UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia “Galileo Galilei”

Dipartimento di Ingegneria dell’Informazione

Master Degree in Physics

Final Dissertation

Development of a 1310 nm Quantum Key Distribution system

Thesis supervisor

Prof. Giuseppe Vallone

Thesis co-supervisor

Dr. Marco Avesani

Candidate

Mattia Sabatini

Academic Year 2021/2022

Abstract

Quantum Key Distribution (QKD) represents an innovative technique of generating an encryption key shared between two interlocutors which allows overcoming the problems of classical cryptography. The purpose of the thesis is to build and test a QKD system operating at a wavelength of 1310 nm, which allows a better coexistence of the quantum signal with a classic communication signal at 1550 nm on the same optical fiber. Another objective of the thesis is to demonstrate the operating principle of an advanced version that works for both discrete and continuous variable QKD.

Contents

1 Introduction to Quantum Key Distribution

1.1 Cryptography

Cryptography is the art of making a message understandable only by the recipient authorized to read it and incomprehensible to unauthorized ones. A cryptographic algorithm is a set of processes that, by processing information called a key, allows to encode or decode the message to be kept safe from any unwanted interceptors.

Looking back over the history of cryptography it seems that every culture that develops writing then starts using cryptography shortly thereafter. [1][2][3][4][5]

Scytale

One of the earliest known cryptographic methods is the scytale, which was used in 404 BC by the Spartans to communicate in secret during military campaigns. A long narrow strip of parchment was wrapped around a wooden stick on which the secret message to be sent was written as shown in Figure 1.1. The parchment was then sent to the recipient (without the stick) who, in order to obtain the original text, had to wrap it on another stick of the same diameter. In this case the diameter of the stick acted as a decryption key. [6][7]

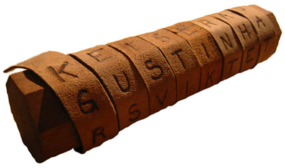


Figure 1.1: Reconstruction of a scytale. [8]

Caesar cipher

Another of the earliest known cryptographic methods is the Caesar cipher, used around 100 BC by Julius Caesar during the Gallic War to secretly communicate with his officers. The message to be sent was encrypted simply using a translated alphabet, in which each letter was replaced with another letter translated into the alphabet by a fixed number of steps as shown in Figure 1.2. In this case, the key consisted of the number of translation steps from the original alphabet. The problem with this method is that there are only 25 possible keys (since the letters of the alphabet are 26), and therefore it is possible to decrypt the message even without knowing the key through a brute force attack, i.e. simply by trying all the possible keys.

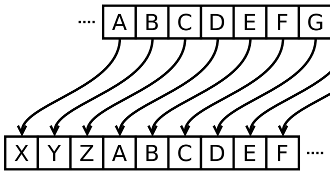


Figure 1.2: The action of a Caesar cipher is to replace each letter with a different one a fixed number of places down the alphabet. The Caesar cipher illustrated here uses a left shift of three. [9]

The security of cryptographic systems initially, as in those discussed so far, was mainly based on being able to keep the cryptographic method hidden. But as cryptography progressed, in 1880, Auguste Kerckhoffs formulated the Kerckhoffs Principle, which states that the security of a cryptographic system must not reside in the cryptographic algorithm but in keeping the decryption key hidden. [5][7][10][11]

Enigma machine

Moving on to more recent times, in the 1920s the Nazis used a machine, called Enigma, to encrypt and decrypt secret messages exchanged during World War II. It was an electromechanical machine consisting of a sequence of rotors, wired gear wheels on which the letters of the alphabet were imprinted. The machine shuffled the letters of the alphabet by connecting an input letter to a different output letter generated by the machine. It was possible to vary: the settings on the single rotor and the sequence in which the rotors operated in such a way as to have numerous possible combinations of setting the machine. Arrangements were made so that each day the settings of the Enigma machine were changed according to a calendar cipher distributed in advance with each machine. The safety was based on the fact that the possible combinations of the machine were so many that it was not possible to test them all in the entire life of a human being. The British, led by the mathematician Alan Turing, used another electromechanical machine, called the Bomb, to decipher the messages encrypted by the Enigma machine.

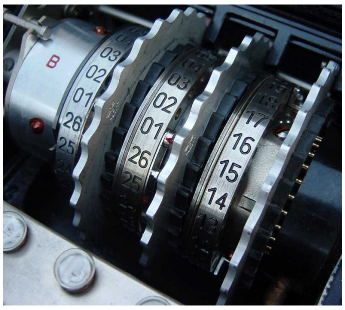


Figure 1.3: Stack of rotors inside an Enigma machine. [12]

World War II brought advances that marked a turning point for cryptography. Later in the Information Age, thanks to the development and spread of personal computers, the ability to exchange data in a secure manner has become a priority and encryption has become an area of central importance and a tool within everyone's reach. [2][7][13][14]

1.1.1 One-time pad

In 1917 Gilbert Vernam invented a cryptographic system, called the Vernam cipher or one-time pad, which was later shown to be unconditionally secure by Claude Shannon in 1949. The one-time pad works as follows: let's consider that we have a message written as a binary sequence to be encrypted and suppose to add to this message, through a bitwise XOR operation, a sequence of completely random bits that represent our key. This way we get a completely random encrypted message. An example is shown in Figure 1.4. To decrypt the message and recover the original message, the same random key must be added to the encrypted message again. The key must satisfy the following conditions:

- it must be composed of completely random data,
- it must be as long as the message to be encrypted,
- it can never be reused (this is the reason for the name one-time pad),
- it must be shared between sender and recipient and kept completely secret.

message	1	0	1	1	1	0	0	1	1	0	1	0	1	0
							⊕							
random key	1	0	0	0	1	0	1	0	1	1	0	1	0	1
							=							
encrypted message	0	0	1	1	0	0	1	1	0	1	1	1	1	1

Figure 1.4: Example of one-time pad encryption.

The feature of this cryptographic system is that it is unconditionally secure. All cryptographic systems devised before the one-time pad could theoretically be broken using enough computational power, while the one-time pad is in principle undecipherable. The one-time pad was used, for example, during the Cold War to communicate securely between the US and the USSR. The main limitation of this system, however, is that it is necessary to have a secure method of sharing a key as long as the entire message to be encrypted. This is the main reason why most cryptographic systems currently rely on other systems that use short keys and are not unconditionally secure but are computationally secure. [2][7][15]

1.1.2 RSA

In cryptography, by convention, the sender of the message is called Alice, the recipient Bob and any interceptor who wants to decrypt the message is called Eve. Two types of cryptographic systems can be distinguished:

- Symmetric cryptography (or private key cryptography): the same private key is used to encode and decrypt the message and must be known only by the sender and receiver as shown in Figure 1.5. An example of such encryption is the one-time pad (discussed in Section 1.1.1).

- Asymmetric cryptography (or public key cryptography): two different keys are used, a public one to encrypt the message and a private one to decrypt it as shown in Figure 1.6. The two keys are linked by a function that is easy to calculate in one direction but very difficult (computationally) to calculate in the opposite direction so it is easy to obtain the public key from the private one, but vice versa is very difficult. An example of asymmetric cryptography is the RSA.

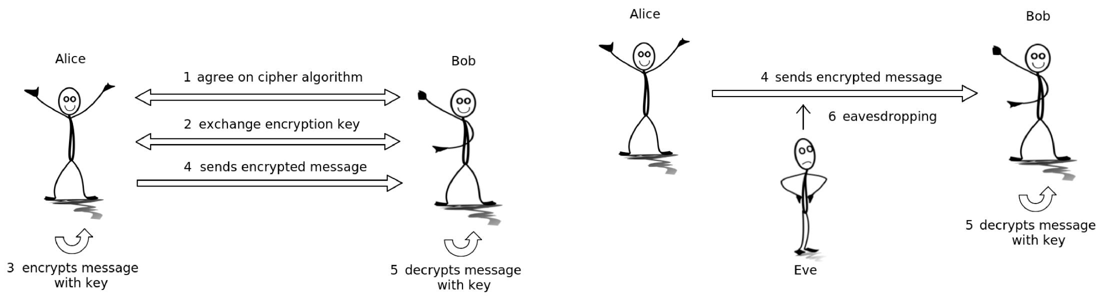
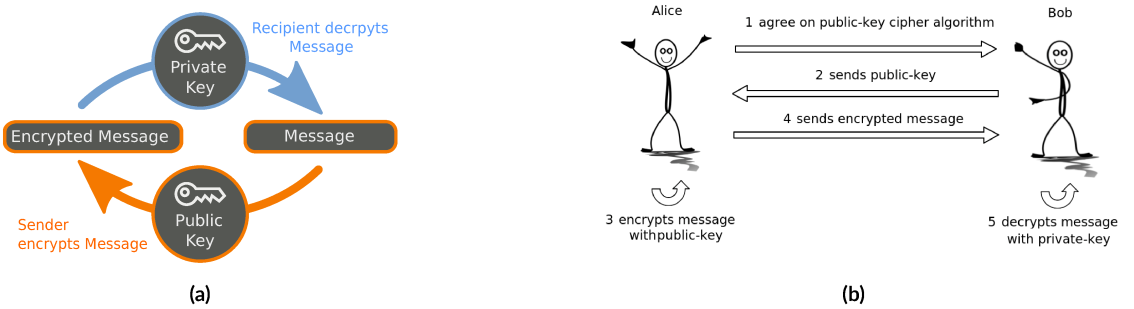

Alice
1 agree on cipher algorithm
Bob
2 exchange encryption key
4 sends encrypted message
3 encrypts message with key
5 decrypts message with key
Alice
Bob
4 sends encrypted message
6 eavesdropping
5 decrypts message with key
Eve

Figure 1.5: Symmetric cryptography scheme. 1. Alice and Bob agree on which encryption algorithm to use. 2. One of the two creates a private key and sends it to the other, the key can be used both to encrypt and decrypt the message. 3. Alice uses the key to encrypt the message. 4. Alice sends the encrypted message to Bob. 5. Bob uses the key to decrypt Alice's message. 6. Now let's assume that Eve tries to intercept the messages exchanged between Alice and Bob. The problem with symmetric encryption is key exchange: if this is not done securely, Eve can get hold of it and decrypt the messages exchanged between Alice and Bob. [16]


Private Key
Recipient decrpyts Message
Encrypted Message
Message
Public Key
Sender encrypts Message
Alice
1 agree on public-key cipher algorithm
Bob
2 sends public-key
4 sends encrypted message
3 encrypts message withpublic-key
5 decrypts message with private-key

(a)

(b)

Figure 1.6: Asymmetric cryptography scheme. (a) Two different keys are used: a public one to encrypt the message and a private one (which remains secret and is not exchanged) to decrypt it. The keys depend on each other but the math power is very expensive when trying to calculate the private key from the public one. (b) 1. Alice and Bob establish an agreement on which encryption algorithm to use. 2. Bob generates a pair of keys: a public and a private one and sends the public key to Alice. 3. Alice encrypted the message with the public key. 4. Alice sends the encrypted message to Bob. 5. Bob decrypts the message using the private key. In this way, even if Eve steals the public key, she cannot still decrypt the message because she needs the private key which is only owned by Bob. This avoids the problem of symmetric encryption key distribution.

The RSA (acronym for Rivest, Shamir and Adleman, the names of its inventors) is one of the cryptographic systems currently most used and is an asymmetrical encryption system designed in 1977. The basic idea is that it is easy to multiply two prime numbers with each other, but it is complicated to make vice versa, that is, to make a number in the two prime numbers. The problem of factoring very large integers is a mathematical problem that is computationally difficult to solve with current knowledge and technology, it would take such a long time to make it unsolvable in practice. To give an example, a classic computer would need about 300 trillion years to break a key of 2048 bit. The RSA works like this:

- Bob randomly chooses two very large prime numbers p and q and calculates their product $n = pq$;
- Bob chooses a coprime number e with $(p-1)(q-1)$ and such that

$$1 < e < (p-1)(q-1) \tag{1.1}$$

  (two numbers are coprime if they have no different common divisor from 1 and -1);
- Bob calculates d such that

$$ed \equiv 1 \pmod{(p-1)(q-1)} \ ; \tag{1.2}$$

- (n, e) constitute the public key and (n, d) the private key;
- Bob shares the public key with Alice;
- Alice encodes the message m using the public key with the operation:

$$c = m^e \pmod{n} \ ; \tag{1.3}$$

- Alice sends the encoded message c to Bob;
- Bob decodes Alice's message using the operation:

$$m = c^d \pmod{n} \ ; \tag{1.4}$$

The advantages compared to the Vernam cipher are that:

- the public key can be known by anyone, while the secret key is owned only by Bob and it is not necessary to exchange it;
- the public key can be reused.

If the prime factors p and q of n are found, then d can be easily calculated from Eq. (1.2) since e is known and the RSA cryptosystem can be hacked. But the best classical algorithm currently known for factoring integer prime numbers requires exponential time with the number of bits. On the contrary, the operation of multiplying two prime numbers requires a polynomial time. Therefore it is easy to obtain the public key from the private one, but vice versa takes such a long time that it is not practicable. However, it is not excluded that a more efficient classical factorization algorithm may be discovered in the future. Furthermore, the security of cryptography depends on the length of the key and this has been increased over the years because advances in technology have led to computers with greater computational capabilities, which have shown that the length used was no longer secure. Today the suggested key length is 2048 bits. The General Number Field Sieve (GNFS) algorithm is the most efficient classical algorithm known for factoring large integers (greater than 10^{100}), for factoring an integer N it works in sub-exponential time:

$$O\left(e^{\sqrt[3]{\frac{64}{9}}(\ln N)^{1/3}(\ln\ln N)^{2/3}}\right) \ . \tag{1.5}$$

In 1994 Peter Shor devised a quantum algorithm, called Shor's algorithm, which is able to solve the problem of factorising integer primes on a quantum computer in polynomial rather than exponential time:

$$O\big((\ln N)^2(\ln\ln N)(\ln\ln\ln N)\big) \ . \tag{1.6}$$

For example, the GNFS would take more than a billion years to factor a 2048 digit key, but using Shor's algorithm (at 1 MHz) it would take between tens of seconds and less than a month (depending on the architecture). This means that a quantum computer, with enough qubits, could use Shor's algorithm to break currently used public key cryptographic schemes such as RSA. Such a quantum computer does not yet exist today, because they do not have a sufficient number of qubits and the error rate that we have in quantum computers today is too high for factorising large integers, but research in this field continues to continue. So the threat of making current cryptographic systems vulnerable is real. [2][7][10][13][17][18][19]

1.2 Quantum mechanics

1.2.1 Qubit

In the classical case, the exchange of information takes place using the bit, the smallest unit in which the classical information can be encoded. The bit is a Boolean variable that can only take two values: 0 or 1, and can be implemented in any physical two-state system. An example is two distinct levels of voltage or current in an electrical circuit, or two distinct levels of light intensity.

In quantum systems, the equivalent of the bit is the qubit (contraction of quantum bit). The qubit is represented by a vector in a two-dimensional complex vector space $\mathbb{C}^2$ with a scalar product, called Hilbert space, which has two linearly independent states, called $|0\rangle \equiv \binom{1}{0}$ and $|1\rangle \equiv \binom{0}{1}$, which form an orthonormal basis. The most important difference is that, while the bit admits only two possible values, the qubit can assume infinite values given by the overlapping of the base states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad\qquad \text{with } \alpha, \beta \in \mathbb{C} \ . \tag{1.7}$$

In Dirac notation, widely used in quantum mechanics, the symbol ket $|\psi\rangle$ denotes a vector of a Hilbert space and represents a state of a quantum system. Similarly, the symbol bra $\langle\psi|$ represents the hermitian conjugate of $|\psi\rangle$, that is its conjugate transpose, while the symbol $\langle\psi|\psi\rangle$ denotes their scalar product.

As for the bit, the result of a qubit measurement can assume only one of the two states that form the measurement basis. A measure on the qubit of Eq. (1.7) will return the state $|0\rangle$ with probability $|\alpha|^2$ and the state $|1\rangle$ with probability $|\beta|^2$. Following the measure, the state will collapse on the base state corresponding to the result of the measure and therefore the state will be known with probability equal to 1. From the condition of normalization of the probabilities we have that: $|\alpha|^2 + |\beta|^2 = 1$. This implies that the qubit is represented by a unit vector and Eq. (1.7) can be rewritten as:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \ , \tag{1.8}$$

with θ, ϕ and γ real numbers. In quantum mechanics, a state is represented by a vector radius of a Hilbert space, where by vector radius is meant the equivalence class of vectors having the same direction. So a state is defined except for a global phase and $e^{i\gamma}$ of (1.8) can be ignored. We, therefore, have that

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \ . \tag{1.9}$$

So for the qubit we have only two real parameters that specify the quantum state of the system and it is possible to identify them as the angles of the spherical coordinates: $0 \leq \phi \leq 2\pi$ and $0 \leq \theta \leq \pi$, which describe a point on the surface of a three-dimensional sphere of unit radius, called Bloch sphere, which can be represented as in Figure 1.7b.

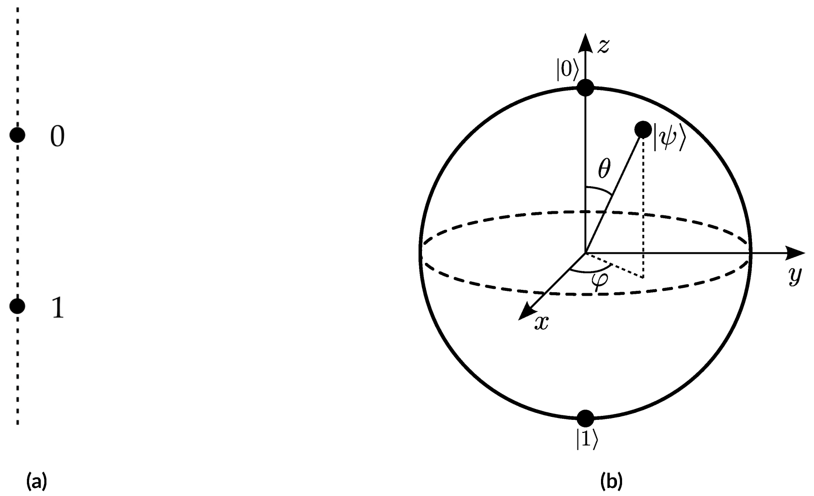


Figure 1.7: (a) Bit representation. [2] (b) Qubit representation on the Bloch sphere. [7]

It is important to point out that the Bloch sphere is a different thing from the Hilbert space in which the qubit is bounded: the qubit actually belongs to a complex two-dimensional space, while the Bloch sphere is in a real three-dimensional space and is useful for representing it geometrically and visualize it. For example, states that are orthogonal in Hilbert space are opposites in the Bloch sphere.

In addition to the states $|0\rangle$ and $|1\rangle$, it is possible to choose other orthonormal states as the basis for a qubit, such as the vectors $|+\rangle$ and $|-\rangle$, defined as

$$|+\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \quad \text{and} \quad |-\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \ . \tag{1.10}$$

The qubit of Eq. (1.7) can be expressed using this new base:

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \ . \tag{1.11}$$

If we measure using this basis, we obtain with a probability of $\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2$ the state $|+\rangle$ and with a probability $\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2$ the state $|-\rangle$.

Some examples of qubits are: the polarization of photons and the spin of electrons.[2][7][20][21][22]

1.3 Idea of quantum cryptography

As already mentioned in Section 1.1.1, the one-time pad cryptographic system provides unconditional security and is in principle indecipherable but it is necessary that the key be completely random and that it be shared secretly between sender and recipient. A system that guarantees such secrecy and randomness can be provided only by quantum mechanics. The meeting point between quantum mechanics and cryptography is called quantum cryptography. This has the advantage of having security based on physical laws such as the no-cloning theorem and Heisenberg's uncertainty principle. In particular, Quantum Key Distribution (QKD) is an application of quantum cryptography that allows a key to be shared securely and secretly between two parties. This key can then be used to apply classical encryption algorithms, such as the one-time pad. The two parties who want to establish secret communication, traditionally called Alice and Bob, have two channels available to communicate with each other: a quantum, through which they transmit information encoded as qubits and a classic public one. A third party, usually called Eve, aims to intercept the communication between Alice and Bob and steal the information exchanged. The quantum channel is used to transmit a random sequence of qubits, which can be used as a key. The classic channel allows Alice and Bob to identify themselves (it is therefore an authenticated channel), while Eve, although she can intercept, cannot participate in the conversation. The quantum channel, on the other hand, allows manipulation by third parties. Unlike the classic case, however, if this were to happen, the information exchanged would be modified so that Alice and Bob could discover it and act accordingly. This is due precisely to the fact that a quantum system is being used in which the following theorems hold, a summary of which is reported:

1. No-cloning: an unknown quantum state cannot be copied.
2. Information gain implies disturbance: it is not possible to distinguish two non-orthogonal quantum states without introducing noise to the signal.

The only way Eve can obtain the encrypted information is to perform a measurement on the system, not being able to obtain a copy of the message. The second statement implies that measurements made on the system perturb it and cause a disturbance, which can be detected by comparing a part of the data on the classic channel. In this way it is also possible to estimate the amount of information leaked, an estimate that would be impossible in the classic case. Essentially, Alice sends Bob a key through a quantum channel and, if it is intercepted, Alice and Bob find out and discard the key, and then generate another. Since the key is completely random, it does not contain any information on the secret message to be transmitted and can be safely discarded. Once Alice and Bob are sure they have shared a secret key, they can use it to encrypt and decrypt messages sent over the classic channel. [1][15][20][22][23]

2
Discrete-Variable QKD

2.1 BB84 protocol

BB84 is the first QKD protocol, published in 1984, and owes its name to Bennett and Brassard. In this protocol, it is assumed that Alice uses a source of single photons whose polarization state, which represents the qubit, will be exploited. It is possible to use a two-component vector to describe the polarization of an electromagnetic wave, using the Jones formalism. In Table 2.1 some polarization states and the corresponding vector according to this formalism are reported, while in Figure 2.1 there is a representation on the Bloch sphere of these states.

Polarization state	Jones vector
Linear horizontal (0°)	$\lvert H\rangle = \binom{1}{0}$
Linear vertical (90°)	$\lvert V\rangle = \binom{0}{1}$
Linear diagonal (45°)	$\lvert D\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$
Linear antidiagonal (−45°)	$\lvert A\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}$
Left circular	$\lvert L\rangle = \frac{1}{\sqrt{2}}\binom{1}{i}$
Right circular	$\lvert R\rangle = \frac{1}{\sqrt{2}}\binom{1}{-i}$

Table 2.1: Jones vectors and corresponding polarization states. [2]

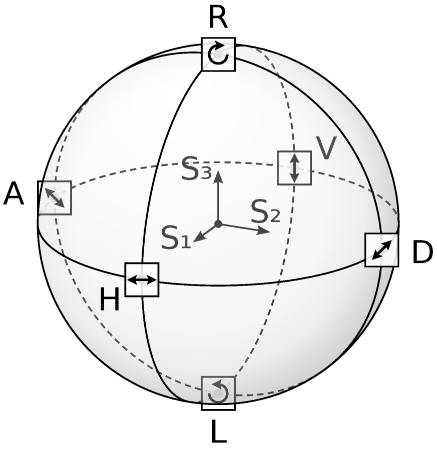


Figure 2.1: Representation of polarization states on the Bloch sphere. This type of representation is also known as the Poincaré sphere. [24]

Alice can send photons to Bob with horizontal or vertical linear polarization, corresponding to 0° and 90° respectively, and diagonal or antidiagonal, corresponding to +45° and −45°. The horizontal polarization is used to represent the qubit $|0\rangle$, while the vertical one indicates the qubit $|1\rangle$. The diagonal and antidiagonal polarizations represent the states $|+\rangle$ and $|-\rangle$ respectively. The states $|H\rangle$ and $|V\rangle$, orthonormal to each other, form the basis $\oplus$, while the states $|D\rangle$ and $|A\rangle$, also orthonormal between they form the base $\otimes$. It is not possible to measure a state using the $\oplus$ and $\otimes$ bases at the same time. Furthermore, states belonging to two different bases are non-orthogonal. This fact implies that if, for example, we measure a state (1.7) with $\beta = 0$ and $\alpha = 1$ using the basis $\otimes$, we obtain, for the (1.11), the state $|+\rangle$ or the state $|-\rangle$ with the same probability. On the other hand, if this state is measured using the basis $\oplus$, the starting state $|0\rangle$ is obtained with probability 1. In other words, a measurement made with the "right" base does not cause a loss of information, while a measurement made with the "wrong" base generates a random result. The QKD protocols exploit this fact since, to intercept the communication, Eve is forced to measure the state using a random basis. This is right in the 50% cases where Eve gets the correct information, while in the cases where she is wrong there is a 50% chance of getting the wrong information. So in total Eve has a 75% chance of getting the correct bit. However, she must send Bob a copy of the message in order not to be discovered (attack called intercept resend), but since for the no-cloning theorem it is not possible to obtain a copy of an unknown state, this copy will contain an error in 25% of cases. It is precisely based on this that Alice and Bob can find out if an interception has occurred.

The BB84 protocol has two phases: the first uses the quantum channel and the second the classical one.

1. Quantum communication:

   - Alice sends Bob a completely random sequence of bits, each encoded by the polarization of a photon as in Table 2.2, using a randomly chosen base.

Bit	State	Polarization	Base
0	$\|0\rangle$	$\|H\rangle$	$\oplus$
1	$\|1\rangle$	$\|V\rangle$	
0	$\|+\rangle$	$\|D\rangle$	$\otimes$
1	$\|-\rangle$	$\|A\rangle$	

Table 2.2: Polarization bit encoding in BB84 protocol.

- To measure the state of each received photon, Bob uses a randomly chosen base.
- Bob thus obtains a sequence of bits. Those that correspond to the qubits measured using the same base as Alice retain the information sent, while the others assume a random value.

2. Public discussion:

    - Sifting: Alice and Bob compare the bases used for each bit through the classic channel and eliminate the bits obtained using different bases from the sequence. The remaining bits make up the sifted key.
    - Security check: Alice randomly chooses a portion of bits from the remaining sequence and compares them with Bob in the classic channel to understand if an interception has occurred. In the ideal case, with no noise in the channel and no interception, there would be no discrepancy in the comparison. In this case, proceed using the remaining bits, otherwise, the presence of errors could be due to noise or an interception. In the latter case, the sifted key is discarded and the procedure is repeated.
    - At the end of the process Alice and Bob have a shared and secret key, built from the sifted key.

