori, Ibuki Matsukura, Suzuna Tagawa, and Kiyoshi Tamaki. Differential-phase-shift qkd with practical mach-zehnder interferometer, 2024.

[79] Kyo Inoue and Toshimori Honjo. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Phys. Rev. A*, 71:042305, Apr 2005.

[80] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.*, 111:130501, Sep 2013.

[81] Wolfgang Tittel and Gregor Weihs. Photonic entanglement for fundamental tests and quantum communication, 2001.

[82] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98:060503, Feb 2007.

[83] Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J. Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, and Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3), September 2013.

[84] Ali Anwar, Chithrabhanu Perumangatt, Fabian Steinlechner, Thomas Jennewein, and Alexander Ling. Entangled photon-pair sources based on three-wave mixing in bulk crystals. *Review of Scientific Instruments*, 92(4), April 2021.

[85] Deny Hamel. Realization of novel entangled photon sources using periodically poled materials, 2011. Master thesis (University of Waterloo) available online at `https://uwspace.uwaterloo.ca/items/c773165a-2a82-401e-904b-02953af19afb`.

[86] Sebastian Philipp Neumann, Thomas Scheidl, Mirela Selimovic, Matej Pivoluska, Bo Liu, Martin Bohmann, and Rupert Ursin. Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources. *Phys. Rev. A*, 104:022406, Aug 2021.

[87] Niccolò Calandri, Qing-Yuan Zhao, Di Zhu, Andrew Dane, and Karl K. Berggren. Superconducting nanowire detector jitter limited by detector geometry. *Applied Physics Letters*, 109(15), October 2016.

[88] Fabian Beutel, Helge Gehring, Martin A. Wolff, Carsten Schuck, and Wolfram Pernice. Detector-integrated on-chip qkd receiver for ghz clock rates. *npj Quantum Information*, 7(1):40, Feb 2021.

[89] Single quantum. Superconducting nanowire single photon detection system, 2024. Accessed on 07 25, 2024.

[90] R. Paschotta. P–i–n photodiodes. RP Photonics Encyclopedia. Available online at `https://www.rp-photonics.com/p_i_n_photodiodes.html`. Accessed on July 15, 2024.

[91] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters for communication, 1998.

[92] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1), April 2017.

[93] Thorlabs. Single mode fiber (smf-28-j9), 2024. Accessed on 07 24, 2024.

[94] Stefano Pirandola. End-to-end capacities of a quantum communication network. *Communications Physics*, 2(1):51, May 2019.

[95] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, March 2002.

[96] GNS Components. Diverses causes d'atténuation des fibres, 202. Accessed on 07 25, 2024.

[97] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden. Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods. *The European Physical Journal D*, 30(1):143–148, July 2004.

[98] Cristian Bonato, Markus Aspelmeyer, Thomas Jennewein, Claudio Pernechele, Paolo Villoresi, and Anton Zeilinger. Influence of satellite motion on polarization qubits in a space-earth quantum communication link. *Opt. Express*, 14(21):10050–10059, Oct 2006.

[99] Alessandro Fedrizzi, Rupert Ursin, Thomas Herbst, Matteo Nespoli, Robert Prevedel, Thomas Scheidl, Felix Tiefenbacher, Thomas Jennewein, and Anton Zeilinger. High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics*, 5(6):389–392, May 2009.

[100] P. R. Tapster J. G. Rarity and P. M. Gorman. Secure free-space key exchange to 1.9km and beyond. *Journal of Modern Optics*, 48(13):1887–1901, 2001.

[101] S. Chaabani. Advances in free-space quantum key distribution, 2023. Master thesis (University of Liège) available online at `http://hdl.handle.net/2268.2/17887`.

[102] Michael A. Nielsen and Isaac L. Chuang. *The Infrared Electro-Optical Systems Handbook, vol. 2: Atmospheric propagation of radiation editor: Frederick G. Smith.* Infrared Information Analysis Center SPIE Optical Engineering Press, 1993.

[103] C Bonato, A Tomaello, V Da Deppo, G Naletto, and P Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, apr 2009.

[104] Bahaa Saleh and Malvin Carl Teich. *Electro-Optics*, chapter 18, pages 696–736. John Wiley Sons, Ltd, 1991.

[105] R. Paschotta. Electro-optic modulators. RP Photonics Encyclopedia. Available online at `https://www.rp-photonics.com/electro_optic_modulators.html`.

[106] Esa. Eagle-1, 2024. Publication available online at `https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1`. Accessed on July 28, 2024.

[107] Chip Elliott. Building the quantum network*. *New Journal of Physics*, 4(1):46, jul 2002.

[108] Chip Elliott, Alexander Colvin, David Pearson, Oleksiy Pikalo, John Schlafer, and Henry Yeh. Current status of the darpa quantum network, 2005.

[109] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387, May 2011.

[110] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1):16025, Nov 2016.

[111] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X*, 6(1), March 2016.

[112] Liao Shengkai, Jin Lin, Jianyu Wang, Weiyue Liu, Jia Qiang, Juan Yin, Yang Li, Qi Shen, Xue-Feng Zhang, Liangand Liang, Hai-Lin Yong, Feng-Zhi Li, Ya-Yun Yin, Yuan Cao, Wen-Qi Cai, Wen-Zhuo Zhang, Jian-Jun Jia, Jin-Cai Wu, Xiao-Wen Chen, and Jian-Wei Pan. Space-to-ground quantum key distribution using a small-sized payload on tiangong-2 space lab. *Chinese Physics Letters*, 34:090302, 08 2017.

[113] Luca Mazzarella, Christopher Lowe, David Lowndes, Siddarth Koduru Joshi, Steve Greenland, Doug McNeil, Cassandra Mercury, Malcolm Macdonald, John Rarity, and Daniel Kuan Li Oi. Quarc: Quantum research cubesat—a constellation for quantum communication. *Cryptography*, 4(1), 2020.