

Master's Thesis

Master's Degree in Telecommunication
Engineering

Quantum Cryptography: an Overview
from Physics Foundations to Engineering
Development

Author: Alfonso Tello Castillo

Supervisor: Alejandro Carballar Rincón

Department of Electronic Engineering
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019



Master's Thesis
Master's Degree in Telecommunication Engineering

Quantum Cryptography: an Overview from Physics Foundations to Engineering Development

Author:
Alfonso Tello Castillo

Supervisor:
Alejandro Carballar Rincón
Professor

Department of Electronic Engineering
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019

Master's Thesis

: Quantum Cryptography: an Overview from Physics Foundations to Engineering Development

Author: Alfonso Tello Castillo

Supervisor: Alejandro Carballar Rincón

El tribunal nombrado para juzgar el trabajo arriba indicado, compuesto por los siguientes profesores:

Presidente:

Vocal/es:

Secretario:

acuerdan otorgarle la calificación de:

El Secretario del Tribunal

Fecha:

Acknowledgements

Completing this dissertation has been a daily effort for four months. However, it would have been impossible without the background and the skills developed during my education at the University of Seville. A long (and often tough) journey, which now concludes with a rewarding feeling.

Although this dissertation is a direct result of my work, many people have contributed to its finalization. Therefore, I would like to thank my family, because of all the efforts they made so that I could study at the university the degree I wanted. Also, to my classmates and closer friends, without their help this journey would have been much longer. Finally, I would like to thank all the professors that spent their time on teaching us, their dedication and contribution to the development of society is not often recognized as it should be. Special thanks to Prof. Juan José Murillo Fuentes, without his help this project would have not make sense, to Prof. Alberto Casado Rodríguez, who has spent his time in helping me disinterestedly, and to my supervisor, Prof. Alejandro Carballar Rincón, because of his patience, his guidance and all the time he spent in this Master's Thesis.

Alfonso Tello Castillo
Sevilla, 2019

Resumen

La criptografía cuántica es un campo relativamente nuevo (empezó a desarrollarse en 1984), que parece estar dando sus últimos pasos para poder llegar a ser comercializable, convirtiéndose, de esta forma, en la primera tecnología directamente cuántica que lo consiga. La motivación detrás de ella no es pequeña, ya que permitirá codificar un mensaje de forma absolutamente segura e indescifrable, debido a las leyes de la mecánica cuántica, e independientemente de la potencia de cualquier ordenador, incluso uno cuántico.

En lo que parece un futuro no muy lejano, se comenzarán a necesitar ingenieros que comprendan y sean capaces de trabajar con este tipo de sistemas. Por ello, este trabajo de Fin de Master pretende dar una introducción al desarrollo actual del campo, desde los conceptos físicos que subyacen en ella, hasta el estado del arte de la tecnología. El texto está pensado para personas con una formación base en Ingeniería de las Telecomunicaciones, y con poco o ningún conocimiento en mecánica cuántica. Sin embargo, otros lectores con formación en ingeniería o física también podrán sacar provecho de él. Tras la lectura de éste, el lector podrá tener un buen punto de partida en el campo, desde el que seguir desarrollando su trabajo.

Abstract

Quantum cryptography is a relatively new field (which began to be developed in 1984), which seems to be taking its last steps to become commercially available, thus becoming the first directly quantum technology to do so. The motivation behind it is not small, since it will allow coding a message in an absolutely secure and illegible way, due to the laws of quantum mechanics, and independently of the power of any computer, even a quantum one.

In what seems like a not-too-distant future, engineers who understand and are able to work with such systems will be needed. Therefore, this Master's Thesis aims to give an introduction to the current development of the field, from the physical concepts that underlie it, to the state of the art of the technology. The text is intended for people with a background in Electrical Engineering, and little or no knowledge of quantum mechanics. However, other readers with a background in engineering or physics will also be able to take advantage of it. After reading it, the reader will be able to have a good starting point in the field, from which to continue developing their work.

Contents

<i>Resumen</i>	III
<i>Abstract</i>	V
1 Introduction and motivation	1
2 An Overview of Quantum Mechanics	5
2.1 Formalism of Quantum Mechanics	5
2.1.1 The Schrödinger equation and the wave function	5
2.1.2 Position and momentum operators	6
2.1.3 Hermitian operators	7
Determinate states	7
Generalized statistical interpretation	7
2.1.4 Time-independent Schrödinger equation	8
The harmonic oscillator	8
2.1.5 The uncertainty principle	9
2.1.6 Dirac Notation	9
2.1.7 The density operator	9
2.2 Quantum mechanics in real systems	10
2.2.1 Schrödinger equation in spherical coordinates	10
2.2.2 The Hydrogen atom	11
2.2.3 Angular momentum	12
2.2.4 The spin	13
Triplet vs singlet state	14
Addition of angular momentum	14
2.2.5 Two-particles systems	15
The periodic table	15
2.2.6 Solids	16
2.2.7 Time-independent perturbations	17
The fine structure of the Hydrogen	18
The hyper-fine structure of the Hydrogen	18
2.2.8 Time-dependent perturbations	18
Absorption and stimulated emission	19
Spontaneous emission	19
Transition rates	20
Selection rules	20
3 Quantum Light	23
3.1 Electromagnetic field quantization	23
3.1.1 Photon number state	26
3.1.2 Quadrature operators	27
3.2 Quantum light	28

3.2.1	Coherent states	28
3.2.2	The vacuum field	29
3.2.3	Squeezed states	29
3.2.4	The second order correlation function ($g^{(2)}(\tau)$)	31
3.2.5	Sub-Poissonian light	33
	Degradation of photon statistics by losses	33
	Theory of photodetection	33
	Shot noise and observation of sub-Poissonian light	33
3.2.6	Photon antibunching	34
	Experimental demonstration of photon antibunching	34
4	Quantum Cryptography	35
4.1	An overview of information theory	35
4.1.1	Information	35
4.1.2	Entropy	36
4.1.3	Mutual information	37
	Channel capacity	37
4.1.4	Shannon's theorems	37
4.2	Introduction to quantum cryptography	37
4.2.1	The motivation	38
	Asymmetrical cryptosystems	38
	Symmetrical cryptosystems	38
	Quantum cryptosystems	38
4.2.2	The uncertainty principle on photons	39
4.2.3	Bell's inequality	40
4.3	Protocols	42
4.3.1	The BB84 protocol	42
	No cloning theorem	43
	Intercept-resend strategy	43
4.3.2	The E91 protocol	44
4.3.3	Other protocols	44
	B92	45
	6-states	45
	SARG04	45
	Decoy states	45
	BBM92	45
	COW	46
4.4	Eavesdropping	46
4.4.1	The simplest attack: the intercept-resend strategy	46
4.4.2	Optimal individual attack	47
4.4.3	Other attacks	49
	A Feasible Attack	49
	Trojan horse attack	49
5	Photon Sources	51
5.1	Weak coherent pulses	51
5.2	The simplest source: the single hydrogen atom	52
5.3	Quantum dots	53
5.3.1	Quantum confinement	53
5.3.2	Quantum dots	54
5.3.3	Electrical triggered single photon source	54
5.4	Generation of entangled photons	54
5.5	Parametric down conversion	55
5.6	Current development	55

6	Quantum Channels	57
6.1	Optical Fibers	57
6.1.1	Polarization effects	57
	Geometric phase	58
	Birefringence	58
	Polarization mode dispersion	58
	Polarization dependent losses	59
6.1.2	Chromatic dispersion	59
6.1.3	Codifying information	59
	Polarization coding	59
	Phase coding	59
	Frequency coding	60
6.2	Free space	61
6.2.1	Free space links	61
6.2.2	Satellite QKD	62
7	Receivers	65
7.1	Avalanche photo diodes	65
7.1.1	The p-n junction	65
	The biased p-n junction	67
7.1.2	Photodetectors	68
7.1.3	Avalanche photo diode	69
7.1.4	The Geiger mode	69
	Photon detection efficiency	70
	Dark count rate (DCR)	71
	Afterpulsing	71
	Timing jitter	72
	Crosstalk	72
	Optical crosstalk	72
	Electrical crosstalk	72
	Fill factor	72
7.1.5	Quenching	72
7.1.6	Technologies	73
	Silicon	73
	Germanium	74
	Indium-phosphide-based	74
	Future work	74
7.2	Other receivers	75
7.2.1	Photomultiplier tubes	75
7.2.2	Hybrids	75
7.2.3	Quantum dots	75
7.2.4	Superconductors	75
7.2.5	Up-conversion	76
8	Conclusions	77
	Appendix A A complete BB84 system	79
	<i>List of Figures</i>	81
	<i>List of Tables</i>	83
	<i>Bibliography</i>	85

1 Introduction and motivation

Computer security is one of the most worrisome and conscious issues today. Not only for the average user, increasingly concerned about their privacy, but also for institutions of the importance of governments, armies or banks. These last examples handle a large amount of very sensitive data for the security of a person, a business, and even a country. This concern is not capricious, since history proves that whoever has access to more information is usually victorious or benefited in any type of circumstance.

Therefore, the exchange of information has always been a key factor for any society. However, it has always been susceptible to attack by an unwanted third party, an eavesdropper. That is why, since very early in history, the concept of cryptography arose, that is, encoding the message according to certain rules, so that only someone who knows them will be able to decode it. The encryption of messages is something that already worried even the Romans, who were inventors of some well-known algorithms such as Caesar's cipher (see figure 1.1), in which each letter is substituted for the one that followed it after a displacement of x positions. Such encryption is certainly not very complex to break nowadays, although it is believed that it was enough at a time when most enemies could not even read.

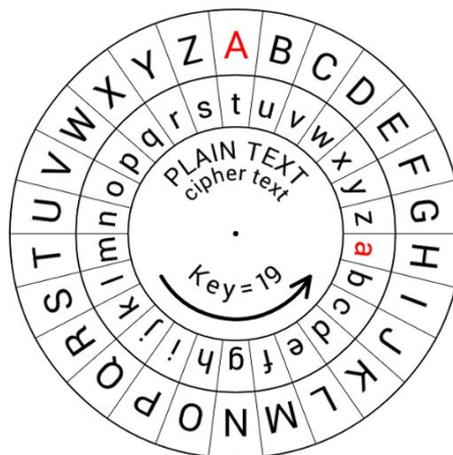


Figure 1.1 The Caesar cipher is named after the roman emperor, who was the first in using it.

The situation became much more complex when electromagnetic signals began to be used for sending messages, since this new technology allowed messages to be exchanged at infinitely higher speeds, although it also allowed an eavesdropper to listen the communication without being detected. Because of this, the field of cryptography grew rapidly into more complex algorithms, a situation that evolved even faster with the raise of computers. Cryptanalysis (the field that studies how to decode encrypted messages) has also evolved

at a similar pace.



Figure 1.2 An artistic representation of the cryptography field [1].

Nowadays, the situation has reached a point where encryption algorithms are, at the moment, extremely difficult to break, with the power of today's computers. An ideal situation, if not for the foreseeable arrival of quantum computers in the near future. The calculation power promised by them will be more than enough to tear down the security of current algorithms in just a few minutes, thus compromising the security and privacy of the entire world. It is in this context that the field of quantum cryptography has emerged, offering the solution to the threat of quantum computers. This new technology takes advantage of the counter-intuitive quantum mechanics laws, in order to develop protocols that guarantee the absolute security (theoretically proven) of an encrypted message. Quantum cryptography has also meant a small revolution in the researching world, as it has rarely required the union of so many fields for the development of a technology. Specifically, this field makes use of knowledge of quantum mechanics, mathematics, computer science, information theory or telecommunications engineering, among others.

As it can be deduced, finding profiles that master all these fields is practically impossible, which means that people from many branches of knowledge have been incorporated into the research of the field. One of these demanded profiles, is the telecommunications engineer, due to for implementing quantum cryptography systems, optical technology is used. However, engineering schools rarely teach the knowledge of the branch that underlies this field, quantum mechanics. It is for this reason that this document intends to start from the beginning of this theory. From this basis, the thesis reaches the current development of the technology, explaining its weakness and future lines of research, which will make quantum cryptography a commercially available technology.

As it is logical, this dissertation does not intend to teach quantum mechanics as any course or book dedicated to it would do. This report only tries to summarize the most important concepts, giving some more detailed explanations of what is considered necessary, in order to justify all the reasoning supported by this theory. On the other hand, it is based on a basic knowledge of optical communications, waves and semiconductor technology. For all the subjects in which the reader needs a more detailed explanation, the work includes some of the classic and most accepted references in each of the treated fields, so that it is possible to continue widening the study.

Specifically, the report includes the following chapters, some of them independent of each other, for others, it is recommended to read previous chapters as it is shown in the figure 1.4.

- Chapter 2. An overview of quantum mechanics: As mentioned above, the most relevant physical and mathematical results, for the purpose of this report, are summarized. It is recommended to be read by any reader who is not familiar with this theory.



Figure 1.3 An artistic representation of quantum mechanics [2].

- Chapter 3. Quantum optics: This chapter summarizes the theory of quantum optics, which applies the knowledge of quantum mechanics and takes it to the field of optics, to understand the experiments made with light when it is studied as a set of photons.
- Chapter 4. Quantum cryptography: It is the most important chapter of the dissertation. It summarizes the ideas that underlie this field, giving a more detailed historical context, and commenting on the most important protocols.
- Chapter 5. Photon sources: Entering into how the implementation of quantum cryptography can be carried out, this chapter discusses the possible sources of light that exist, their weakness and future lines of research.
- Chapter 6. Quantum channel: The channel through which light is sent to carry out the communication is explained. In this case, there are two options: the optical fibers and the free space.
- Chapter 7. Receivers: Finally, there is an introduction to the devices which detect light in these applications. Special emphasis is made on the most promising one (avalanche photodiodes), briefly commenting some other candidates.

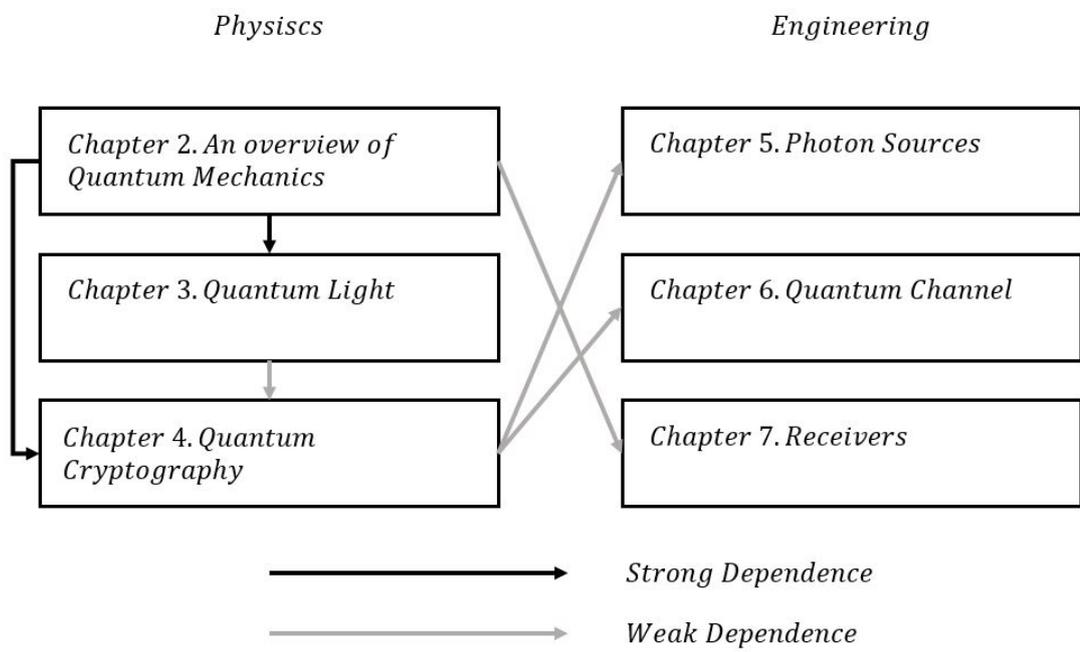


Figure 1.4 The dependences among the chapters of the dissertation.

2 An Overview of Quantum Mechanics

Quantum mechanics is, together with Information theory, the most important theory developed in the 20th century. These two fields are the basis to understand the main topic concerning this dissertation: quantum cryptography. A brief introduction to Information theory can be found in chapter 4. The aim of this chapter is to present a summary on quantum mechanics key concepts. The deduction of most of the formulas falls out the scope of the chapter, however, they can be found in the main references: David J. Griffiths (1982). *Introduction to Quantum Mechanics*, Robert Eisberg (1974). *Quantum Physics* and Mark S. Fox (2006). *Quantum Optics: An Introduction*.

This chapter is organized as follows. The formalism of quantum mechanics is introduced first in section 2.1, in order to understand how systems are represented in this field. Then, some important real systems and their main conclusions are presented in section 2.2.

2.1 Formalism of Quantum Mechanics

In this section the formalism of quantum mechanics is presented. It begins by examining Schrödinger equation. From there, some of the main concepts such as operators, determinate states, the uncertainty principle and the difference between pure and mixed states are explained. The section concludes with the Dirac notation used in quantum mechanics and with an introduction of the density matrix formalism.

2.1.1 The Schrödinger equation and the wave function

Solving a system using quantum mechanics is analogous to classical mechanics. In the latter, Newton's second law, together with some initial conditions, are used to define the system. With them, the position and the velocity of an object are well defined. In the former, Schrödinger equation (equation 2.1) is used instead of Newton's second law, together with initial conditions as well [19].

$$i\hbar \frac{\partial \Psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2 \Psi(x,t)}{\partial x^2} + V\Psi(x,t) \quad (2.1)$$

However, when solving the equation, the greatest difference is that the solution function $\Psi(x,t)$ not only depends on time, but also on position. This gives the magnitudes in quantum mechanics a wave behavior different from classical mechanics (the reason why they are known as wave functions). A wave function (for a fixed x or t) may look like in figure 2.1.

A key question in the theory is how to understand this solution. The answer is provided by Born's statistical interpretation, which says that the probability of an object (usually a particle in quantum mechanics) to have the value x at time t is given by $|\Psi(x,t)|^2$. Therefore,

$$\int_{-\infty}^{\infty} |\Psi(x,t)|^2 dx = 1, \quad (2.2)$$

because the particle must have a value. At this point, one could ask (saying $\Psi(x,t)$ represents the position of a particle) if the position is well defined then, since every time a measurement is made the result is probabilistic.

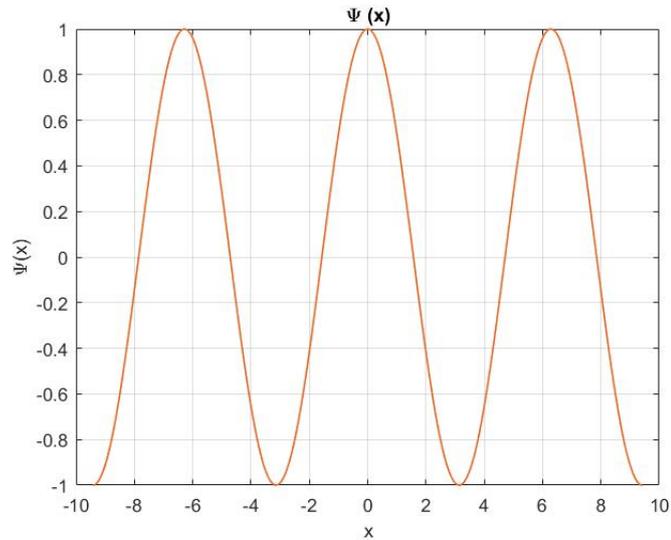


Figure 2.1 An example of a wave function Ψ versus the position x .

Surprisingly, it was discovered that if a measurement is made just after the previous one, the result will be exactly the same. This is why physicists say the wave function collapses, upon a measurement, to the measured point, as in figure 2.2. Therefore, it seems that particles do not have a well defined position until it is measured. Being this the first, and one of the most important counter-intuitive result of quantum mechanics.

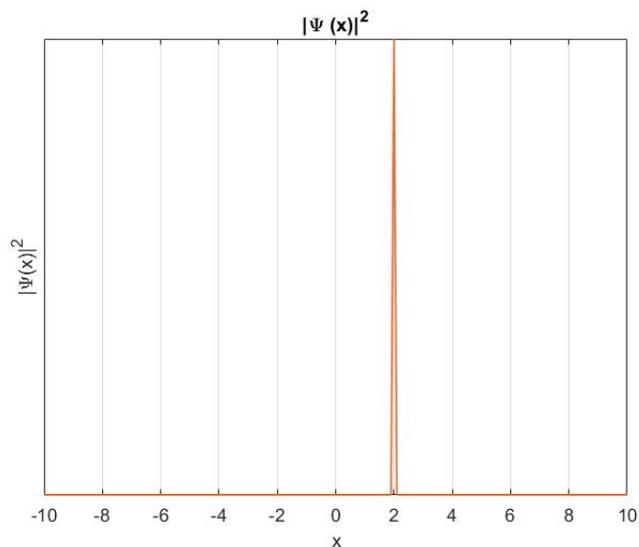


Figure 2.2 A representation of a wave function after it has just collapsed.