For greater clarity, Figure 2.2 shows a schematic of the process.

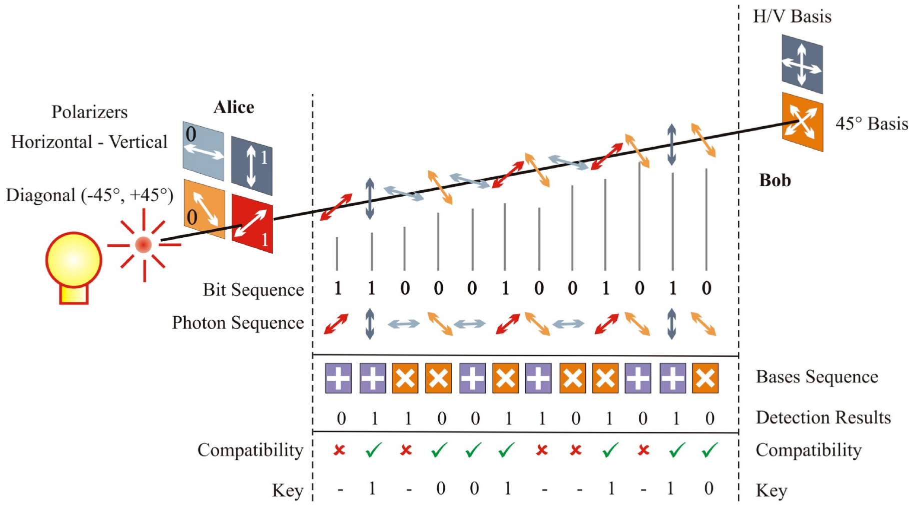


Figure 2.2: Schematic of the BB84 protocol. [25]

In the real case, the protocol foresees that there are errors within a certain threshold value. The sifted key obtained may not be identical for Alice and Bob not only due to eavesdropping, but also due to noise, and it is not possible to distinguish them. These errors are measured using the Quantum Bit Error Rate (QBER), defined as the ratio between the number of wrong bits and the total number of bits of the sifted key. The exchange is considered safe if the QBER is below a threshold value of 11%. In this case, the sequences obtained are quite similar and the key is accepted, but corrections must be made so that the final key is the same.

There are several types of attacks that Eve can perform and that exploit some weaknesses of the protocol. For example, Eve could simply cut or block the quantum channel line or pretend to be Alice or Bob (man-in-the-middle attack). Authentication is important to avoid this occurrence. In the case of the BB84, another possible attack is the PNS (Photon Number Splitting). The BB84 protocol provides for a communication that uses a single photon, but it is very complex to obtain a source of this type. In practice, a strongly attenuated laser source is used, in order to obtain a Poissonian statistic. The coherent pulse of a laser has a relatively small average number of photons μ, such that the probability of having n photons in a single pulse follows a Poisson distribution:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu} \; . \tag{2.1}$$

So there is a non-zero probability that these sources will produce more than one photon, and if so, Eve could intercept the excess photons and use them to obtain information without causing any detectable perturbation. This type of attack can be thwarted by using the decoy state protocol, an implementation of BB84. [1][2][7][10][15][21][23]

2.1.1 Decoy state protocol

The idea behind the decoy state is that Alice prepares a set of additional states, called decoy state, created specifically to detect PNS attacks. For the decoy state the intensity of the laser pulse μ is used as a parameter: using a laser attenuated at the single photon level, Alice modulates its intensity by randomly choosing between several possible values of the average number of photons. The μ parameter carries no information about the key, but it is only used to check for Eve's presence. Typical values are: $\mu_1 = 0.5, \mu_2 = 0.1$ and $\mu_3 = 0$. Alice randomly changes the value of μ between pulses and, at the end of the exchange, she reveals the sequence of values sent. During a PNS attack, Eve alters Bob's photon statistic, revealing her presence. [15][26][27]

2.1.2 Efficient BB84 protocol

In the original BB84 protocol, 50% of the exchanged bits are discarded because the bases randomly chosen by Alice and Bob do not coincide in the sifting process. To make the process more efficient, in the efficient BB84 protocol, the two bases are used with different probabilities. Typically one base, called base $\mathbb{Z} = \{|0\rangle, |1\rangle\}$, is used for generating the key, while the other mutually unbiased base, called base $\mathbb{X} = \{|+\rangle, |-\rangle\}$, is used for detecting the interceptor. The $\mathbb{Z}$ base is used with high probability $p_Z \sim 1$, while the $\mathbb{X}$ base is used with very low probability $p_X = 1 - p_Z \ll 1$. This is true both for the sender, who encodes the bits with high probability in base $\mathbb{Z}$ and with low probability in base $\mathbb{X}$, and for the receiver, who measures with high probability in base $\mathbb{Z}$ and with low probability in base $\mathbb{X}$. In this way, the sifting probability, i.e. the probability that Alice and Bob both use the base $\mathbb{Z}$, is given by p_Z^2 which is very close to 1. Unlike the standard BB84 protocol, where the key is generated by the measures on both bases, in efficient BB84 only the bits in base $\mathbb{Z}$ are used to generate the key. The bits in base $\mathbb{X}$ are used only to understand what the interceptor is aware of, by measuring the quantum bit error rate.

Bit	State	Polarization	Base	Probability	Use
0 1	$\|0\rangle$ $\|1\rangle$	$\|H\rangle$ $\|V\rangle$	$\mathbb{Z}$	$p_Z \sim 1$	key generation
0 1	$\|+\rangle$ $\|-\rangle$	$\|D\rangle$ $\|A\rangle$	$\mathbb{X}$	$p_X \ll 1$	Eve detection

Table 2.3: Bit encoding in efficient BB84 protocol.

2.1.3 Three-state and one-decoy state protocol

The three-state and one-decoy state protocol is a further variation of the BB84 protocol that simplifies practical implementation using fewer polarization states. Specifically, three polarization states are needed instead of four and one decoy state. Below is a summary of the key steps in the protocol:

1. State preparation: for the coding Alice randomly chooses a base between $\mathbb{X}$ and $\mathbb{Z}$ with probability p_X^A and $p_Z^A = 1 - p_X^A$ respectively. When she uses the base $\mathbb{Z}$ she generates the states $|H\rangle$ or $|V\rangle$, while when she uses the base $\mathbb{X}$ she only prepares the state $|D\rangle$. The laser pulse is also modulated by randomly choosing between two average numbers of photons: μ_1 and μ_2, with probability respectively p_1 and $p_{\mu_2} = 1 - p_{\mu_1}$ and so that $\mu_1 > \mu_2 > 0$. μ_1 is denoted as the signal level while μ_2 is the decoy level. Alice sends the qubits to Bob.

2. Bob performs a measurement of the qubits received by randomly choosing a base between $\mathbb{X}$ and $\mathbb{Z}$ with probability p_B^X and $p_B^Z = 1 - p_B^X$.

3. Basis reconciliation: Alice and Bob communicate the bases they have chosen. The events of the base $\mathbb{Z}$ are used to generate the key, while those of the base $\mathbb{X}$ are used to check if there have been interceptions.

[28]

2.2 Coexistence of classical and quantum channels

2.2.1 Attenuation in optical fibers

In optical fibers, attenuation limits the optical power transmitted and therefore also the performance as a data transmission channel. Due to absorption, the optical power of a light beam travelling through an optical fiber decreases exponentially with distance according to the Lambert-Beer law:

$$P(l) = P(0)e^{-\alpha l} \ , \tag{2.2}$$

where $P(l)$ is the optical power transmitted through a fiber of length l and $P(0)$ is the incident optical power. α is the attenuation coefficient, which has the unit of measurement of the inverse of a length

$$\alpha = \frac{1}{l} \ln \frac{P(0)}{P(l)} \ . \tag{2.3}$$

Expressing it in units of decibels it becomes:

$$\alpha_{\mathrm{dB}} = \frac{1}{l} 10 \log_{10} \frac{P(0)}{P(l)} \ . \tag{2.4}$$

Therefore it follows that:

$$\alpha_{\mathrm{dB}} = \frac{10}{\ln 10} \alpha \simeq 4.34 \, \alpha \ . \tag{2.5}$$

The power transmission ratio is defined as:

$$T = \frac{P(l)}{P(0)} = e^{-\alpha l} = 10^{-\alpha_{\mathrm{dB}} l} \, . \tag{2.6}$$

If different absorption systems are considered, the total power transmission ratio will be the product of the single power transmission ratios. Due to the logarithm in Eq. (2.3), the total absorption coefficient will be the sum of the individual absorption coefficients.

Fused silica (amorphous silicon dioxide, SiO_2) is the most widely used material in optical fibers. The absorption coefficient of silica depends on the wavelength, as shown in Figure 2.3. There is a mid-infrared absorption band due to vibrational transitions and an ultraviolet absorption band resulting from electronic and molecular transitions.

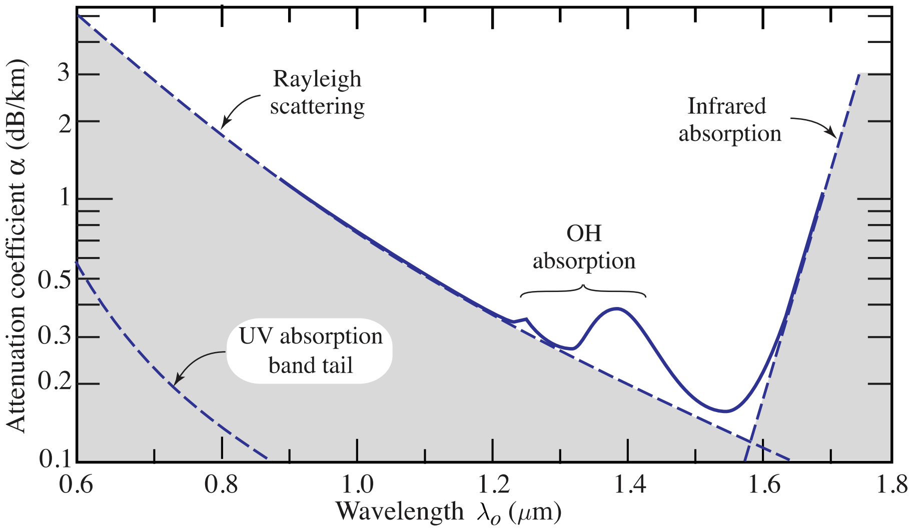


Figure 2.3: Attenuation coefficient α of silica glass versus free-space wavelength λ_0. There is a local minimum at 1310 nm ($\alpha \simeq 0.3$ dB/km) and an absolute minimum at 1550 nm ($\alpha \simeq 0.15$ dB/km). [29]

Another phenomenon that contributes to the attenuation of light in silica is Rayleigh scattering. Rayleigh scattering is generated from the interaction of the light with fluctuations in the index of refraction due to random thermal motion in the silica glass. The random localized variations of the molecular positions in the silica glass create random inhomogeneities in the refractive index that act as tiny scattering centers. The amplitude of the Rayleigh scattering field is proportional to the square of the angular frequency of the light ω and to the square of the reciprocal of the wavelength λ. The scattering intensity is therefore proportional to $1/\lambda^4$, so that the short wavelengths are scattered more than the long wavelengths. Light in the visible spectrum region is therefore scattered more than infrared light. As shown in Fig. 2.3, in the visible region Rayleigh scattering is a more important absorption source than the tail of the ultraviolet absorption band. However, Rayleigh scattering becomes negligible compared to infrared absorption for wavelengths greater than ~ 1600 nm. Total absorption in silica, therefore, is dominated by Rayleigh scattering for short wavelengths and by infrared absorption for long wavelengths. In the near infrared, at the wavelength of 1550 nm, there is an absolute minimum of the absorption coefficient and a second local minimum at 1300 nm. So 1550 nm is the wavelength that minimizes absorption losses in silica optical fibers and this is the reason why current commercial communication systems in optical fiber are designed to operate at that specific wavelength. [29]

2.2.2 Raman scattering

Three important scattering processes in photonics are Rayleigh, Raman, and Brillouin scattering. Rayleigh scattering is a process in which a photon incident on a material interacts in an elastic way and only changes its direction but the energy remains the same, as schematized in Figure 2.4 (a). It is engendered by variations in a medium that are finer than the wavelength of light, such as random density fluctuations in air or random refractive index inhomogeneities in glass. It can also be brought about by the presence of particles whose sizes are much smaller than the wavelength of light, such as electrons, atoms or molecules. As already mentioned, the scattered intensity is proportional to ν^4, and thus to $1/\lambda^4$, where ν and λ are the frequency and wavelength of the illumination. Short wavelengths thus undergo greater scattering than long wavelengths. Raman scattering, on the other hand, is a process in which a photon of frequency ν_1 interacts inelastic with a material and emerges at a lower frequency $\nu_A = \nu - \nu_R$ (Stokes scattering) or at a higher frequency $\nu_A = \nu_1 + \nu_R$ (anti-Stokes scattering), as shown in Figures 2.4 (b) and (c), respectively. In the inelastic scattering process, the change in the photon frequency is due to an exchange of $h\nu_R$ energy with a rotational or vibrational mode of a molecule. In the Stokes scattering the photon gives energy to the molecule, while in the anti-Stokes scattering vice versa occurs. In general, the spectrum of light scattered from a material contains a Rayleigh-scattered component, at the incident frequency, together with red-shifted and blue-shifted sidebands corresponding to inelastically scattered Stokes and anti-Stokes components, respectively. In crystalline materials, the vibrational spectrum is usually discrete and Raman lines are narrow, while glasses have wide vibrational spectra and wide Raman spectra. Brillouin scattering, on the other hand, is conceptually the same as Raman scattering but the exchange of $h\nu_B$ energy occurs with acoustic modes of the medium, rather than vibrational ones.

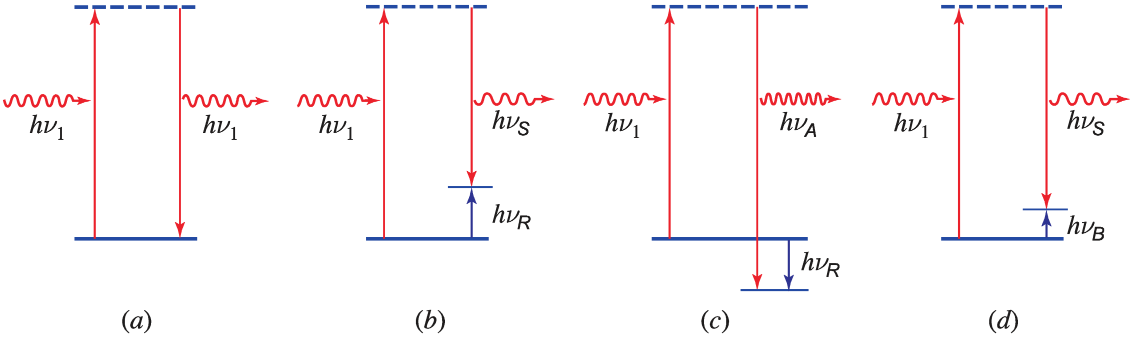


Figure 2.4: Several forms of light scattering: (a) Rayleigh; (b) Raman (Stokes); (c) Raman (anti-Stokes); and (d) Brillouin. Dashed horizontal lines indicate virtual states and therefore nonresonant scattering. [29]

Usually, in QKD protocols made of optical fiber, the classical and quantum channel are implemented in two different optical fibers at a wavelength of 1550 nm. Being able to use a single optical fiber instead of two separate optical fibers would simplify practical implementations because it would allow using the telecommunication infrastructures already present to do QKD without having to use additional optical fibers. One method to achieve this is to use the same optical fiber but with two wavelengths: one for the classical channel and one for the quantum one, using Wavelength Division Multiplexing (WDM) technology. Using two WMDs, one at the beginning of the optical fiber and one at the end, in order to separate the two different wavelengths into two different channels (classical and quantum) at the input and output of the optical fiber.

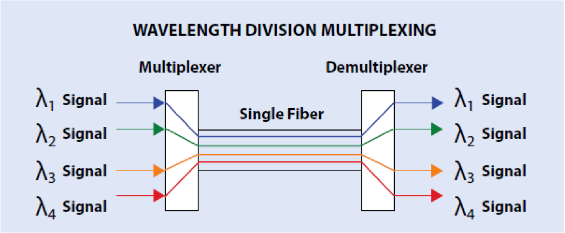


Figure 2.5: Basic Wavelength Division Multiplexing (WDM) technology diagram.

For the classic channel, for example, the wavelength of 1550 nm could be used, which is the current standard in the field of telecommunications and would allow the use of existing instrumentation. Regarding the choice of the wavelength of the quantum channel, one could choose a wavelength close to 1550 nm, but one of the biggest drawbacks is due to Raman scattering which can greatly limit the performance of QKD. One possibility to limit this problem is to use a wavelength corresponding to one of the two largest minima of the Raman scattering cross-section in silica optical fibers, visible in Figure 2.4.

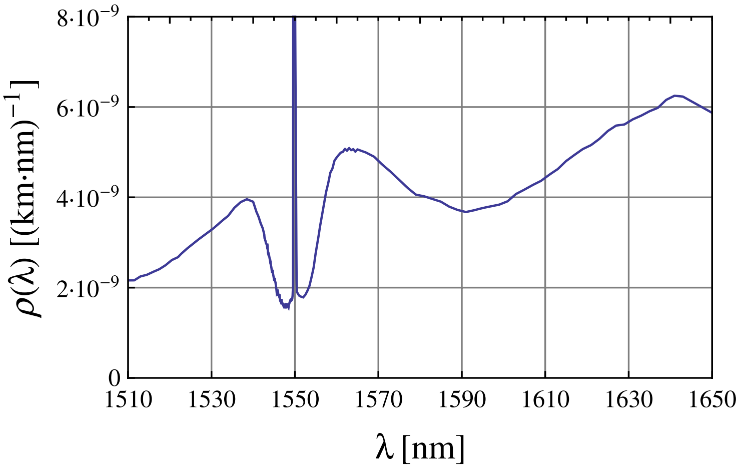


Figure 2.6: Measured effective Raman cross-section $\rho(\lambda)$ (per km fibre length and nm bandwidth) for a pump laser wavelength centred at 1550 nm in a standard single mode fibre at room temperature. [30]

The other big problem in choosing the wavelength for the quantum channel is related to the losses in the optical fibers in silica, which has already been discussed in the previous section. From Figure 2.3 it can be seen that 1310 nm is the wavelength corresponding to the second minimum of the absorption losses in the optical fibers in silica, therefore an alternative is to use the classical channel at 1550 nm and the quantum one at 1310 nm. Using this wavelength would simultaneously reduce the problems due to Raman scattering and have few absorption losses in silica optical fibers. This is why it was decided to build a QKD system at a wavelength of 1310 nm.

2.3 Components of a state source for QKD

A QKD source must allow the realization of states of different intensity and polarization. In practice, these are created by an intensity modulator and a polarization modulator respectively, controlled via Field Programmable Gate Array (FPGA). The optical pulses are generated by a laser, which is also controlled by the FPGA. The intensity modulator is useful for generating decoy states, as it allows you to adjust the intensity of the optical pulse coming from the laser through an electrical signal. The polarization modulator, on the other hand, is used to control, again by means of electrical impulses, the state of polarization that encodes a qubit. Figure 2.7 schematically represents a state source for QKD consisting of these devices.

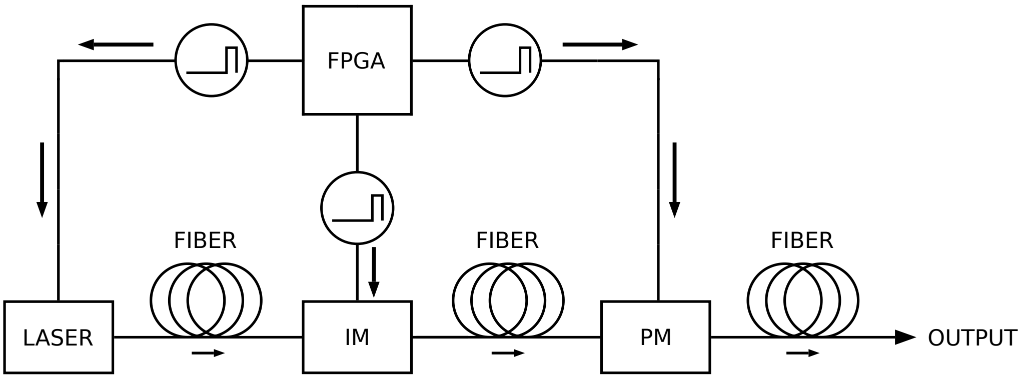


Figure 2.7: Schematic of a QKD state source consisting of a laser, an intensity modulator (IM), a polarization modulator (PM) and a Field Programmable Gate Array (FPGA), which allows devices to be controlled by electrical signal. [22]

2.3.1 iPOGNAC polarization modulator

2.3.1.1 Birefringence

Birefringence is a property of optically anisotropic materials in which the refractive index depends on the polarization direction of the incident wave. In a crystal, there are three directions orthogonal to each other, known as the optical axes of the crystal. In an anisotropic crystal, by choosing these axes as coordinate axes, it is possible to define the ellipsoid of the refractive indices:

$$\frac{x^2}{n_x^2} + \frac{y^2}{n_y^2} + \frac{z^2}{n_z^2} = 1 \; . \tag{2.7}$$

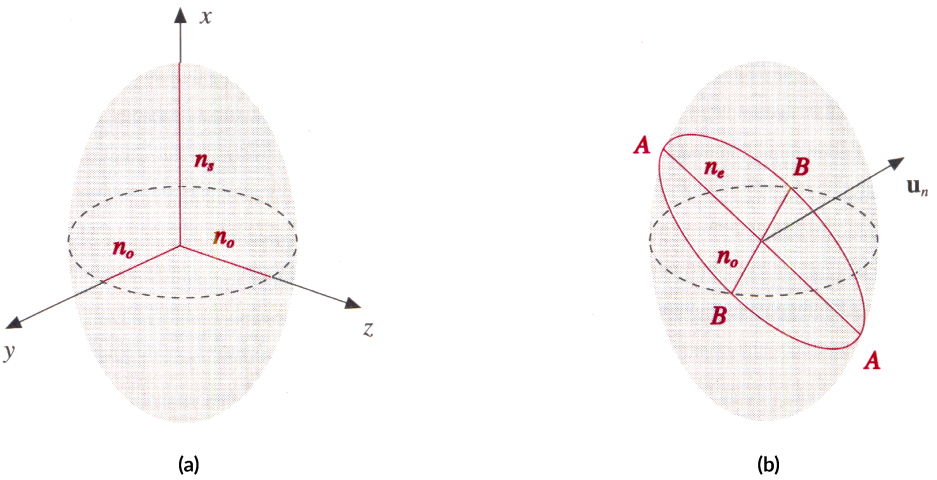
Crystals exhibiting birefringence are divided into monoaxial and biaxial. Biaxial crystals have the refractive indices $n_x \neq n_y \neq n_z$, but they will not be dealt with in this thesis because only monoaxic crystals were used in the experiments. The latter are also called uniassic and have the property of having refractive indices $n_x \neq n_y = n_z$. In the latter case, the axis along the refractive index n_x is an axis of symmetry of the crystal and is called the optical axis or extraordinary axis. The axes along the refractive indices n_y and n_z are, on the other hand, indicated by the name of ordinary axes. Therefore n_x is called extraordinary refractive index and denoted by n_s, while $n_y = n_z$ ordinary refractive index, denoted by n_o. The ellipsoid (2.7) then becomes:

$$\frac{x^2}{n_s^2} + \frac{y^2 + z^2}{n_o^2} = 1 \; , \tag{2.8}$$

and is represented in Figure 2.8a. Consider the front of a plane wave passing through the center of the ellipsoid (2.8): the intersection between this and the ellipsoid is an ellipse with semiaxis n_o and n_e, of which an example is shown in Figure 2.8b. The semiaxis n_e varies with the direction normal to the wavefront $\hat{u}_n$, assuming values between n_o and n_s. There are three situations: if $\hat{u}_n$ is parallel to the optical axis, the intersection ellipse is a circle with radius $n_e = n_o$; if $\hat{u}_n$ is perpendicular to the optical axis, the intersecting ellipse has half-axes n_o and $n_e = n_s$; if instead $\hat{u}_n$ forms a generic angle θ with the optical axis, a point n_e distant from the center will have coordinates such that $x^2 = (n_e \sin\theta)^2$ and $y^2 + z^2 = (n_e \cos\theta)^2$. In this last case, Eq. (2.8) becomes:

$$n_e(\theta) = \frac{1}{\sqrt{\frac{\sin^2\theta}{n_o^2} + \frac{\cos^2\theta}{n_s^2}}}\ , \tag{2.9}$$

therefore the intersecting ellipse has half-axes n_o and Eq. (2.9). Consider a plate with parallel planar faces of a monoaxial crystal: a non-polarized incident plane wave splits into two separate waves that propagate in the crystal at different speeds and directions. The component of the electromagnetic wave that propagates along the ordinary axis obeys Snell's law with refractive index n_o, has polarization orthogonal to the optical axis and is called ordinary wave. The component that propagates along the extraordinary axis does not obey Snell's law: the effect is equivalent to a change in the refractive index with the direction of propagation between n_o and n_s. This wave has a polarization perpendicular to the ordinary wave and is called extraordinary wave. [22][31] [32]



(a)

(b)

Figure 2.8: (a) Representation of the refractive indices ellipsoid of an anisotropic crystal. (b) Representation of the intersection between the front of a plane wave and the refractive indices ellipsoid of an anisotropic crystal. [31]

2.3.1.2 Electro-optical effect

The electro-optical effect is the phenomenon on which the operation of the intensity and phase modulators is based. This consists in the variation of the refractive index of a material caused by the application of an electric field. The dependence of the refractive index on the strength of the electric field is usually of two types: linear or quadratic. In the first case, we speak of the Pockels effect, and in the second of the Kerr effect. The latter will not be explored in this thesis work, because no tool has been used that exploits it. The materials that manifest the