2.1.2 Position and momentum operators

In quantum mechanics is not possible, in general, to know a value of a magnitude deterministically. On the other hand, it is possible to calculate the expected value of magnitudes. E.g. the position expected value can be expressed as follows:

$$\langle x \rangle = \int x |\Psi(x,t)|^2 dx = \int \Psi^*(x) \Psi dx \quad (2.3)$$

where x is called the *position operator*. Another important operator is the *momentum operator* which is defined as the position derivative with respect to time [19].

$$\langle p \rangle = m \frac{d\langle x \rangle}{dt} = \int \frac{\hbar}{i} \frac{\partial}{\partial x} |\Psi(x,t)|^2 dx = \int \Psi^* \left(\frac{\hbar}{i} \frac{\partial}{\partial x} \right) \Psi dx \quad (2.4)$$

These are the two most important operators, since every other magnitude can be expressed as a function of them.

In quantum mechanics, to calculate the expected value of a magnitude $Q(x,p)$, p is replaced by its quantum operator $(\hbar/i)(\partial/\partial x)$, then Q is inserted between Ψ^* y Ψ , and integrated:

$$\langle Q(x,p) \rangle = \int \Psi^* Q(x, \frac{\hbar}{i} \frac{\partial}{\partial x}) \Psi dx = \int \Psi^* \hat{Q} \Psi dx \quad (2.5)$$

2.1.3 Hermitian operators

A key idea in quantum mechanics are the hermitian operators, since observables (\hat{Q}) in a system are represented by them. Because observables are real magnitudes, one important property of them is:

$$\langle \hat{Q} \rangle = \langle \hat{Q} \rangle^* \quad (2.6)$$

and therefore,

$$\langle \Psi | \hat{Q} \Psi \rangle = \langle \hat{Q} \Psi | \Psi \rangle \quad (2.7)$$

All the operators that satisfy equation (2.6) are hermitian operators [19]. Position and momentum are examples of hermitian operators, the ladder operator (see section 2.1.4) is an example of a non-hermitian one.

Determinate states

As it was discussed in section 2.1.2, the measurement of a magnitude in a quantum system is probabilistic. However, there are some states which, after conducting on them some measurements, always give the same set of results. These states are called determinate states, and are eigenstates of the operator (measurement) \hat{Q} . The set of results returned are called the eigenvalues of \hat{Q} [19].

$$\hat{Q} \psi_n = q \psi_n \quad (2.8)$$

Where ψ_n is one of the possible eigenstates. An important example is the time-independent Schrödinger equation (see section 2.1.4), which can be expressed also as:

$$\hat{H} \psi_n = E_n \psi_n \quad (2.9)$$

$$\text{where } \hat{H} = -\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + V \quad (2.10)$$

\hat{H} is known as the Hamiltonian of the system. It is the operator used for knowing the energy (E) of a system, which makes sense since it is the sum of the kinetic energy operator ($\frac{p^2}{2m}$) and the potential energy V .

Generalized statistical interpretation

Since ψ_n are a set of eigenstates, they form an orthonormal basis. Therefore, the complete state of a system can be expressed as the sum of these solutions,

$$\Psi(x,t) = \sum_n c_n \psi_n(x) \quad (2.11)$$

Being the coefficient c_n equal to:

$$c_n = \langle \psi_n | \Psi \rangle = \int \psi_n(x)^* \Psi(x,t) dx \quad (2.12)$$

which means that after measuring the observable \hat{Q} of an object with state $\Psi(x,t)$, one of the eigenstates ψ_n will be obtained with probability $|c_n|^2$. Referring back to section 2.1.1, after measuring a system, the wave

function collapses in one of the eigenstates [19]. When a system is found in a state $\Psi(x,t)$ with different eigenstates $\psi_n(x)$, it is said to be in a superposition of states, each of them with probability $|c_n|^2$

2.1.4 Time-independent Schrödinger equation

Let us see now how Schrödinger's equation can be solved. One of the first approximations physicists take, whenever they find a system where the function depends on more than one variable, is the separation of variables, where they look for solutions of the form:

$$\Psi(x,t) = \psi(x)\phi(t) \quad (2.13)$$

Clearly, this is only valid for a subset of solutions. However, it is an important subset, since others more general solutions can be constructed from them. Substituting (2.13) in (2.1), and operating:

$$\frac{d\phi}{dt} = -\frac{iE}{\hbar} \phi \quad (2.14)$$

$$-\frac{\hbar^2}{2m} \frac{d^2\psi}{dx^2} + V\psi = E\psi \quad (2.15)$$

Equation (2.14) is easy to solve, and it has a general solution of the form [19]:

$$\phi(t) = e^{-iEt/\hbar} \quad (2.16)$$

Equation (2.15) is known as **time-independent Schrödinger equation**, and in order to solve it, the potential V must be defined.

The subset of solutions found are known as stationary solutions, because its probability density function is time-independent.

$$\Psi(x,t) = \psi(x)e^{-iEt/\hbar} \quad (2.17)$$

$$|\Psi(x,t)|^2 = \Psi^*\Psi = \psi^*e^{+iEt/\hbar}\psi e^{-iEt/\hbar} = |\psi(x)|^2 \quad (2.18)$$

The harmonic oscillator

The harmonic oscillator is an important result in quantum mechanics, since it will be the model used for the study of the electromagnetic field. Hence, the main results are presented here, although a more detailed resolution can be found in the next chapter.

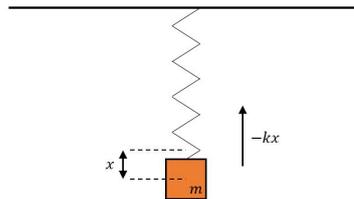


Figure 2.3 The Harmonic oscillator scheme for an object with mass m .

First, the potential V must be defined. This potential is the classic elastic potential,

$$V(x) = \frac{1}{2}m\omega^2x^2 \quad (2.19)$$

Substituting in 2.15,

$$-\frac{\hbar^2}{2m} \frac{d^2\psi}{dx^2} + \frac{1}{2}m\omega^2x^2\psi = E\psi \quad (2.20)$$

The resolution of this equation is complex, and a detailed one can be found in the references [19]. Nevertheless, the solution throws an important conclusion: the system can only be found in a subset of states, each of them represented with ψ_n :

$$\psi_n(x) = A_n (a_+)^n \psi_0(x), \quad \text{with } E_n = (n + \frac{1}{2})\hbar\omega \quad (2.21)$$

$$\psi_0(x) = (\frac{m\omega}{\pi\hbar})^{1/4} e^{-\frac{m\omega}{2\hbar}x^2} \quad (2.22)$$

Being A_n a normalization constant, a_+ the so called *ladder operator* (which will be introduced in the next chapter), m the mass of the object, and ω the angular frequency of the vibration. Each state has a definite energy E_n , and notice how even the ground state ψ_0 has energy no zero.

2.1.5 The uncertainty principle

The uncertainty principle is one of the key results in quantum mechanics, as well as one of the most famous. A detailed deduction of it can be found in the references [19], here only the formulation is presented:

$$\sigma_A^2 \sigma_B^2 \geq (\frac{1}{2i} \langle [\hat{A}, \hat{B}] \rangle)^2 \quad (2.23)$$

$$\text{where } [\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} \quad (2.24)$$

That is to say, for the observables \hat{A} and \hat{B} , if they do not commute ($[\hat{A}, \hat{B}] \neq 0$), the variance in the measurement of both of them will be greater than a certain value. In other words, if they do not commute, knowing both values at the same time will be impossible.

The most famous example are the operators position and momentum, for which $\sigma_x^2 \sigma_p^2 \geq \frac{\hbar}{2}$. It is important to notice that the uncertainty principle does not mean that if someone makes a measurement in the position (for instance), then it will become impossible to measure the momentum, although the object has a definite one. What it really means is that, if someone measures the position, then the momentum is in practice indeterminate, the object will not have a definite one. This is one of the concept behind quantum cryptography, which will be introduced in chapter 4.

2.1.6 Dirac Notation

The Dirac notation is the one generally used in quantum mechanics [16]. This notation simplify the writing but not the system resolution.

The eigenstates are represented as:

$$\psi \equiv |\psi\rangle \quad (2.25)$$

its conjugate:

$$\psi^* \equiv \langle\psi| \quad (2.26)$$

the inner product:

$$\langle\psi|\phi\rangle = \int \psi^* \phi d^3r \quad (2.27)$$

the expected value:

$$\langle\psi|\hat{Q}|\psi\rangle = \int \psi^* \hat{Q} \psi d^3r \quad (2.28)$$

and finally the element of a matrix:

$$\langle n|\hat{Q}|m\rangle = \int \psi_n^* \hat{Q} \psi_m d^3r \quad (2.29)$$

2.1.7 The density operator

So far, quantum mechanics has been presented only using the formalism of state vectors. Yet, another useful formalism is possible using the **density operator** or the **density matrix** [7]. This formalism is equivalent and leads to the same results. However, in some scenarios it is more convenient its use. One of these scenarios

is quantum cryptography, since it is the main topic of this dissertation, it is worth it to introduce the formalism.

If a quantum system is in a state $|\psi_i\rangle$ with probability p_i , the density operator for the system is define as follows:

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (2.30)$$

Suppose that the evolution of the system is described by the unitary operator U . If the system is in the state $|\psi_i\rangle$ with probability p_i , after the evolution the system will be in the state $U|\psi_i\rangle$ with probability p_i [7]. The density operator (or density matrix) is expressed then as:

$$\rho = \sum_i p_i U |\psi_i\rangle \langle \psi_i| U^\dagger = U \rho U^\dagger \quad (2.31)$$

Finally, let us introduce a useful language. If the state of a quantum system is known exactly, it is said to be in a *pure state* (a bunch of particles all in the state $|\psi\rangle$). In this case the state vector would be $|\psi\rangle$ and its density operator would be $\rho = |\psi\rangle \langle \psi|$. Otherwise, ρ is in a mixed state, a mixture of different pure states (a bunch of particles, some in the state $|\psi\rangle$ and other in the state $|\phi\rangle$, for instance). A pure state satisfies $\text{tr}(\rho^2) = 1$ while a mixed state satisfies $\text{tr}(\rho^2) < 1$, where $\text{tr}()$ is the trace of a matrix. It is important not to confuse the difference between a superposition of states and a mixed state. If a particle is in the former, its state is perfectly known, although the specific value of a magnitude may not be deterministic. In the latter case, you do not know whether a particle is in the state $|\psi\rangle$ or in the state $|\phi\rangle$, which can be both a superposition of states.

This formalism is specially useful when describing individual subsystems of a composite quantum system, and it will be used in chapter 4 when studying the limits of the protocol BB84.

2.2 Quantum mechanics in real systems

Once the quantum mechanics formalism has been reviewed, this section will introduce some important real systems, together with their main conclusions. In particular, it will be discussed: the Hydrogen atom, as well as its angular momentum and spin, the two state systems, and finally the chapter will conclude with a discussion of the perturbation theory, a concept related with the absorption and emission processes within the atom.

2.2.1 Schrödinger equation in spherical coordinates

However, it is important to understand first, how to generalize the Schrödinger equation into spherical coordinates. The equation in spherical coordinates reads as follows [19]:

$$i\hbar \frac{\partial \Psi}{\partial t} = -\frac{\hbar^2}{2m} \nabla^2 \Psi + V \Psi \quad (2.32)$$

$$\text{where } \nabla^2 \equiv \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} \quad (2.33)$$

Following the same method than in section 2.1.4, solutions of the form $\Psi_n(x,t) = \psi_n(r,\theta,\phi) e^{-iE_n t/\hbar}$ are studied. Once again, in order to find solutions for ψ , the separation of variables method is used:

$$\psi(r,\theta,\phi) = R(r)Y(\theta,\phi) \quad (2.34)$$

Substituting 2.34 in the time-independent Schrödinger equation in spherical coordinates:

$$-\frac{\hbar^2}{2m} \left[\frac{Y}{r^2} \frac{d}{dr} \left(r^2 \frac{dR}{dr} \right) + \frac{R}{r^2 \sin\theta} \frac{\partial}{\partial \theta} \left(\sin\theta \frac{\partial Y}{\partial \theta} \right) + \frac{R}{r^2 \sin^2\theta} \frac{\partial^2 Y}{\partial \phi^2} \right] + VRY = ERY \quad (2.35)$$

Dividing by RY and multiplying by $-2mr^2/\hbar^2$

$$\left[\frac{1}{R} \frac{d}{dr} \left(r^2 \frac{dR}{dr} \right) - \frac{2mr^2}{\hbar^2} (V(r) - E) \right] + \frac{1}{Y} \left[\frac{1}{\sin\theta} \frac{\partial}{\partial \theta} \left(\sin\theta \frac{\partial Y}{\partial \theta} \right) + \frac{1}{\sin^2\theta} \frac{\partial^2 Y}{\partial \phi^2} \right] = 0 \quad (2.36)$$

The first part of the equation depends only on r while the second one depends on θ and ϕ . The sum of the two arguments gives always zero, meaning both parts of the equations must be constant. Hence:

$$\frac{1}{R} \frac{d}{dr} \left(r^2 \frac{dR}{dr} \right) - \frac{2mr^2}{\hbar^2} [V(r) - E] = l(l+1) \quad (2.37)$$

$$\frac{1}{Y} \left[\frac{1}{\sin\theta} \frac{\partial}{\partial\theta} \left(\sin\theta \frac{\partial Y}{\partial\theta} \right) + \frac{1}{\sin^2\theta} \frac{\partial^2 Y}{\partial\phi^2} \right] = -l(l+1) \quad (2.38)$$

The first equation is known as the radial equation, while the second one is known as the angular equation.

The angular equation is the same for all the systems with a spherical symmetric potential $V(r)$ (which is the common situation), so for most of the cases only the radial equation needs to be solved, since the solution for the angular is well known.

In order to solve the angular equation, the separation of variables technique is again used,

$$Y(\theta, \phi) = \Theta(\theta)\Phi(\phi) \quad (2.39)$$

Using the same reasoning as before, two new independent equations are found:

$$\frac{1}{\Theta} \left[\sin\theta \frac{d}{d\theta} \left(\sin\theta \frac{d\Theta}{d\theta} \right) \right] + l(l+1)\sin^2\theta = m^2 \quad (2.40)$$

$$\frac{1}{\Phi} \frac{d^2\Phi}{d\phi^2} = -m^2 \quad (2.41)$$

It is important to notice how every time the separation of variable technique is used, some constant values are defined (l y m), these constant values are known as quantum numbers, and they will be very important to characterize a system.

The resolution of these two equations is not easy, so here only the final result is presented:

$$Y_l^m(\theta, \phi) = \varepsilon \sqrt{\frac{(2l+1)(l-|m|)!}{4\pi(l+|m|)!}} e^{im\phi} P_l^m(\cos\theta) \quad (2.42)$$

$$l = 0, 1, 2, \dots, N \quad (2.43)$$

$$m = -l, -l+1, \dots, l-1, l \quad (2.44)$$

where P_l^m is the associated Legendre function.

Finally, the radial equation is simplified, and it will be solved for different systems in next sections, after defining $V(r)$. Establishing,

$$u(r) = rR(r) \quad (2.45)$$

and substituting,

$$-\frac{\hbar^2}{2m} \frac{d^2u}{dr^2} + \left[V + \frac{\hbar^2}{2m} \frac{l(l+1)}{r^2} \right] u = Eu \quad (2.46)$$

2.2.2 The Hydrogen atom

The Hydrogen atom model consists in an electron of charge $-e$ orbiting a proton much heavier of charge e . In this model the potential is given by Coulomb's law:

$$V(r) = -\frac{e^2}{4\pi\epsilon_0} \frac{1}{r} \quad (2.47)$$

and the radial equation reads as,

$$-\frac{\hbar^2}{2m} \frac{d^2 u}{dr^2} + \left[-\frac{e^2}{4\pi\epsilon_0 r} + \frac{\hbar^2}{2m} \frac{l(l+1)}{r^2} \right] u = Eu \quad (2.48)$$

Solving this equation is again complex [19], so only the final solution is given. Nevertheless, an important conclusion can be deduced: as usually in quantum mechanics, only certain states are allowed in this system (which are defined by three quantum numbers n , l and m), each of these states has a definite energy E_n :

$$\psi_{nlm}(r, \theta, \phi) = R_{nl}(r) Y_l^m(\theta, \phi) \quad (2.49)$$

$$\text{with, } R_{nl} = \sqrt{\left(\frac{2}{na}\right)^3 \frac{(n-l-1)!}{2n[(n+l)!]^3}} e^{-r/na} \left(\frac{2r}{na}\right)^l [L_{n-l-1}^{2l+1}(2r/na)] \quad (2.50)$$

$$E_n = -\left[\frac{m}{2\hbar^2} \left(\frac{e^2}{4\pi\epsilon_0}\right)^2\right] \frac{1}{n^2}, \quad n = 1, 2, 3, \dots \quad (2.51)$$

Where L_{n-l-1}^{2l+1} is the associated Lagerre polynomial, and ψ_{nlm} is the position wave function of the electron. These equations define the famous Hydrogen orbitals (see figure 2.4) (each state is called here an orbital), which constitute the most accurate model of the atom so far.

The energy of the states depends only on n , this is why it is known as the main quantum number. If an electron is in a stationary state, it will remain there indefinitely, unless a perturbation is introduced in the system (see section 2.2.8). If so happens, a photon will be absorbed or emitted depending on whether the transition is to a more or less energetic state respectively. The wave length of this photon will be proportional with the two states energy gap.

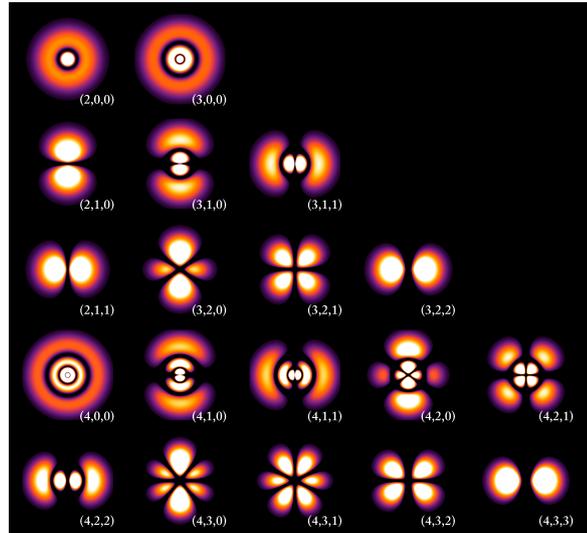


Figure 2.4 A representation of some Hydrogen orbitals in 2D [38].

2.2.3 Angular momentum

In classical physics, energy and angular momentum are the two fundamental quantities which are always conserved in a system. Therefore, it is also interesting to study the latter. Moreover, among the three quantum numbers presented, n is related with the state energy, and it turns out that l and m are related with the angular momentum.

The angular momentum of a particle is defined as,

$$\mathbf{L} = \mathbf{r} \times \mathbf{p} \quad (2.52)$$

with,

$$L_x = yp_z - zp_y, \quad L_y = zp_x - xp_z, \quad L_z = xp_y - yp_x \quad (2.53)$$

In order to get the quantum operators, p must be replaced by its quantum operator. However, these operators do not commute among them, that is to say, it is not possible to know the three components of the angular momentum x , y , and z at the same time. On the other hand, the square of the total angular momentum does commute with these three operators:

$$L^2 \equiv L_x^2 + L_y^2 + L_z^2 \quad (2.54)$$

$$[\hat{L}^2, \hat{L}_x] = 0, \quad [\hat{L}^2, \hat{L}_y] = 0, \quad [\hat{L}^2, \hat{L}_z] = 0 \quad (2.55)$$

It is possible then, knowing the square of the angular momentum and one of its components (usually \hat{L}_z). With a complex deduction which can be found in the references [19], the eigenvalues of these two operators can be deduced without knowing the eigenstates, these are:

$$\hat{L}^2 f_l^m = \hbar^2 l(l+1) f_l^m; \quad L_z f_l^m = \hbar m f_l^m \quad (2.56)$$

$$l = 0, 1/2, 1, 3/2, \dots; \quad m = -l, -l+1, \dots, l-1, l \quad (2.57)$$

being f_l^m an eigenstate.

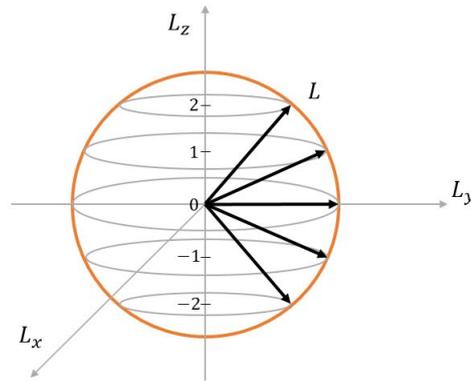


Figure 2.5 The angular momentum states of an atom with the quantum number $l = 2$.

In figure 2.5 there is a representation of the angular momentum of an electron for $l = 2$ and different values of m , where the length of the arrow is $\sqrt{l(l+1)}$. However, this representation is only a method to try to imagine the angular momentum in quantum mechanics since, in order to have a well defined L_z , then L_x and L_y , the three operators should commute among them. Therefore, the representation is far from what happens in reality, although can be helpful in order to understand the results.

If the eigenstates are calculated now, it can be proven that they are indeed the angular equations solutions. This means that ψ is in fact, an eigenstate of three different operators:

$$\hat{H}\psi = E\psi, \quad \hat{L}^2\psi = \hbar^2 l(l+1)\psi, \quad \hat{L}_z\psi = \hbar m\psi \quad (2.58)$$

There is an interesting point here: in section 2.2.1, after solving the angular equation, only the integer values of l were allowed, while here, half-integer values of l are allowed as well. Someone could think that these half-integer values are then just possible mathematically, but they are referring to another property of the particles, the spin, as next section will show.

2.2.4 The spin

The spin S is a magnitude in quantum mechanics with no counterpart in classical physics, although sometime

it is compared with the angular momentum of an object which rotates about its axis [19]. However, this analogy is not accurate again, since a particle is, by definition, a dimensionless point in the space. Therefore, saying a particle rotate about its axis is a vague concept. Suffice is to say that particles have an intrinsic angular momentum apart from the extrinsic one they may have.

The spin theory is analogous to the angular momentum one. Two new operators that commute are defined: \hat{S}^2 y \hat{S}_z ; and the same results appear.

$$\hat{S}^2|\chi\rangle = \hbar^2 s(s+1)|\chi\rangle; \quad \hat{S}_z|\chi\rangle = \hbar m|\chi\rangle \quad (2.59)$$

$$s = 0, 1/2, 1, 3/2, \dots; \quad m = -s, -s+1, \dots, s-1, s \quad (2.60)$$

However, this time, the eigenstates (represented as χ) are not the angular equation solutions, and then the half-integer values of s cannot be discarded. It turns out, that all the particles have an spin associated with the kind of particles they are, and this spin is constant and immutable. E.g. electrons have spin $\frac{1}{2}$, while photons have spin 1. Electron's spin have two different states ($s = \frac{1}{2}$ and $m = \frac{1}{2}$ or $s = \frac{1}{2}$ and $m = -\frac{1}{2}$), which are known as spin-up and spin-down ($|\uparrow\rangle, |\downarrow\rangle$).

Triplet vs singlet state

Suppose there is a system with two electrons, both of them will have spin $+1/2$ or $-1/2$, therefore, there are four possible states for the system:

$$\uparrow\uparrow, \uparrow\downarrow, \downarrow\uparrow, \downarrow\downarrow \quad (2.61)$$

The total spin function for the system must be symmetric or antisymmetric [19] [10] (see section 2.2.5). The only way to have an antisymmetric function is:

$$|\chi\rangle = \frac{1}{\sqrt{2}}(\uparrow\downarrow - \downarrow\uparrow) \quad (2.62)$$

which is called the singlet configuration. For symmetric functions, there are three options:

$$|\chi\rangle = \uparrow\uparrow \quad (2.63)$$

$$|\chi\rangle = \frac{1}{\sqrt{2}}(\uparrow\downarrow + \downarrow\uparrow) \quad (2.64)$$

$$|\chi\rangle = \downarrow\downarrow \quad (2.65)$$

which is called the triplet configuration for obvious reasons. An interesting question would be which is the total spin for these four states. Applying the rules for the addition of angular momentum (see next section), it is found that the quantum numbers for these states are:

$$s = 0, 1 \quad m = -s, \dots, s \quad (2.66)$$

If the spins are in a symmetric configuration, the angular momentum will be added constructively giving a total spin of $s = 1$, with $m = -1, 0$ or 1 for the three different cases. On the other hand, if the spins are in a antisymmetric configuration, the angular momentums will cancel each other giving a total spin of $s = 0$ with $m = 0$.

Addition of angular momentum

If a particle possesses both orbital and spin angular momentum, the total angular momentum j is defined as [10]:

$$j = l + s \quad (2.67)$$

In a particle with both momentum there will be an interaction between them, the so called spin-orbit interaction. If this would not exist, the measures on orbital and angular momentum would be independent. However, that is not the case, and because each one influences the other, two new quantum numbers are used to measure the total angular momentum, j and m_j . j can take any value from $|l - s|$ to $(l + s)$ with integer steps as it is illustrated in figure 2.6, while m_j can take any value from $-j$ to j with integer steps as well.

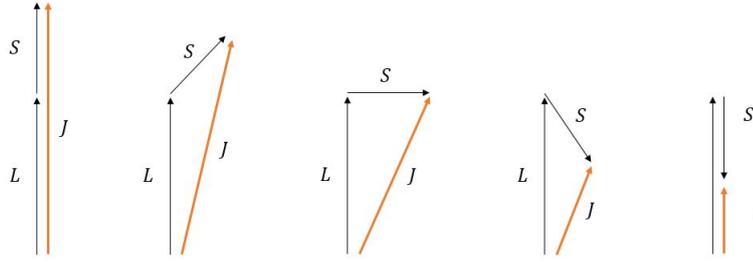


Figure 2.6 Different total angular momentum depending on the sum of l and s .

2.2.5 Two-particles systems

So far, only one-particle systems have been introduced (the Hydrogen atom). In this section the two-particle systems will be considered. Ignoring spin for now, and looking for time-independent solutions, in these systems the particles wave function would be the product of the two wave functions of each particle,

$$\psi(r_1, r_2) = \psi_a(r_1)\psi_b(r_2) \quad (2.68)$$

Nevertheless, this assumes that there is method to distinguish between the two particles, something that is intuitive in classical physics but it is not in quantum mechanics. This is because, if someone measures the system in order to know which is the particle one, then the wave function would collapse, raising doubts as to whether the two had switches places. In quantum mechanics two particles are indistinguishable, so the only thing that can be done in order to define the wave function is not defining which particle is in which state. There are two methods to do so:

$$\psi_{\pm}(r_1, r_2) = A[\psi_a(r_1)\psi_b(r_2) \pm \psi_b(r_1)\psi_a(r_2)] \quad (2.69)$$

If sign $+$ is used, then we talk about bosons. On the other hand, if sign $-$ then we talk about fermions [19]. There is another quite important conclusion here, known as Pauli exclusion principle: two fermions cannot occupy the same state, otherwise there would not be wave function at all. It also turns out, that all fermions have a half-integer spin, while all bosons have an integer spin.

Furthermore, there is a more general method to formulate this problem. If the exchange operator P is defined as:

$$\hat{P}\psi(r_1, r_2) = \psi(r_2, r_1) \quad (2.70)$$

It can be demonstrated that this operator has eigenvalues ± 1 . Moreover, if the two particles are identical then,

$$[\hat{P}, \hat{H}] = 0 \quad (2.71)$$

That is to say, in a system with two identical particles, the solutions to the Schrödinger equation must be symmetric (eigenvalue $+1$) or antisymmetric (eigenvalue -1) under exchange:

$$\psi(r_1, r_2) = \pm \psi(r_2, r_1) \quad (2.72)$$

If they are symmetric then we talk about bosons, if they are antisymmetric we talk about fermions. For an atom, the state of an electron is given by the product of its position wave function (ψ) and its spinor (the wave function for the spin, χ). Therefore, it is the product of this two that must be antisymmetric, since electrons are fermions.

The periodic table

The theory above explains the atom configurations. Each atom has (in general) the same number of electrons than protons, and each of this electron is in a state represented by its quantum numbers. Because electrons are fermions, any of them cannot occupy the same state, so for any state represented by the three quantum numbers n , l and m , there can be only two electrons (one with spin-up and one with spin-down). This is

represented with an standard method [16]: $l = 0$ is called s , $l = 1$ is p , $l = 2$ is d , and after that it continues alphabetically (g, h, i - not j, k , etc). n is represented with a number and m has not any representation, but an exponent is used to indicate how many states are occupied for each nl pair. An example of this configuration could be:

$$(1s)^2(2s)^2(2p)^2 \quad (2.73)$$

which says that there are two electrons in the orbital $(1, 0, 0)$, two in the orbital $(2,0,0)$ and then two in some combination of the orbitals $(2,1,1)$, $(2,1,0)$ and $(2,1,-1)$.

In the example above, there were two electrons with angular momentum $l = 1$, so its total angular momentum L (capital letter because is the total) would be 2, 1 or 0 according to addition of angular momentum rules (see section 2.2.4). Meanwhile, the two electrons in the orbital $(1,0,0)$ are locked in the singlet configuration with total spin 0, as well as the two electrons in the orbital $(2,0,0)$, but the two electrons in $(2p)$ could be in the singlet or triplet configuration so its total spin S could be 1 or 0. Then, as it was explained in section 2.2.4 the total angular momentum $J = (L + S)$, could be 3, 2, 1 or 0. There are some rules, known as Hund's Rules, in order to figure out which of these J would be. The final result is expressed as:

$$^{2S+1}L_J \quad (2.74)$$

2.2.6 Solids

A key property in solids is that, due to its atomic structure, the free electrons within the solid suffer a periodic potential. The shape of that potential is not as important as the fact that it is periodic,

$$V(x+a) = V(x) \quad (2.75)$$

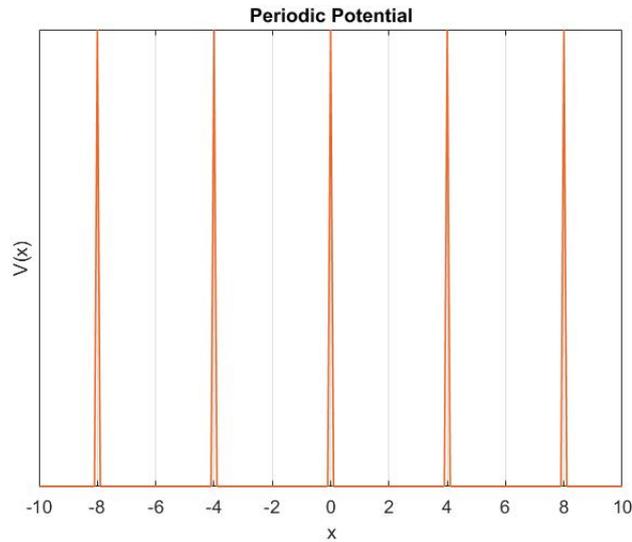


Figure 2.7 An example of a periodic potential suffer by an electron within a solid.

Solving Schrödinger equation [19], the solutions have the following properties,

$$\psi(x+a) = e^{iKa} \psi(x) \quad (2.76)$$

$$|\psi(x+a)|^2 = |\psi(x)|^2 \quad (2.77)$$

If the potential is define as a Dirac comb (see figure2.7):

$$V(x) = \alpha \sum_{j=0}^{N-1} \delta(x - ja) \quad (2.78)$$

The general solution is of the form:

$$\psi(x) = A\sin(kx) + B\cos(kx), \quad (0 < x < a) \quad (2.79)$$

and for the period immediately to the left,

$$\psi(x) = e^{-iKa} [A\sin(kx) + B\cos(kx)], \quad (-a < x < 0) \quad (2.80)$$

Applying boundary conditions (the function must be continuous between periods), we finally find the equation:

$$\cos(Ka) = \cos(ka) + \frac{m\alpha}{\hbar^2 k} \sin(ka) \quad (2.81)$$

This result gives an important conclusion: the function $f(ka) = \cos(ka) + \frac{m\alpha}{\hbar^2 k} \sin(ka)$ takes values outside of the range $(-1, 1)$, for these values, the wave function is not well defined. These "gaps" are the forbidden energies of the solids, and they are separated by the allowed energy bands, creating the well known band structure of solids.

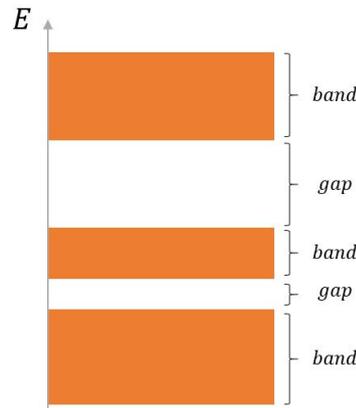


Figure 2.8 The band structure of a solid. Different allowed energy bands, separated each of them by a forbidden band where electrons can not exit.

The outer band in a solid is called the conduction band, while the band just below is called the valance band.

In solids, when the outer band is full, a considerable energy is needed in order to excite an electron to the next band (where it could move through the structure), these solids are called insulators. On the other hand, if the band is only partly filled, the energy needed to excite an electron is much more lower, so the solids are called conductors. Finally, if an insulator is doped with different atoms, this puts some extra atoms in the outer band or create holes in the valance band, and such solids are called semiconductors.

2.2.7 Time-independent perturbations

When Schrödinger equation is solved, it is possible to find some states with the same energy. E.g. the Hydrogen atom has, from $n = 2$, different states ψ_{nlm} with the same energy, since the energy is defined by the quantum number n . These states are called degenerative states, and when a perturbation is introduced in the system, they tend to split their energies [19].

If ψ_a y ψ_b are two solutions with same energy, then ψ is a solution as well:

$$\psi = \alpha\psi_a + \beta\psi_b \quad (2.82)$$

If a perturbation is introduced, the Hamiltonian can be expressed as:

$$H = H^0 + \lambda H' \quad (2.83)$$

where H^0 is the Hamiltonian without the perturbation and H' is the perturbation. The energies and states are approximated as follow:

$$E_n = E_n^0 + \lambda E_n^1 + \lambda^2 E_n^2 + \dots \quad (2.84)$$

$$\psi_n = \psi_n^0 + \lambda \psi_n^1 + \lambda^2 \psi_n^2 + \dots \quad (2.85)$$

E_n^1 is the first-order correction to the n th eigenvalue, and ψ_n^1 is the first order correction to the n th eigenstate. Substituting in the Schrödinger equation and operating, for the first order correction the next equation is found:

$$\alpha \langle \psi_a^0 | H' | \psi_a^0 \rangle + \beta \langle \psi_b^0 | H' | \psi_b^0 \rangle = \alpha E^1 \quad (2.86)$$

defining:

$$W_{ij} \equiv \langle \psi_i^0 | H' | \psi_j^0 \rangle \quad (2.87)$$

the final energy for the first-order correction is:

$$E_{\pm}^1 = \frac{1}{2} [W_{aa} + W_{bb} \pm \sqrt{(W_{aa} - W_{bb})^2 + 4|W_{ab}|^2}] \quad (2.88)$$

Notice this first-order correction has two different values. Hence, after introducing a perturbation in the system the two states will split their energies a certain quantity.

The fine structure of the Hydrogen

The Hamiltonian introduced in section 2.2.2 is not the whole account for the Hydrogen atom, it should be corrected due to two different mechanisms: the relativistic theory and the spin-orbit coupling, these corrections are studied as perturbations [19].

The lowest order relativistic correction to the Hamiltonian is:

$$H'_r = -\frac{p^4}{8m^3c^2} \quad (2.89)$$

and for the spin-orbit interaction,

$$H'_{ls} = -\frac{e^2}{8\pi\epsilon_0} \frac{1}{m^2c^2r^3} \mathbf{S} \cdot \mathbf{L} \quad (2.90)$$

Considering both Hamiltonian and solving the system, the allowed energies are now:

$$E_{nj} = -\frac{13.6eV}{n^2} \left[1 + \frac{\alpha^2}{n^2} \left(\frac{n}{j+1/2} - \frac{3}{4} \right) \right] \quad (2.91)$$

This equation explains the so-called fine structure of the Hydrogen, an important result in high-resolution spectroscopy applications.

The hyper-fine structure of the Hydrogen

There is another even finer correction to the Hydrogen atom due to the magnetic interaction between the electron dipole moments and the nuclear spin. This correction gives an even smaller energy shift between states which defines the hyper-fine structure of the Hydrogen [19].

2.2.8 Time-dependent perturbations

So far, only the stationary states have been introduced. According to the theory, a particle in any of these should remain there indefinitely. However, this is not what how particles behave, on the contrary, they are always promoting to states with more energies, or decaying to states with lower energies. In order to explain

this behavior, the time-dependent perturbations should be introduced [19]. To explain this theory, the simplest system will be considered: a particle within a two states system, with two possible states ψ_a y ψ_b . The system wave function without perturbations is,

$$\Psi(x,t) = c_a \psi_a(x) e^{-iE_a t/\hbar} + c_b \psi_b(x) e^{-iE_b t/\hbar} \quad (2.92)$$

Defining the Hamiltonian as in previous section,

$$H = H^0 + H'(t) \quad (2.93)$$

and solving the Schrödinger equation, the coefficients variation rates \dot{c}_a y \dot{c}_b are calculated:

$$\dot{c}_a = -\frac{i}{\hbar} H'_{ab} e^{-i\omega_0 t} c_b, \quad \dot{c}_b = -\frac{i}{\hbar} H'_{ba} e^{-i\omega_0 t} c_a \quad (2.94)$$

where $H'_{ij} = \langle \psi_i | H' | \psi_j \rangle$. These rates depend on the perturbation introduced so, in order to continue, the perturbation must be defined. Nevertheless, among all possible perturbations, there is a quite interesting one: the sinusoidal perturbations. For this kind, the probability for a particle to promote from state a to state b is:

$$P_{a \rightarrow b}(t) = |c_b(t)|^2 = \frac{|V_{ab}|^2}{\hbar^2} \frac{\sin^2[(\omega_0 - \omega)t/2]}{(\omega_0 - \omega)^2} \quad (2.95)$$

The most important conclusion is that the probability is time-dependent. That is to say, after some time, the probability to find the particle in the same state a becomes greater again. In other words, in order to maximize the probability to promote a particle, the perturbation must be short. Moreover, the closer the perturbation frequency is to the particle natural transition frequency, the more likely is to find the particle in the state b .

Absorption and stimulated emission

If a particle, in a two state system, is in the state ψ_a and the system is illuminated (a sinusoidal perturbation is introduced), the perturbation is defined as [19],

$$H' = -qE_0 \cos(\omega t) z \quad (2.96)$$

The transition probabilities from state a to state b and vice versa are:

$$P_{a \rightarrow b}(t) = P_{b \rightarrow a}(t) = \left(\frac{|p|E_0}{\hbar} \right)^2 \frac{\sin^2[(\omega_0 - \omega)t/2]}{(\omega_0 - \omega)^2} \quad (2.97)$$

This result shows a surprising conclusion: in a sinusoidal perturbation is introduced in a system, not only the electron will absorb some energy (photon) to promote to state b , but also it will emit energy to decay to the state a , furthermore, these two processes have the same probability. These two phenomenon are called absorption and stimulated emission, and the latter was the basis for the development of the laser.

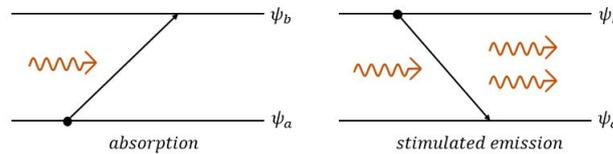


Figure 2.9 An illustration of the absorption and stimulated emission processes.

Spontaneous emission

There is a third mechanism, the spontaneous emission, in which the particle decay from state b to state a emitting a photon without any perturbation [19]. At first sight, this mechanism should not make sense since the state ψ_b is stationary. However, in quantum mechanics the electromagnetic field never has zero energy (see next chapter), so there is always a radiation no matter how cold or dark a room could be. This "vacuum" field is why spontaneous emissions occur (there are always perturbations in the system). That is to say, the

spontaneous emission is actually an stimulated emission due to the "vacuum" electromagnetic field.

Einstein proved that there is a relation between the spontaneous and the stimulated emission rates,

$$A_{21} = \frac{\hbar\omega^3}{\pi^2c^3}B_{21}^w \quad (2.98)$$

where A_{21} is the spontaneous emission rate, and B_{21}^w is the stimulated emission rate.

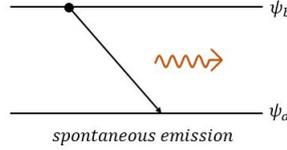


Figure 2.10 An illustration of the spontaneous emission process.