Pockels effect are called electro-optical materials and are devoid of inversion symmetry (for this reason they are called non-centrosymmetric). A widely used material of this type is lithium niobate (LiNbO$_3$). For an anisotropic crystal the ellipsoid of the refractive indices is described by Eq. (2.7) where x, y and z are the principal dielectric axes, i.e. the directions in the crystal along which the electric displacement vectors $\vec{D}$ and electric field $\vec{E}$ are parallel. The application of an external electric field, in the specific case of the Pockels effect, introduces a perturbative contribution:

$$\Delta\left(\frac{1}{n^2}\right)_i = \sum_{k=1}^{3} r_{ik}E_k \ , \tag{2.10}$$

where i can only assume the values $i = 1, 2, 3, 4, 5, 6$ and E_k is the component of the electric field applied in the k direction. r_{ijk} is the electro-optic tensor which, since the symmetry $r_{ijk} = r_{jik}$ holds, could be written using a contracted notation on two indices where i replaces the pair ij with the following convention: $i = 1, 2, 3, 4, 5, 6$ corresponds, respectively, to $ij = 11, 22, 33, 23, 13, 12$ with the relation $1 = x,\ 2 = y,\ 3 = z$. Therefore the ellipsoid takes the form

$$\left(\frac{1}{n_x^2} + \sum_{k=1}^{3} r_{1k}E_k\right)x^2 + \left(\frac{1}{n_y^2} + \sum_{k=1}^{3} r_{2k}E_k\right)y^2 + \left(\frac{1}{n_z^2} + \sum_{k=1}^{3} r_{3k}E_k\right)z^2 + \\ + 2yz\sum_{k=1}^{3} r_{4k}E_k + 2zx\sum_{k=1}^{3} r_{5k}E_k + 2xy\sum_{k=1}^{3} r_{6k}E_k = 1 \ . \tag{2.11}$$

It can be seen that the electric field has changed both the direction of the dielectric axes and the length of the half-axes of the ellipsoid. Since the variations in the refractive index are generally small, the first order Taylor expansion can be used:

$$\frac{1}{n^2} \approx \frac{1}{n_0^2} - \frac{2}{n^3}(n - n_0) \ \Rightarrow\ \Delta\left(\frac{1}{n^2}\right)_i \approx -\frac{2}{n_i^3}\Delta n_i$$

$$\Rightarrow\ \Delta n_i \approx -\frac{n_i^3}{2}\Delta\left(\frac{1}{n^2}\right)_i = -\frac{n_i^3}{2}\sum_{k=1}^{3} r_{ik}E_k \ , \tag{2.12}$$

from which the linear dependence between the variation of the refractive index and the applied electric field is evident. Depending on the crystalline symmetry of the considered material, some coefficients of the electro-optic tensor may be zero. For example, for the LiNbO$_3$, which belongs to the $3m$ symmetry group, the only non-zero coefficients are $r_{12} = -r_{22} = r_{61},\ r_{13} = r_{23},\ r_{33}, r_{42} = r_{51}$. The largest tensor element is r_{33} and, for this reason, it is the one usually used for electro-optical modulators built with this material. [22][29][33][34][35][36]

2.3.1.3 Phase modulator

An electro-optical modulator is a device that generally uses the Pockels effect to modulate the phase, amplitude (and thus intensity) or polarization of a light beam via an electrical control signal. Depending on what the modulator modulates, it is called phase, intensity or polarization modulator. The simplest phase modulator consists of a Pockels cell. This is nothing more than an electro-optical crystal connected to electrodes which, by varying the electrical voltage applied, allows to control of the phase delay of a beam of light that propagates through the crystal, modifying its refractive index. If the polarization of the incident wave is not to be modified, it must be aligned with one of the optical axes of the crystal. Consider a phase modulator consisting of a Pockels cell of $LiNbO_3$ of length L, which exploits the high coefficient r_{33} of the crystal. Have an incident beam of wavelength λ_0 polarized linearly along the optical axis and apply an electric field E_3 to the crystal in the direction of this axis. Using Eq. (2.12) the phase shift produced by the Pockels effect will be:

$$\phi = \frac{2\pi}{\lambda_0}\Delta n_3 L = -\frac{2\pi}{\lambda_0}\frac{r_{33}n_3^3E_3}{2}L \; . \tag{2.13}$$

In particular, if the crystal is shaped like a parallelepiped with thickness d along the optical axis, a potential difference V applied along this axis, produces an electric field $E_3 = \frac{V}{d}$, from which the Eq. (2.13) becomes:

$$\phi = -\frac{\pi}{\lambda_0}\frac{r_{33}n_3^3V}{d}L = -\pi\frac{V}{V_\pi} \quad \text{with} \quad V_\pi = \frac{\lambda_0}{r_{33}n_3^3}\frac{d}{L} \; . \tag{2.14}$$

Therefore there is a linear dependence between the phase shift and the applied potential difference, which allows, by modifying the voltage, to modulate the phase of an incident ray. V_π is the electrical voltage necessary to induce a phase change of π in a Pockels cell and is called half-wave voltage. Usually, Pockels cells have voltages V_π of hundreds or thousands of Volts but using highly non-linear crystals, such as $LiNbO_3$, lower voltages are sufficient. Since V_π depends linearly on d and inversely on L, decreasing d and increasing L you can decrease the value of V_π: thanks to this you can build electro-optical modulators that work on the same principle, but at lower voltages, using waveguides in such a way that $d \ll L$. These particular modulators are part of the integrated optics. An example of a phase modulator of this type is constituted by a waveguide, created in a substrate of electro-optical material, and by electrodes that act on the waveguide (Figure 2.9).

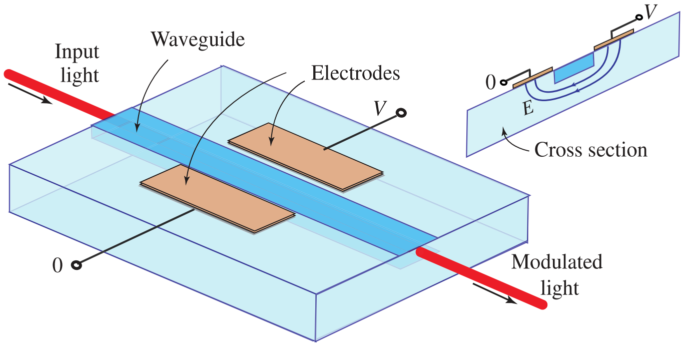


Figure 2.9: An integrated-photonic phase modulator using the electro-optic effect. [29]

In particular, it is possible to create a waveguide in a substrate of $LiNbO_3$ by doping with titanium (titanium-indiffused), in order to slightly increase the refractive index compared to that of pure crystal. It is also possible to use these modulators with optical fibers in input and output. [22][29][35][36][37][38]

2.3.1.4 Polarization modulator

A polarization modulator allows, using an electrical signal, to control the state of polarization at the output. Modulating the polarization of photons is useful for encoding qubits in QKD. A simple method of doing this is to use as many different lasers as there are polarization states required by the QKD protocol. The disadvantages, however, are that:

1. this system is expensive in economic terms and wasteful in energy terms because it requires several lasers and different systems to manage them such as temperature controllers and laser current drivers;

2. very high precision is required in the calibration and control of lasers because the pulse differences belonging to different lasers could be exploited to find out the polarization state without making a direct measurement.

To solve these problems it is possible to use a single laser together with a simple polarization modulator consisting of a birefringent phase modulator in an inline configuration, which exploits a birefringent material and the electro-optical effect. Entering with photons polarized at 45° with respect to the optical axis of the birefringent crystal and applying an electrical voltage to its ends, the ordinary and extraordinary refractive indices of the crystal will vary differently, allowing to control of the relative phase between the polarizations $|H\rangle$ and $|V\rangle$.

Describing in more detail how this type of polarization modulator works: the orientation of the electro-optical material and the direction of the electric field can be configured to control the value of the refractive indices of the ordinary and extraordinary axes. In this way, due to the

Pockels effect, it is possible to have electro-optical coefficients r_x and r_y, such that the refractive indices hold

$$\begin{cases} n_{x'} \approx n_x - \frac{1}{2} n_x^3 r_x E \\ n_{y'} \approx n_y - \frac{1}{2} n_y^3 r_y E \end{cases} , \tag{2.15}$$

where n_x and n_y are the refractive indices in the absence of an electric field. Therefore the two components of the wave propagate inside the material at two different speeds, producing a relative phase difference between the two, which is

$$\Gamma = \frac{2\pi}{\lambda_0}(n_{x'} - n_{y'})L = \Gamma_0 - \frac{\pi}{\lambda_0}(n_x^3 r_x - n_y^3 r_y)EL \ , \tag{2.16}$$

where $\Gamma_0 = \frac{2\pi}{\lambda_0}(n_x - n_y)L$ is the phase delay in the absence of applied voltage. In other words, through a variation of the electric field, it is possible to modulate the phase difference between the components of the wave, thus changing its polarization. Eq. (2.16) can also be written as a function of the V_π parameter:

$$\Gamma = \Gamma_0 - \pi \frac{V}{V_\pi} \quad \text{dove} \quad V_\pi = \frac{d}{L} \frac{\lambda_0}{r_x n_x^3 - r_y n_y^3} \ . \tag{2.17}$$

V_π represents the voltage necessary to obtain a phase delay of π. Figure 2.10 shows an example of an experimental setup to modulate the polarization through a birefringent phase modulator in an inline configuration. The phase modulator has a polarization-maintaining fiber (PMF) at the input with the fiber input of the modulator rotated 45° with respect to the optical axis of the crystal. PMF is a type of fiber that preserves the state of input polarization if parallel to one of the optical axes of the fiber. In this way, entering the fiber with a linear polarization parallel to the optical axis, a wave with diagonal polarization arrives at the modulator, which allows for the exploitation of the ordinary and extraordinary refractive indices. An electrical signal consisting of square waves sent to the modulator allows you to switch between two different polarization states. V_π is the potential difference necessary to have a transition between two states orthogonal to each other. To obtain the necessary states for the realization of the BB84 it is sufficient to apply an appropriate potential difference to the electrodes of the modulator. For example: if the state $|D\rangle$ corresponds to 0 V, the state $|A\rangle$ is obtained with a voltage equal to V_π, while if you pass from a voltage of $-\frac{V_\pi}{2}$ to that of $\frac{V_\pi}{2}$, we obtain a transition between the states $|H\rangle$ and $|V\rangle$.

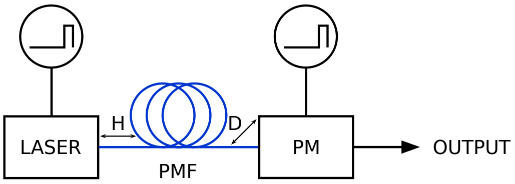


Figure 2.10: Schematic of a simple experimental setup with a polarization modulator consisting of a birefringent phase modulator in an inline configuration. The phase modulator has a polarization-maintaining fiber at the input with the fiber input of the modulator rotated by 45° with respect to the optical axis of the crystal. The abbreviations indicate: PMF = polarization-maintaining fiber, PM = phase modulator, H = horizontal polarization and D = diagonal polarization.

In this case, the drawbacks are that:

1. polarization modulation is very sensitive to temperature and bias voltage drift, which generate an involuntary variation of the modulator output and requires active stabilization;
2. polarization mode dispersion (PMD) induced by birefringence reduces the degree of polarization, the two orthogonal components of the polarization travel at different speeds and the phase shift can be large enough to separate them by a value greater than the coherence length of the source;
3. it is necessary to apply high electrical voltages to the modulator to be able to obtain all the polarization states required by the QKD protocol.

To solve problem 1 it is possible to use the birefringent phase modulator together with a Faraday mirror (FM) in a two-pass scheme, as in the diagram in Figure 2.11, but in this way points 2 and 3 are not solved.

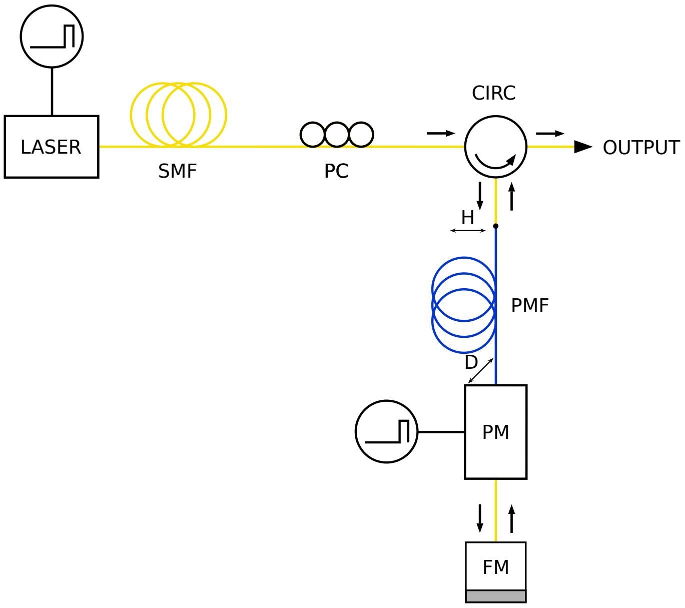


Figure 2.11: Schematic of an experimental setup with a polarization modulator consisting of a birefringent phase modulator together with a Faraday mirror in a two-pass scheme. The abbreviations indicate: SMF = single-mode fiber, PC = polarization controller, CIRC = circulator, PMF = polarization-maintaining fiber, PM = polarization modulator, FM = Faraday mirror, H = horizontal polarization, D = diagonal polarization. SMFs are represented in yellow, while PMFs are represented in blue.

In general, an optical fiber is a waveguide consisting of two concentric layers: a cylindrical core and the layer that surrounds it, the cladding. The core has a refractive index higher than the cladding: the interface between these two parts, therefore, behaves like a perfectly reflective surface and therefore the light that travels through the core is confined within it. In the case of a single-mode fiber (SMF), the core is very thin compared to the wavelength of the light and this means that there is no more reflection, so the light cannot travel in different ways and can only propagate along the axis of the fiber. A SMF uncontrollably changes the polarization direction of a wave passing through it. The reason is that the phenomenon of birefringence can occur due to imperfections, mechanical stress, curvature or other factors that cause a break in the circular symmetry of the fiber. For this reason, in the apparatus in Figure 2.11 there is a polarization controller (PC), which allows you to change the polarization state of the light inside the optical fiber to any desired one. A circulator, on the other hand, is an optical device, usually with three doors, which allows light to be transmitted from door 1 to door 2 and from door 2 to door 3, preventing other possible configurations. This serves to separate signals travelling in opposite directions in an optical fiber, for example to achieve bidirectional transmission over a single fiber. In the apparatus in Figure 2.11, the circulator allows photons to go from the laser to the circulator, then to the Faraday mirror and back to the circulator, and finally to the output. The Faraday mirror, on the other hand, is an optical device that reflects the incident light and changes its polarization state in its orthogonal. In this way, considering the round trip from the circulator to the Faraday mirror, two orthogonal components of the polarization will travel the same path, therefore the phase shifts due to drift will be compensated and the alterations of the polarization state will be minimized. [22][29][39][40] [41]

2.3.1.4.1 POGNAC To solve all three of the problems listed above, the POGNAC polarization modulator shown in Figure 2.12 has been devised. This consists of a circulator connected to a polarization controller and a Sagnac interferometer via single-mode fiber. The Sagnac loop is composed of a fiber polarization beam splitter (PBS), polarization maintenance fiber and a phase modulator. Thanks to the polarization controller the photons enter the PBS with a polarization which is a balanced superposition of the horizontal $|H\rangle$ and vertical $|V\rangle$ polarization modes, for example a diagonal polarization $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, after having crossed the Sagnac loop they leave the PBS with a state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\phi}|V\rangle\right) \tag{2.18}$$

with ϕ determined by the phase modulator, and finally they come out from the circulator outlet door.

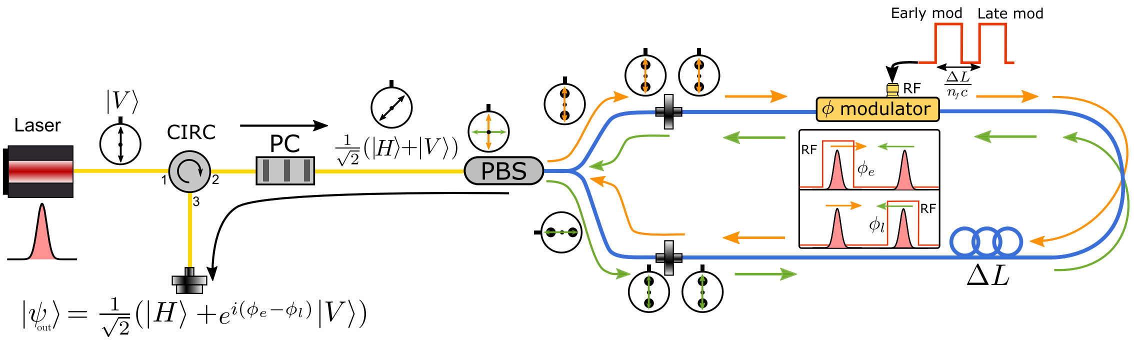

Early mod
Late mod
RF
$\frac{\Delta L}{n_f c}$
$|V\rangle$
Laser
CIRC
1
2
3
PC
$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
PBS
ϕ modulator
RF
ϕ_e
ϕ_l
RF
ΔL
$|\psi_{out}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l)}|V\rangle)$

Figure 2.12: Schematic representation of the working principle of the POGNAC. SMFs are drawn in yellow while PMFs are in blue. [41]

The disadvantages of POGNAC however are that:

1. SMF before the PBS requires a polarization calibration via the PC to obtain a balanced overlap of the horizontal and vertical polarization modes at the input of the Sagnac interferometer;

2. SMF at the output from the Sagnac interferometer (which goes from the PBS to the circulator output) introduces a unitary transformation of the polarization state not known a priori, which complicates things in the case of QKD implementations in free-space because implies that a polarization calibration will also be required at the receiver;

3. the drift due to temperature variations and the mechanical stresses of the SMFs require a recalibration of the polarization (this is true both at the transmitter before the Sagnac and at the receiver).

[40][41]

2.3.1.4.2 iPOGNAC To solve all three of these problems, the iPOGNAC shown in Figure 2.13 was designed, which does not require polarization calibration either at the transmitter or at the receiver (in the case of QKD in free-space, in the case of fiber-based QKD it still requires a receiver calibration).

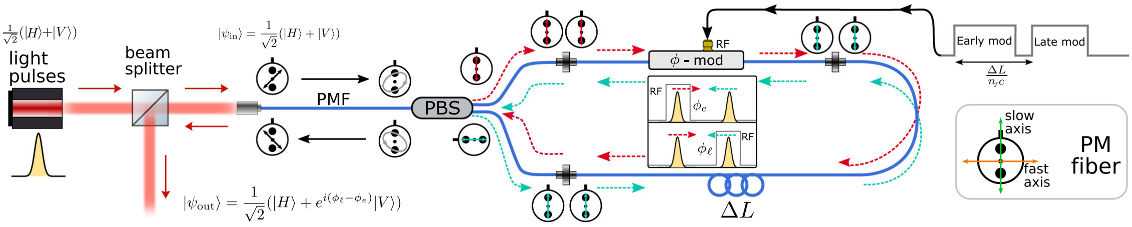

$\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$
light pulses
beam splitter
$|\psi_{\rm in}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$
PMF
PBS
$|\psi_{\rm out}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_\ell-\phi_e)}|V\rangle)$
RF
ϕ - mod
RF
ϕ_e
ϕ_ℓ
RF
ΔL
Early mod
Late mod
$\frac{\Delta L}{n_f c}$
slow axis
fast axis
PM fiber

Figure 2.13: Schematic representation of the working principle of the iPOGNAC. The free-space BS is used to separate incoming from outcoming light. A Sagnac interferometer including a fiber PBS, a phase modulator, and PMFs (indicated in blue) is used to modulate the polarization state. We always consider a left-handed reference frame whose z axis is directed toward the photon's propagation direction. [40]

Laser pulses with a polarization that is a balanced superposition of $|H\rangle$ and $|V\rangle$ propagate in free-space and impact a free-space BS. Photons reflected by the BS are discarded and those transmitted are injected with a collimator into a PMF. Thanks to the birefringence of the PMF the polarization modes $|H\rangle$ and $|V\rangle$ see different refractive indices and the polarization state is changed into an elliptical polarization:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{i\delta}|V\rangle\right) \tag{2.19}$$

where phase δ depends on the length of the optical fiber, the difference between the fast and slow refractive indices of the PMF and the differences in temperature and mechanical deformations of the PMF. For laser pulses with short coherence, the δ phase can be large enough to depolarize the light. After the PMF there is a fiber PBS and a Sagnac loop composed entirely of PMFs equal to that of the POGNAC. The fiber PBS separates orthogonal linear polarizations, then the two outputs of the PBS are connected to PMFs so that each of the beams exiting the PBS is aligned with the slow axis of the PMF and the polarized light travels only along the slow axis of the fibers. The vertically polarized component travels clockwise (CW), first encounters the phase modulator which introduces an "early" phase ϕ_e on the pulse, then encounters a PMF delay line, returns to the PBS and exits the interferometer Sagnac with horizontal polarization.

The horizontally polarized component instead travels counterclockwise (CCW), first encounters the PMF delay line and then the phase modulator so that it arrives on the modulator after the CW pulse, the phase modulator introduces a phase "late" ϕ_e on impulse, then returns to the PBS and exits the Sagnac interferometer with vertical polarization. If we do not consider the effect of the phase modulator, the Sagnac loop sends $|H\rangle \rightarrow -|V\rangle$ and $|V\rangle \rightarrow |H\rangle$ (while a FM sends $|H\rangle \rightarrow |V\rangle$ and $|V\rangle \rightarrow |H\rangle$). So with respect to the polarization at the PBS input of Eq. (2.19), this will change the sign of the δ phase and introduce an extra shift of π:

$$|\Psi_2^{\phi_e,\phi_l}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - e^{-i\delta}|V\rangle\right) \tag{2.20}$$

Considering also the effect of the phase modulator, the polarization state at the output of the PBS will be:

$$|\Psi_2^{\phi_e,\phi_l}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - e^{-i\left(\phi_l-\phi_e-\delta\right)}|V\rangle\right) \tag{2.21}$$

Since both polarizations travel along the slow axis of the PMFs within the Sagnac interferometer, PMD does not occur. Furthermore, the phase modulator modulates a single polarization mode but the voltage signal that drives the modulator must have a frequency twice as high as the pulse generation frequency. The optical pulse, after exiting the Sagnac loop, retraces backwards the PMF that it had travelled on the outward journey and in this way compensates for the phase δ between the polarization modes $|H\rangle$ and $|V\rangle$ that it had accumulated at the gone. The $|H\rangle$ polarization first travels the fast axis of the PMF, after the Sagnac loop it becomes $-|V\rangle$ and retraces the PMF backwards along the slow axis, while the $|V\rangle$ polarization first travels along the slow axis of the PMF, after the Sagnac loop it becomes $|H\rangle$ and retraces the PMF backwards along the fast axis. After the PMF, the collimator transports the pulse to free-space which hits the free-space BS again. This time the component transmitted by the BS is discarded while the reflected one is the output of the iPOGNAC and will have a polarization:

$$|\Psi_{\text{OUT}}^{\phi_e,\phi_l}\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + e^{-i\left(\phi_l-\phi_e\right)}|V\rangle\right) \tag{2.22}$$

where an additional π shift due to reflection from the BS was taken into account.

Inside the Sagnac loop, the CW pulse arrives on the phase modulator before the CCW one by a factor $\frac{\Delta L}{n_f c}$ (where ΔL is the length of the fiber delay and n_f is the refractive index of the slow axis of the PMF). By changing the phases ϕ_e and ϕ_l (accurately timing the voltage applied on the phase modulator), one can generate any state that is a balanced overlap of the horizontal $|H\rangle$ and vertical $|V\rangle$ polarization modes, i.e. lying on the equator of the Bloch sphere (Figure 1.7b). For example, if no voltage is applied to the CW and CCW pulses, the polarization state remains:

$$|\Psi_{\text{OUT}}^{0,0}\rangle = |D\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \tag{2.23}$$

If a voltage $V_{\pi/2}$ is applied to the CW pulse and no voltage is applied to the CCW pulse, the output state becomes:

$$|\Psi_{\text{OUT}}^{\pi/2,0}\rangle = |L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i\,|V\rangle\right) \tag{2.24}$$

If no voltage is applied to the CW pulse and the voltage $V_{\pi/2}$ is applied to the CCW pulse, the output state becomes

$$|\Psi_{\text{OUT}}^{0,\pi/2}\rangle = |R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i\,|V\rangle\right) \tag{2.25}$$

So with a voltage: $\pm V_{\pi/2}$ (which corresponds to the voltage required to introduce a phase shift of $\pi/2$ in the phase modulator) it is possible to generate the states $|D\rangle$, $|L\rangle$ and $|R\rangle$, allowing the implementation of the three-state version of the BB84 protocol.

The tests performed on the iPOGNAC have provided excellent performances in terms of quantum bit error rate (QBER). An intrinsic $QBER < 0.2\%$ and long-term stability measured over 24h was obtained. [40][41]

2.3.2 Sagnac-based intensity modulator

It is possible to build an intensity modulator conceptually similar to the iPOGNAC polarization modulator, which consists of a Sagnac optical fiber interferometer composed of a BS 70:30 fiber, a lithium niobate birefringent phase modulator and a long fiber delay line 1 m, as schematized in Figure 2.14. All optical fibers are PMF with the light propagating along the fibers' slow axis. This type of modulator allows long time stability.