Transition rates

The transition rates from one state to another can be calculated according to Fermi's golden rule [16]:

$$W_{1 \rightarrow 2} = \frac{2\pi}{\hbar} |M_{12}|^2 g(\hbar\omega), \quad (2.99)$$

where $g(\hbar\omega)$ is the density of states, and

$$M_{12} = \langle 2|H'|1 \rangle = \int \psi_2^*(r) H'(r) \psi_1(r) d^3r \quad (2.100)$$

where H' is the perturbation caused by the light. Solving equation 2.99, it is possible to find the solutions for the final transition rates in a two states system:

$$B_{21}^w = \frac{\pi}{3\epsilon_0\hbar^2} |\mu_{12}|^2 \quad (2.101)$$

$$A_{21} = \frac{\omega^3}{3\pi\epsilon_0\hbar c^3} |\mu_{12}|^2 \quad (2.102)$$

where μ_{12} is the electric dipole moment of the transition.

Selection rules

In a system, not all the transitions between two states are allowed. Studying the Hydrogen atom, we realize that some transitions have the electric dipole moment equal to zero, and hence, the the rate is equal to zero too [16]. These transitions are said to be forbidden. The derivation of these rules are not simple and they can be found in the references. However, a summary is given in table 2.1:

Table 2.1 The selection rules for electron transitions.

Quantum number	Selection rule
<i>Parity</i>	<i>Changes</i>
l	$\Delta l = \pm 1$
m	$\Delta m = \pm 1$ or 0
s	$\Delta s = 0$
m_s	$\Delta m_s = 0$

These rules can be understood as follows:

- The parity change rule follows from the fact that the electric-dipole moment is proportional to r , which is an odd function.
- The Δl rule follows from the fact that the photon has spin 1, so the rules for addition of angular momentum will allow $l' = l + 1$, $l' = l$, or $l' = l - 1$.
- The Δm rule follows from the fact that the photon has spin 1 too (hence m could be 1, 0 or -1 , conservation of angular momentum requires that the atom give up whatever the photon takes away.
- Finally, spin rules follow from the fact that photons do not interact with the electron spin, so the quantum numbers never change.

3 Quantum Light

Once quantum mechanics has been introduced, this third chapter examines the quantum nature of light. Light is essential in quantum cryptography, since it is the element used for sending the information. The chapter begins with a deduction of the electromagnetic field quantization, where the concept of photon will appear. Then, the classic coherent light and some quantum lights are introduced within quantum mechanics formalism, and finally, the chapter will conclude with some quantum light phenomenons with no classic counterpart.

In order to get broader deductions or explanations, the two main references followed during the chapter are listed here: Mark S. Fox (2006). *Quantum Optics: An Introduction*, Christopher Gerry (2004). *Introductory Quantum Optics*.

3.1 Electromagnetic field quantization

It is convenient to start the deduction of the electromagnetic field quantization with the simplest case: a single-mode electromagnetic field confined in a cavity with volume V , length L , perfectly conducting walls at $z = 0$ and $z = L$, and with no sources (see figure 3.1). Maxwell's equations under these conditions read as follows [25]:

$$\nabla \cdot \mathbf{E} = 0 \quad (3.1)$$

$$\nabla \cdot \mathbf{B} = 0 \quad (3.2)$$

$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t} \quad (3.3)$$

$$\nabla \times \mathbf{B} = \mu_0 \epsilon_0 \frac{\partial \mathbf{E}}{\partial t} \quad (3.4)$$

Assuming the wave propagates along the z -axis, and that the electric field is polarized along the x -direction, the single-mode field that satisfies these equations and the boundaries conditions is:

$$E_x(z, t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} q(t) \sin(kz) \quad (3.5)$$

being ω the angular frequency of the mode, k the wave number ($k = \omega/c$), and $q(t)$ a factor dependent on time with dimension of length, which will be related with the position operator later.

The solution for the magnetic field is:

$$B_y(z, t) = \left(\frac{\mu_0 \epsilon_0}{k}\right) \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \dot{q}(t) \cos(kz) \quad (3.6)$$

where $\dot{q}(t)$ is a factor dependent on time, which will play the role of the momentum for a "particle" with unit mass.

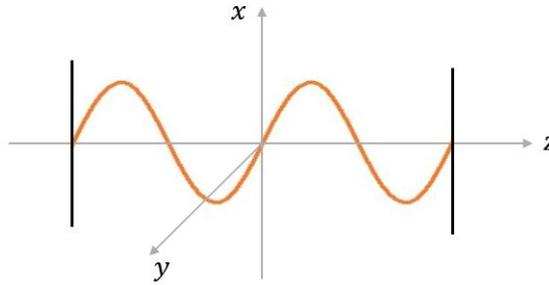


Figure 3.1 A single-mode electric field confined in a cavity.

The classic field energy (its Hamiltonian) is defined as:

$$H = \frac{1}{2} \int [\epsilon_0 E_x^2(z,t) + \frac{1}{\mu_0} B_y^2(z,t)] dV \quad (3.7)$$

$$H = \frac{1}{2} (p^2 + \omega^2 q^2) \quad (3.8)$$

where $p(t) = \dot{q}(t)$. This Hamiltonian is the same that the one defined for the harmonic oscillator. Hence, a single-mode field is formally equivalent to a harmonic oscillator of unit mass, where the electric and magnetic fields play the roles of position and momentum respectively. In the first chapter, only the solution of the harmonic oscillator was showed. However, the resolution of this problem will be showed more detailed now, since it is interesting to understand the topic.

Taking the definition of the position and momentum operators:

$$\hat{H} = \frac{1}{2} (\hat{p}^2 + \omega^2 \hat{q}^2) \quad (3.9)$$

$$\text{with, } [\hat{q}, \hat{p}] = i\hbar \quad (3.10)$$

the electric and magnetic fields can be expressed as operators as well:

$$\hat{E}_x(z,t) = \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \hat{q}(t) \sin(kz) \quad (3.11)$$

$$\hat{B}_y(z,t) = \left(\frac{\mu_0\epsilon_0}{k}\right) \left(\frac{2\omega^2}{V\epsilon_0}\right)^{1/2} \hat{p}(t) \cos(kz) \quad (3.12)$$

Although \hat{p} and \hat{q} are hermitian operators, for reasons that will become clear shortly, in order to study quantum light, two new operators are commonly defined. These two operator are called the ladder operators (none of them are hermitians) [25],

$$\hat{a} = \frac{1}{(2m\hbar\omega)^{1/2}} (m\omega\hat{x} + i\hat{p}_x) \quad (3.13)$$

$$\hat{a}^\dagger = \frac{1}{(2m\hbar\omega)^{1/2}} (m\omega\hat{x} - i\hat{p}_x) \quad (3.14)$$

It can be showed that:

$$[\hat{a}, \hat{a}^\dagger] = 1 \quad (3.15)$$

With these two operators, the position and momentum ones are redefined as:

$$\hat{q} = \left(\frac{\hbar}{2m\omega}\right)^{1/2}(\hat{a} + \hat{a}^\dagger) \quad (3.16)$$

$$\hat{p} = -i\left(\frac{m\hbar\omega}{2}\right)^{1/2}(\hat{a} - \hat{a}^\dagger) \quad (3.17)$$

and the electric and magnetic field operators:

$$\hat{E}_x(z,t) = \mathcal{E}_0(\hat{a} + \hat{a}^\dagger)\sin(kz) \quad (3.18)$$

$$\hat{B}_y(z,t) = \mathcal{B}_0\frac{1}{i}(\hat{a} - \hat{a}^\dagger)\cos(kz) \quad (3.19)$$

The Hamiltonian reads then as follows:

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \quad (3.20)$$

where,

$$[\hat{H}, \hat{a}^\dagger] = \hbar\omega\hat{a}^\dagger \quad (3.21)$$

$$[\hat{H}, \hat{a}] = -\hbar\omega\hat{a} \quad (3.22)$$

Finally, taking the Schrödinger time-independent equation:

$$\hat{H}\psi_n = E_n\psi_n \quad (3.23)$$

and operating on ψ_n with the operator $\hat{H}\hat{a}^\dagger$

$$\begin{aligned} \hat{H}\hat{a}^\dagger\psi_n &= (\hat{H}\hat{a}^\dagger - \hat{a}^\dagger\hat{H} + \hat{a}^\dagger\hat{H})\psi_n \\ &= ([\hat{H}, \hat{a}^\dagger] + \hat{a}^\dagger\hat{H})\psi_n \\ &= (\hbar\omega\hat{a}^\dagger + \hat{a}^\dagger E_n)\psi_n \\ &= (\hbar\omega + E_n)\hat{a}^\dagger\psi_n \end{aligned} \quad (3.24)$$

Summing up, it has been proved that $\hat{a}^\dagger\psi_n$ is an eigenstate of \hat{H} with a definite energy of $(\hbar\omega + E_n)$. Analogously,

$$\hat{H}\hat{a}\psi_n = (-\hbar\omega + E_n)\hat{a}\psi_n \quad (3.25)$$

Similarly, $\hat{a}\psi_n$ is an eigenstate of \hat{H} with a definite energy of $(\hbar\omega - E_n)$.

Equations 3.24 and 3.25 show that the allowed energies of the electromagnetic field form a "ladder" with steps of $\hbar\omega$, as it is represented in figure 3.2. This is the reason why, the operators \hat{a}^\dagger y \hat{a} are known as the *raising operator* and the *lowering operator*, respectively.

Nevertheless, the lowering operator cannot be applied indefinitely. There must be a state with a minimum positive energy (as there was in the harmonic oscillator example), since both, the kinetic and potential energy of the electromagnetic field, are always positive. This state is represented as $\psi_0(x)$, and it is known as the ground state. If the lowering operator is applied to it, the energy must be zero.

$$\hat{a}\psi_0 = 0 \quad (3.26)$$

Applying this to equation 3.20,

$$\hat{H}\psi_0 = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)\psi_0 = \frac{1}{2}\hbar\omega\psi_0 \quad (3.27)$$



Figure 3.2 Allowed energy levels for a single-mode electromagnetic field.

it shows that the energy for the ground state is:

$$E_0 = \frac{1}{2} \hbar \omega \quad (3.28)$$

Which leads to a fundamental conclusion: as it was the case with the harmonic oscillator, the minimum energy for an electromagnetic field is greater than zero. In other words, even in an absolutely dark room at 0K, there will be always a vacuum electromagnetic field. This is the field responsible of the spontaneous emissions presented in section 2.2.8.

From ψ_0 , all the other states can be constructed, only applying the raising operator n times [25].

$$\psi_n(x) = C_n (\hat{a}^\dagger)^n \psi_0(0) \quad (3.29)$$

$$E_n = (n + \frac{1}{2}) \hbar \omega \quad (3.30)$$

where C_n is a normalization constant. Finally an important operator known as the **number operator** is introduced here, its importance will become clear in the next section.

$$\hat{n} = \hat{a}^\dagger \hat{a} \quad (3.31)$$

3.1.1 Photon number state

It has been showed how the electromagnetic field has quantized solutions, each of them with an energy determine by the quantum number n . This leads to the photon number state concept, where a system is represented by the state n or, with Dirac notation, $|n\rangle$.

The operators \hat{a} and \hat{a}^\dagger are important in this representation again. These operators increase or decrease the energy of the system in one quantum, leaving the system in the state $|n+1\rangle$ or $|n-1\rangle$ respectively. Therefore, the **creation operator** is defined as [25]:

$$\hat{a}^\dagger |n\rangle = (n+1)^{1/2} |n+1\rangle \quad (3.32)$$

and the **annihilation operator** is defined as:

$$\hat{a} |n\rangle = (n)^{1/2} |n-1\rangle \quad (3.33)$$

where the factors $(n+1)^{1/2}$ and $(n)^{1/2}$ are needed for normalization. The ground state is represented as $|0\rangle$. Others states can be constructed from it:

$$|n\rangle = \frac{1}{(n!)^{1/2}} (\hat{a}^\dagger)^n |0\rangle \quad (3.34)$$

If the number operator is applied,

$$\hat{a}^\dagger \hat{a} |n\rangle = n |n\rangle \quad (3.35)$$

becomes clear why it is called like that, and we say that an electromagnetic field with n excitations (with n quantum of energy) has n photons. Summarizing, the photon number state represents the number of photons excited at angular frequency ω . Notice how the mass of the oscillator does not enter in any of these formulas, so that the harmonic oscillator is a valid formalism for massless harmonic oscillator such as photons. On the other hand, the solutions found for ψ in section 2.1.4 are not valid. Nevertheless, this is not that important.

These states has a perfect definite number of photons. In contrast, its electric field is not, since the expected value of its operator is:

$$\langle n | \hat{E}_x(z,t) | n \rangle = \mathcal{E}_0 \sin(kz) [\langle n | \hat{a} | n \rangle + \langle n | \hat{a}^\dagger | n \rangle] = 0 \quad (3.36)$$

and its square expected value,

$$\langle n | \hat{E}_x^2(z,t) | n \rangle = 2\mathcal{E}_0^2 \sin^2(kz) (n + \frac{1}{2}) \quad (3.37)$$

Hence, the electric field variance is:

$$\Delta E_x = \sqrt{2\mathcal{E}_0^2 \sin^2(kz) (n + \frac{1}{2})} \quad (3.38)$$

Equation 3.38 shows that even when there are no photons ($n = 0$), the electric field has fluctuations, which is consistent with the fact that the energy is no zero, this fluctuations are called vacuum fluctuations.

This last result is consistent with the quantum mechanics theory as well, since the two operator \hat{n} and \hat{E}_x do not commute.

$$[\hat{n}, \hat{E}_x] = \mathcal{E}_0 \sin(kz) (\hat{a}^\dagger - \hat{a}) \quad (3.39)$$

3.1.2 Quadrature operators

Let us present now a quite important concept in quantum optics, the quadrature operators. These operators are related with the position and momentum, and they are very useful to characterize the light [16].

If the time dependence is included within the electric field operator,

$$\hat{E}_x(z,t) = \mathcal{E}_0 (\hat{a} e^{-i\omega t} + \hat{a}^\dagger e^{i\omega t}) \sin(kz) \quad (3.40)$$

It is convenient to define the quadrature operators:

$$\hat{X}_1 = \frac{1}{2} (\hat{a} + \hat{a}^\dagger) \quad (3.41)$$

$$\hat{X}_2 = \frac{1}{2i} (\hat{a} - \hat{a}^\dagger) \quad (3.42)$$

the electric field operator reads then:

$$\hat{E}_x(z,t) = 2\mathcal{E}_0 \sin(kz) [\hat{X}_1 \cos(\omega t) + \hat{X}_2 \sin(\omega t)] \quad (3.43)$$

Taking the definitions of \hat{a} and \hat{a}^\dagger is easy to see how \hat{X}_1 is related with the position operator and how \hat{X}_2 is related with the momentum operator.

$$\hat{X}_1 = \left(\frac{\omega}{2\hbar}\right)^{1/2} \hat{q} \quad (3.44)$$

$$\hat{X}_2 = \left(\frac{1}{2\hbar\omega}\right)^{1/2} \hat{p} \quad (3.45)$$

These operators satisfy the commutation,

$$[\hat{X}_1, \hat{X}_2] = \frac{i}{2} \quad (3.46)$$

and hence,

$$\Delta\hat{X}_1\Delta\hat{X}_2 \geq \frac{1}{4} \quad (3.47)$$

During the next sections, they will be used in order to characterize different kind of lights.

3.2 Quantum light

The quadrature operators formalism will allow this section to review the most important kind of classic and quantum lights. It will begin with the quantum equivalent of a classic monochromatic light, going through the vacuum field, the squeezed states, and concluding with some phenomenons that can only be explained within quantum theory.

3.2.1 Coherent states

The quantum equivalent of a classic monochromatic light is a coherent state, these states are represented by a complex number α , or $|\alpha\rangle$ with the Dirac notation. They can be described using the quadrature operators as [16]:

$$\alpha = X_1 + iX_2 \quad (3.48)$$

or, using the photon number states as:

$$|\alpha\rangle = \exp(-|\alpha|^2/2) \sum_{n=0}^{\infty} \frac{\alpha^n}{(n!)^{1/2}} |n\rangle \quad (3.49)$$

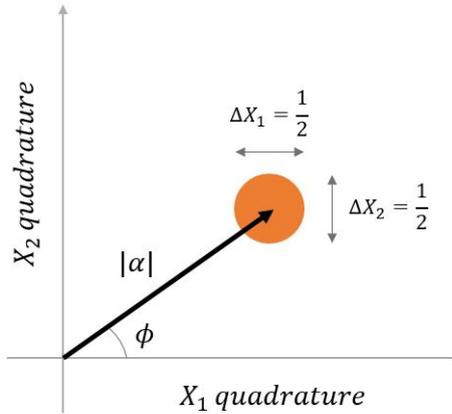


Figure 3.3 Phasor diagram for a coherent state.

In figure 3.3 there is a representation of a coherent state in a phasor diagram. $|\alpha|$ is the length of the arrow, and the uncertainty in the quadrature operator is represented by the orange circle. It can be proven that the coherent states are minimum uncertainty states, hence:

$$\Delta X_1 = \Delta X_2 = \frac{1}{2} \quad (3.50)$$

These states are not eigenstates of the Hamiltonian, therefore, they are not orthogonal to each other. However, it can be showed that,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \quad (3.51)$$

and taking the Hermitian,

$$\begin{aligned} (\hat{a}|\alpha\rangle)^\dagger &= (\alpha|\alpha\rangle)^\dagger \\ \langle\alpha|\hat{a}^\dagger &= \langle\alpha|\alpha^* \end{aligned} \quad (3.52)$$

With these two results it is possible to calculate the expected value of the number operator:

$$\begin{aligned} \langle\alpha|\hat{n}|\alpha\rangle &= \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle \\ &= \langle\alpha|\alpha^*\alpha|\alpha\rangle \\ &= \alpha^*\alpha \end{aligned} \quad (3.53)$$

which shows that the expected number of photons is given by $|\alpha|^2$:

$$|\alpha|^2 = X_1^2 + X_2^2 \quad (3.54)$$

The variance of these states is:

$$\begin{aligned} (\Delta n^2) &= \langle\alpha|(\hat{n} - \bar{n}^2)|\alpha\rangle \\ &= \langle\alpha|\hat{n}^2|\alpha\rangle - 2\bar{n}\langle\alpha|\hat{n}|\alpha\rangle + \bar{n}^2\langle\alpha|\alpha\rangle \\ &= \langle\alpha|\hat{n}^2|\alpha\rangle - \bar{n}^2 \\ &= \bar{n} + \bar{n}^2 - \bar{n}^2 \\ &= \bar{n} \end{aligned} \quad (3.55)$$

That is to say, the variance of the number of photons is equal to its expected value. This is the definition of a Poisson distribution, which is the one found in a classic monochromatic light. Finally, the probability of finding n photons in a coherent state is:

$$|\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^2^n}{n!} \quad (3.56)$$

Substituting $|\alpha|^2 = \bar{n}$, equation 3.56 is equal to a Poisson distribution not surprisingly.

There is an interesting conclusion to discuss. Figure 3.3 shows how there is an uncertainty in both the number of photons $|\alpha|^2$ and the phase ϕ in a classic monochromatic light. In contrast, in the classic theory there is no such uncertainty in the phase, which is always well defined. This contradiction can be explained if we think in a coherent state with a large $|\alpha|^2$, where quantum effects are lost. In such a state the phase uncertainty is negligible, since a movement of the arrow within the circle will not cause almost any change in the phase. This is represented in figure 3.4.

3.2.2 The vacuum field

Equation 3.28 shows how the energy of the harmonic oscillator is not zero, even when there are not photons excited. In quantum optics this result is attributed to random fluctuations of the electric field, which are called the vacuum field. The magnitude of this field is [16]:

$$\mathcal{E}_{vac} = \left(\frac{\hbar\omega}{2\epsilon_0 V}\right)^{1/2} \quad (3.57)$$

which shows how the magnitude is larger for small cavities. This field is a minimum uncertainty state, and because there are no photons excited, its representation in a phasor diagram is as shows figure 3.5. Notice how this light has a perfect definite number of photons, on the other hand, it has a completely indeterminate phase.

3.2.3 Squeezed states

Coherent states and the vacuum field are two examples of minimum uncertainty states, nevertheless, they are not the only valid options. Uncertainty principle claims that the variance of the two quadrature operators must be greater equal than $1/4$, but it does not say how to do so. Therefore, some other kind of lights are

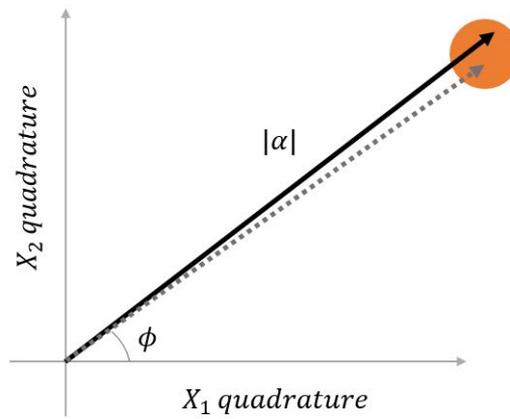


Figure 3.4 Phasor diagram for a classic coherent state.

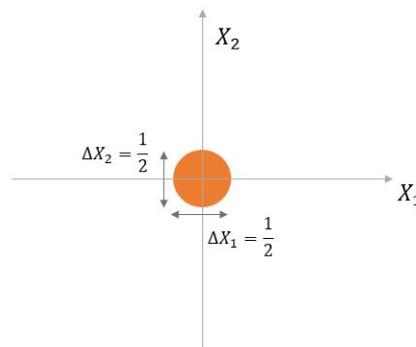


Figure 3.5 Phasor diagram for the vacuum field.

possible in quantum optics: the squeezed states [16].

These states have not the same uncertainty for both quadrature operators, which leads to a infinite number of options. However, there are three important cases.

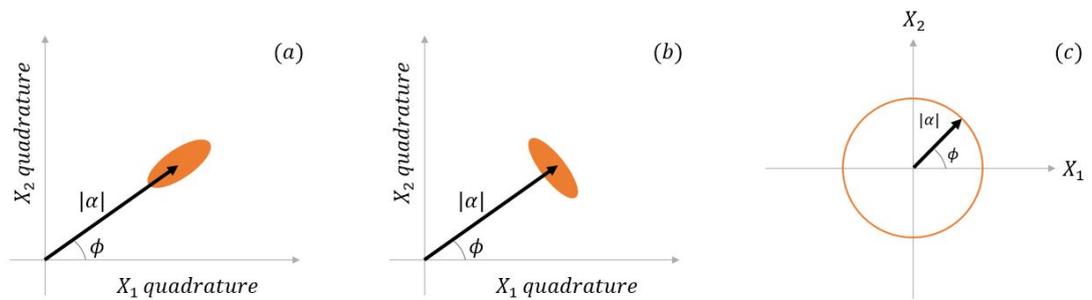


Figure 3.6 Phasor diagram for three different squeezed states.

Figure 3.6(a) shows a **phase-squeezed light**. In this state the uncertainty of the phase is reduced, on the other hand, the uncertainty of the number of photons is increased. The use of these states allows interferometric measurements with greater precision than coherent states. Figure 3.6(b) shows a **amplitude-squeezed light**, these states has a lower shot noise, as it will be discussed in section 3.2.5. Finally, 3.6(c) shows the photon number states discussed in section 3.1.1. Notice how in these states the photon number is well defined and the phase is completely undefined at the same time, it is said that this light is a superposition of states with all the possible phases.

3.2.4 The second order correlation function ($g^{(2)}(\tau)$)

The formalism in quantum optics to characterize the light has been already presented, in the next sections some quantum light phenomena will be introduced. However, before moving on, it is important to define a very useful function in this field, which is used to measure the statistical properties of the light: the second order correlation function ($g^{(2)}(\tau)$) [25].

In order to do so, Hanbury Brown and Twiss developed an experiment (a scheme of it is illustrated in figure 3.7). In it, a beam was divided by a 50:50 beam splitter and detected by two detectors $D1$ and $D2$. Signal detected by $D2$ was then delayed τ and multiplied and integrated with signal detected by $D1$. Hence, the output of the experiment would be proportional to $\langle \Delta I_1(t) \Delta I_2(t + \tau) \rangle$. If τ was shorter than the coherence time, then the two signals would be correlated, for $\tau = 0$:

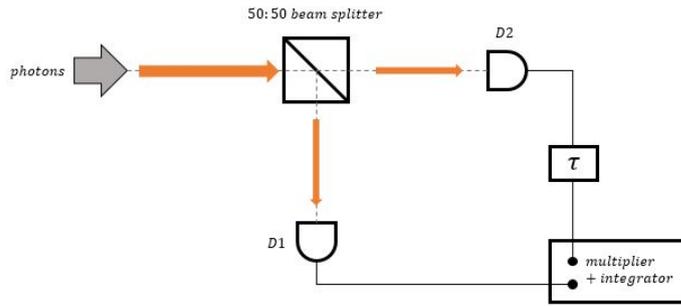


Figure 3.7 The Hanbury Brown-Twiss experiment scheme.

$$\langle \Delta I(t) \Delta I(t + \tau) \rangle_{\tau=0} = \langle \Delta I(t)^2 \rangle \quad (3.58)$$

otherwise, for $\tau \gg \tau_c$

$$\langle \Delta I(t) \Delta I(t + \tau) \rangle_{\tau \gg \tau_c} = 0 \quad (3.59)$$

The second order correlation function is defined as follows:

$$g^{(2)}(\tau) = \frac{\langle I(t) I(t + \tau) \rangle}{\langle I(t) \rangle \langle I(t + \tau) \rangle} \quad (3.60)$$

Considering light with constant intensity $\langle I(t) \rangle = \langle I(t + \tau) \rangle$, and $\langle \Delta I(t) \rangle = 0$, two special cases are studied: $\tau \gg \tau_c$ and $\tau = 0$.

For $\tau \gg \tau_c$:

$$\langle I(t) I(t + \tau) \rangle_{\tau \gg \tau_c} = \langle I \rangle^2 \quad (3.61)$$

$$g^{(2)}(\tau \gg \tau_c) = \frac{\langle I(t) I(t + \tau) \rangle}{\langle I(t) \rangle^2} = \frac{\langle I(t) \rangle^2}{\langle I(t) \rangle^2} = 1 \quad (3.62)$$

and for $\tau = 0$:

$$g^{(2)}(0) = \frac{\langle I(t)^2 \rangle}{\langle I(t) \rangle^2} \quad (3.63)$$

Moreover, it can be proven that for any intensity variation:

$$g^{(2)}(0) \geq 1 \quad (3.64)$$

$$g^{(2)}(0) \geq g^{(2)}(\tau) \quad (3.65)$$

In order to understand this function, it is important to discuss some important results. If a coherent light is considered, with constant intensity I_0 , the function $g^{(2)}(\tau)$ will be constant and equal to 1 for all τ . On the other hand, for any other light with intensity fluctuations, $g^{(2)}(0) \geq 1$, since $\langle I(t)^2 \rangle > \langle I(t) \rangle^2$.

Table 3.1 Properties of the second-order correlation function for classical light.

Light Source	Property
All classical light	$g^{(2)}(\tau) \geq 1$ $g^{(2)}(0) \geq g^{(2)}(\tau)$
Coherent light	$g^{(2)}(\tau) = 1$

From another point of view, different results can be deduced if the Hanbury Brown-Twiss experiment is designed considering the light as a stream of photons (see figure 3.8). In this scheme, photons detected by $D1$ starts a counter which stops photons detected by $D2$, and the second-order correlation function will be proportional to the events detected with a difference time of τ .

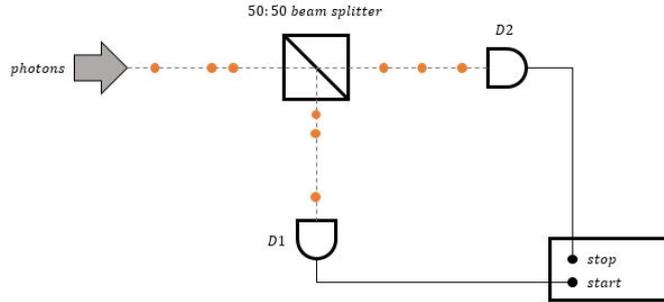


Figure 3.8 The Hanbury Brown-Twiss experiment with photons scheme.

For a single-mode field, $g^{(2)}(\tau)$ reads as follows:

$$g^{(2)}(\tau) = 1 + \frac{\langle (\Delta \hat{n})^2 \rangle - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2} \quad (3.66)$$

It is clear then, that for a coherent state $|\alpha\rangle$,

$$g^{(2)}(\tau) = 1 \quad (3.67)$$

and it can be proven again that, for any classical light, $g^{(2)}(\tau) \geq g^{(2)}(0)$. However, at this point some other scenarios may be considered. Imagine photons arriving evenly space, the time gap between the first photon detected by $D1$ and the first photon detected by $D2$ (after $D1$ has already detected one), will be greater than 0, since photons arrive one by one. Hence, $g^{(2)}(0) \leq g^{(2)}(\tau)$, this is known as **photon antibunching**. According to equation (3.66), there is another important case, if $\langle \hat{n} \rangle > \langle (\Delta \hat{n})^2 \rangle$, then $g^{(2)}(\tau) < 1$, which

cannot be explained with the classic theory, and it is a clear sign of quantum light. This light is known to be sub-Poissonian statistics. Sub-Poissonian light and photon antibunching will be discussed in more detail in the next sections.

3.2.5 Sub-Poissonian light

In classic optics, it is showed that, for a perfect coherent light with constant intensity, the arriving of photons has Poissonian statistics ($\Delta n = \sqrt{\bar{n}}$), any other more chaotic light will have super-Poissonian statistics ($\Delta n > \sqrt{\bar{n}}$). It can be difficult to imagine which kind of light could have sub-Poissonian statistics. Nevertheless, this has already been introduced, referring back to section 3.2.3, the amplitude-squeezed light has less uncertainty in the number of photons arriving, giving a variance lower than for a coherent light and therefore, having sub-Poissonian statistics. This light classification is listed below [16]:

- sub-Poissonian light: $\Delta n < \sqrt{\bar{n}}$
- Poissonian light: $\Delta n = \sqrt{\bar{n}}$
- super-Poissonian light: $\Delta n > \sqrt{\bar{n}}$

Observing sub-Poissonian light is not an easy task because losses and the detection efficiency have big influence. During the next subsections these issues will be commented.

Degradation of photon statistics by losses

One of the reasons why the observation of sub-Poissonian light is difficult is because of the medium losses. Medium losses can be understood as a probabilistic occurrence caused by the absorption process. In this scenarios, the medium will degrade the photons statistics, since the uncertainty in the number of photons will increase because some of them will be lost [16].

Theory of photodetection

An optic detector is a device which produces a electric current when photons reach it. From a classic point of view, considering light as wave with intensity I , some assumptions are made [16]:

1. The probability of generating an electron within a time interval Δt is proportional to the intensity I , the illuminated area A , and the time interval Δt .
2. If Δt is small enough, the probability of generating two electrons is negligible.
3. The electrons generated at different times are uncorrelated.

With these assumptions, it can be showed that the probability of detecting n photons within a time t is:

$$P_n(t) = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \quad (3.68)$$

which is a Poisson distribution. That is to say, with classic theory sub-Poissonian light detection cannot be explained. Therefore, it is necessary to study this problem with quantum theory, which proves the relation between the variance in the electrons generated and the variance of the incident light. According to this theory:

$$(\Delta N)^2 = \eta^2 (\Delta n)^2 + \eta(1 - \eta)\bar{n} \quad (3.69)$$

where η is the quantum efficiency, i.e. the number of photons detected divided by the number of incident photons. The conclusion is clear: in order to detect sub-Poissonian light, a high quantum efficiency is needed. With current technology, it is possible to find detectors with these efficiencies.

Shot noise and observation of sub-Poissonian light

One method used for observing sub-Poissonian light is to study the shot noise of a source. The shot noise is a noise that every source has because of the fluctuations in the number of photons, as it is showed in figure 3.9 [16].

This noise is a white noise, in classic theory it is a noise not possible to mitigate, since it is intrinsic to the source. Nevertheless, it is easy to understand that a sub-Poissonian light will have a lower shot noise than classic lights. Therefore, some experiments have focused on study this shot noise for some specific sources, observing lower noise than the theory predicts.

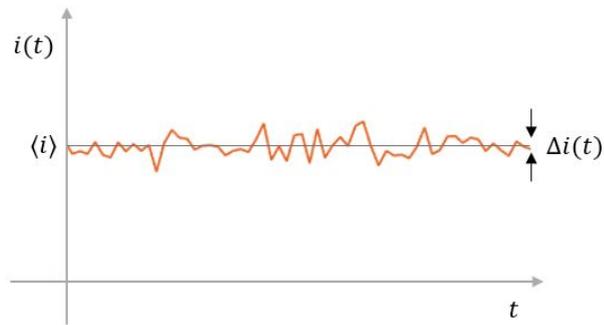


Figure 3.9 The shot noise caused by the intensity fluctuations of the intensity due to the uncertainty on the number of photons arriving.

3.2.6 Photon antibunching

The other important quantum light phenomenon was photon antibunching. As it was explained in previous sections, this occurs when photons arrive evenly spaced (see figure 3.10) or, mathematically when $g^{(2)}(0) \geq g^{(2)}(\tau)$. This kind of light is mentioned here since it is the basis for the single-photon sources. These sources are key in quantum cryptography applications as it will be discussed in chapter 4. Currently, there is an important investigation which tries to make them commercially available [16].

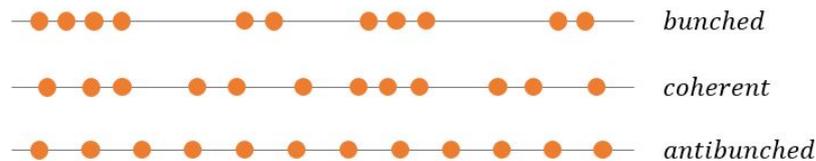


Figure 3.10 Photon bunched vs. coherent light vs. photon antibunched.

Experimental demonstration of photon antibunching

The basic idea to demonstrate photon antibunching was to isolate an atom and shine it with a laser, taking advantage of the absorption and spontaneous emission processes. The idea is to excite the electrons of a single atom and wait for them to decay, emitting a photon in the process. Many experiments have been conducted with this idea, obtaining results such as $g^{(2)}(0) = 0.4$ in 1977, or $g^{(2)}(0) = 0.054$ more recently, in 2007. This kind of experiments have a key importance since it has helped to develop single photon sources as it is explained in chapter 5 [16].

4 Quantum Cryptography

After introducing quantum mechanics and quantum light formalism, this chapter will lead to the main topic: quantum cryptography, which will feasibly bring the first quantum application to become commercially available in the near future: the quantum key distribution.

As it was mentioned in chapter 2, this field combines the theory of quantum mechanics and information theory. A brief introduction to the latter will be given in section 4.1. The chapter continues with the following sections: and introduction to quantum cryptography is given in section 4.2, as well as its underlying ideas; then, the most important protocols are introduced in section 4.3, giving a brief summary of others more advanced too. To conclude, the limits of quantum cryptography are studied using the theory of quantum information (which is based on the classic information theory and on quantum mechanics) in section 4.4.

4.1 An overview of information theory

Information theory studies the quantification, storage and the communication of information. It was first developed by Shannon in 1948, who wanted to find the limits in signal processing, and in some communication concepts such as data compression. The theory has turned out to be crucial for the development of some of the most important current technologies, such as the Internet, the cryptography or even the understanding of black holes.

Along with this section, the main concepts and some important conclusions of the theory will be discussed. However, the field is large enough for writing several books and for completing some courses. Therefore, a full deduction of it is beyond the scope of the section. For widening the concepts presented here, one of the main references in the field is: Thomas Cover (1991) - *Elements of Information Theory* [43].

4.1.1 Information

Information is an abstract concept difficult to define sometimes. One of these definitions could be: *a measure of the uncertainty lost in a variable after conducting an experiment*. Mathematically, is defined as follows [33]:

Definition 4.1.1 Given a discrete random variable X , which takes the value $a \in \mathcal{X}$ with probability $P_X(a)$, the information given by a is:

$$I_X(a) = \log \frac{1}{P_X(a)} = -\log P_X(a) \quad (4.1)$$

being \mathcal{X} all the possible values of X . The unit for the information depends on the basis chosen for the logarithm: if it is 2, we talked about **bits**; if it is e , then we talked about **nats**.

Example 4.1.1 The information given by the experiment 'tossing a coin' will always be 1 bit, since:

$$t_X(\text{heads}) = \log_2 \frac{1}{0.5} = 1 \text{ bit} \quad (4.2)$$

$$t_X(\text{tails}) = \log_2 \frac{1}{0.5} = 1 \text{ bit} \quad (4.3)$$

The definition of information can be extended to several random variables and to conditioned random variables.

Definition 4.1.2 Given two discrete random variables X and Y , which take values from \mathcal{X} and \mathcal{Y} respectively, and with a mass probability function P_{XY} , the joint information is defined as [33]:

$$t_{XY}(a,b) = \log \frac{1}{P_{XY}(a,b)} \quad (4.4)$$

Definition 4.1.3 Given two discrete random variables X and Y , which take values from \mathcal{X} and \mathcal{Y} , the information given by $X = a$ conditioned to $Y = b$, is defined as:

$$t_{X|Y}(a|b) = \log \frac{P_Y(b)}{P_{XY}(a,b)} \quad (4.5)$$

From these definitions, an important relation can be deduced:

$$t_{XY}(a,b) = t_Y(b) + t_{X|Y}(a|b) \quad (4.6)$$

Hence, the information given by the experiment $X = a, Y = b$ is always greater than the information given by the experiment $X = a|Y = b$, something logical if it is considered.

Although they will not be introduced in this dissertation, information and all the followings definitions have a counterpart for the continuous random variables [43].

4.1.2 Entropy

A very important concept in information theory is the entropy of a discrete random variable X ($H(X)$), which is defined as the expected value of the random variable $t_X(X)$ [33].

$$\begin{aligned} H(X) &= \mathbb{E}[t_X(X)] = \\ &= \mathbb{E}\left[\log \frac{1}{P_X(X)}\right] = \\ &= \sum_{x \in \mathcal{X}} P_X(x) \log \frac{1}{P_X(x)} \end{aligned} \quad (4.7)$$

The entropy $H(X)$ is a number, which gives a quantification of the uncertainty in an experiment. E.g. if the experiment is deterministic $H(X) = 0$, since there is not uncertainty in the output. For other cases, the greater the uncertainty is, the greater the entropy will be.

Example 4.1.2 The entropy of the experiment *throwing a die*, modeled by a discrete random variable X with $\mathcal{X} = \{ 1, 2, 3, 4, 5, 6 \}$ is:

$$H(X) = \sum_{x=1}^6 \frac{1}{6} \log 6 = 2.585 \text{ bits} \quad (4.8)$$

Another important result is the definition of the binary entropy $h_b(p)$, which is defined as the entropy of a Bernoulli with probability p ,

$$H(X) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} = h_b(p) \quad (4.9)$$

The generalization done for the joint and conditional information previously, can be also applied to the entropy, leading to the definition of joint and conditional entropy [34]:

$$H(X,Y) = \mathbb{E}[t_X Y(X,Y)] = \sum_{a \in \mathcal{X}} \sum_{b \in \mathcal{Y}} P_{XY}(a,b) \log \frac{1}{P_{XY}(a,b)} \quad (4.10)$$

$$\begin{aligned} H(X|Y) &= \sum_{y \in \mathcal{Y}} P_Y(y) H(X|Y=y) = \\ &= \sum_{y \in \mathcal{Y}} P_Y(y) \sum_{x \in \mathcal{X}} P_{X|Y}(x|y) \log \frac{1}{P_{X|Y}(x|y)} = \\ &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} P_{XY}(x,y) \log \frac{1}{P_{X|Y}(x|y)} \end{aligned} \quad (4.11)$$

4.1.3 Mutual information

A key question in information theory is: how much information a random variable Y gives about another random variable X . From Shannon's perspective, the information was always a difference of uncertainty. Hence, he called this quantity **mutual information** and he defined it as [34]:

$$I(X;Y) = H(X) - H(X|Y) \quad (4.12)$$

This is a key quantity, which is the result of many problems. For instance, one of the most important is the capacity of a channel, a result which defines the theoretical limit for a communication given within a particular channel.

Channel capacity

The channel capacity C , is the maximum rate at which information can be exchanged across a channel between two sources, with a negligible error. It is defined as follows [35]:

$$C = \max_{p_X(x)} I(X;Y) \quad (4.13)$$

4.1.4 Shannon's theorems

Shannon gave several important theorems with his information theory [43]. Two are remarked in this section, due to its importance in quantum cryptography.

Theorem 4.1.1 *If the entropy of the source is lower than the channel capacity ($H(X) \leq C$), then there exists a codification scheme for which it is possible to achieve a negligible error rate.*

This is known as the second Shannon's theorem, and gives the upper bound for being feasible a communication.