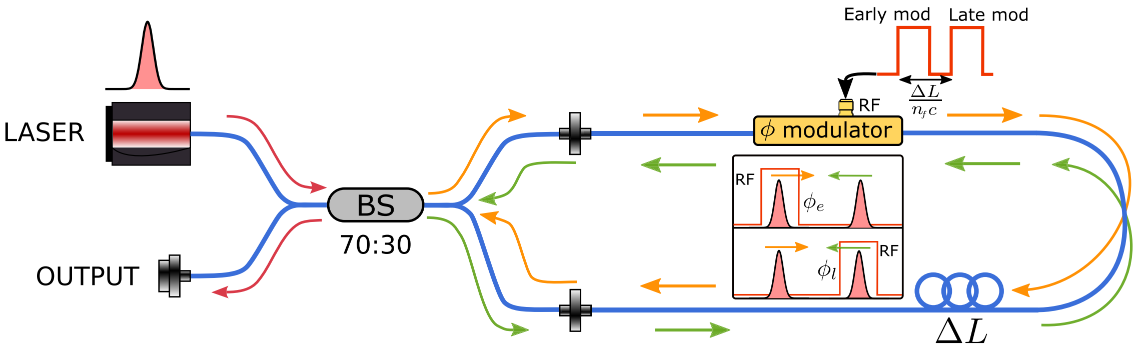


Figure 2.14: Schematic representation of the Sagnac-based intensity modulator. [41]

BS 70:30 separates the amplitude of the incoming laser signal into two components: one component that travels clockwise in the Sagnac loop A_{CW} and another that travels anticlockwise A_{CCW}. The component travels clockwise, first encounters the phase modulator which introduces an "early" phase ϕ_e on the pulse, then encounters a PMF delay line, returns to the BS and exits the interferometer Sagnac. The component travels counterclockwise instead, first encounters the PMF delay line and then the phase modulator so that it arrives on the modulator after the CW pulse, the phase modulator introduces a phase "late" ϕ_l on pulse, then returns to the BBS and exits the Sagnac interferometer. It is possible to calculate the modulator output intensity as a function of the input intensity and the phase introduced by the phase modulator:

$$\begin{aligned} I_{\text{OUT}} &= A_{\text{CW}}^2 + A_{\text{CCW}}^2 + 2A_{\text{CW}}A_{\text{CCW}}\cos(\Delta\phi) = \\ &= I_{\text{CW}} + I_{\text{CCW}} + 2\sqrt{I_{\text{CW}}I_{\text{CCW}}}\cos\left(\phi_e - \phi_l\right) = \\ &= \left(\frac{7}{10}\right)^2 I_{\text{IN}} + \left(\frac{3}{10}\right)^2 I_{\text{IN}} + 2\frac{7}{10}\frac{3}{10}I_{\text{IN}}\cos\left(\phi_e - \phi_l\right) = \\ &= \frac{I_{\text{IN}}}{50}\left[29 + 21\cos\left(\phi_e - \phi_l\right)\right] \end{aligned} \tag{2.26}$$

$$\begin{aligned} \text{if } \phi_e - \phi_l = 0 \quad &\Rightarrow \quad I_{\text{OUT}}^{max} = I_{\text{IN}} \\ \text{if } \phi_e - \phi_l = \pi \quad &\Rightarrow \quad I_{\text{OUT}}^{min} = 0.16\, I_{\text{IN}} \\ \text{if } \phi_e - \phi_l = \pm\frac{\pi}{2} \quad &\Rightarrow \quad I_{\text{OUT}} = 0.58\, I_{\text{IN}} \end{aligned} \tag{2.27}$$

In this way, if for example one chooses a intensity state with $\phi_e - \phi_l = \frac{\pi}{2}$ and another state with $\phi_e - \phi_l = \pi$, it is possible to obtain a ratio between the two intensities of $\simeq 3.6$.

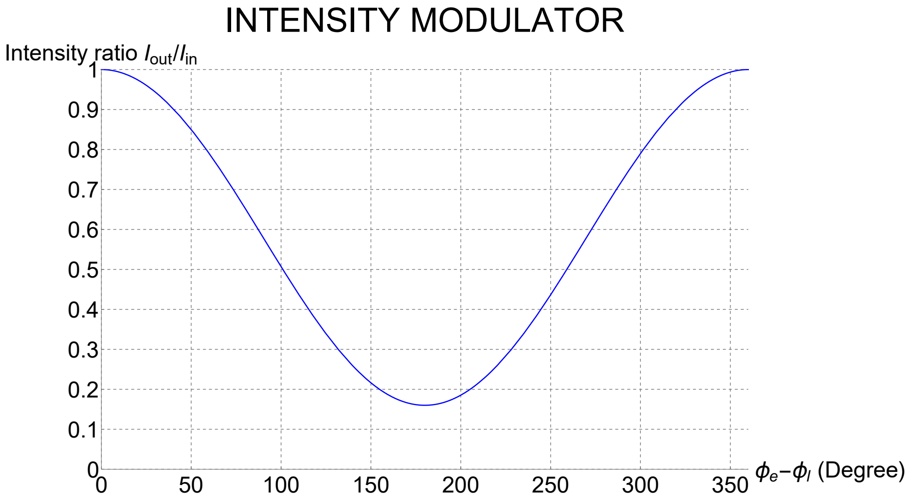


Figure 2.15: Theoretical trend of the ratio between output and input intensity as a function of the phase modulated for the Sagnac-based intensity modulator. The plotted function is Eq. (2.26)

To use the modulator to implement the three-state and one-decoy state protocol (described in Section 2.1.3), it is necessary to be able to choose between two different average numbers of photons (signal μ and decoy ν) for the transmitted pulse in such a way that $\mu > \nu$. [42] [43]

2.4 Experimental setup

2.4.1 Quantum trasmitter

Figure 2.16 shows a schematic of the experimental setup used on the quantum transmitter. The source is a gain-switched distributed feedback (DFB) laser that emits a 50 MHz stream of phase-randomized pulses with ∼200 ps FWHM duration at 1310 nm. The system consists of two main parts: the intensity modulator followed by the iPOGNAC polarization modulator. The intensity modulator (described in Section 2.3.2) is based on a fiber optic Sagnac loop and includes a 70:30 BS, a $LiNbO_3$ phase modulator and a 1 m long delay line. This system implements the decoy-state protocol by setting two possible mean photon numbers (μ and ν) for the transmitted pulse. μ and ν are chosen in such a way that their ratio is $\frac{\mu}{\nu} \simeq 3.3$. Laser and intensity modulator are composed only of PMF with the light propagating along the slow axis of the fibers. Like the intensity modulator, the iPOGNAC polarization modulator (described in Section 2.3.1.4.2) is made up of an unbalanced Sagnac interferometer with the BS replaced by a PBS. Before entering the PBS, the light passes through a free-space BS used like a circulator. The polarization entering the PBS is a balanced superposition of vertical and horizontal states, in this way the light is equally split into the clockwise and counterclockwise components of the loop. Thanks to the asymmetry of the interferometer, by properly setting the voltage of the modulator and timing the two pulses, one can generate $|L\rangle$ or $|R\rangle$ polarization states. If no phase is applied to any of the two pulses, the resulting polarization state is $|D\rangle$. These three states allow us to implement the 3-state efficient BB84 protocol, where the keying basis is $\mathcal{K} = \{|L\rangle, |R\rangle\}$ and the check basis is $\mathcal{C} = \{|D\rangle, |A\rangle\}$. The polarization modulated light emerges from the free-space BS, is attenuated to the single-photon level by a variable optical attenuator (VOA) and is transmitted over the quantum channel to the receiver. The synchronized electronic signals used to drive the laser and the two electro-optical phase modulators were generated by a field programmable gate array (FPGA) mounted on a dedicated board (ZedBoard by Avnet). [43]

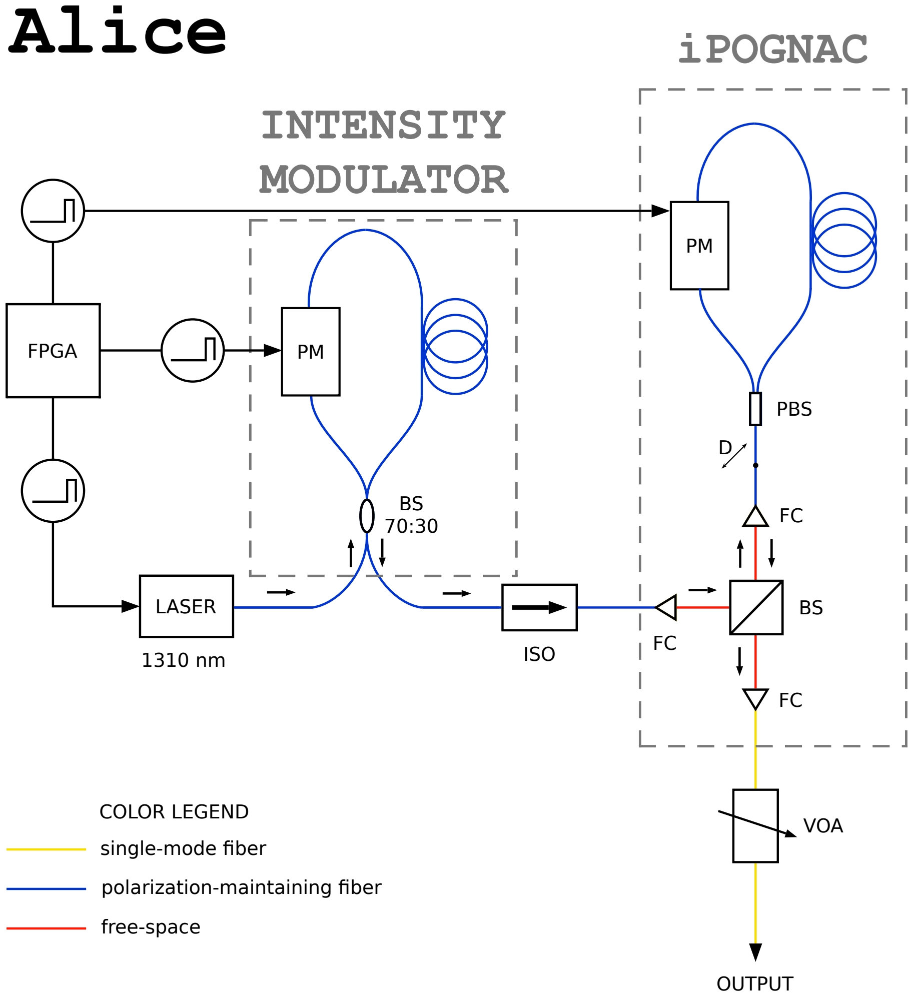


Figure 2.16: Schematic representation of the QKD transmitter setup employed in the experiment.

2.4.2 Quantum receiver

Figure 2.17 shows a schematic of the experimental setup used on the quantum receiver. Bob measures the incoming photons by randomly choosing between the key basis ($\mathcal{K}$) and the check basis ($\mathcal{C}$) with equal probability using a BS 50:50. Projective measurements are performed using an Automatic Polarization Controller (APC) together with a PBS for each base. An APC is nothing more than a motorized polarization controller that can be electrically controlled via a PC. Before starting to run the QKD protocol, the APCs are aligned by sending a public states sequence and monitoring the resulting QBER. Furthermore, during the key exchange, Alice interleaves 4 pre-shared and publicly known bits every 36 private key bits and Bob uses them to keep his measurement bases aligned with the APC. A time multiplexing scheme was used to perform the measurements on two bases using only a single photon detector. Specifically, an InGaAs/InP single-photon avalanche diode (SPAD) was used (the PDM-IR model from Micro Photon Devices), with a 15% quantum efficiency. The time multiplexing system works by differently delaying the pulses exiting the PBSs and directing them to the detector via two other PBSs and a final BS. The time tags corresponding to the photons arrivals are recorded by a time-to-digital converter (quTAU from qutools GmbH) and transmitted to Bob's PC for data processing. The time synchronization is provided by the Qubit4Sync algorithm which reconstructs, according to the detection events, the clock period without any external reference signal. To ease the system deployment, both the transmitter and receiver were built to fit a standard 4U rack case (only the single-photon detector is external to the 4U rack). [43]

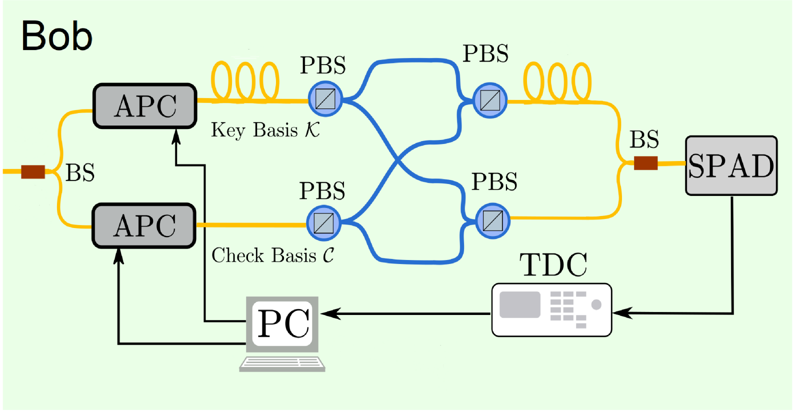


Figure 2.17: Schematic representation of the setup for the quantum receiver employed in the experiment. [43]

2.5 Results

2.5.1 Characterization of the source components

2.5.1.1 Laser

The distributed feedback laser (DFB) is an InGaAsP/InP multi-quantum well laser diode (Gooch & Housego model AA0701). A Thermo Electric Cooling Temperature Controller (Meerstetter Engineering GmbH model TEC-1091) was used to manage the laser temperature. This is equipped with Pt100, Pt1000 and NTC temperature sensors, and uses a PID controller to drive a Peltier element. After setting the parameters of the PID controller, to characterize the laser pulse, the output current and the trigger input were modified to obtain a pulse that was as narrow, symmetrical and stable as possible. To observe the laser pulse it was used a superconductive nanowire single-photon detector (SNSPD, manufactured by ID Quantique) cooled to 0.8 K thanks to a helium cycle was used. Figure 2.18 shows the histogram of the laser pulse counts for a 50 MHz repetition rate in the best laser control setting that has been achieved.

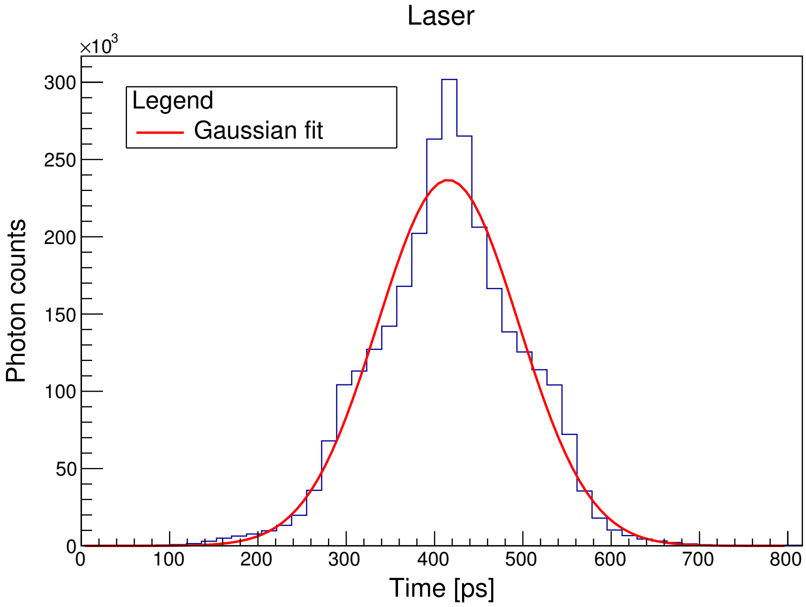


Figure 2.18: Histogram of the laser pulse counts in an acquisition time of 10 s. From the gaussian fit of the histogram, it was obtained: σ = (79.94±0.04) ps.

From a gaussian fit of the histogram of the laser pulse counts FWHM∼200 ps was found.

Gaussian fit result	
σ [ps]	FWHM [ps]
79.94 ± 0.04	188.23 ± 0.08

Table 2.4: Standard deviation σ and full width at half maximum (FWHM) obtained from the gaussian fit of the histogram of the laser pulse counts of Figure 2.18. Where FWHM$= 2\sqrt{2\ln 2}\,\sigma$.

2.5.1.2 Intensity modulator

To characterize the Sagnac-based intensity modulator described in Section 2.3.2, the optical power output was measured as a function of the electrical voltage applied to the phase modulator. It was necessary to use a voltage amplifier for the RF signal generated by the FPGA for the phase modulator. Optical power measurements were performed with an InGaAs photodiode.

From Eq. (2.14), the optical power output from the Sagnac based intensity modulator is:

$$P_{\text{OUT}}(V) = \frac{P_{IN}}{50}\left[29 + 21\cos\left(\phi_0 - \pi\frac{V}{V_\pi}\right)\right] \tag{2.28}$$

Figure 2.20 shows a plot of the normalized optical power output from the Sagnac-based intensity modulator as a function of the voltage applied to the phase modulator. Eq. (2.14) was used to fit only a portion of the data due to the effects introduced by the voltage amplifier visible at low voltages.

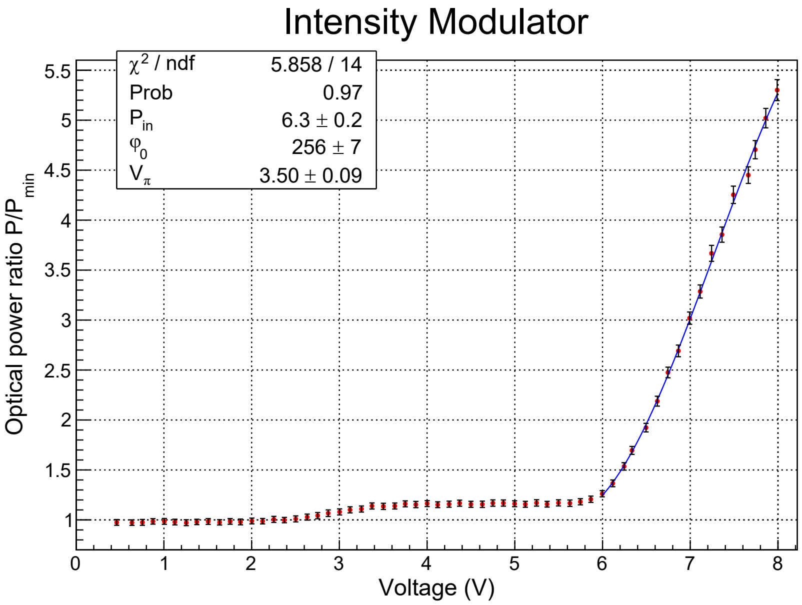


Figure 2.19: Plot of the normalized optical power output from the Sagnac-based intensity modulator as a function of the applied voltage. Function 2.28 was only fit on a restricted region of the data due to the effects introduced by the voltage amplifier. A zoom only on the part with the fit is shown in Figure 2.20.

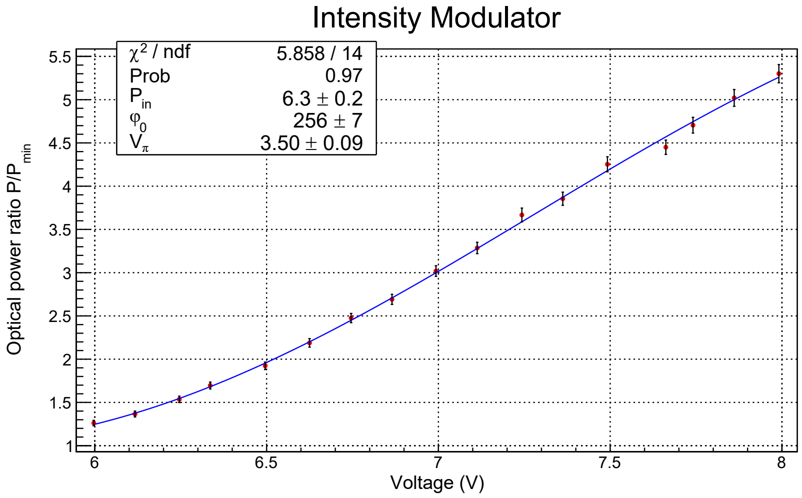


Figure 2.20: Zoom on part of the plot with the fit of Figure 2.19.

To use the modulator to implement the three-state and one-decoy state protocol, it is necessary to be able to choose between two different average numbers of photons for the transmitted pulse (signal μ and decoy ν, with μ>ν). We have chosen in such a way that its ratio is $\mu/\nu \simeq 3.33$.

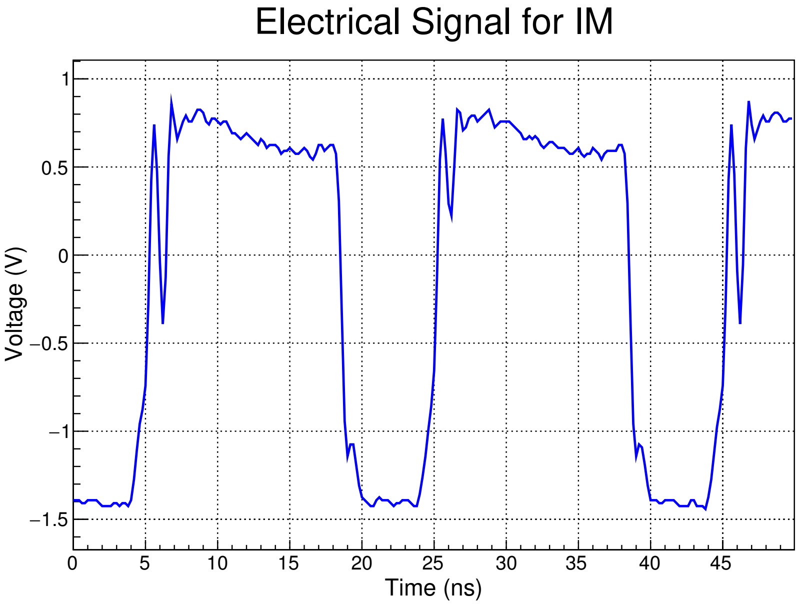


Figure 2.21: Example of the electrical signal used for the Sagnac-based intensity modulator. The electrical signal is generated by the FPGA, passes through a delay line and a voltage amplifier.

2.5.1.3 Polarization modulator

To characterize the iPOGNAC polarization modulator described in Section 2.3.1.4.2, the polarization state was measured as a function of the electrical voltage applied to the phase modulator. It was necessary to use a voltage amplifier for the RF signal generated by the FPGA for the phase modulator, while a polarimeter was used to carry out the measurements (Thorlabs model PAX1000IR2). Figure 2.22 shows a plot of the angle between the states $|R\rangle$, $|D\rangle$ and $|L\rangle$, $|D\rangle$ in output from the iPOGNAC polarization modulator as a function of the voltage applied to the phase modulator.

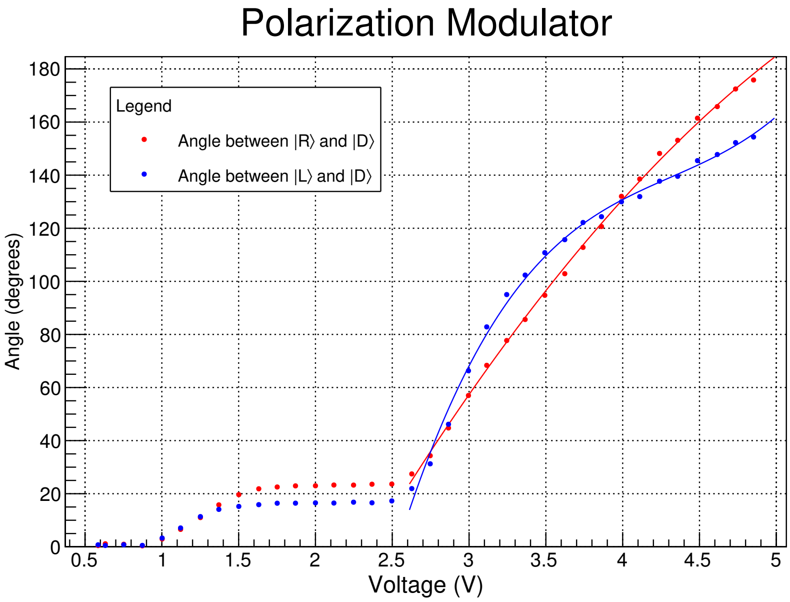


Figure 2.22: Plot of the angle between the states $|R\rangle$, $|D\rangle$ and $|L\rangle$, $|D\rangle$ in output from the iPOGNAC polarization modulator as a function of the applied voltage.

The trends of the two data sets visible in Figure 2.22 should in theory be the same. The reason they are not may be due to imperfections in the electrical signal used for the phase modulator or in the iPOGNAC. The polarization state entering the Sagnac loop may not be a perfect balanced superposition of the horizontal and vertical polarization states. Furthermore, the optical fibers present in the transmitter setup have all been spliced together to avoid losses and reflection problems due to the fiber connectors and there may be imperfections due to the splicing process.