Theorem 4.1.2 *If a message X is encoded with a key Z , the message will be perfectly secret if and only if $H(Z) \geq H(X)$.*

This is known as Shannon's perfect secret. Moreover, the key Z must be perfectly random and can be only used once. As it will be discussed in next section, this was the motivation behind the development of quantum cryptography.

4.2 Introduction to quantum cryptography

Quantum mechanics has some counter-intuitive properties such as the uncertainty principle, the entanglement, or the fact that a measure destroys the system state, which may appear that only make more complex the study of a system. On the contrary, these properties can be also exploited for a self benefit. This is what quantum cryptography does, using them in order to achieve a perfect secure encryption. For doing so, two kinds of protocols were invented at the beginning of the field, the so called *prepare-and-measure* protocols, and the so called *entanglement-based* protocols.

This section is organized as follows: first, it is briefly discussed the main motivation for quantum cryptography. Second, the two ideas that underlie the two kinds of protocols are explained, leaving the protocols themselves for the next section.

4.2.1 The motivation

Quantum cryptography is an improvement of classic cryptography using quantum properties. Therefore, it is interesting to ask why this improvement was needed in the first place. For understanding so, classic cryptography should be reviewed briefly.

Cryptography is the field which studies how to transform a message to a sequence of intelligible characters to any unauthorized party. Cryptoanalysis would be the field which studies how to break this coded messages. They have a key importance in current society, since we live in a world where information is more important and valued every day. Keep it secret has become a major issue for institutions such as governments, banks or the armies.

Nevertheless, encoding a message perfectly secret is often too difficult to implement, so most of the time the message is encoded in such a way that it is just very difficult to decode. Currently, two strategies are mainly used: the asymmetrical cryptosystems, and the symmetrical cyrptosystems.

Asymmetrical cryptosystems

Asymmetrical cryptosystems are based on public-private pair keys [48]. In these systems, the interested party on receiving a message (in cryptography is usually called Bob) has a private and a public key. The public key is computed from the private one, and it is shared publicly. The interested on sending a encrypted message to Bob (again, in cryptography is usually called Alice) will encrypt the message with this public key, so that only Bob will be able to decoded it. This idea works because of mathematical objects called one-way function $f(x)$. These functions are easy to compute given x , on the contrary, it is very difficult to compute x from $f(x)$, unless you have some additional information.

In practice, these systems are based on factorization. It is easy to understand how simple is to compute two prime number, e.g. $53 * 67$. However, it is much more difficult to compute the prime factors of the number 3551. In asymmetrical systems 3551 would be the public key, and 53 and 67 the private key. In real applications, huge prime numbers are used, because the computation needed to factorize a multiplication of them is much greater. Nevertheless, despite factorizing huge prime numbers is a quite complex task, it is not impossible. Moreover, as computation is always increasing its capacity, there will come a day when computers will be powerful enough to break these systems (quantum computers are a huge threat here). Therefore, for the future, to keep a message perfectly secret, only the symmetrical systems are feasible.

Symmetrical cryptosystems

Symmetrical cryptosystems are based on a secret key shared between Alice and Bob [48]. In these systems Alice will add the key to its message to obtain the scrambled text ($s = a \oplus k$, where \oplus means the binary addition modulo 2 without carry), and then it will be send to Bob, who will substrate the key to obtain the original message ($s \ominus k = a \oplus k \ominus k = a$). For this system being perfectly secret, according to Shannon's perfect secret, $H(Z) \geq H(X)$, being Z a random variable modeling the key, and X a random variable modeling the message.

In addition, the key must be used only once, since if not, an eavesdropper could record two different messages to obtain the sum of the plain texts ($s_1 \oplus s_2 = a_1 \oplus a_2 \oplus k \oplus k = a_1 \oplus a_2$), gaining some additional information. This is an important issue, because the sharing of the different secret keys must be trusted, or the whole system would not work. Distributing the keys securely and safely is currently a very slow process, and it is the reason why symmetrical systems are not used in practice. It is here where quantum cryptography plays a key role, since it solves the problem of sharing secret keys between two partners.

Quantum cryptosystems

The aim of quantum cryptosystems is to provide a way for sharing secret keys (the reason why they are called quantum key distribution (QKD) systems) [48]. In these systems, an eavesdropper can still intercept the communication between Alice and Bob and get the keys, nevertheless, in that case they will be able to notice the presence of the eavesdropper, not using the key then, and trying to share a new one. This make the system

perfectly secret, since Alice and Bob will only use the secret when they know no eavesdropper was listening.

For this purpose, quantum cryptosystems use the fact that every measurement perturbs the system. Imagine Alice wants to send a message to Bob, she will encode her bits using a quantum system (sending photons for instance). If Bob receives these photons unperturbed, then it can be inferred no one got any information of the system, and the key is secret. After checking that the key is secret, they will move to a classic public channel and they will use the classic symmetric cryptosystem. Whenever they will have to use another secret key, the quantum system will provide them a new one, repeating the process. The next sections will explain more deeply how to do so.

4.2.2 The uncertainty principle on photons

Previous sections have already introduced the uncertainty principle in quantum mechanics. However, an important case has been omitted: photons polarization. Since it is impossible to know at the same time both, the polarization of a photon in the vertical-horizontal basis, and the polarization in the diagonal basis (45° - 135°).

Imagine a photon polarized vertically as in figure 4.1. If the photon is measured in the horizontal-vertical basis as it is in figure 4.1(a), there is no uncertainty in the measure. On the contrary, if the photon is measured in the diagonal basis, this photon can be also understood as a superposition of two states, one polarized along the 45° axis with a probability equal to $|\sin \alpha|^2$, and the other polarized along the 135° axis with probability $|\cos \alpha|^2$ (see figure 4.1(b)). Hence, upon a measurement in this basis, it is impossible to know the output with absolutely certainty. Moreover, the wave function will collapse in one of the two possibilities, leaving the photon no longer polarized along the vertical axis.

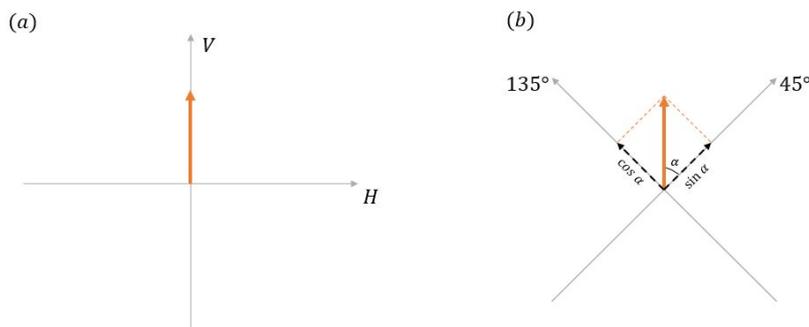


Figure 4.1 A vertically polarized photon in the vertical-horizontal and in the diagonal basis.

There is a quite simple and interesting experiment to visualize this. Imagine two polarized filters, which are on the way of a beam with no polarization. Let us say that the first filter is pointing along the vertical axis, and the second filter is oriented along the horizontal axis. It is easy to understand that no photon will be able to pass both filters, since, across the first filter, only vertically polarized photons will go, which will be blocked by the second filter (see figure 4.2).

However, if a third filter is placed between the first two, oriented along the 45° axis, some photons go now through the three filters. This happens because of the uncertainty principle. The vertically polarized photons after the first filter, will be measured in the diagonal basis. As it has been discussed, these photons can be understood as a superposition of two states, and a measurement will destroy this superposition state and will force the wave function to collapse. If the wave function collapses in a photon with 45° polarization, it will go through the second filter, however, the photon will not be vertically polarized any longer. Understanding a 45° polarized photon as a superposition of a photon with vertical and a horizontal polarization, the same reasoning can be applied to the third filter. Hence, it is understandable how some photons pass through the three filters now.

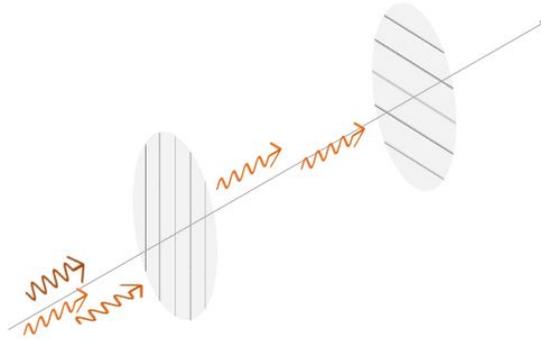


Figure 4.2 A beam going through two polarized filters, one vertically polarized and the other horizontally polarized.

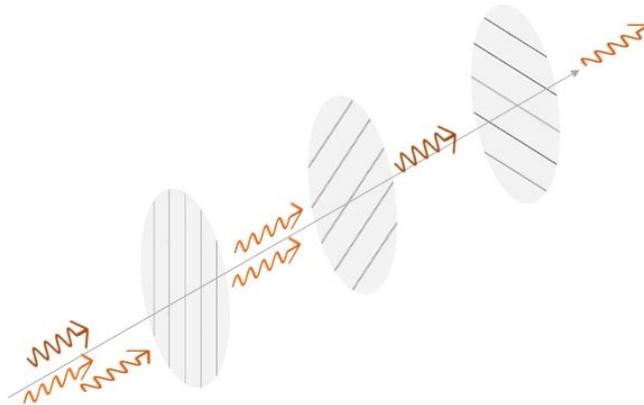


Figure 4.3 A beam going through three polarized filters, the first vertically polarized, the second polarized along 45° axis, and the last horizontally polarized.

The uncertainty principle is the idea behind the prepare-and-measure quantum cryptography protocols. In section 4.3.1, the BB84 will be studied to see how it uses this.

4.2.3 Bell's inequality

The superposition of states (see section 2.1.7) is one of the most counter-intuitive concepts in quantum mechanics. The fact that a particle has a not well defined value of magnitude, and only the probability of some values can be known, does not seem very logical. This is what Einstein, Podolsky and Rosen thought in 1935. They did not doubt quantum mechanics was incorrect, they just thought it was incomplete. For proving it, they designed an experiment (the EPR experiment): consider a source S emitting two correlated photons as in figure 4.4, which means that if one of the photons has a vertical polarization, the other one will have a horizontal polarization, or that if one has a vertical polarization the other one will have it too. Either way, the polarization of one will determine the polarization of the other. Before making any measurement it is impossible to know if photon one is vertically or horizontally polarized. Nevertheless, the second photon will be correlated. This is what quantum mechanics describes as entangled states, their wave functions can be written as [19]:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|0_1, 0_2\rangle \pm |1_1, 1_2\rangle) \quad (4.14)$$

for the case of perfect positive correlation, or

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0_1, 1_2\rangle \pm |1_1, 0_2\rangle) \tag{4.15}$$

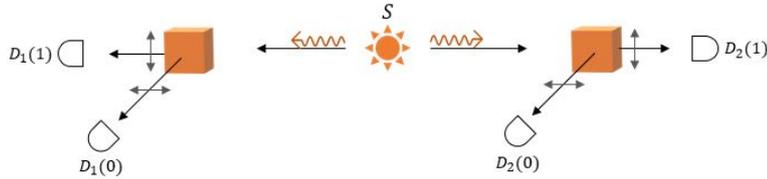


Figure 4.4 The EPR experiment.

for the case of perfect negative correlation. Now suppose that both particles travel 10 light years in opposite directions, then the photon one is measured and it is found to be vertically polarized. Suddenly, the wave function for both photons will collapse at the same time, since they are correlated. In other words, something would have had to traveled instantaneously from the photon one to the photon two. Einstein, Podolsky and Rosen considered this impossible, since nothing can travel faster than light. In this respect, they concluded that quantum mechanics was incomplete, and that there must be another theory which could say which polarization the photons had when leaving the source.

The wave function must not define the system completely, there must be another variable λ which fully characterize the system. This variable was called *the hidden variable*, and many theories were proposed in order to demonstrated it. However, in 1964 Bell proved that any hidden variable theory was incompatible with quantum mechanics.

He proposed a generalization of the EPR experiment, where the beam splitters could be rotated along their axis. Suppose we have a perfect negative correlation situation, and we establish that a photon vertically polarized is equal to $+1$, and a photon horizontally polarized is equal to -1 . Then, if both detector are parallel ($\mathbf{b} = \mathbf{a}$, see figure 4.5), both values will be anti-correlated and the average value of the product will be -1 :

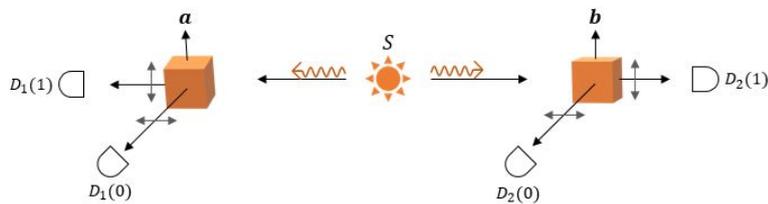


Figure 4.5 Bell's generalization for the EPR experiment.

$$P(\mathbf{a}, \mathbf{a}) = -1 \tag{4.16}$$

On the other hand, if they are anti-parallel ($\mathbf{b} = -\mathbf{a}$):

$$P(\mathbf{a}, -\mathbf{a}) = +1 \tag{4.17}$$

And for any arbitrary orientation:

$$P(\mathbf{a}, \mathbf{b}) = \mathbf{a} \cdot \mathbf{b} \quad (4.18)$$

What Bell discovered was that this result was incompatible with any hidden variable theory. Suppose there is a hidden variable which determinate the polarization of the two photons. Then there exists some function $A(\mathbf{a}, \lambda)$ and $B(\mathbf{b}, \lambda)$ which take the values ± 1 deterministically:

$$A(\mathbf{a}, \lambda) = \pm 1 \quad B(\mathbf{b}, \lambda) = \pm 1 \quad (4.19)$$

If the detectors are aligned:

$$A(\mathbf{a}, \lambda) = -B(\mathbf{a}, \lambda) \quad (4.20)$$

The average value of the product of the measurements is:

$$P(\mathbf{a}, \mathbf{b}) = \int \rho(\lambda) A(\mathbf{a}, \lambda) B(\mathbf{b}, \lambda) d\lambda \quad (4.21)$$

Using equation (4.20):

$$P(\mathbf{a}, \mathbf{b}) = - \int \rho(\lambda) A(\mathbf{a}, \lambda) A(\mathbf{b}, \lambda) d\lambda \quad (4.22)$$

and for any other unit vector \mathbf{c}

$$P(\mathbf{a}, \mathbf{b}) - P(\mathbf{a}, \mathbf{c}) = - \int \rho(\lambda) [A(\mathbf{a}, \lambda) A(\mathbf{b}, \lambda) - A(\mathbf{a}, \lambda) A(\mathbf{c}, \lambda)] d\lambda \quad (4.23)$$

Operating [19], the famous Bell's inequality is found:

$$|P(\mathbf{a}, \mathbf{b}) - P(\mathbf{a}, \mathbf{c})| \leq 1 + P(\mathbf{b}, \mathbf{c}) \quad (4.24)$$

This inequality should be true if there exists any hidden variable (notice no assumption on the hidden variable was made). Nevertheless, this result is inconsistent with quantum mechanics, e.g. for $\mathbf{a} = 0$, $\mathbf{b} = 90$ and $\mathbf{c} = 45$:

$$P(\mathbf{a}, \mathbf{b}) = 0, \quad P(\mathbf{a}, \mathbf{c}) = P(\mathbf{b}, \mathbf{c}) = -0.707 \quad (4.25)$$

In other words, either quantum mechanics theory was completely wrong, or the EPR assumption was wrong. Nowadays, no one doubt the veracity of quantum mechanics.

4.3 Protocols

Once the concepts behind the two kind of QKD protocols have been introduced, this section will explain how the two most important protocols work, giving a brief introduction to other more modern protocols.

4.3.1 The BB84 protocol

The BB84 protocol was the first QKD protocol proposed. It was presented by Charles H. Bennett and Gilles Brassard in 1984, hence the name BB84 [6].

The protocol is divided into two stages: in the first one a quantum channel is used, while the second one uses a classic channel. During the first stage, Alice and Bob will generate a secret key using any two-level quantum system (during this section the photon polarization is assumed, although Bennett and Brassard used the electron spin). First, Alice will generate random bits, codifying them randomly with the vertical-horizontal or the diagonal basis, according to table 4.1. She will send these qubits then to Bob.

Whenever Bob receives a photon, he will choose a random basis for measuring it. As it was discussed in section 4.2.2, if Bob chooses the same basis as Alice, the result will be correlated. On the other hand, if Bob chooses the wrong basis, the result will be uncorrelated (with a 50% probability of error). This, will leave Alice and Bob with a key with an error of 25%, known as the *raw key*.

Anyway, this error is not important, since in the second stage Alice and Bob discard the uncorrelated photons. Over a public channel, Bob will announce when he received a photon and which basis he used to measure it.

Table 4.1 Qbits representation in BB84 protocol.

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

Alice will tell Bob whether he chose the correct basis or not, and then Alice and Bob will discard all the photons for which they chose different basis. Hence, this process will finally leave them with a key with no errors (in an ideal channel with no eavesdropper and no errors) known as the *sifted key*.

Consider now the security of this protocol. During the first stage, an eavesdropper (usually known as Eve) could try to intercept some photons, something not so difficult. Nevertheless, if she does so, Bob will not receive those photons. Then, during the second stage, and because Bob announces the time he received the photons, Alice and Bob will be able to discard them. Therefore, for a real eavesdropping, Eve must resend those qubits to Bob again. She would like to send him the same qubit she received, but the no cloning theorem makes this impossible. Hence, every time Eve tries to eavesdrop the communication, she will leave a sign (introducing errors), and Alice and Bob will be able to notice it.

No cloning theorem

The no cloning theorem shows that a perfect copying in quantum mechanics is impossible [19]. Suppose Eve has a quantum copy machine, which would take a particle in state $|\psi\rangle$ as an input, and another particle in state $|X\rangle$ (known as blank copy), to produce two particles in the state $|\psi\rangle$. Imagine Eve has a machine which successfully clones the state $|\psi_1\rangle$:

$$|\psi_1\rangle|X\rangle \rightarrow |\psi_1\rangle|\psi_1\rangle \quad (4.26)$$

And it also works for the state $|\psi_2\rangle$:

$$|\psi_2\rangle|X\rangle \rightarrow |\psi_2\rangle|\psi_2\rangle \quad (4.27)$$

Then, if the input of the machine is a linear combination of these two states $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$, because of the linearity of quantum mechanics, the output will be:

$$|\psi\rangle|X\rangle \rightarrow \alpha|\psi_1\rangle|\psi_1\rangle + \beta|\psi_2\rangle|\psi_2\rangle \quad (4.28)$$

However, this is not what the machine should generate, since what it really should produce would be:

$$\begin{aligned} |\psi\rangle|X\rangle \rightarrow |\psi\rangle|\psi\rangle &= [\alpha|\psi_1\rangle + \beta|\psi_2\rangle][\alpha|\psi_1\rangle + \beta|\psi_2\rangle] \\ &= \alpha^2|\psi_1\rangle|\psi_1\rangle + \beta^2|\psi_2\rangle|\psi_2\rangle + \alpha\beta[|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle] \end{aligned} \quad (4.29)$$

Hence, it could be possible to have a machine which could copy the states $|\psi_1\rangle$ and $|\psi_2\rangle$, but it will fail copying a linear combination of these states, making impossible to have a perfect quantum copying machine.

Intercept-resend strategy

Eve can apply some complex strategies to get information about the secret key (see section 4.4). Nevertheless, let us first review the simplest strategy Eve could use: the intercept-resend strategy. In this case, Eve will intercept Alice photons, and she will measure them as Bob would do it. Then, she will send to Bob new qubits according to what she measured. In 50% of the cases, Eve will choose the correct basis, and Alice and Bob will not notice the system was disturbed. However, in the other cases, Eve will send to Bob the wrong qubit, so Bob will receive an uncorrelated photon. Among these uncorrelated photons, Bob's result and Alice's bit will coincidence 50% of the times. Hence, after Alice and Bob exchange the information during the second stage, they will end with a sifted key with 25% errors, therefore, they can infer the system was disturbed and decide not to use the key.

Nevertheless, for now the channel has been considered ideal only. This is not the real case, and because of the channel, the sifted key will contain some errors. If the error (in quantum cryptography is called the QBER) is low enough, Alice and Bob can deduce no one perturbed the communication. In contrast, for a

high QBER, they will not be able to distinguish if the error was produced because of the channel, or because of an eavesdropper, hence, the secret key will be no longer secure. These bounds will be discussed during section 4.4 as well.

4.3.2 The E91 protocol

In 1991 Artur Ekert designed another kind of protocol based on the entanglement particles and Bell's inequality [11]. Using the states defined in section 4.2.3, it is possible to detect an eavesdropper with Bell's inequality.

In this protocol, instead of Alice sending photons to Bob, there is a central source which sends entanglement particles to both, Alice and Bob at the same time. Ekert used spin singlet configuration for the entangled particles in his paper, although many others entangled systems can be used. Suppose the source produces electrons in the singlet configuration. For every pair, Alice and Bob will measure them in one of three possible basis (a_i for Alice's vectors and b_i for Bob's vectors), with angles: $\phi_0^a = 0$, $\phi_1^a = 45$, $\phi_2^a = 90$ for Alice, and $\phi_0^b = 45$, $\phi_1^b = 90$, $\phi_2^b = 135$ for Bob.

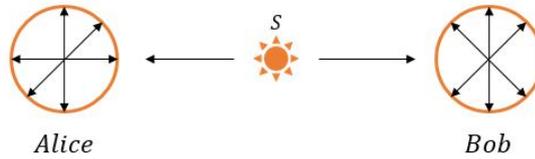


Figure 4.6 The basis used for measuring in the E91 protocol.

The probability for Alice and Bob to choose the same basis is $1/3$. If they do so, their measurements will be completely correlated, that is to say, if Alice measures the electron with a spin up, Bob will measure it with spin down. On the other hand, if they do not choose compatible basis, the measurements will be completely uncorrelated. Comparing in a public channel which basis were used, they are able to know in which measurements they will have correlated results. These correlated bits will be used for generating the secret key if there was no eavesdropper.

Imagine now Eve tries to eavesdrop the system. It is impossible stealing information since there is no information until Alice or Bob perform the measure. Therefore, for trying to eavesdrop the system, Eve will have to measure the electron coming to Bob (or Alice), however, when doing so, she will have to send again another electron to Bob, and this one will not be correlated to the one Alice receives any longer.

The correlation coefficient of the measurement is defined as:

$$E(a_i, b_i) = P_{++}(a_i, b_i) + P_{--}(a_i, b_i) - P_{+-}(a_i, b_i) - P_{-+}(a_i, b_i) \quad (4.30)$$

where P_{\pm} is the probability of obtaining ± 1 along a_i and ± 1 along b_i . Defining the quantity S as:

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \quad (4.31)$$

Bell proved that if quantum mechanics was incomplete then $S \leq 2$. On the other hand, quantum mechanics predict $S = 2\sqrt{2}$. Hence, Alice and Bob can used the uncorrelated bits to calculate S , if it is not equal to $2\sqrt{2}$ they can infer an eavesdropper perturbed the system.

4.3.3 Other protocols

There are many other QKD protocols, all of them are based on the two kind of protocols explained above. This section will give a brief introduction to some of them.

B92

In 1992, Bennett noticed that the 4 states in BB84 were not needed [4]. Instead, the same protocol could be realized with only two non-orthogonal states. Because they are non-orthogonal, it is impossible to Eve to distinguish between them without perturbing the system.

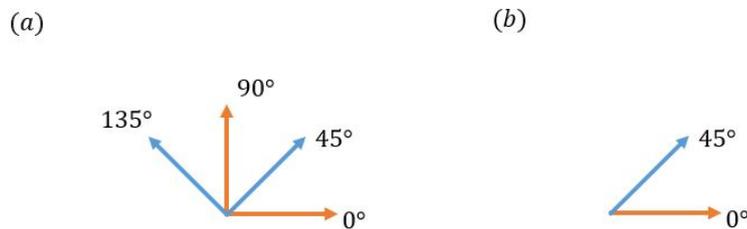


Figure 4.7 The BB84 states (a) versus the B92 states (b).

Although this protocol is easier to implement, it is also less secure for a real system. Hence, it is only used at experimental level in laboratories.

6-states

In this protocol, two new non-orthogonal states are added to the 4 four states of BB84 [17]. As a result, in this protocol Alice and Bob must distinguish between three basis. Therefore, the probability of choosing the right one is $\frac{1}{3}$. Complementary to B92, this protocol is more difficult to implement, but it is also more secure.

SARG04

This protocol was proposed in 2004 [18]. The first stage (the one using the quantum channel) is equal to BB84. It is the second stage which differs. During it, Alice does not announce the basis she used. Instead, she announces two non-orthogonal states, one of which is the state sent. Imagine Alice sent the state $|\leftrightarrow\rangle$, and that she announces $|\leftrightarrow\rangle$ and $|\nearrow\rangle$. Then, if Bob measured with the same basis, he could only get the state $|\leftrightarrow\rangle$. On the other hand, if he measured with the wrong basis he could get the states $|\nearrow\rangle$ and $|\nwarrow\rangle$ with same probability. In the case Bob measured the state $|\nwarrow\rangle$ (and only in this case) he can infer which states was sent by Alice.

For a system with a perfect single-photon source, this protocol has the same security than BB84, however, for real system with attenuated lasers, SARG04 is more robust against photon-number split attacks.

Decoy states

This is the most widely implemented protocol currently [20]. It was designed for being resistant against the photon number splitting attack (one of the main issues in quantum cryptography with the current technology). The protocol BB84 for instance, is secure with a perfect single-photon source, but if in a pulse more than one photon is sent, Eve could intercept just one, without interacting with the others. Unfortunately, single-photon sources are not commercially available yet, instead very attenuated lasers are used. These lasers emit pulses with zero, one or two or more photons (see section 5.1), whenever the laser emits more than one photon, Eve could attack the system without being noticed.

In order to avoid this kind of attacks, this protocol introduced decoy states with different intensities. After Alice has sent all the qubits, she will announce in the public channel which were the intensities she used. For a successful PNS attack, Eve should maintain the QBER constant for every intensity, which is not possible for her in this scheme [29]. Hence, Alice and Bob can detect a PNS attack measuring the QBER for every intensity.

BBM92

This protocol was presented by Bennett, Brassard and Mermin just one year after Ekert's protocol [30]. In their paper, they argued that the E91 protocol can be deduced from the BB84 protocol using entanglement-based sources, and that the violation of the Bell inequality was not necessary for the security of the protocol. They presented an entanglement-based version of BB84, which only difference is that in BB84 Alice had to

choose randomly the polarization of the photons, whereas in this protocol the randomness is inherent to the measurement.

COW

This protocol is based on weak coherent pulses, it was presented by Nicolas Gisin in 2004 [41]. It is experimentally simple and tolerance to PNS attacks. In this protocol the information is encoded in time: Alice sends coherent pulses with zero or less than one mean photons (as well as some decoy states). Bob measures the time of arrival of the photons, since it is different for the binary "0" and the binary "1". For checking if an eavesdropper was listening, Bob measures randomly in another detector the coherence between successive non-empty pulses. If someone disturbed the system, the coherence between these pulses will be lost, and Bob would be able to notice it.

4.4 Eavesdropping

In quantum cryptography, designing new more advanced protocols is as important as studying their limits. Cryptoanalysis is the field that studies how to break these protocols and what are their bounds. For doing so, the field uses the theory of quantum information, which combines the quantum mechanics and the information theory in a relatively new and complex theory. This section introduces briefly this topic, with a few strategies for Eve to eavesdrop the systems.

4.4.1 The simplest attack: the intercept-resend strategy

As it has been discussed in section 4.1.1, in the intercept-resend strategy Eve measures the photons before Bob receives them, and then she sends new photons to Bob according to her results. This is the simplest strategy one could think for eavesdropping the communication.

Assuming long keys are used, this strategy would give Eve full information of half of the bits, then $I_E = 0.5$ (where I_E is the information that Eve has about the key). Eve will also introduce an error (QBER) of 25% ($Q = 25\%$). The question is whether it is possible to extract a secure key from this raw key. The answer is positive as long as the mutual information between Alice and Bob ($I(A,B)$) is greater than the information of Eve, where:

$$I(A,B) = H(A) - H(A|B) \quad (4.32)$$

Assuming bit 0 and bit 1 are equally probable [36]:

$$I(A,B) = 1 - h_b(Q) \quad (4.33)$$

In this case, $I(A,B) = 1 - 0.81 = 0.19$, so $I(A,B) < I_E$ and no secret key can be extracted. Notice that this does not mean the protocol is not secure, since Alice and Bob can check the QBER of the system and infer that an eavesdropper was listening. Nevertheless, Eve could try another strategy which will introduce less QBER. For instance, she could try to intercept only a fraction p of the photons, in this case $Q = p/4$ and $I_E = p/2$. This generalized model concludes that if Alice and Bob detect a QBER greater than 17%, a secure key can not be extracted, since it is not possible to guarantee that Eve has less information than them.

In the real world, the systems are not perfect, so they introduce errors as well. Any system introducing an error greater than 17% is not usable for quantum cryptography applications for the reasons explained. This is why it is important to characterized well the system, its devices and the channel, and the reason why many investigations are trying to develop some more accuracy devices. The technological state and challenges for quantum cryptography will be introduced in chapters 4, 5 and 6 of this dissertation.

As it is shown in figure 4.8, Eve could gain some information about the key, without introducing too much error in the system, if she just intercept a small fraction of the photons. For overcoming this issue, after Alice and Bob has completed the second stage of the protocol, they will perform some classic algorithms known as error-correction and privacy amplification. The former is used for generating a longer sifted key correcting some errors introduced by the channel (any classic error-correction algorithms can be used), while the latter will perform some operations to reduce the amount of information Eve might have. For instance, Alice could tell Bob to perform the operation XOR with bits number x and y , if Eve does not know any of the the two bits, she will no be able to infer the new result.

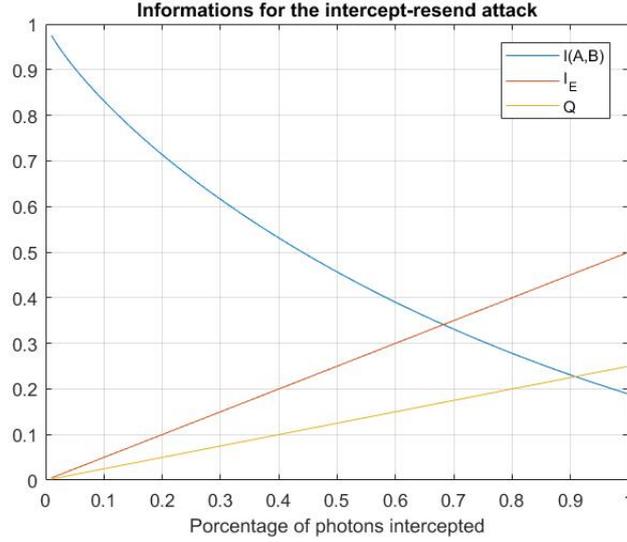


Figure 4.8 The limit for the intercept-resend attack.

4.4.2 Optimal individual attack

Previous section analyzed the limits of the intercept-resend attack. This is the simplest attack Eve could think for eavesdropping the communication between Alice and Bob, nevertheless, it is not the best. There are more sophisticated attacks she could perform. This section will analyze the optimal individual and symmetric attack [48]. Individual because photons are attacked one by one, and symmetrical because the disturbance produced in one basis, is exactly the same for the other basis. The theory commented here, is more advanced than the one commented during the dissertation. For understanding the mathematics, the reader should have a deeper knowledge about quantum entanglement and the density matrix formalism [7]. If not, the section is written so the main idea of this kind of attacks can be extracted.

The principle of the attack is based on exploiting the quantum entanglement properties. In quantum mechanics, when a system (for instance, a photon) interact with another system (for instance, another photon), the whole system can be no longer described independently for each photon. Instead, the photons will be entangled now, and this has to be considered for extracting information about the system. Notice, however, that this interaction must follow the rules of the quantum mechanics, therefore, it should be unitary. The density matrix formalism is very useful when working under this conditions. For performing the attack then, Eve will let a system of her choice, interact with the photons sent by Alice. If $|\vec{m}\rangle$ denotes the initial state of Alice's photon, $|0\rangle$ the initial state of Eve's probe, and U the unitary interaction, then the state received by Bob is given by the density matrix obtained by tracing out Eve's probe:

$$\rho_{Bob}(\vec{m}) = Tr_{Eve}(U|\vec{m}, 0\rangle\langle\vec{m}, 0|U^\dagger) \quad (4.34)$$

If the unitary transformation is applied when Alice sends a photon vertically polarized ($|\uparrow\rangle$) or horizontally polarized ($|\downarrow\rangle$) (the Bloch sphere notation is used here), then the interaction can be expressed as:

$$U|\uparrow, 0\rangle = |\uparrow\rangle \otimes (|\phi_\uparrow\rangle + |\theta_\uparrow\rangle) = |\uparrow\rangle \otimes |\phi_\uparrow\rangle + |\downarrow\rangle \otimes |\theta_\uparrow\rangle \quad (4.35)$$

$$U|\downarrow, 0\rangle = |\downarrow\rangle \otimes (|\phi_\downarrow\rangle + |\theta_\downarrow\rangle) = |\downarrow\rangle \otimes |\phi_\downarrow\rangle + |\uparrow\rangle \otimes |\theta_\downarrow\rangle \quad (4.36)$$

where $|\phi_\uparrow\rangle$ belongs to Eve's probe Hilbert space when the photon $|\uparrow\rangle$ has not been perturbed, while $|\theta_\uparrow\rangle$ belongs to Eve's probe Hilbert space when the photon $|\uparrow\rangle$ has been perturbed, and satisfy $\phi_\uparrow \perp \theta_\uparrow$ and $\phi_\downarrow \perp \theta_\downarrow$. $|\phi_\uparrow|^2$ or $|\phi_\downarrow|^2$ will define the fidelity of the system (\mathcal{F}), while $|\theta_\uparrow|^2$ or $|\theta_\downarrow|^2$ will define the QBER (\mathcal{D}). Imposing the unitary conditions, it can be found that:

$$\mathcal{F} + \mathcal{D} = 1 \quad (4.37)$$

$$\langle \phi_{\uparrow} | \theta_{\downarrow} \rangle + \langle \theta_{\uparrow} | \phi_{\downarrow} \rangle = 0 \quad (4.38)$$

Understanding the diagonal states as a superposition of the vertical and horizontal states, it is not difficult to show that:

$$U | \rightarrow, 0 \rangle = U \frac{|\uparrow, 0\rangle + |\downarrow, 0\rangle}{\sqrt{2}} = | \rightarrow \rangle \otimes |\phi_{\rightarrow}\rangle + | \leftarrow \rangle \otimes |\theta_{\rightarrow}\rangle \quad (4.39)$$

$$U | \leftarrow, 0 \rangle = U \frac{|\uparrow, 0\rangle - |\downarrow, 0\rangle}{\sqrt{2}} = | \leftarrow \rangle \otimes |\phi_{\leftarrow}\rangle + | \rightarrow \rangle \otimes |\theta_{\leftarrow}\rangle \quad (4.40)$$

where:

$$|\phi_{\rightarrow}\rangle = \frac{1}{2}(\phi_{\uparrow} + \theta_{\uparrow} + \phi_{\downarrow} + \theta_{\downarrow}) \quad (4.41)$$

$$|\theta_{\rightarrow}\rangle = \frac{1}{2}(\phi_{\uparrow} - \theta_{\uparrow} - \phi_{\downarrow} + \theta_{\downarrow}) \quad (4.42)$$

$$|\phi_{\leftarrow}\rangle = \frac{1}{2}(\phi_{\uparrow} - \theta_{\uparrow} + \phi_{\downarrow} - \theta_{\downarrow}) \quad (4.43)$$

$$|\theta_{\leftarrow}\rangle = \frac{1}{2}(\phi_{\uparrow} + \theta_{\uparrow} - \phi_{\downarrow} - \theta_{\downarrow}) \quad (4.44)$$

It can be showed that all scalar products among Eve's states are real, and hence, the subspace generated by ϕ and θ are orthogonal, since:

$$\langle \phi_{\uparrow} | \theta_{\downarrow} \rangle = \langle \theta_{\uparrow} | \phi_{\downarrow} \rangle = 0 \quad (4.45)$$

This is a key result, since it will be used by Eve to optimize the measurement. Finally, by symmetry, $|\phi_{\rightarrow}\rangle^2 = \mathcal{F}$. Operating $|\phi_{\rightarrow}\rangle\langle\phi_{\rightarrow}|$, it can be proved that:

$$\mathcal{F} = \frac{1 + \langle \hat{\theta}_{\uparrow} | \hat{\theta}_{\downarrow} \rangle}{2 - \langle \hat{\phi}_{\uparrow} | \hat{\phi}_{\downarrow} \rangle + \langle \hat{\theta}_{\uparrow} | \hat{\theta}_{\downarrow} \rangle} \quad (4.46)$$

where hats denote normalized states. Therefore, the fidelity of the system only depends on two scalar products: $\langle \hat{\phi}_{\uparrow} | \hat{\phi}_{\downarrow} \rangle = \cos(x)$ and $\langle \hat{\theta}_{\uparrow} | \hat{\theta}_{\downarrow} \rangle = \sin(y)$. Being x and y the angles between Eve's states ϕ and θ respectively.

Because of the symmetry of the system, it is sufficed to analyzed the measurement when Alice has sent the photon $|\uparrow\rangle$ and Bob has measured in the same basis (otherwise the qbit will be dropped so it will be not useful). For Eve performing an optimal attack, she will wait till Alice and Bob have published the basis they used for their photons (Eve can know this information because it is sent across a classic channel). Knowing this, Eve can deduce that her probe will be in one of these two states:

$$\rho_{Eve}(\uparrow) = \mathcal{F} |\phi_{\uparrow}\rangle\langle\phi_{\uparrow}| + \mathcal{D} |\theta_{\uparrow}\rangle\langle\theta_{\uparrow}| \quad (4.47)$$

$$\rho_{Eve}(\downarrow) = \mathcal{F} |\phi_{\downarrow}\rangle\langle\phi_{\downarrow}| + \mathcal{D} |\theta_{\downarrow}\rangle\langle\theta_{\downarrow}| \quad (4.48)$$

However, because ϕ and θ are orthogonal, Eve could distinguish if her probe is in the subspace generated by ϕ or by θ without perturbing the system. After doing so, Eve will have to distinguish again between two pure states, with an overlap of $\cos(x)$ or $\cos(y)$. The first happens with a probability of \mathcal{F} , while the second happens with a probability of \mathcal{D} . Hence, Eve will obtain the correct measurement when distinguish the two states with overlap $\cos(x)$ with a probability of $\frac{1+\sin x}{2}$ [37]

Hence, Eve and Alice mutual information can be expressed as:

$$I(A,E) = \mathcal{F} \left(1 - h_b\left(\frac{1 + \sin x}{2}\right)\right) + \mathcal{D} \left(1 - h_b\left(\frac{1 + \sin y}{2}\right)\right) \quad (4.49)$$

which is maximal when $x = y$

$$I^{max}(A,E) = 1 - h_b\left(\frac{1 + \sin x}{2}\right) \quad (4.50)$$

Remembering Alice and Bob mutual information was $I(A,B) = 1 - h_b(\mathcal{D})$. The condition $I(A,B) = I^{max}(E,A)$ is satisfied when:

$$I(A,B) = I^{max}(A,E) \Leftrightarrow \mathcal{D} = \mathcal{D}_0 = \frac{1 - 1/\sqrt{2}}{2} = 15\% \tag{4.51}$$

Consequently, the bound for the individual symmetric attacks is 15%, and not the 17% found with the intercept-resend strategy. If instead of individual attacks, coherent attacks (where Eve manipulate several photons at the same time) are considered, even a lower bound of $QBER = 11\%$ is found [48].

4.4.3 Other attacks

A Feasible Attack

Many attacks presented and studied in papers are viable in principle, however, the technology they required is only available at laboratory levels or it is even not yet developed. This section will overview a feasible attack with the devices that are currently available [48].

In this attack Eve will introduce a beamsplitter between Alice and Bob, dividing each pulse in two, each one would be measured with a different basis according to figure 4.9. If Eve can distinguish among pulses with 0, 1 or 2 photons, she will be able to intercept the pulses with 2 photons, blocking the other pulses. Whenever a pulse with two photons go through a 50:50 beamsplitter, there is a 50% chance that both photons will come out from the same detector. In this case, if the basis is the same one Alice used, the outcome of the two photons will be the same, in the other case there is a 50% chance that the outcome will be the same. Hence, for all pulses with two photons, the probability of getting the same outcome is:

$$\begin{aligned} P_{same} &= P_{same-way} \cdot P_{same-basis} \cdot P_{same-out} + P_{same-way} \cdot P_{different-basis} \cdot P_{same-out} \\ &= \frac{1}{2} \cdot \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8} \end{aligned} \tag{4.52}$$

If Eve only resend a photon to Bob whenever she detects the same output, she will resend only a fraction of 3/8 of the pulses with two photons. She will introduce a $QBER = 1/6$, gaining an information of $I_E = 2/3$, leaving Eve in a better situation than the intercept-resend attack.