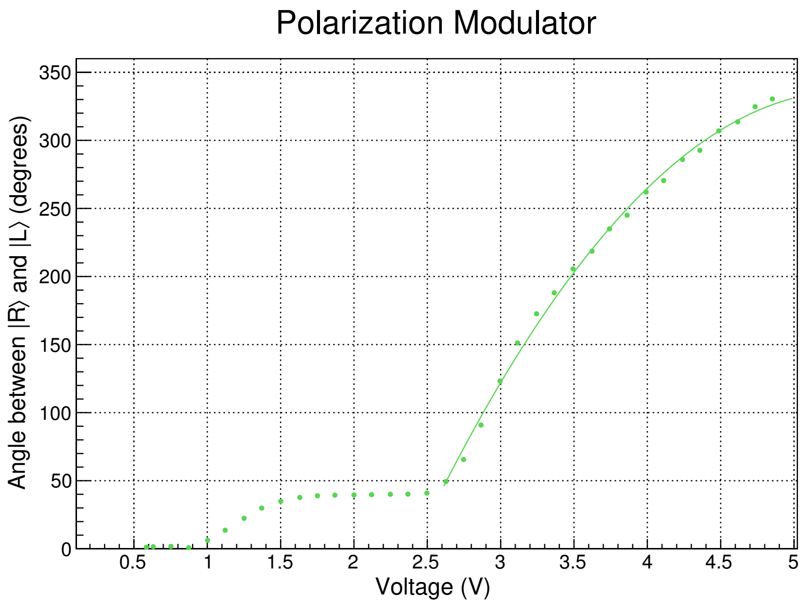


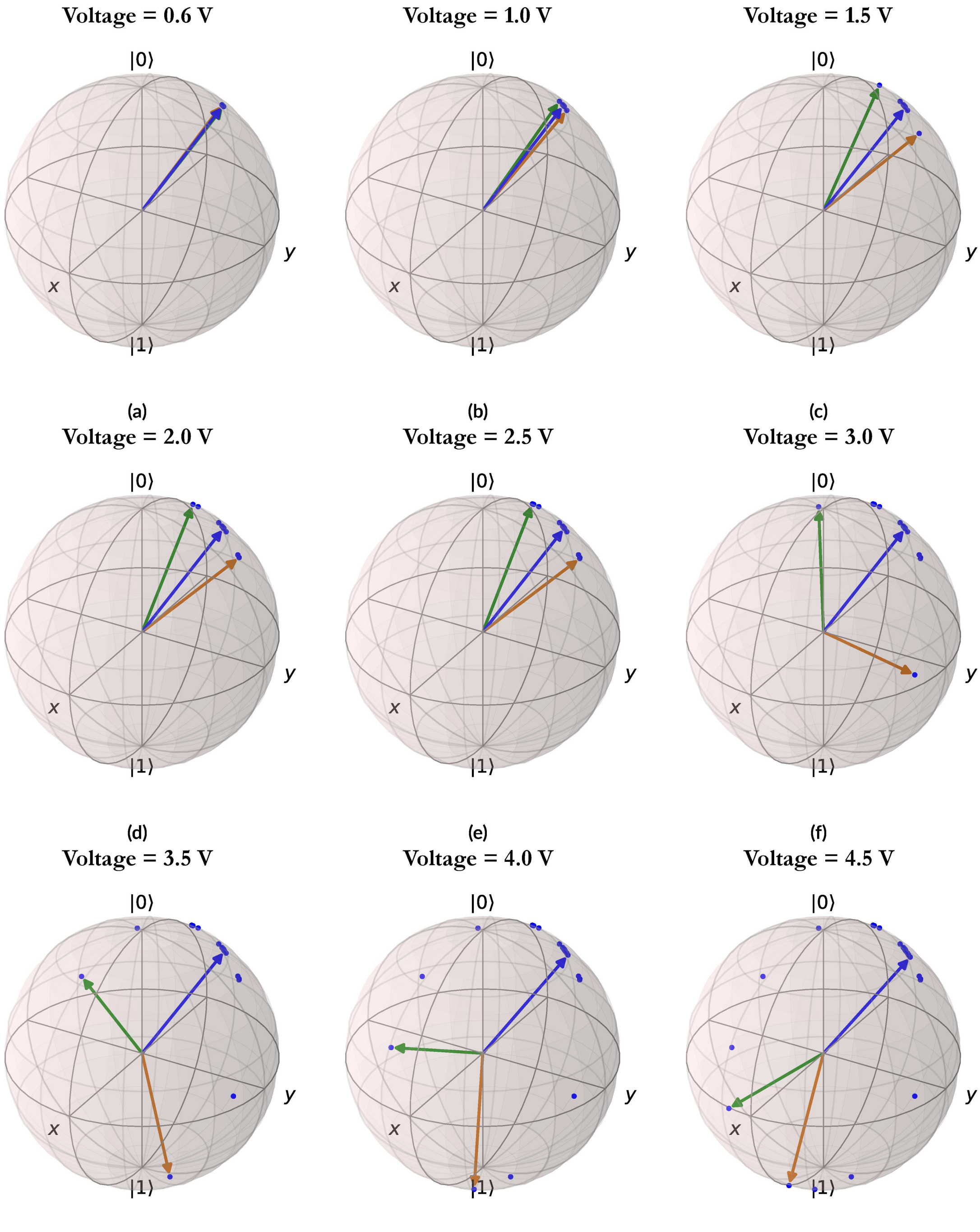
Figure 2.23: Plot of the angle between the states $|R\rangle$ and $|L\rangle$ in output from the iPOGNAC polarization modulator as a function of the applied voltage.

Polynomial fits were performed to reproduce the trend of the experimental data and to be able to predict at what voltage to set the phase modulator to obtain a certain polarization at the output of the iPOGNAC. The fits were performed only on a portion of the data due to the effects introduced by the voltage amplifier visible at low voltages (it can be noticed that the trend is very similar to that of Figure 2.19 for the intensity modulator). The results of the polynomial fits are shown in Table 2.5.

Polynomial fit results				
Dataset	p_0 [°]	p_1 [°/V]	p_2 [°/V^2]	p_3 [°/V^3]
$\|R\rangle , \|L\rangle$	$(-77 \pm 4) \cdot 10$	$(41 \pm 2) \cdot 10$	-38 ± 3	
$\|R\rangle , \|D\rangle$	$(-28 \pm 1) \cdot 10$	141 ± 7	-9.7 ± 0.9	
$\|L\rangle , \|D\rangle$	$(-13 \pm 1) \cdot 10^2$	$(10 \pm 1) \cdot 10^2$	$(-22 \pm 3) \cdot 10$	17 ± 3

Table 2.5: Results of the parabolic fits of the angles between the states $|R\rangle$, $|D\rangle$ and $|R\rangle$, $|L\rangle$ and of the cubic fit of the angles between the states $|L\rangle$ and $|D\rangle$ as a function of the voltage applied to the polarization modulator. The fit function is: $\theta = p_0 + p_1 \mathrm{V} + p_2 \mathrm{V}^2 + p_3 \mathrm{V}^3$. The data fit plots are shown in Figure 2.22 and 2.23.

Figure 2.25 shows the polarization states on the Bloch sphere generated by the iPOGNAC as a function of the applied electrical voltage. The reference system of the Bloch sphere is arbitrary, the aim is just to visualize the variation of the angle between the different polarization states.


Voltage = 0.6 V

Voltage = 1.0 V

Voltage = 1.5 V

(a)

(b)

(c)

Voltage = 2.0 V

Voltage = 2.5 V

Voltage = 3.0 V

(d)

(e)

(f)

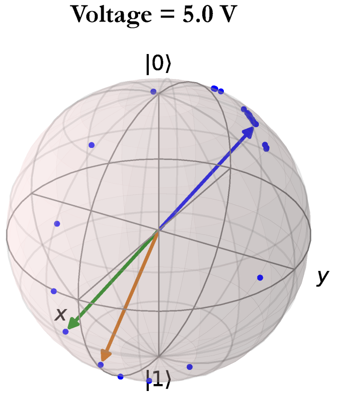
Voltage = 3.5 V

Voltage = 4.0 V

Voltage = 4.5 V

(g)

(h)



(a)

Figure 2.25: Representation of the polarization states on the Bloch sphere generated by the iPOGNAC as a function of the applied electrical voltage. The reference system of the Bloch sphere is arbitrary, the aim is just to visualize the variation of the angle between the different states.

To use the modulator to implement the three-state and one-decoy state protocol, it is necessary to be able to set between three different polarization states belonging to two non-orthogonal bases, e.g. $|D\rangle$, $|R\rangle$ and $|L\rangle$. So they must be coplanar and the angle on the Bloch sphere must be 90° to each other.

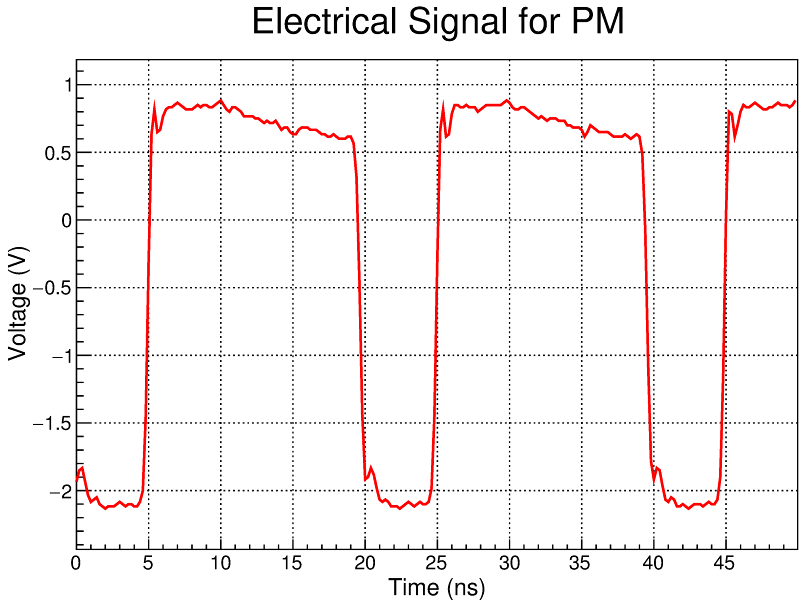


Figure 2.26: Example of the electrical signal used for the iPOGNAC polarization modulator. The electrical signal is generated by the FPGA, passes through a delay line, a low pass filter and a voltage amplifier.

2.5.1.4 VOA

The electronically Variable Optical Attenuator (VOA) makes it possible to vary the attenuation of the optical signal transmitted through the device using an electrical signal. The characterization of the VOA is necessary to be able to attenuate the output of the transmitter at a single photon level. Figure 2.27 shows a plot of the photon counts as a function of the electrical voltage applied to the VOA. An exponential fit of the data was performed and the results are reported in Table 2.6. The data were acquired with an SNSPD detector.

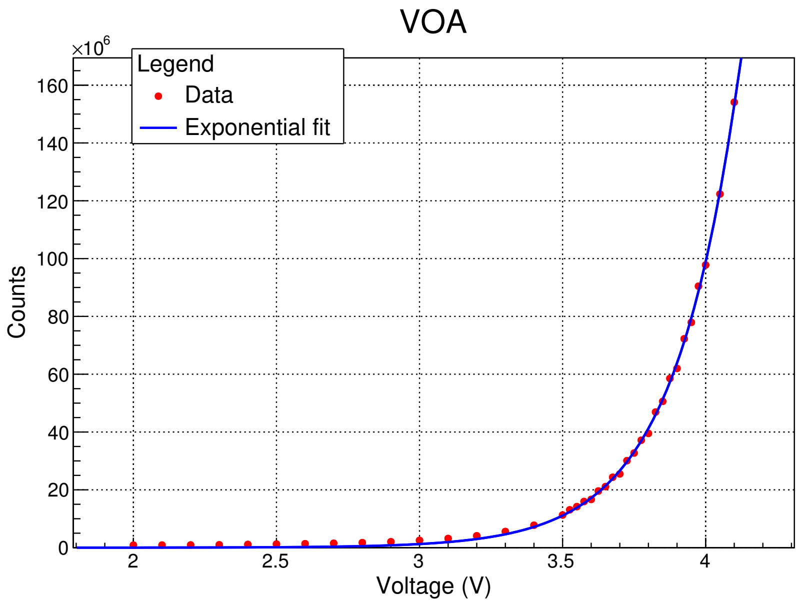


Figure 2.27: Plot of photon counts as a function of the electrical voltage applied to the VOA. An exponential fit of the data was performed.

Exponential fit result	
Costant	Slope [1/V]
0.9 ± 0.1	4.37 ± 0.03

Table 2.6: Results of the exponential fit of the data in Figure 2.27.

2.5.2 QBER

QKD protocols expect errors to occur within a certain threshold value. The sifted key obtained may not be identical for Alice and Bob not only due to eavesdropping, but also due to noise and experimental imperfections (due to the channel or detector), and it is not possible to distinguish them. These errors are measured using the Quantum Bit Error Rate (QBER), defined as the ratio between the number of wrong bits and the total number of bits of the sifted key. The exchange is considered safe if the QBER is below a threshold value of 11%.

Once the setup was completed, the intrinsic QBER (only due to noise and experimental imperfections) was measured in the two bases necessary for the three-state and one-decoy protocol. Measurement was performed by sending a pseudo-random qubit sequence of states and measuring the QBER of the sifted string recovered by Bob. In Figure 2.28a, 2.28b and 2.29 we show the QBERs behavior for an acquisition set, while in Table 2.7 are reported the average QBER values.

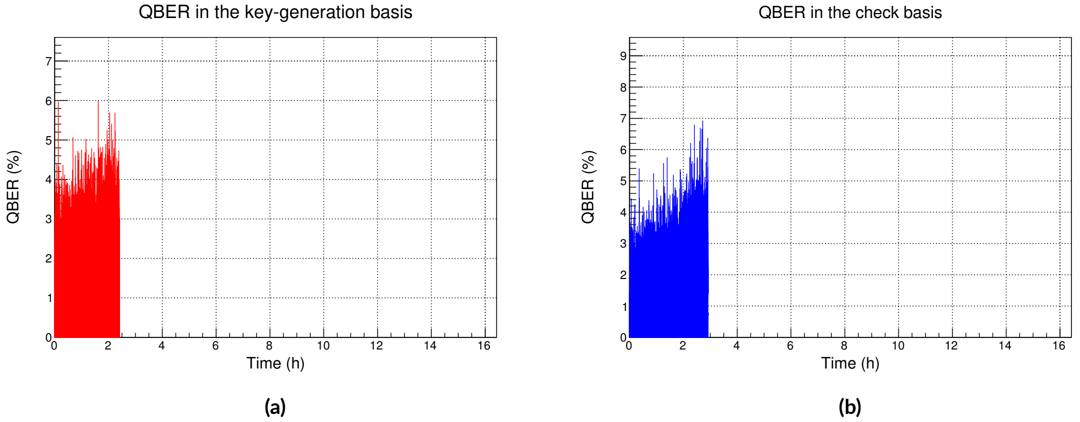


Figure 2.28: (a) Behavior of the QBER in the key-generation basis. (b) Behavior of the QBER in the check basis. The data acquisition duration is 16.4 hours.

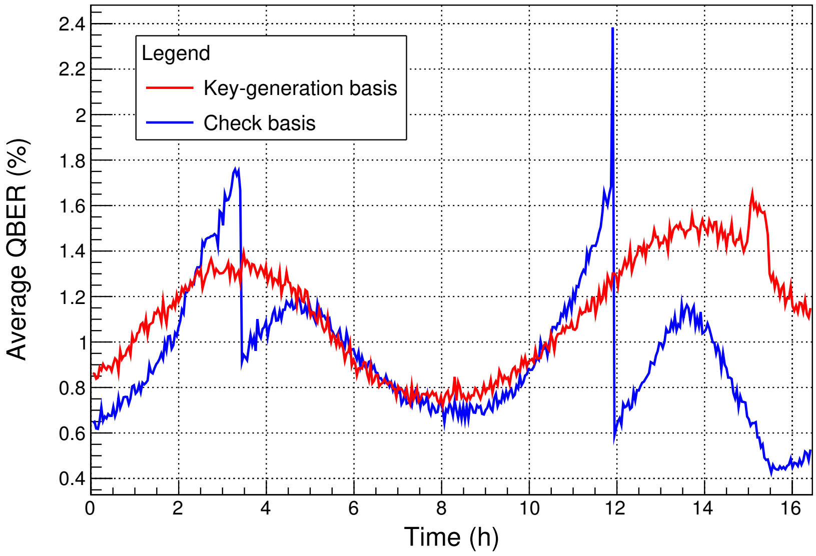


Figure 2.29: Behavior of the QBERs in the key-generation and in the check basis during an acquisition lasting 16.4 hours. To better visualize the trend, an average of every 1000 QBER data was performed for the plot.

Average *QBER* for the $\mathcal{K}$ basis	Average *QBER* for the $\mathcal{C}$ basis	Acquisition time
(1.1 ± 0.8) %	(0.9 ± 0.9) %	16.4 h

Table 2.7: Average QBER values in the key-generation basis $\mathcal{K} = \{|R\rangle, |L\rangle\}$ and in the check basis $\mathcal{C} = \{|D\rangle, |A\rangle\}$ for the case is shown in Figure 2.29.

The fluctuations of QBER visible in the plots are mostly due to temperature changes. Whenever the QBER grows too large, the automatic polarization alignment mechanism provides to reduce it.

In conclusion, a low intrinsic QBER<2% and long-term stability measured over 16 h was obtained. The obtained QBER values are much lower than the protocol threshold value of 11% and these performances are well-suited for QKD systems. [43]

3
Continuous-Variable QKD

So far, only discrete variable QKD protocols (DV-QKD) have been discussed. As an alternative to the DV-QKD, there is the continuously variable QKD (CV-QKD).

In discrete variable QKD protocols:

- the information is encoded in discrete degrees of freedom of the single photon, such as polarization or phase;
- single photon detectors are required to measure the quantum states received.

In CV-QKD on the other hand:

- the information is encoded in continuous degrees of freedom of the electric field, such as the quadratures;
- receiver requires homodyne (or heterodyne) detectors composed of classical photodiodes.

An homodyne detector measures a single quadrature of the electric field of the incident light. The measurement outcomes of such a measurement are a projection of the phase and amplitude of the electric field of light onto the quadrature axes. This projection ideally yields a continuous value as a measurement result, therefore justifying the name continuous-variable quantum key distribution. In practice, however, there is always a finite discretization of such measurements, due to the finite resolution of the experimental apparatus. Comparing the two types of protocols: homodyne detectors have lower costs, higher speed and higher efficiency than single photon ones. However, CV protocols present greater problems of information deterioration in optical fibers over long distances and the status of security proofs is less advanced with respect to their DV counterpart. Therefore at short distances, CV protocols are preferable because they have a higher key rate, while at long distances DV protocols are more efficient. For example, the transmission distance record for a CV protocol (the GG02 protocol) for fiber-based QKD was established in 2020 and is approximately 200 km.[44] While the distance record for a DV protocol (the twin-field protocol) was established in 2021 and is over 800 km.[45]

Figure 3.1 shows an example comparison of the key rate between a CV (4-PSK protocol) and a DV protocol (T12 protocol). It can be seen that in this case, below 40 km of distance the CV protocol is more efficient, while above 40 km the DV protocol is more performing and the difference in key rates can be of several orders of magnitude.

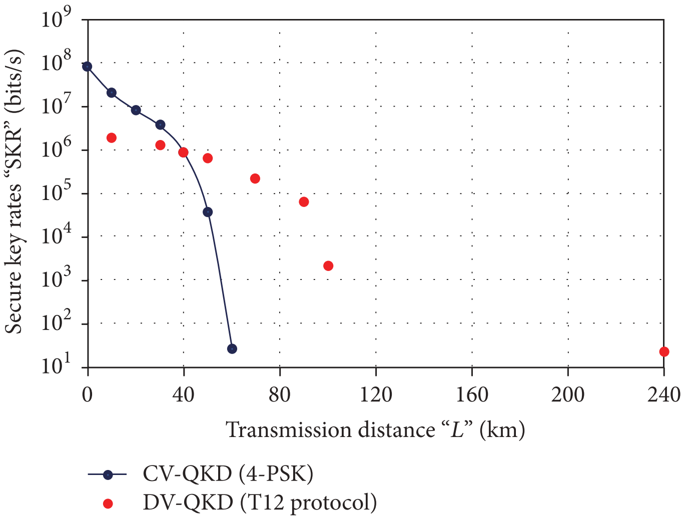


Figure 3.1: Performance comparison of CV-QKD versus DV-QKD for access and metro networks. [46]

CV-QKD protocols consist of the exchange of coherent states modulated in the phase space and measurements with coherent detection. The main difference from classical coherent optical communication is that CV-QKD works in the quantum regime with attenuated coherent states and low-noise detectors. As far as the security of CV protocols is concerned, their demonstration is more complicated than DV protocols because a description in the entire infinite dimensional Fock space is required. In DV protocols, on the other hand, small Hilbert spaces are used. The most widely used and safest CV protocols are those in which coherent states with a Gaussian modulation are prepared. One of the best-known CV-QKD protocols is the Gaussian-Modulated Coherent States (GMCS) protocol.[47][48] The coherent state

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{3.1}$$

is sent to Bob, where α is a random complex variable from a Gaussian distribution. Bob finally measures the state with a homodyne detector. From a theoretical point of view, the more coherent states can be generated, the safer the system is, but Gaussian modulation is only an idealization since real modulators have finite ranges and precision and therefore the number of possible states is finite. It can be shown that with sufficiently large constellations of states in phase space it is possible to obtain safety levels close to those for Gaussian modulation. Protocols with 2 coherent states are called Binary Phase-Shift Keying (BPSK), while those with 4 states are called Quadrature Phase-Shift Keying (QPSK), both are represented in Figure 3.2. The BPSK and QPSK protocols are part of the most general class of the M-PSK phase-shift keying protocols where Alice sends coherent states of the form:

$$|\alpha_k\rangle = \alpha\, e^{\frac{2\pi i k}{M}} \qquad \text{for } \alpha > 0 \tag{3.2}$$

The BPSK and 3-PSK cases do not guarantee good safety performance like the QPSK. In PSK modulation the only parameters are the number of states and the amplitude α of the coherent states, but there are protocols with more complex constellations. For example, the coherent states can lie on a grid or circles with different radii (as in Figure 3.2d).

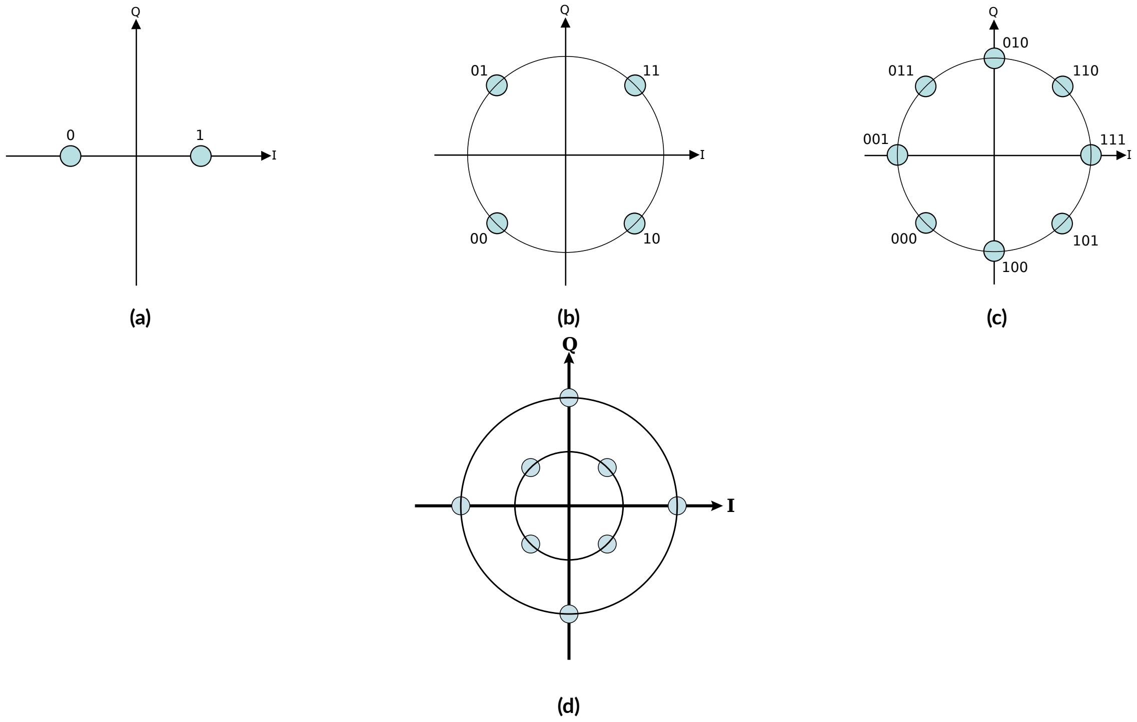


Figure 3.2: (a) BPSK constellation diagram. [49] (b) QPSK constellation diagram. [50] (c) 8-PSK constellation diagram. [51]. (b) Circular 8-QAM constellation diagram. [52]

PSK can be seen as a particular case of Quadrature Amplitude Modulation (QAM), which exploits both amplitude and phase modulation: amplitude modulation allows to an increase the radius of states in the phase space, while phase modulation allows to vary the radius (as shown in Figure 3.2). Another class of CV protocols uses squeezed states, however, these protocols are usually avoided in real implementations due to the complexity of generating squeezed states experimentally. [53] [54]

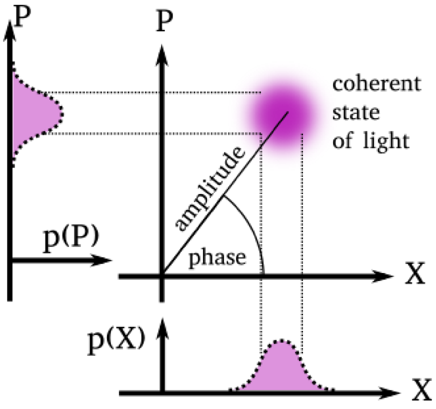


Figure 3.3: Coherent state of light represented in the optical phase space. [55]

A coherent state has a two-dimensional Gaussian distribution in optical phase space due to the Heisenberg uncertainty relation. Heisenberg's uncertainty relation states that the simultaneous determination of physical properties, called non-commuting observables, is not possible with arbitrary precision. An example are the position x and the momentum p, the optical analogue are the quadratures of the electric field X and P. Classically it is possible to bit-encode the information transmitted through an optical fiber by turning off (bit 0) and turning on (bit 1) a laser. Representing this in the optical phase space, there will be a state at the centre of the system corresponding to the laser off and a distinct state at a certain distance from the center, corresponding to the laser on, as shown in Figure 3.4a.

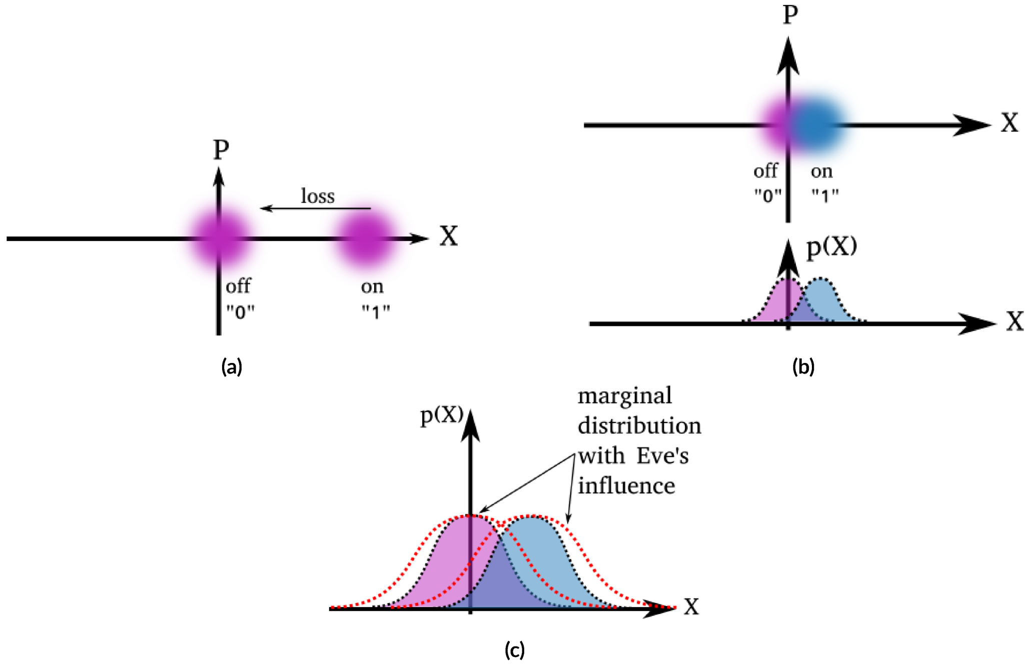


Figure 3.4: (a) Diagram with two distinct coherent states in which one is centred in the coordinate system, corresponding to the laser turned off, and the other with a certain amplitude and phase when the laser is turned on. (b) Diagram with two coherent states with an overlap and their distribution. (c) Distribution broadening due to an interception. The increased variance is indicated by the dotted red line. [55]

Since in this case it is easy to discriminate between the two states in phase space, an interceptor can detect the signal and return it undetected. However, if the amplitude of the states is chosen in such a way that the two Gaussian distributions have a certain overlap between them (as shown in Figure 3.4b), thanks to the Heisenberg uncertainty principle an interceptor will not be able to discriminate between the two states without making errors and therefore will introduce a turn of the errors in the states that he will send to Bob (Figure 3.4c). Bob, however, can take a random portion of his measurements and confront Alice, who tells him which states she has sent. This way he can plot the distribution and calculate the variance. If the variance is greater than that of a coherent state limited by quantum noise, he can conclude that there has been an interception. If, on the other hand, Bob does not reveal any interception he can obtain a secret key from the measured data, where, however, the data compared publicly with Alice are discarded. In reality, due to the noise alone, the data obtained by Bob will not be the same as that sent by Alice, therefore it will be necessary to apply error correction processes to obtain a secret key that is the same for both. Finally, the secret key obtained can be used with the one-time pad cryptographic method. This intuitive explanation can be formally stated and the security of CV-QKD can be proven under different assumptions. A more complete and comprehensive description can be found in [56].

[55] [57] [58]

3.1 QKD system design for both CV and DV

The idea is to design and test the feasibility of creating a Quantum Key Distribution system that works for both discrete and continuous variables. The motivation for designing such a system is that in this way it would be possible to choose the most efficient protocol depending on the optical fiber communication distance. Furthermore, thinking about satellite communication in free-space, wanting to test the different types of QKD protocol, in this case the size of the system is very important and having a single device capable of using both types of protocols would save space and costs.

To design a QKD transmitter that works for both discrete and continuous variables, you could try to modify the setup described in Section 2.4.1 and represented in Figure 2.16 as little as possible. For example, it can be modified as shown in Figure 3.5. As already discussed, a QKD-DV transmitter usually consists of three main components: laser, intensity modulator and polarization modulator. For a DV protocol such as the BB84, it is important that the laser is gain-switching so that the pulses generated are not in phase with each other, otherwise it would be possible for an interceptor to steal information from the relative phase between two pulses. For a CV protocol, on the other hand, it is important to be able to control the relative phase between two pulses. To make a QKD transmitter that works for both CV and DV, one could use a single laser that does gain switching for the DV protocol and injection locking for the CV protocol, so that it can be used for both protocols. Gain switching allows to obtain not correlated pulses in phase and very narrow, while injection locking allows to obtain pulses in phase with each other using a laser pump. The pump laser could also be used for the homodyne detector which requires a local oscillator to perform the measurements. Regarding the Sagnac-based intensity modulator it could be left unchanged so that it can be used for both protocols. The iPOGNAC polarization modulator, on the other hand, can be modified by inserting an electrically controlled optical switch to select or avoid the fiber delay line. In this way, by selecting it you could get the standard iPOGNAC for QKD-DV, avoiding it you could control the relative phase between two optical pulses for the CV protocol.

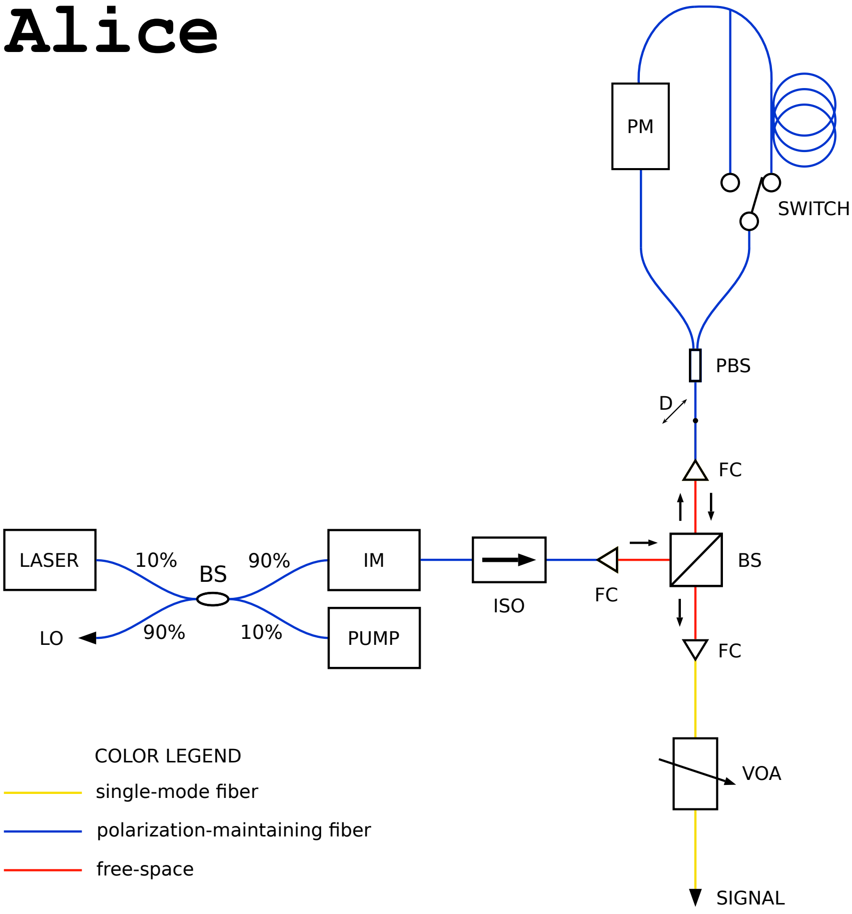


Figure 3.5: Schematic of a possible QKD transmitter for both discrete and continuous variables. The laser can do injection locking. The polarization modulator is the standard iPOGNAC except for the optical switch that allows you to avoid or not the fiber delay line. The switch allows you to choose between a DV (delay line) and a CV (no delay line) protocol. The abbreviations indicate: BS = beam splitter, IM = intensity modulator, PUMP = laser pump, ISO = isolator, FC = fiber collimator, PBS = polarizing beam splitter, D = diagonal polarization, PM = phase modulator, VOA = variable optical attenuator, LO = local oscillator. The yellow lines indicate single-mode fiber, the blue ones indicate polarization-maintaining fiber, and the red ones free-space.

Similarly to the receiver, an electrically controlled optical switch can be inserted to select the single photon detector for the discrete variable protocol or the homodyne (or heterodyne) detector for the continuous variable protocol. The homodyne detector extracts phase information on a beam by comparing it to a reference beam (local oscillator, LO). This can for example be taken directly from the sender's laser pump.

3.2 Mach-Zehnder intensity modulator

It is possible to realize an intensity modulator, called Mach-Zehnder modulator, simply by placing a phase modulator in an arm of a Mach-Zehnder interferometer. This consists of two beam splitters and two mirrors: a beam splitter divides the light beam into two beams of equal intensity, which travel along two different paths and, through the mirrors, recombine in another beam splitter which allows the two beams to interfere, as depicted in Figure 3.6.

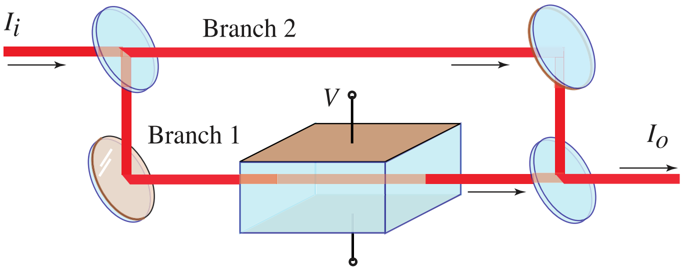


Figure 3.6: A phase modulator placed in one branch of a Mach-Zehnder interferometer can serve as an intensity modulator. [29].

The intensity of their overlap is then detected by measuring, by means of two photodetectors, the two rays exiting the second beam splitter. Consider a single output of the interferometer, let ϕ_0 be the phase term due to the optical path difference of the two arms of the interferometer when no voltage is applied and ϕ the phase difference due to the phase modulator, the intensity will be

$$\begin{aligned} I_o &= A_1^2 + A_2^2 + 2A_1A_2\cos\left(\Delta\phi\right) = \\ &= \left(\frac{A_i}{2}\right)^2 + \left(\frac{A_i}{2}\right)^2 + 2\left(\frac{A_i}{2}\right)\left(\frac{A_i}{2}\right)\cos\left(\phi_0+\phi\right) = \\ &= \frac{I_i}{4} + \frac{I_i}{4} + \frac{I_i}{2}\cos\left(\phi_0+\phi\right) = \frac{I_i}{2}\left[1+\cos\left(\phi_0+\phi\right)\right] = \\ &= I_i\cos^2\left(\frac{\phi_0+\phi}{2}\right) = I_i\cos^2\left(\frac{\phi_0}{2} - \frac{\pi}{2}\frac{V}{V_\pi}\right) \end{aligned} \tag{3.3}$$

which is nothing more than the transfer function in the ideal case (without considering the optical power losses inside the modulator), where the (2.14) has been used, A_i is the input amplitude and I_i is the input intensity of the interferometer. Therefore, by changing the potential difference of the phase modulator, the two beams can be made to interfere in a constructive or destructive way and, in this way, the amplitude (and therefore the intensity) at the output can be controlled. For example, the optical path difference can be constructed so that $\phi_0 = 0$, if $V = 0 \Rightarrow I_o = I_i$, while if $V = V_\pi \Rightarrow I_o = 0$. Therefore, by applying the voltages between $0 \leq V \leq V_\pi$, it is possible to produce at the output of the interferometer the intensities between $0 \leq I_o \leq I_i$.

The Mach-Zehnder intensity modulator can also be realized in the form of an integrated optical device, which does not use mirrors and beam splitters, but has a completely equivalent operation to the previous one. This is constructed using a substrate of electro-optical material and Y waveguides instead of the two beam splitters, as shown in Figure 3.7. Optical fibers can be used at the output and input. The Thorlabs LN81S-FC Mach-Zehnder intensity modulator used for this thesis work is of this last type and is constructed in such a way as to have the two arms of the interferometer symmetrical.

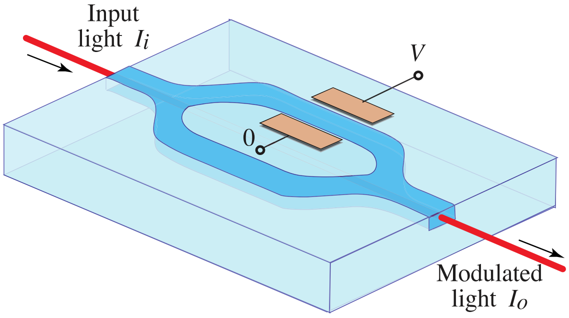


Figure 3.7: An integrated-photonic intensity modulator. A Mach-Zehnder interferometer and an electro-optic phase modulator are implemented using optical waveguides fabricated from a material such as $LiNbO_3$ indiffused with Ti. [29].

The intensity modulator used for this thesis work is an Z-cut $LiNbO_3$ intensity modulator based on titanium-indiffused waveguide technology. Lithium niobate IMs can be fabricated with X-cut or Z-cut. X-cut IMs, as can be seen in Figure 3.8a, allow both arms of the Mach-Zehnder interferometer to be symmetrically modulated, in this way the modulated output is not shifted in phase. Z-cut IMs represented in Figure 3.8b, on the other hand, have a difference in the phase shift between the two arms of the Mach-Zehnder interferometer and this results in a phase shift in the output in addition to the intensity modulation. Z-cut IMs are also characterized by a higher frequency-chirp in the modulated signal and a lower V_π voltage than X-cut IMs. These are the reasons why in our case it is necessary to have a Z-cut $LiNbO_3$ intensity modulator. [22][29][36][59][60]

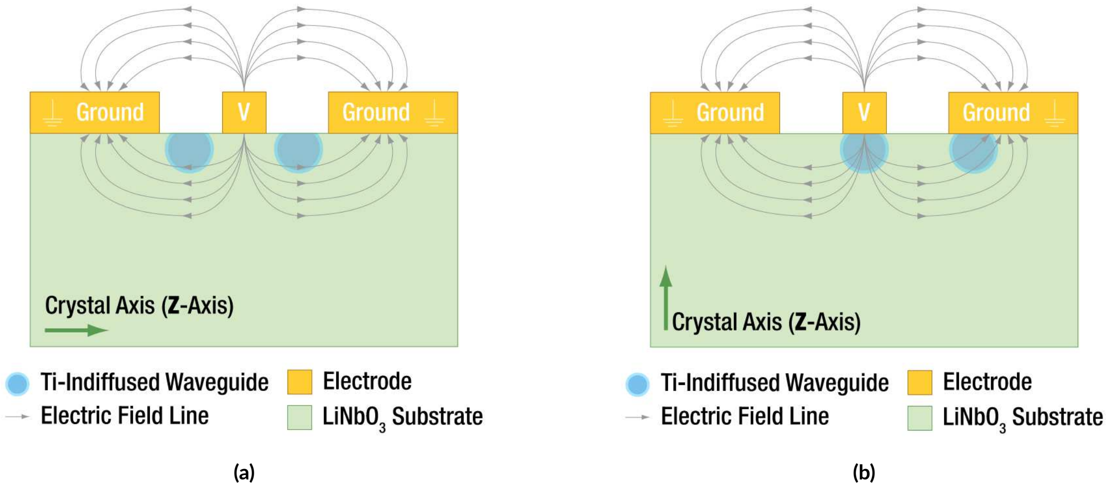


Figure 3.8: (a) X-cut $\mathrm{LiNbO_3}$ intensity modulator cross-section. (b) Z-cut $\mathrm{LiNbO_3}$ intensity modulator cross-section. [60]

3.2.1 Drift

A change in the output of the Mach-Zehnder modulator may not even be due to an applied electrical modulation signal. In this case the change is unintentional and is called drift. The most frequent causes of drift are: temperature variations, thermal inhomogeneity, aging, photorefractive effects and accumulation of electrostatic charges. All these phenomena can introduce a phase term ϕ_0, due to a small non-symmetrical variation of the optical path inside the two arms of the interferometer, causing a shift of the transfer function. In these cases the electrical modulation signal is then applied to a variable operating point, which can strongly modify the modulation obtained. For this reason, in the LN81S-FC modulator, in addition to the pair of electrodes to which the modulation voltage is applied (called RF voltage), there is another pair of electrodes to which a DC voltage is applied, called bias voltage. The bias voltage allows you to select the desired operating point of the modulator, compensate for its possible drift and block the operating point of the device, in order to maintain stable operating conditions. It is possible to carry out these operations through an automatic control system, which was built and programmed ad hoc for this thesis work. The LN81S-FC modulator has a monitoring photodiode inside that uses a small part of the modulated laser signal coming out of it. The control system receives the current generated by this photodiode and adjusts the bias voltage of the modulator. Considering this bias voltage V_{bias} Eq. (3.3) becomes:

$$I = I_i \cos^2\left(\frac{\phi_0}{2} - \frac{\pi}{2}\frac{V + V_{bias}}{V_\pi}\right) , \tag{3.4}$$

where in this case ϕ_0 is the phase term due to drift alone. [22][59]

3.2.2 PID controller

Whenever a device must keep a certain physical parameter of a system constant, for example a temperature, a speed or a direction, a control action is needed to correct any unwanted variations with respect to the preset value. In the case in question, the physical parameter to be kept constant is the intensity of the laser coming out of the Mach-Zehnder intensity modulator. To create the control system, a PID controller can be used, an acronym that indicates a proportional, integral and derivative action controller. The PID controller is one of the most used negative feedback control systems in the industry due to its simplicity, because it allows to obtain good performances, even in the presence of little knowledge of the system model, and because it presents non-complex parameters calibration techniques. The PID accepts the device output variable as input and compares it with a predetermined setpoint, which is the reference value to be reached and kept as constant as possible. The difference between setpoint and input value is the error and is used to determine the controller output variable. The control law, i.e. the link between error $e(t)$ and the output variable of the regulator $u(t)$, is given by the sum of three contributions:

$$u(t) = K_P\, e(t) + K_I \int_{t_0}^{t} e(\tau)d\tau + K_D \frac{de(t)}{dt}\ . \tag{3.5}$$

The first term linearly depends on the error, the second is proportional to the integral of the error and the third depends on the derivative of the error, therefore K_P is called the proportional action coefficient, K_I coefficient of the integral action and K_D coefficient of the derivative action. With only the proportional action $K_P\, e(t)$, if in a certain instant the error were to be null, this would be canceled in turn. If in the next instant the error was not null, there would be no preventive correction. A possible solution to this problem is the introduction of the integral action $K_I \int_{t_0}^{t} e(\tau)d\tau$. This depends on the sum of all previous errors over time, so it varies until the setpoint is reached, and in this case it remains constant. Therefore, even if the proportional action were null, there would be corrective action. The derivative action $K_D \frac{de(t)}{dt}$, on the other hand, thanks to its dependence on the speed with which the error varies, allows to further improve the performance of the controller, trying to compensate the error variations and ensuring greater stability to the system. [22][61][62]

3.2.3 Controller realization

An Adafruit HUZZAH32 ESP32 with Arduino Programming Language programming code was programmed to create the controller. The programming code was written in Arduino Programming Language. To exploit the weak current signal outgoing from the photodiode of the modulator, a transimpedance amplifier has been assembled that uses the Analog Devices AD8513ARUZ operational amplifier, specially made with high gain to work with low currents. This circuit allowed the current to be amplified into a voltage readable by the ESP32. It was necessary to insert a capacitor in parallel to the inverting branch of the circuit. This acts as an active low pass filter to limit the bandwidth of the circuit and thus the noise generated. The bias voltage supported by the modulator is between -8 V and 8 V, but the output voltage of a single pin of the ESP32 is between 0 V and 3.3 V. For this reason, a MAX11300PMB1 peripheral module (from Maxim Integrated) was used, equipped with 20 pins that can work as ACD or DAC and can generate a voltage difference of 10 V. The MAX11300PMB1 output allowed to obtain a voltage between -5 V and $+5$ V and a non-inverting amplifier was built (using the same operational AD8513ARUZ equipped with several outputs), which allowed to amplify the voltage up to ±8 V. Figure 3.9 shows a diagram of the system created:

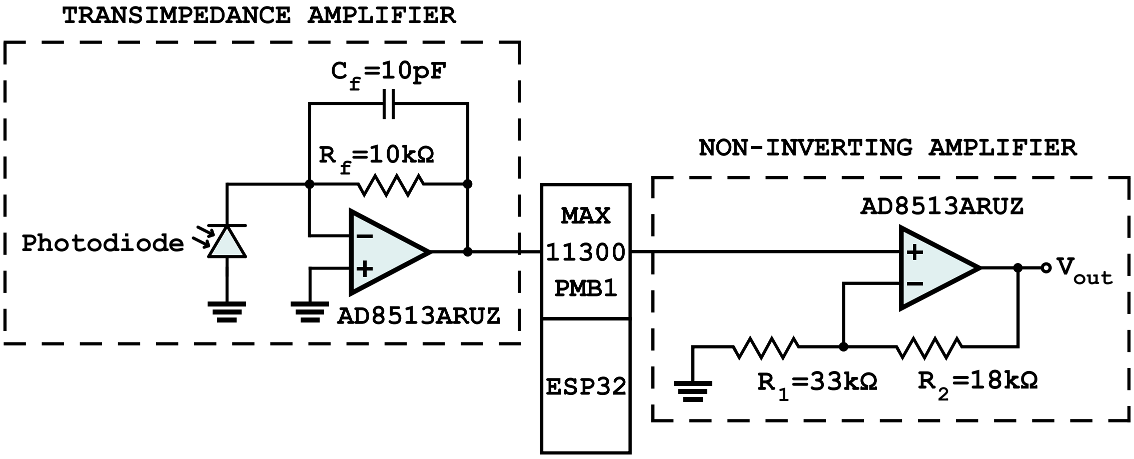


Figure 3.9: Electronics diagram created for the controller of the Mach-Zehnder IM. [63] [64]

To generate a DC voltage of ±12 V, for both the operational amplifier and the MAX11300PMB1, starting from a single voltage of +15 V, the circuit in Figure 3.10 was assembled. The Analog Devices LTC3260 is a low noise dual polarity output power supply that includes an inverting charge pump. A charge pump is a DC-to-DC converter that uses capacitors for energetic charge storage to raise or lower voltage. In a two-stage cycle, in the first stage a capacitor is charged to the supply voltage and in the second stage the capacitor passes in series with the supply. In this way the voltage across the load, also connected in series, doubles. [65][66]

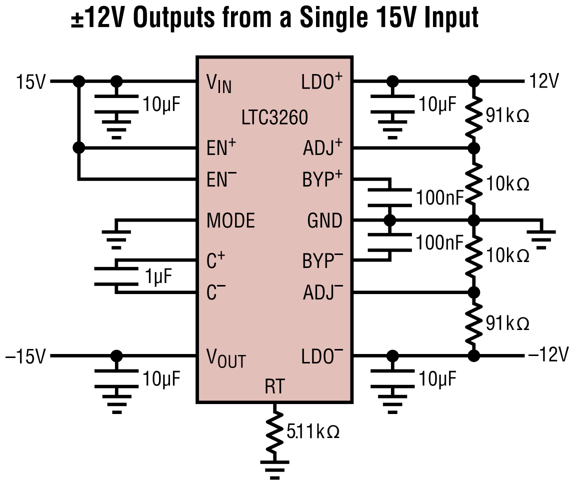


Figure 3.10: Typical circuit diagram for an Analog Devices LTC3260 with charge pump function. [65]

3.2.3.1 Linear voltage regulator

It is possible to realize an adjustable positive linear voltage regulator using the integrated LM317. This, in a suitable circuit, allows to obtain a stable output voltage and to regulate it in a determined range. In addition, the LM317 is equipped with an internal protection system against overcurrents and short circuits, in order to limit the output current when it enters protection. The LM317 has three terminals: input, output and adjustment and maintains a constant voltage difference $V_{ref} = 1.25$ V (called internal reference voltage) between the adjustment terminal and the output terminal (as shown in Figure 3.11).

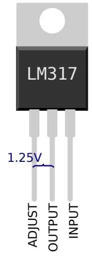


Figure 3.11: LM317 pinout showing its constant voltage reference. [67]

Usually the input terminal of the integrated is connected to the voltage source, the adjustment terminal to a circuit that fixes the output voltage and the output terminal to the device to be powered. If the adjustment pin is grounded, the output pin provides a voltage of 1.25 V and currents up to 1.5 A maximum. Instead, connecting the adjustment pin to a circuit that fixes the output voltage, such as a resistive voltage divider between the output and ground as in

Figure 3.12a, it is possible to obtain an output voltage of:

$$V_{out} = V_{ref}\left(1 + \frac{R_2}{R_1}\right) + I_{adj}R_2 \simeq V_{ref}\left(1 + \frac{R_2}{R_1}\right) \tag{3.6}$$

The term $I_{adj}R_2$ is due to the fact that a small quiescent current I_{adj} of a maximum of 100 µA flows from the adjustment pin of the device, which is usually negligible. By appropriately choosing the voltages R_1 and R_2 it is possible to adjust the output voltage which, however, can never be lower than V_{ref}. In order to adjust the output voltage by changing the ratio between R_1 and R_2 in a simpler way, it is possible to use a trimmer instead of the two resistors as in Figure 3.12b.

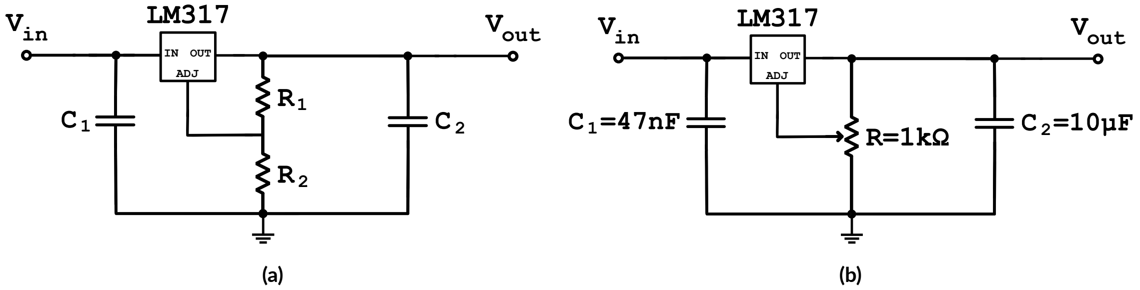


Figure 3.12: Schematic of LM317 in two typical voltage regulator configurations, including decoupling capacitors to reduce input noise and to improve output transient response. Usually the input bypass capacitor C_1 is used of 0.1 µF, while C_2 of 10 µF. [68]

The integrated introduces a voltage drop between input and output (called drop-out voltage) of no more than 3 V.

Different voltage regulators of the type in Figure 3.12b were made, used to set and regulate the voltage of the amplifiers. In the voltage regulators made in the laboratory with an input voltage of V_{in} = 12.1 V, by adjusting the trimmer, it was possible to obtain a range of voltages between 1.25 V $\leq$ V_{in} $\leq$ 10.7 V. In conditions of output currents close to the maximum deliverable by the integrated (which is I_{max} = 1.5 A) the power dissipated by the LM317 tends to increase and with it also the heat generated by the device. For this reason it usually also requires a heat sink to prevent the temperature from rising too high and entering protection. [69][70]

3.2.4 Test

An important parameter for the characterization of the modulator is the Extinction Ratio (ER), which is the ratio between the maximum modulated optical power P_1 and the minimum P_0 output from the modulator:

$$ER = \frac{P_1}{P_0} \tag{3.7}$$

The experimental apparatus in Figure 3.13 was used to estimate the ER of the LN81S-FC intensity modulator. The source is a laser that emits a linearly polarized beam at a wavelength $\lambda_0 = 1550$ nm. The electromagnetic wave exiting the laser, via an SMF fiber, passes through a polarization controller. This is configured in such a way as to obtain a horizontal polarization which enters the intensity modulator through a PMF fiber which preserves the state of polarization even in the presence of curvatures. The optical signal outgoing from the modulator is then measured by a superconductive nanowire single-photon detector (SNSPD) cooled to 0.8 K thanks to a helium cycle. Square waves of frequency 50 MHz generated by an FPGA connected to a voltage amplifier were used as an electrical modulation signal (Figure 3.15). The data obtained from the measurements are represented in Figure 3.14. In order to have an estimate of the photon counts of the detector, corresponding to the maximum and minimum of the modulation, averages were carried out on the modulated pulse, represented in figure with a red segment. The extinction ratio found is: $ER = (23.8 \pm 0.2)$ dB. Comparing this value with the one present on the datasheet of the modulator [71], which reports a minimum ER value of 20 dB, we note that the result obtained is compatible.

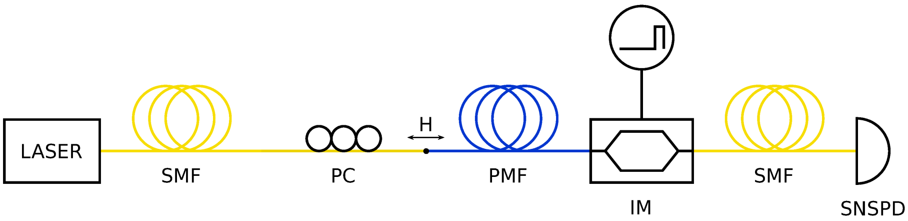


Figure 3.13: Schematic of the experimental setup for testing the iSntensity modulator. The abbreviations indicate: SMF = single-mode fiber, PC = polarization controller, PMF = polarization-maintaining fiber, IM = intensity modulator, SNSPD = Superconductive Nanowire Single-Photon Setector, H = horizontal polarization.

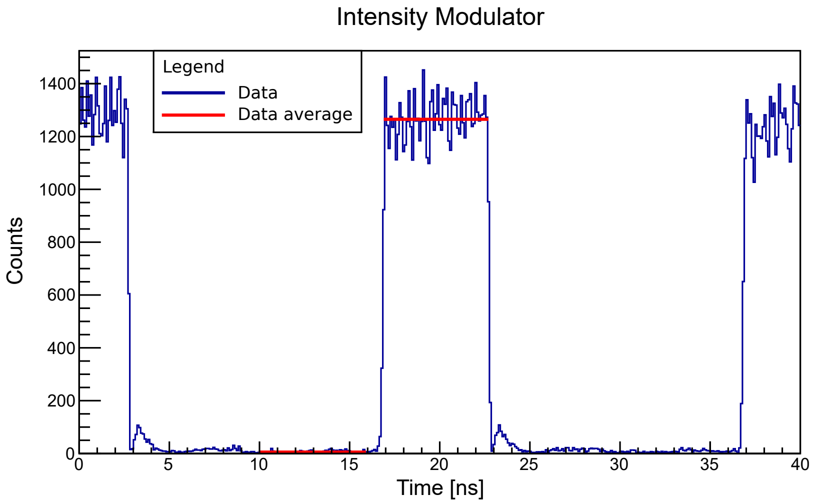


Figure 3.14: Histogram of the photon counts modulated by the intensity modulator. The acquisition time of the dataset is ∼1 s.

Intensity modulator
Extinction ratio
(23.8 ± 0.2) dB

Table 3.1: Results of the ER calculated using the data reported in Figure 3.14.

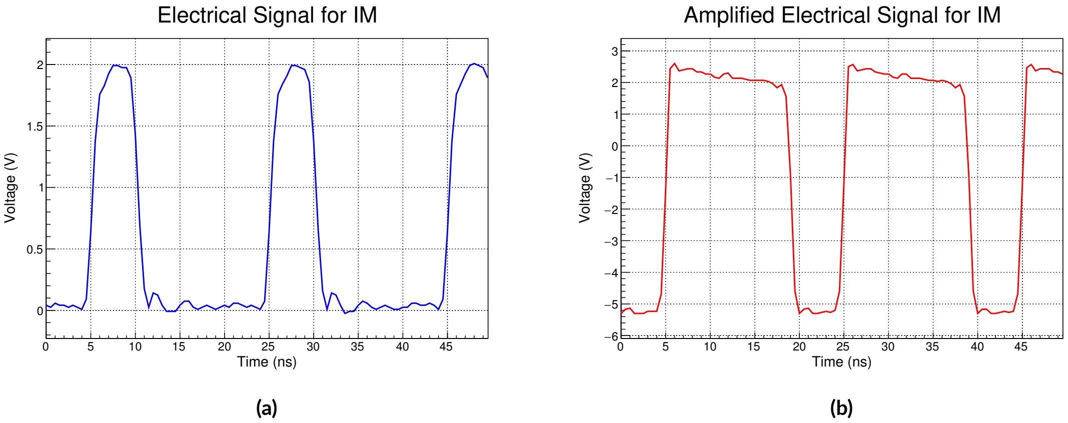


Figure 3.15: Electrical signal used for the Mach-Zehnder intensity modulator. (a) Non-amplified electrical signal generated by the FPGA. (b) Electrical signal generated by FPGA and amplified by an inverting voltage amplifier.

3.3 Homodyne detection

Considering a quantum coherent state with quadrature operators $\hat{q}$ and $\hat{p}$, its annihilation operator is:

$$\hat{a} = \frac{1}{2}\left(\hat{p} + \hat{q}\right) \tag{3.8}$$

If we consider also a classical optical field, this can represented by:

$$\alpha_{\mathrm{LO}} = q + ip = \left|\alpha_{\mathrm{LO}}\right| e^{i\theta} \tag{3.9}$$

Where the abbreviation LO means local oscillator. If the quantum field $\hat{a}$ and the classical field α_{LO} hit a 50:50 BS, its transformation matrix is:

$$\mathrm{BS} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.10}$$

So its action will be

$$\mathrm{BS}\begin{pmatrix} \hat{a} \\ \alpha_{\mathrm{LO}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \hat{a} + \alpha_{\mathrm{LO}} \\ \hat{a} - \alpha_{\mathrm{LO}} \end{pmatrix} =: \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \tag{3.11}$$

$\hat{a}_1$ and $\hat{a}_2$ represent the annihilation operators at the output of the BS. The photon number operators at the output of the BS will be:

$$\begin{aligned} \hat{n}_1 &= \hat{a}_1^\dagger \hat{a}_1 = \frac{1}{2}\left(\hat{a}^\dagger + \alpha_{\mathrm{LO}}^*\right)\left(\hat{a} + \alpha_{\mathrm{LO}}\right) = \frac{1}{2}\left(\hat{a}^\dagger \hat{a} + \alpha_{\mathrm{LO}}^*\alpha_{\mathrm{LO}} + \alpha_{\mathrm{LO}}\hat{a}^\dagger + \alpha_{\mathrm{LO}}^*\hat{a}\right) \\ \hat{n}_2 &= \hat{a}_2^\dagger \hat{a}_2 = \frac{1}{2}\left(\hat{a}^\dagger - \alpha_{\mathrm{LO}}^*\right)\left(\hat{a} - \alpha_{\mathrm{LO}}\right) = \frac{1}{2}\left(\hat{a}^\dagger \hat{a} + \alpha_{\mathrm{LO}}^*\alpha_{\mathrm{LO}} - \alpha_{\mathrm{LO}}\hat{a}^\dagger - \alpha_{\mathrm{LO}}^*\hat{a}\right) \end{aligned} \tag{3.12}$$

The number-difference operator is:

$$\Delta\hat{n} = \hat{n}_1 - \hat{n}_2 = \alpha_{\mathrm{LO}}\hat{a}^\dagger + \alpha_{\mathrm{LO}}^*\hat{a} \tag{3.13}$$

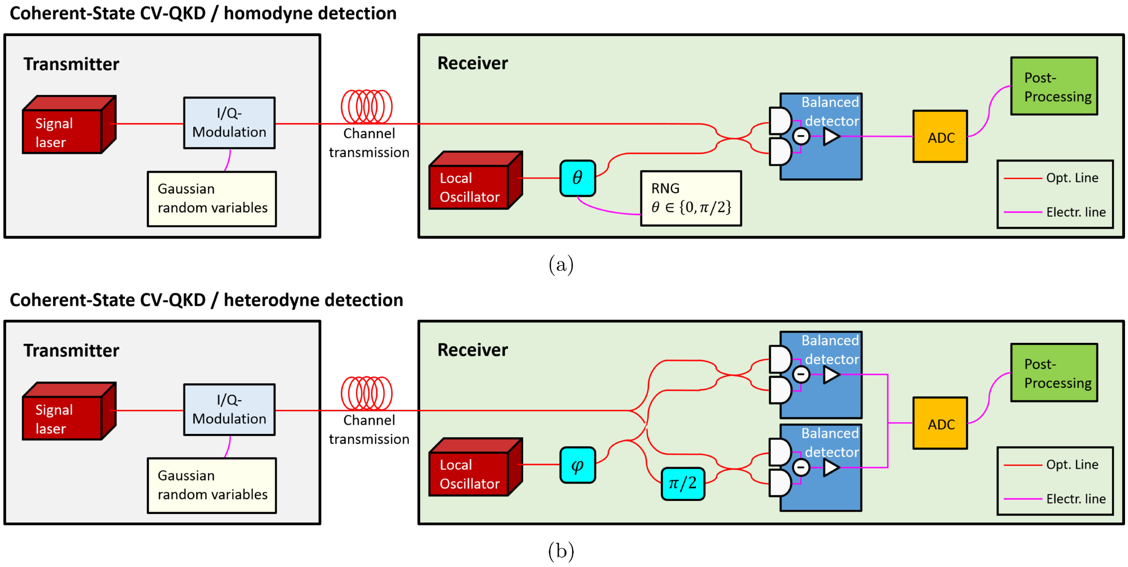
Using Eq. (3.9) and (3.8) we have

$$\begin{aligned} \Delta\hat{n} &= \left|\alpha_{\mathrm{LO}}\right|\left(\hat{a}^\dagger e^{i\theta} + \hat{a}e^{-i\theta}\right) = \frac{\left|\alpha_{\mathrm{LO}}\right|}{2}\left[\left(\hat{q} - i\hat{p}\right)e^{i\theta} + \left(\hat{q} + i\hat{p}\right)e^{-i\theta}\right] = \\ &= \frac{\left|\alpha_{\mathrm{LO}}\right|}{2}\hat{q}\underbrace{\left(e^{i\theta} + e^{-i\theta}\right)}_{2\cos\theta} + i\hat{p}\underbrace{\left(-e^{i\theta} + e^{-i\theta}\right)}_{-2i\sin\theta} = \left|\alpha_{\mathrm{LO}}\right|\left(\hat{q}\cos\theta + \hat{p}\sin\theta\right) \end{aligned} \tag{3.14}$$

$$\begin{aligned} &\text{if } \theta = 0 \qquad \Delta\hat{n} = \left|\alpha_{\mathrm{LO}}\right|\hat{q} \\ &\text{if } \theta = \tfrac{\pi}{2} \qquad \Delta\hat{n} = \left|\alpha_{\mathrm{LO}}\right|\hat{p} \end{aligned} \tag{3.15}$$

Depending on the local-oscillator phase θ, $\Delta\hat{n}$ is either proportional to the $\hat{p}$ or $\hat{q}$ quadrature operator.

Homodyne detection is the extraction of phase information about a laser beam by comparing it to a reference beam, called local oscillator (LO). This is achieved by interfering beams on a BS and subtracting the intensity of the two output ports, as shown in Figure 3.16. Selecting the phase shift θ between signal and LO, the photon number difference at the output ports of the BS is proportional to either the q or p quadrature, as described from Eqs. (3.14) and (3.15). On the same principle is based the heterodyne detection, where the signal is split using an additional balanced BS. One arm is used to measure q, the other one, after a LO phase shift of $\pi/2$, to measure p. Differently from the homodyne detector, the heterodyne detector allows you to measure p and q simultaneously, paying the price of an additional 3 dB of noise on the measurement, due to the mixing of the signal with an additional vacuum mode at the beamsplitter. [56]



(a)

(b)

Figure 3.16: Distinction between the (a) homodyne and (b) heterodyne detection. In the first case it is possible to select the phase of the local oscillator: 0 or $\pi/2$ to measure q or p, respectively. Only one homodyne detector is used, measuring one quadrature at a time. In the case of heterodyne detection the quantum signal is split using a balanced beamsplitter. One arm is used to measure q, the other one, after a LO-phase shift of $\pi/2$, to measure p.

3.4 Experimental setup

The goal of this experiment is to test the feasibility of using an experimental setup that can work simultaneously for both a CV and DV protocol. For this reason, changes have been made to a setup that we know will work for a DV protocol and the potential functioning has been verified in the case of a CV protocol. Unfortunately, there was no laser available that did injection locking as in the setup design of Figure 3.5, so a CW laser (Santec WLS-110) was used together with an intensity modulator (Thorlabs LN81S-FC) to generate pulses in phase between them.

As shown in Figure 3.17, a 1550 nm CW laser signal is split by an asymmetric beam splitter into a signal (10%) and a bright local oscillator (90%). The optical signal is modulated by a Mach-Zehnder intensity modulator which allows to create pulses in phase with each other. Then it encounters a modified iPOGNAC without delay line, so that the phase modulator inside the Sagnac loop can control the relative phase between optical pulses (and not the polarization as in the standard case). Finally it is detected by the heterodyne detector. In the LO branch, on the other hand, there is a delay line to ensure that the two optical paths are approximately the same long. Before entering the heterodyne detector, a VOA is present and 1 % of the LO is sent through a BS to a photodiode for the calibration phase. The polarization controllers before heterodyne are necessary because the latter has been designed to be sensitive to polarization. The heterodyne mixes the signal with the LO and returns two pairs of outputs, featuring a $\pi/2$ phase shift. These optical signals, detected by a couple of high-bandwidth balanced detectors, are proportional to the p and q quadratures of the signal. Finally, both signals from the detectors are sampled using a fast oscilloscope (Tektronix DPO70404C with 25 GS/s of sample rate). [72]

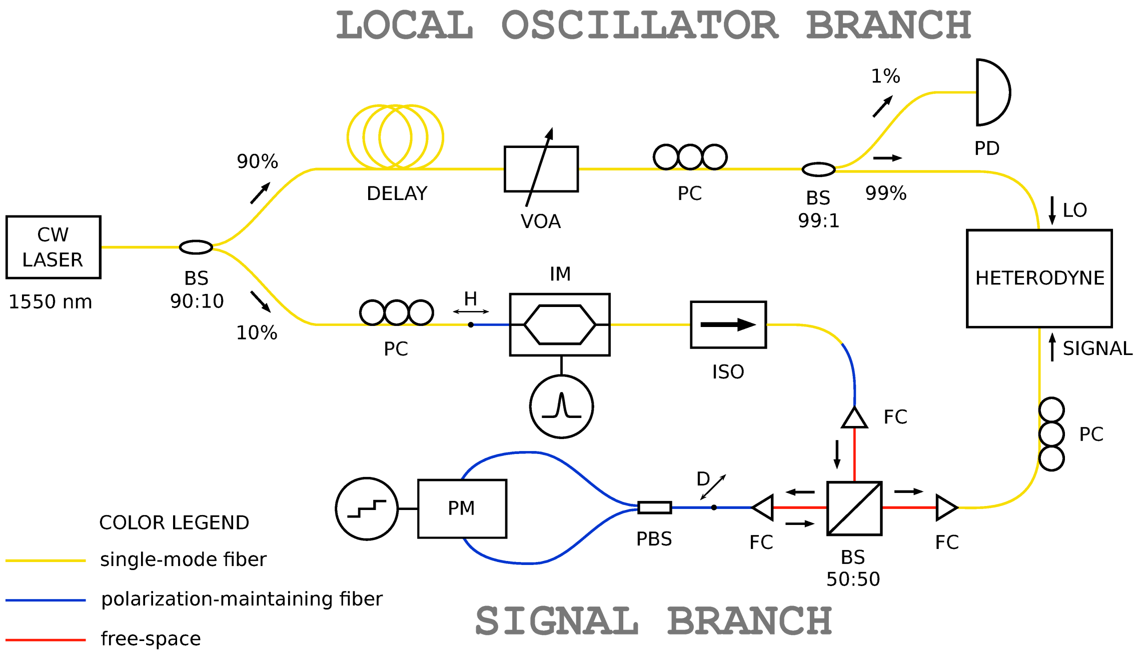


Figure 3.17: Schematic of the experimental setup. The abbreviations indicate: CW LASER = continuous-wave laser, ISO = isolator, BS = beam splitter, VOA = variable optical attenuator, PC = polarization controller, PD = photodiode, LO = local oscillator, H = horizontal polarization, IM = intensity modulator, FC = fiber collimator, PBS = polarizing beam splitter, D = diagonal polarization, PM = phase modulator. The yellow parts indicate single-mode fiber, the blue parts indicate polarization-maintaining fiber, and the red parts free-space.

3.5 Results

3.5.1 Calibration

The relation between the variance in volts units and in shot-noise units is:

$$\sigma^2_{q,p} = \frac{\sigma^2_{V_{p,q}}}{k_{p,q}P_{\mathrm{LO}}} \tag{3.16}$$

where $\sigma_{q,p}$ is the variance in shot-noise units, $\sigma_{V_{p,q}}$ is the variance in volt units, P_{LO} is the power of the local oscillator and k is an unknown constant. During the calibration phase the vacuum is injected in the signal port of the heterodyne, while in the LO port the optical power P_{LO} is made to vary from 0 to the working power. Different values of P_{LO} are recorded as a function of the variance of the electrical signal σ^2_V. From a linear fit for both p and q quadrature we obtain:

$$\sigma^2_{V_{q,p}} = m_{q,p}P_{\mathrm{LO}} + c_{q,p} \tag{3.17}$$

By convection, the theoretical quadrature variance in shot-noise units for a pure vacuum state is $\sigma^2_{q,p} = \frac{1}{2}$. Then using Eqs. (3.16) and (3.17):

$$\sigma^2_{q,p} = \frac{1}{2} \overset{(3.16)}{=} \frac{\sigma^2_{V_{p,q}}}{k_{p,q}P_{\mathrm{LO}}} \overset{(3.17)}{=} \frac{m_{q,p}\cancel{P_{\mathrm{LO}}} + \overbrace{c_{q,p}}^{=0}}{k_{p,q}\cancel{P_{\mathrm{LO}}}} = \frac{m_{q,p}}{k_{p,q}} \tag{3.18}$$

where $c_{q,p} = 0$ because we are considering an ideal condition without electronic noise.

$$\Rightarrow k_{p,q} = 2m_{q,p} \tag{3.19}$$

But in a real experiment $c_{q,p} \neq 0$ and then considering a vacuum input state and a P_{LO} power of the local oscillator, the measured variances in shot-noise units are given by

$$\sigma^2_{q,p} \overset{(3.16)}{=} \frac{\sigma^2_{V_{p,q}}}{kP_{\mathrm{LO}}} \overset{(3.17)}{=} \frac{m_{q,p}P_{\mathrm{LO}} + c_{q,p}}{kP_{\mathrm{LO}}} \overset{(3.19)}{=} \frac{m_{q,p}P_{\mathrm{LO}} + c_{q,p}}{2m_{q,p}P_{\mathrm{LO}}} = \frac{1}{2} + \frac{c_{q,p}}{2m_{q,p}P_{\mathrm{LO}}} \tag{3.20}$$

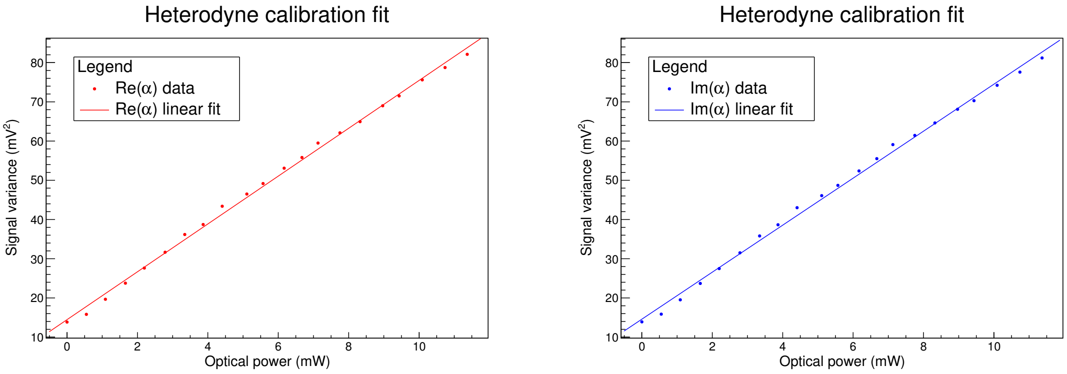
Hence the electrical noise, such as the noise of detectors, produces an increase in the variance of the ideal case as expected.

Before the heterodyne detector, the power of the LO is changed with a variable optical attenuator (VOA) and 1% of this power is measured using a BS 99:1 and a photodiode for the calibration phase. For each P_{LO} value, the signal of the heterodyne detector is recorded and the variance $\sigma_{V_{p,q}}$ is estimated. After the heterodyne detection, an oscilloscope acquires the two signals proportional to the quadrature p and q. The oscilloscope resolution can be converted to the equivalent resolution in the phase space using the results of the calibration fit. [73]

If $|\alpha\rangle$ is the coherent state with complex amplitude α, the output of the heterodyne measurement is represented by:

$$q = \Re\mathrm{e}(\alpha), \quad p = \Im\mathrm{m}(\alpha) \tag{3.21}$$

Figure 3.18 shows the calibration fits obtained for p and q of the heterodyne detector used in the experiment, while Table 3.2 shows the results of the fits.



(a) **(b)**

Figure 3.18: The graph shows the linear dependence of the signal quadrature σ_V^2 as a function of the LO power.

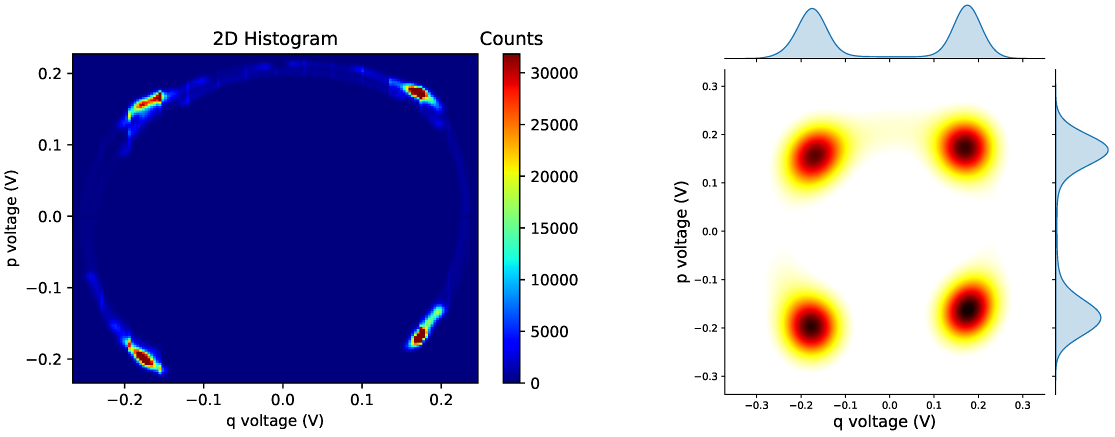
Calibration linear fit result		
	c [mV^2]	m [mV^2/ mW]
q	14.5 ± 0.5	6.10 ± 0.07
p	14.6 ± 0.5	5.99 ± 0.07

Table 3.2: Results of the calibration linear fit for the data shown in Figure 3.18.

3.5.2 Final results

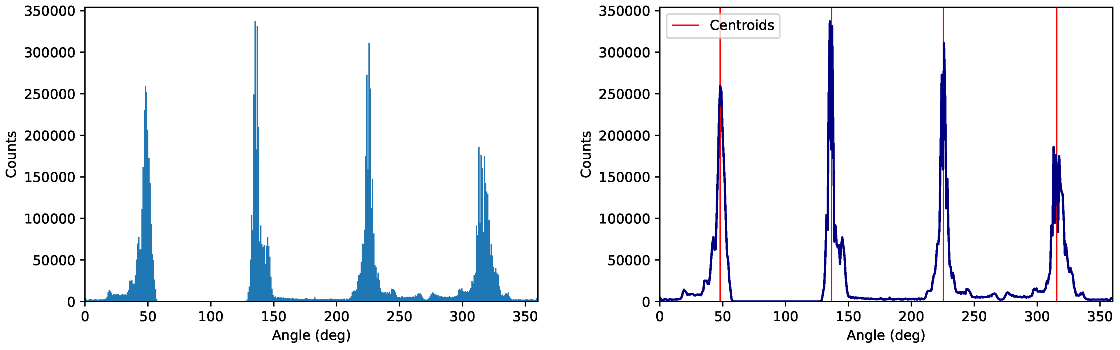
One of the problems initially encountered during the first tests of the experimental setup was that the coherent states rotated so quickly in the phase space that they did not allow in practice to be able to acquire satisfactory measurements. One reason was that the laser's coherence length limits were being reached. In fact, by reproducing approximately the same optical path length in the two arms of the setup (LO and signal), the rotation speed has been significantly reduced, allowing measurements to be acquired. Another reason why rotation occurs in phase space is due to drift caused by optical fibers and phase modulators. For example, the variation of temperatures and the mechanical stresses of SMF fibers induce birefringence. In fact, it was possible to notice that by applying pressure to the SMF optical fibers of the experimental setup, the rotation in the phase space greatly increased until it decreased once the mechanical pressure was removed. Another reason why rotation in phase space can occur is due to the phase stability of the laser. From this it can be concluded that to run QKD CV protocols it is important to have a highly consistent and stable laser along with a fixed and low drift setup. If the rotation in the phase space is not too fast, a post-processing data analysis allows you to rotate the reference system in order to compensate for these effects.

In the datasets obtained with heterodyne and plotted in Figure 3.19 and 3.21, four states were generated and the angle between them was modulated so that it was about 90°. Phase modulation was obtained with the modified iPOGNAC phase modulator. This was possible by carefully controlling the electrical signal sent to the phase modulator via the Pulse/Arbitrary Waveform Generator SIGLENT SDG6032X. Figure 3.23 shows a plot of this electrical signal. Figure 3.20 and 3.22 show the histograms of the angles in polar coordinates of the phase space. An estimate of the centroids of the peaks of the angles was performed and the results are reported in Table 3.3.



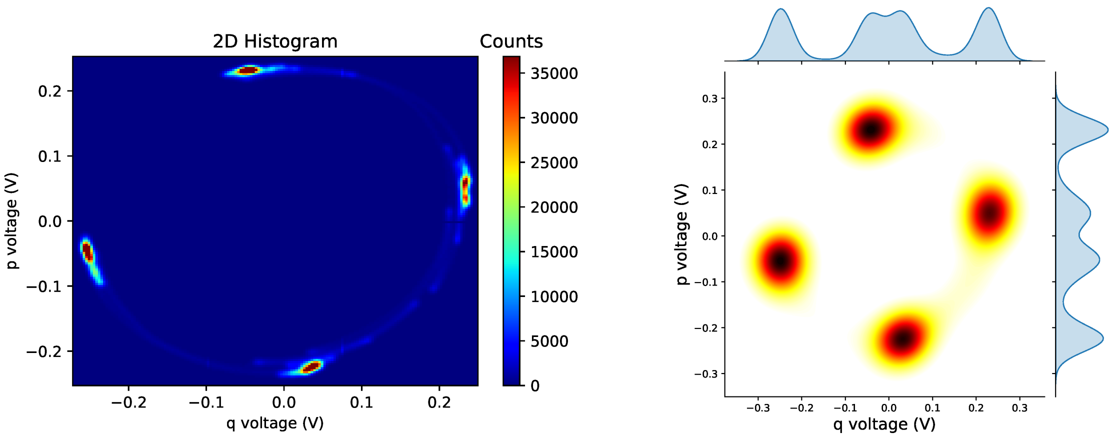
(a) (b)

Figure 3.19: Two-dimensional histogram on the left and Kernel Distribution Estimation (KDE) plot on the right in the phase space obtained from measurements with the heterodyne detector.



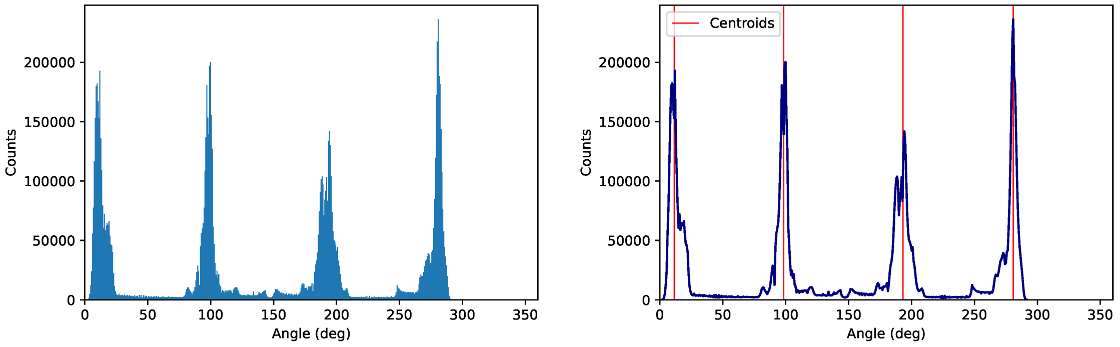
(a) (b)

Figure 3.20: Histogram of the angles in polar coordinates in the phase space of the sample of Figure 3.19. In the figure on the right, the red lines corresponding to the centroids of the peaks.



(a) (b)

Figure 3.21: Two-dimensional histogram on the left and Kernel Distribution Estimation (KDE) plot on the right in the phase space obtained from measurements with the heterodyne detector.



(a)

(b)

Figure 3.22: Histogram of the angles in polar coordinates in the phase space of the sample of Figure 3.21. In the figure on the right, the red lines corresponding to the centroids of the peaks.

Angles between the centroids of the peaks				
Dataset	$\Delta\theta_1$ [°]	$\Delta\theta_2$ [°]	$\Delta\theta_3$ [°]	$\Delta\theta_4$ [°]
1	88.5	88.9	90.0	92.6
2	87.1	94.7	87.7	90.6

Table 3.3: Angles between the centroids of the peaks in Figure 3.20 and 3.22. The angles corresponding to the centroids were calculated with a weighted average around the maximum of the peaks.

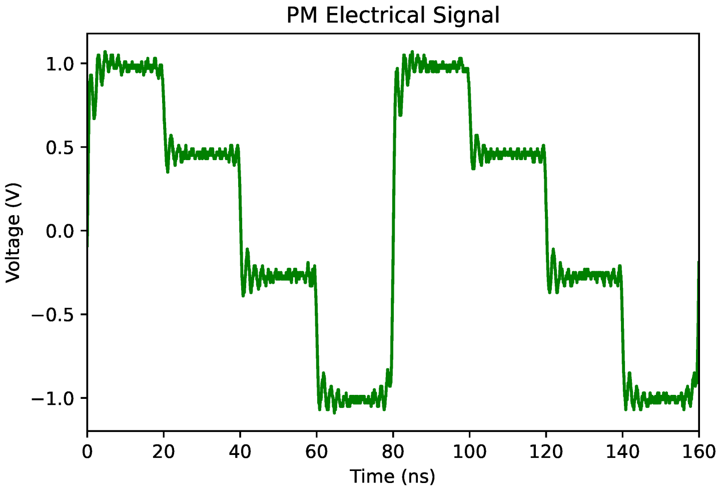


Figure 3.23: Electric signal sent to the phase modulator in the datasets of Figure 3.19 and 3.21. The amplitude of the electric signal is actually not the real one used because it was necessary to attenuate it in order not to damage the oscilloscope during the measurements.

In the samples obtained and shown in Figure 3.25 and 3.24 there are eight states arranged on two different radii in the phase space. In addition to the phase modulation, which allows to control the angle in the phase space, an intensity modulation has been applied with the Mach-Zehnder modulator, which allows to control the radius. The electrical signal of the IM was also generated by the Siglent signal generator, so that it was narrower than the one sent to the PM, and it was also necessary to synchronize them accurately with each other.

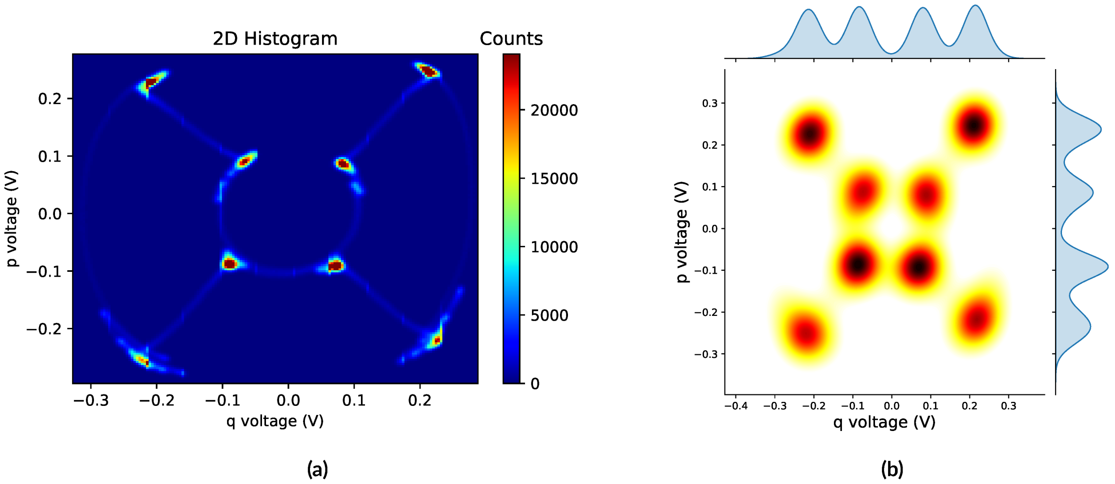


Figure 3.24: Two-dimensional histogram on the left and Kernel Distribution Estimation (KDE) plot on the right in the phase space obtained from measurements with the heterodyne detector.

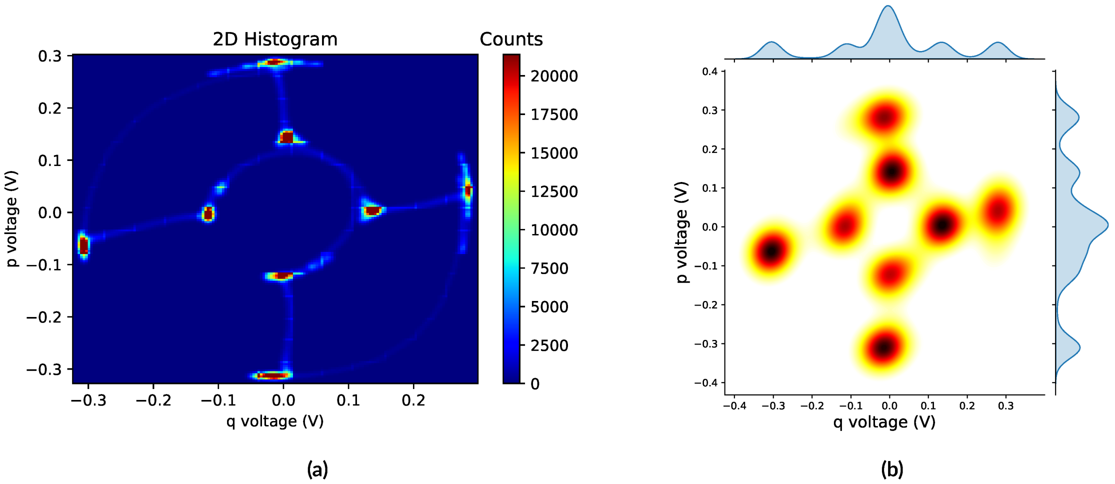


Figure 3.25: Two-dimensional histogram on the left and Kernel Distribution Estimation (KDE) plot on the right in the phase space obtained from measurements with the heterodyne detector.

Looking at the graphs you can see trails that join the signals corresponding to the different states, the reason is due to imperfections in the electrical modulation signals of the phase modulator, such as the slope of the rising and falling edge of the signals. In fact, by improving these signals, it was possible to reduce the presence of contrails and it is possible to note that between some states the contrails are not present (it can also be seen from the histograms of the angles) because there is no passage of the electrical signal between these states.

The last two samples shown in Figure 3.26 contain 2 and 3 states in the phase space obtained by modulating only the PM. This time, however, the Siglent signal generator was not used but the FPGA (ZedBoard by Avnet). The latter is equipped with several channels that can generate electrical signals of 50 MHZ square waves. Two channels of the FPGA have been added with an adder and the FPGA has been programmed so that different signal amplitudes for the PM can be configured via software activating or deactivating two different channels. No signal corresponds to a voltage of 0 V, only one active channel has an amplitude of $V_\pi/2$ and the sum of two active channels will have an amplitude of V_π for the PM. To reach the voltage of V_π the adder, however, it was necessary to use a voltage amplifier.

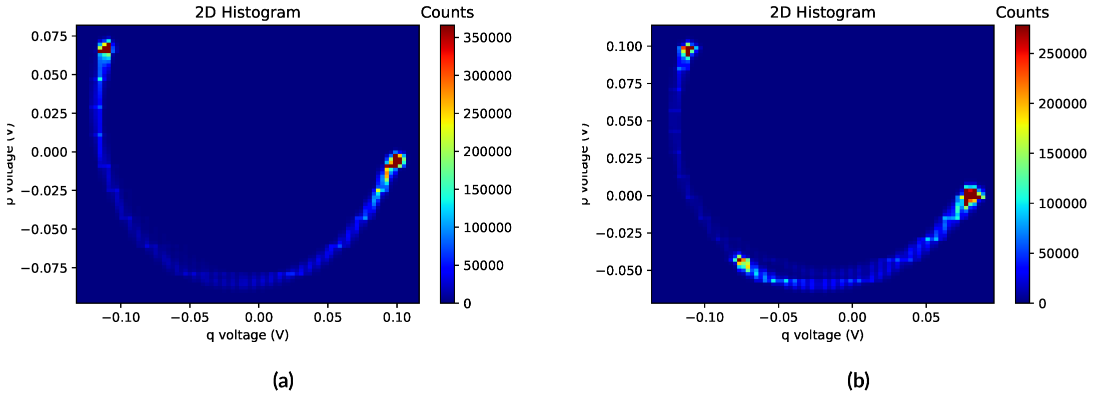


Figure 3.26: Two-dimensional histogram obtained from measurements with the heterodyne detector. The electrical signal for the PM was generated by the FPGA.

In summary, using the experimental setup of Figure 3.17, which has a modified iPOGNAC version inside, it has been shown that it is possible to modulate the phase of the electric field of a coherent light on the quadrature axes. In this way it is possible to generate: 2, 3 and 4 coherent states, as required by the BPSK, 3-PSK and QPSK protocols (Figure 3.26 and 3.19). Similarly, it has been shown that it is possible to use an IM within the setup that allows modulating the amplitude of a coherent light onto the quadrature axes, as required by the QAM protocols (Figure 3.24). The experimental tests were actually all performed with classical light. For a QKD-CV protocol it is necessary to move to the quantum case by attenuating the signal, but the working principle of the tested devices remains the same. So in conclusion, it has been shown that the modified iPOGNAC can be used in a setup as a CV transmitter.

4
Conclusions

In the first part of this thesis work, a QKD system with the three-state and one-decoy protocol was created, characterized and tested. This protocol exploits both the polarization state of the light and its intensity: the first serves to encode the information, the second to ensure greater safety. The QKD system has been specifically developed at a wavelength of 1310 nm so that it can be used to investigate the feasibility of coexisting the classical signal at the wavelength of 1550 nm with the quantum signal at 1310 nm in the same optic fiber. The realized QKD system has provided good performance with an average QBER of (1.1 ± 0.8) % in the key-generation basis and of (0.9 ± 0.9) % in the check basis during 16 h of acquisition, demonstrating that it is possible to use it to do quantum cryptography.

In the second part, the possibility of using a single QKD system for both discrete and continuous variable protocols was investigated. For this reason, a setup has been designed and implemented that can work for both types of protocol. The setup, which we know to work in the DV case, has demonstrated the ability to modulate the phase and the amplitude of the electric field of a coherent light onto the quadrature axes, as required by the CV protocols. It should be emphasized that in reality the system was tested at a classical and non-quantum level, so it would have been necessary to significantly attenuate the signal. However, the system that works in the classical case has no reason not to work even in the quantum case.

One of the goals of quantum communication is to one day be able to build a quantum network on a global scale. The integration of classical and quantum communication in the same physical channel would help achieve this goal. Furthermore, communication via QKD has experimental physical limits of communication rate and distance. These limits depend on the propagation medium (optical fiber or free-space) and the different QKD protocols. The integration of different means of propagation and different types of protocols would allow the creation of a global network suitable for different needs and with optimized performance. The realization of a QKD system that uses different protocols based on the distance of propagation could be a step forward in this direction.

References

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

[2] M. Avesani, "Security of Quantum Protocols certified by the dimension of the Hilbert space," in *Master's degree thesis, Università degli Studi di Padova*, 2015-2016.

[3] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in *2014 international conference on electronics, communication and computational engineering (ICECCE)*. IEEE, 2014, pp. 83–93.

[4] F. Piper and S. Murphy, *Cryptography: A very short introduction*. Oxford Paperbacks, 2002, vol. 68.

[5] C. Bauer, *Secret history: The story of cryptology*. CRC Press, 2021.

[6] F. S. Russell, *Information gathering in classical Greece*. University of Michigan Press, 1999.

[7] D. Bacco, "Comunicazione quantistica finalizzata alla realizzazione di chiavi in spazio libero," in *Tesi di Laurea Magistrale, Università degli Studi di Padova*, 2010-2011.

[8] Wikimedia Commons, "Skytale," Accessed 2022-04-22. [Online]. Available: https://commons.wikimedia.org/wiki/File:Skytale.png

[9] ——, "Caesar cipher left shift of 3," Accessed 2022-04-25. [Online]. Available: https://commons.wikimedia.org/wiki/File:Caesar_cipher_left_shift_of_3.svg

[10] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information: Basic Concepts*. World Scientific, 2004, vol. I.

[11] D. Kahn, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster, 1996.

[12] Wikimedia Commons, "Enigma-rotor-stack," Accessed 2022-04-23. [Online]. Available: https://commons.wikimedia.org/wiki/File:Enigma-rotor-stack.jpg

[13] Y. Piétri, "Quantum cryptography," in *Master's degree thesis, Imperial College London*, 2020.

[14] L. Zeffiro, "Tecniche di decifrazione e modelli matematici della macchina enigma," in *Tesi di Laurea, Università di Bologna*, 2018-2019.

[15] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, p. 1301, 2009.

[16] nerdcoding.org, "2018-12-16-symmetric-cryptography," Accessed 2022-04-29. [Online]. Available: https://nerdcoding.org/post/2018/2018-12-16-tls-x509/

[17] V. Makarov, "Quantum cryptography and quantum cryptanalysis," in *PhD thesis, Norwegian University of Science and Technology*, 2007.

[18] M. Sartore, "Analisi delle prestazioni della quantum key distribution con dispositivi non-ideali," in *Tesi di Laurea, Università degli Studi di Padova*, 2019-2020.

[19] R. Sherwood, "Practical implications of public key infrastructure for identity professionals," *IDPro Body of Knowledge*, vol. 1, no. 6, 2021.

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[21] C. Kollmitzer and M. Pivk, *Applied quantum cryptography*. Springer, 2010, vol. 797.

[22] M. Sabatini, "Realizzazione di una sorgente di stati per distribuzione quantistica di chiave," in *Tesi di Laurea, Università degli Studi di Padova*, 2018-2019.

[23] H. Lo and Y. Zhao, "Quantum Cryptography," *arXiv preprint arXiv:0803.2507*, 2008.

[24] Wikimedia Commons, "Skytale," Accessed 2022-04-22. [Online]. Available: https://commons.wikimedia.org/wiki/File:Poincare-sphere_arrows.svg

[25] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *arXiv preprint arXiv:1804.00200*, 2018.

[26] H. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, no. 23, p. 230504, 2005.

[27] D. Bacco, "Quantum communications between earth and space," in *PhD thesis, Università degli Studi di Padova*, 2015.

[28] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based qkd," *Applied Physics Letters*, vol. 112, no. 5, p. 051108, 2018.

[29] B. E. A. Saleh and M. C. Teich, *Fundamentals of photonics*. John Wiley & Sons, 2019.

[30] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, no. 6, p. 063027, 2010.

[31] P. Mazzoldi, M. Nigro, and C. Voci, *Fisica: Elettromagnetismo - Onde*. EdiSES, 1998, vol. 2.

[32] R. Paschotta, "article on *Birefringence* in the Encyclopedia of Laser Physics and Technology," Accessed 2022-08-14. [Online]. Available: https://www.rp-photonics.com/birefringence.html

[33] ——, "article on *Electro-optic effect* in the Encyclopedia of Laser Physics and Technology," Accessed 2022-08-14. [Online]. Available: https://www.rp-photonics.com/electro_optic_effect.html

[34] ——, "article on *Pockels effect* in the Encyclopedia of Laser Physics and Technology," Accessed 2022-08-14. [Online]. Available: https://www.rp-photonics.com/pockels_effect.html

[35] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications*. Oxford University Press, 2007.

[36] V. Degiorgio and I. Cristiani, *Note di fotonica*. Springer, 2016.

[37] R. Paschotta, "article on *Electro-optic Modulators* in the Encyclopedia of Laser Physics and Technology," Accessed 2022-08-14. [Online]. Available: https://www.rp-photonics.com/electro_optic_modulators.html

[38] ——, "article on *Pockels Cells* in the Encyclopedia of Laser Physics and Technology," Accessed 2022-08-14. [Online]. Available: https://www.rp-photonics.com/pockels_cells.html

[39] F. Träger, *Springer Handbook of Lasers and Optics*. Springer-Verlag, 2012.

[40] M. Avesani, C. Agnesi, A. Stanco, G. Vallone, and P. Villoresi, "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," *Optics Letters*, vol. 45, no. 17, pp. 4706–4709, 2020.

[41] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "All-fiber self-compensating polarization encoder for quantum key distribution," *Optics letters*, vol. 44, no. 10, pp. 2398–2401, 2019.

[42] G. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, "Patterning-effect-free intensity modulator for secure decoy-state quantum key distribution," *arXiv preprint arXiv:1807.07414*, 2018.

[43] M. Avesani, G. Foletto, M. Padovan, L. Calderaro, C. Agnesi, E. Bazzani, F. Berra, T. Bertapelle, F. Picciariello, F. B. Santagiustina *et al.*, "Deployment-ready quantum key distribution over a classical network infrastructure in padua," *Journal of Lightwave Technology*, vol. 40, no. 6, pp. 1658–1663, 2022.

[44] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

[45] P. V. Trinh, T. V. Pham, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Performance of free-space qkd systems using sim/bpsk and dual-threshold/direct-detection," in *2016 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2016, pp. 1–6.

[46] R. Asif and W. J. Buchanan, "Quantum-to-the-home: achieving gbits/s secure key rates via commercial off-the-shelf telecommunication equipment," *Security and Communication Networks*, vol. 2017, 2017.

[47] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[48] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[49] Wikimedia Commons, "Bpsk gray coded," Accessed 2022-09-03. [Online]. Available: https://it.wikiversity.org/wiki/File:BPSK_Gray_Coded.svg

[50] ——, "Qpsk gray coded," Accessed 2022-09-03. [Online]. Available: https://commons.wikimedia.org/wiki/File:QPSK_Gray_Coded.svg

[51] ——, "8psk gray coded," Accessed 2022-09-03. [Online]. Available: https://commons.wikimedia.org/wiki/File:8PSK_Gray_Coded.svg

[52] ——, "Circular 8qam," Accessed 2022-09-03. [Online]. Available: https://en.m.wikipedia.org/wiki/File%3ACircular_8QAM.svg

[53] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of gaussian keys using squeezed states," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[54] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," *Physical review letters*, vol. 109, no. 10, p. 100502, 2012.

[55] InfiniQuant, "Tutorial: Continuous-variable quantum communication," Accessed 2022-09-02. [Online]. Available: http://infiniquant.com/tutorial-continuous-variable-quantum-communication/

[56] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.

[57] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Physical review letters*, vol. 125, no. 1, p. 010502, 2020.

[58] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, 2021.

[59] iXblue, "Introduction to ixblue mach-zehnder modulators bias controllers," Accessed 2022-08-16. [Online]. Available: https://photonics.ixblue.com/sites/default/files/2018-07/Introduction_To_Photline_MBC_2016_1.pdf

[60] Thorlabs, "Lithium niobate electro-optic modulators, fiber-coupled (1260 nm - 1625 nm)," Accessed 2022-08-28. [Online]. Available: https://www.optcore.net/wdm-tutorial/

[61] K. J. Åström and T. Hägglund, *PID Controllers: Theory, Design, and Tuning*. Instrument Society of America, 1995.

[62] P. Bolzern, R. Scattolini, and S. N., *Fondamenti di controlli automatici*. McGraw-Hill, 2004.

[63] Wikimedia Commons, "Tia simple," Accessed 2022-08-14. [Online]. Available: https://commons.wikimedia.org/wiki/File:TIA_simple.svg

[64] ——, "Op-amp non-inverting amplifier," Accessed 2022-08-14. [Online]. Available: https://it.wikipedia.org/wiki/File:Op-Amp_Non-Inverting_Amplifier.svg

[65] *Low Noise Dual SupplyInverting Charge Pump*, Analog Devices, 2021, rev. B. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/ltc3260.pdf

[66] Wikimedia Commons, "Charge pump," Accessed 2022-09-04. [Online]. Available: https://en.wikipedia.org/wiki/Charge_pump

[67] ——, "Lm317 to-220," Accessed 2022-08-17. [Online]. Available: https://en.wikipedia.org/wiki/File:LM317_TO-220.svg

[68] ——, "Lm317 typical schematic," Accessed 2022-08-17. [Online]. Available: https://commons.wikimedia.org/wiki/File:LM317_typical_schematic.svg

[69] *1.2 V to 37 V adjustable voltage regulators*, STMicroelectronics, 2022, version 22.0. [Online]. Available: https://www.st.com/resource/en/datasheet/lm317.pdf

[70] Wikimedia Commons, "Lm317," Accessed 2022-08-17. [Online]. Available: https://en.wikipedia.org/wiki/LM317

[71] Thorlabs, "10 ghz lithium niobate modulators with internal photodetector," Accessed 2022-09-03. [Online]. Available: https://www.thorlabs.com/drawings/831efc4057b79aa1-1B8B14EF-0A6B-B47B-995335E44E0BD31E/LN81S-FC-SpecSheet.pdf

[72] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Advances in optics and photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[73] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 gbps," *Nature communications*, vol. 9, no. 1, pp. 1–7, 2018.