To counter this attack, Alice must use a small photon mean number such that Eve could only apply this attack to a small fraction of this pulses, introducing a high QBER in pulses with 0 or 1 photon.

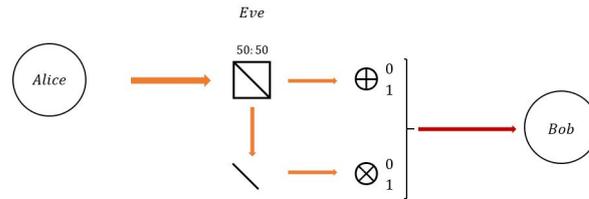


Figure 4.9 The scheme used by Eve to perform a feasible attack.

Trojan horse attack

All the strategies discussed up to now were focus on Eve trying to get the maximum information about Alice qubits. However, Eve can follow some completely different strategies for her attacks, for instance, she could send signals into Alice’s and Bob’s systems in order to know which devices they use every moment. These kind of attacks are called Trojan horse attacks [48].

Eve could in principle send signal across the fiber optic, and analyze the backreflected light, this way she could know which laser Alice just used, or which detector just fired at Bob’s side. The use of shutters is not possible since Alice and Bob must let the light go in and out. What they can do, is set up their systems so that the backreflected light is very small and its analysis very difficult, which can be made with a good calibration

on the devices. Although these kind of attacks can be prevented in practice, they show that the security on QKD protocols not only depend on quantum mechanics but also on technological issues.

5 Photon Sources

Chapter 4 discussed the field of quantum cryptography, introducing its most important protocols. However, these protocols were explained from a theoretical point of view, leaving the discussion of the engineering aspect for the next chapters. From this engineering point of view, two entities are the main concern for QKD systems: the transmitter (or the source) and the receiver (or the detector). They must be studied and well understood in order to being able to perfect them and to develop and implement commercial QKD systems. There is also a third important entity: the channel. Its main difference is that it is much more difficult to change (sometimes impossible), so most of the time it is just analyzed to adapt the systems and the protocols the best way possible.

This chapter will be focused on the transmitter, leaving the other two entities for the next chapters. The transmitter can be very complex, nevertheless, this chapter only introduces the most important devices of it: the single-photon sources. The chapter is organized as follows: first, the only pseudo-single photon source available at the moment is presented in section 5.1; second, some candidates for being the future single photon sources are analyzed in sections 5.2 and 5.3; in section 5.4 the sources for generating entanglement photons are introduced; and to conclude, a brief overview of the current development on sources is given in section 5.6.

5.1 Weak coherent pulses

As it has been commented during this dissertation, the single photons sources are not commercially available yet. They still need much more investment and researching before they can be used for QKD implementations. This is why most of QKD experiments use weak coherent pulses (WCP) currently, which are coherent laser pulses very attenuated (see figure 5.1), so that the mean photon number per pulse (μ) is lower than 1.

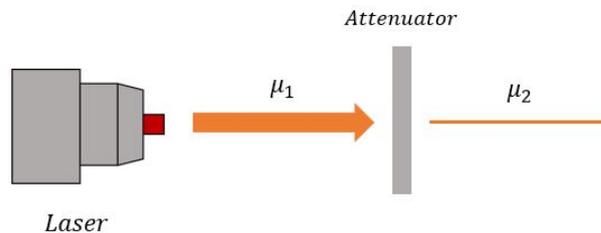


Figure 5.1 Scheme for a weak coherent pulse source.

This means that not every pulse will contain just one photon. On the contrary, there will be pulses with more than one photon (allowing Eve performing PNS attacks), and with no photons at all. Having no photons in a pulse will decrease the bit rate for generating secret keys (although this can be compensated with GHz

modulation). Besides, it will increase the total number of dark counts (since the detector must be active for all pulses), increasing the ratio of dark counts over detected photons, hence, introducing a noise, which will increase whenever μ decrease [8].

The numbers of photons generated per pulse will follow a Poissonian distribution, that is to say, the probability of finding n photon in a pulse emitted by a source with a mean photon number μ is:

$$p(n, \mu) = \frac{\mu^n e^{-\mu}}{n!} \quad (5.1)$$

Deciding which μ should be used depends on the application, however, a typical value for QKD experiments is $\mu = 0.1$. For this one, and other typical values, most of the pulses will contain no photons.

The probability of a pulse which contain photons, containing more than one photon is:

$$p(n > 1 | n > 0, \mu) = \frac{1 - p(0, \mu) - p(1, \mu)}{1 - p(0, \mu)} \quad (5.2)$$

Using equation (5.1):

$$p(n > 1 | n > 0, \mu) = \frac{1 - e^{-\mu}(1 + \mu)}{1 - e^{-\mu}} \quad (5.3)$$

Which gives, for $\mu = 0.1$, a fraction of 5% of the pulses (figure 5.2 shows the probability of finding n photons in different pulses). These would be the pulses Eve could use to performing PNS attacks. It is obvious why these sources are not perfect, therefore, they are just a temporary solution while true single photon sources are developed.

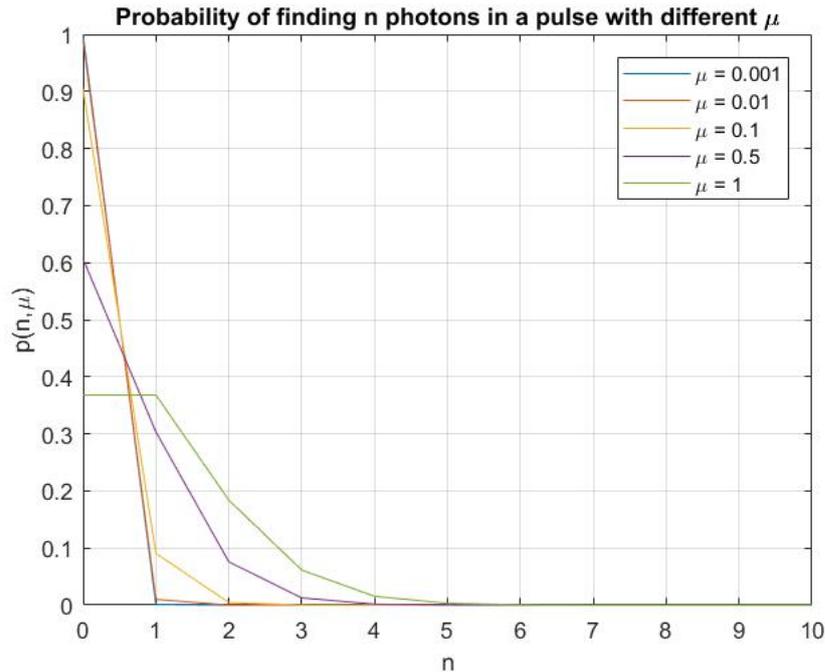


Figure 5.2 The probability of finding n photons in a pulse with mean equal to μ .

5.2 The simplest source: the single hydrogen atom

Because of the disadvantages of WCP, true single photon sources are needed for improving QKD implementations. One of the simplest of these sources is the two level atom system, which takes advantage of the absorption and the spontaneous emission phenomenons. In this system, an electron will be excited

by a pulse to a higher energy state, this electron will eventually decay to the previous state because of the spontaneous emission, emitting a photon in the process (see figure 5.3) [16] [8]. The wavelength of this photon is proportional to the energy gap between the two states, as it follows:

$$\lambda = \frac{hc}{\Delta E} = \frac{c}{\nu} \quad (5.4)$$

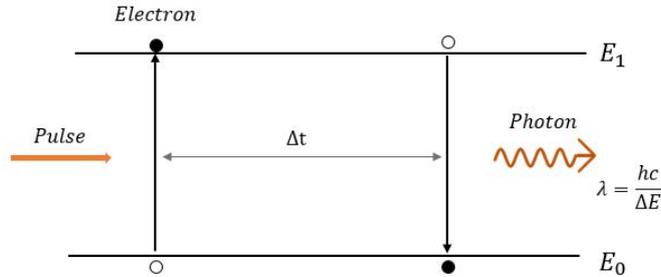


Figure 5.3 The scheme for a two level atom system as a single photon source.

Once the electron has been absorbed, no pulse will excite it again until the electron has decay to the lowest energy level. On the other hand, once the electron decays, it will not be excited again until the next pulse is emitted. This shows the limitations of this kind of source, either is bounded by the frequency of the laser or it is limited by the radiation lifetime of the energy level (τ_{E_1}).

Another issue in this system is the problematic of isolating a single atom. Atomic spacing are of the order of 10^{-1} nm. If a pulse illuminates two or more atoms at the same time, they could generate more than one photon. Hence, although these single photon sources are conceptually simple and easy to understand, the technological issues make them unlikely to become commercially available for QKD applications.

5.3 Quantum dots

Section 2.2.6 introduced the concept of bands and gaps in the structure of a solid. Within a allowed energy band, an electron has a density of states (number of allowed states) almost continuous. However, if the movement of these electrons is confined, the density of states of them is discretized. This quantum confinement allows some interesting properties which can be exploited in order to design single photon sources.

5.3.1 Quantum confinement

For discretizing the states of an electron, it must be confined in a space which volume would be comparable to its de Broglie wavelength λ_{deB} [16]. The de Broglie wavelength is the wave which characterize a particle with a momentum p :

$$\lambda_{deB} = \frac{h}{p} \quad (5.5)$$

The movement of the electron can be confined in each direction independently. If only one direction of the motion is discretized, the structure is called **quantum well**, if two directions of the motion are confined, the structure is called **quantum wire**, finally if the electron is confined along its three directions, the structure is called **quantum dot** (see figure 5.4). In a typical semiconductor, for confining electrons, the scale of the volume must be about 10 nm.

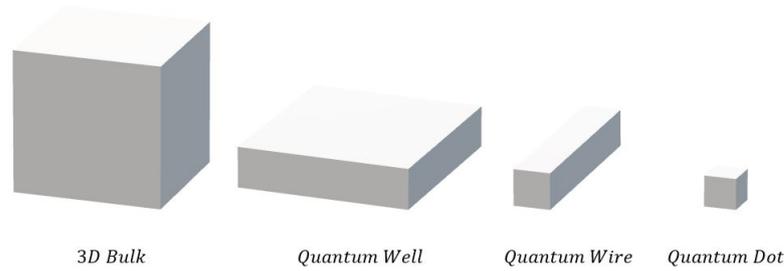


Figure 5.4 Comparison among the different kind of quantum confinement.

5.3.2 Quantum dots

Within a typical quantum dot, there are somewhere in the region of several hundred to thousands atoms. Due to the confinement, quantum dots have discretized energy levels, that is to say, they behave like atoms. These quantum dots are a promising single-photon source since they can be optically excited, promoting electrons to excited levels, which emit photons after they decay to the ground level again. The gap size between the energy bands can be controlled by the size of the confinement, the smaller the size is, the larger the energy gap would be. This makes possible to control the energy of the photon emitted. With this technology, $g^{(2)}(0)$ of 0.4 and 0.166 have been achieved in QKD experiments [5] [40].

5.3.3 Electrical triggered single photon source

The easiest way for exciting the single photon sources is by an optic pulses. However, if they want to be commercially available, systems where the pulse is electric must be developed. An example of such systems is represented in figure 5.5. The source would be a LED with a layer of quantum dots inserted within the active region. The electric pulses will inject electrons and holes into the LED, and the quantum dots will emit photons in response to these pulses. Each quantum dot will emit with different wavelengths, hence they could be selected with a spectral filter [16].

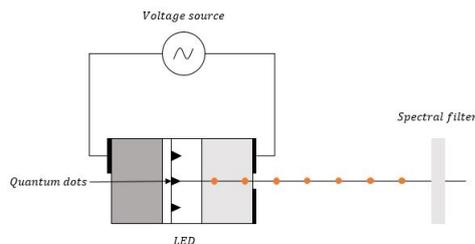


Figure 5.5 An example of a single photon source triggered with electric pulses.

5.4 Generation of entangled photons

The generation of entangled photons pairs is key for entanglement-based protocols. One of the first experiments for generating them, employed atomic cascades. In the experiment, the electrons of a calcium atom were excited to the level $4p^2\ ^1S_0$. The cascade occurs because of the allowed transition to the level $4s^2\ ^1S_0$ via the intermediate level $4p\ 4s\ ^1P_1$. (see figure 5.6) [16].

The initial and final states have both no angular momentum ($J = 0$), which means that the angular momentum of the two generated photons must be zero as well. Moreover, the fact that both states have the same even

parity, requires that the polarization of both photons were correlated. The entanglement was demonstrated by placing polarizers filters after the sources and different detector behind them.

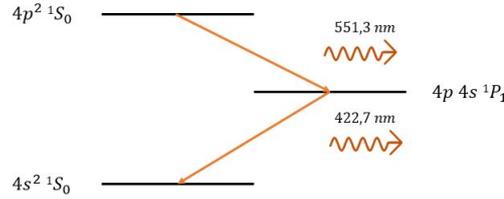


Figure 5.6 The cascade decay for generating a pair of entangled photons within a calcium atom.

5.5 Parametric down conversion

Nowadays, the most common way for generating entanglement photons pair is by the process known as **parametric down conversion**. In this process, non-linear optic effects are used. Taking advantage of the down conversion process, a non-linear crystal is illuminated with a pump laser at angular frequency ω_0 , which is converted into two idler photons with angular frequency ω_1 and ω_2 . Because of conservation of energy and momentum:

$$\omega_0 = \omega_1 + \omega_2 \quad (5.6)$$

$$\mathbf{k}_0 = \mathbf{k}_1 + \mathbf{k}_2 \quad (5.7)$$

where \mathbf{k} is the wave vector. The second condition requires that photons from the pump laser and the idler photons remain in phase through the non linear medium. Therefore, equation 5.6 and 5.7 are known as phase-matching conditions [16].

Because of the dispersion of the nonlinear crystal, satisfying the phase-matching conditions is impossible at first. However, nonlinear crystal are also birefringent, which means that the refractive index depends on the direction of the polarization of the light with respect to the crystal. Birefringence and dispersion can be compensated between them in order to satisfy the phase-matching conditions, which allows to create two kind of entanglement photon pair. In the first kind (type-I), the polarization of the down-converted photons are parallel to each other, while in the second kind (type-II), the polarization is orthogonal. Nevertheless, this method is very inefficient, since it needs about 10^{10} pump photons to generate one pair. With a typical pump power of 1 mW, 10^6 pairs are generated.

In addition, this method can be also used for single-photon sources. If the second photon is detected and it is used as a trigger, a system could let go through the first photon. This way, the number of multi-photons pulses will be reduced to zero, although empty pulses will still remain. With this method, it is possible to achieve a mean photon number per pulse of $\mu = 2/3$, well above of WCP [47].

5.6 Current development

Single photon sources are not yet available for their use in QKD experiments. Besides, the decoy state protocol showed that it is possible to achieve almost the same security with WCP. This is the reason why, most of the experiments and sources designs have been done with attenuated lasers. In this context, one of the main issues for WCP was the need of an active polarization manipulation, which reduced significantly the speed of the source. For solving this, several designs have been proposed.

For overcoming the active polarization issue, a first paper in 2006 suggested using four lasers instead of one [45]. In the design, four laser diodes were arranged around a mirror, in such a way that the four beams

would be collected and pointed into the same direction. Identifying each laser with a different polarization. However, the four spectra of the lasers are not always identical, and this could be taken in advantage by Eve to gain some extra information about the pulses.

A different design (with the same drawback) was proposed in 2011 [28]. In this design, only one laser is used, splitting the beam into four, using single-mode fiber couplers. These new four beams are then amplified via semiconductor optical amplifiers (SOA), and finally they are polarized before leaving the transmitter module. In a recent paper published in 2015 [44], the side channel was closed in a design where an array of single-mode VCSELs are used. In this scheme the beam were rotated for producing the desired polarization, and then they were recombined to result in a single output.

Concerning the entanglement photon sources, there are two main method currently, all of them based on parametric down conversion, but using different kind of crystals. Experiments with beta barium oxide (BBO) has been demonstrated [22] as well as potassium titanyl phosphate (PPKTP) [14].

6 Quantum Channels

For sending information to third parties, it is necessary to use a medium or a vacuum, which in communications is called the channel. If the information sent is quantum, then the channel is known as a quantum channel. For quantum cryptography, there are two kind of them. The first one, and the most obvious since this technology uses light, is the optical fiber. Optical fibers confined the light so it does not disperse. Besides, they are quite well developed nowadays, since they are widely used in telecommunication engineering. Because of that, their current losses are very low (0.2 dB/km). In contrast, they do not maintain the polarization of the light, and their losses, although being low, are not low enough for real QKD applications.

For these reasons, there is an increasing interest in the free space links, where the qubits are sent across the atmosphere. These links have much lower losses (achieving values of 0.07 dB/km), and they do maintain the photon polarization. However, other issues such as the spread of the light, or the pointing between transmitter and receiver play a key role for the losses.

This chapter will discuss all these concepts, being organized as follows: the first section (6.1) discusses the optical fibers, and their main drawbacks are introduced along sections 6.1.1 and 6.1.2; section 6.1.3 explains how to codify the qubits in this kind of channel. The free space links are reviewed in section 6.2, introducing its main issues in section 6.2.1. To conclude, a relatively new scheme for QKD is explained in section 6.2.2: satellite QKD, which promises to bring QKD systems commercially available in a near future.

6.1 Optical Fibers

Optical fibers are currently one of the best ways for sending information using light. Within them, light is guided due to the two different refractive index, one for the core and the other one for the cladding, which make the light bouncing within the core if light is introduced properly. Because it is a very mature technology, fibers losses are nowadays very low: 2 dB/km for 800 nm, 0.35 dB/km for 1310 nm and 0.2 dB/km for 1550 nm. However, even though the losses are low, for QKD applications it might be too high. Moreover, the main disadvantage of optical fibers is their polarization effects, which make impossible to use a polarization codification for QKD applications.

Depending on the diameter of the core in comparison with the wavelength, optical fiber are classified into multimode or singlemode. In a multimode optical fiber, the core is large comparing to the wavelength of photons, and there will exit different guided modes which will coupled between them, degenerating the qubits. Hence, multimode fibers are not appropriate for QKD, instead, in singlemode fibers (when the core is small enough) only one mode will propagate [48].

Optical fibers with a perfect cylindrical symmetry would be an ideal quantum channel. However, all fibers have asymmetries and, because of them, the two polarization modes are degenerated independently.

6.1.1 Polarization effects

Polarization effects are an issue in both, classical and quantum applications. Although nowadays these effects are low enough for classical applications, they always will be an issue in QKD, no matter how small they are.

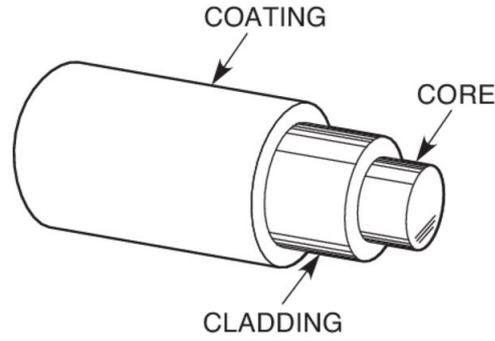


Figure 6.1 Structure of a optical fiber [3].

This is clearly a concern for polarization coding schemes, but it is as well for phase coding schemes (see section 6.1.3), where the interference visibility depends on polarization states. Therefore, it is worth it to introduce these effects, distinguish among four cases: the geometric phase, birefringence, polarization mode dispersion and polarization dependent losses.

Geometric phase

This effect is a special case of the Berry phase, which describes the difference between any parameter of a particle after a loop in the system. For light being guided within an optical fiber, the interesting parameter is the k vector. Because of the Berry phase, the polarization of a photon when entering the fiber will not be the same after exiting the fiber [48]. Nevertheless, this polarization difference is not a big issue most of the times, since it only means that Alice and Bob will have to align their system for defining which is the vertical and the diagonal axis. If this variation is constant or change slowly, Alice and Bob could track it. On the other hand, if it is too fast, the communication will be unfeasible.

Birefringence

Birefringence is the presence of two different phase velocities for two orthogonal states (all beam splitters are made of birefringence materials). The effect of the birefringence in optical fibers is equivalent to the effect of two waveplate (an optical device which changes the polarization of the light), one for each polarization. If this effect is stable, it can be compensated by Alice and Bob, as they do with the geometrical phase. For birefringence being stable, the mechanical and thermal variations must be slow [48].

There is a special case of fibers, the polarization maintaining (PM) fibers, which can maintain two orthogonal polarization modes. However, all other polarization will be disturbed. Hence, this kind of fibers are not valid for QKD.

Polarization mode dispersion

Polarization mode dispersion (PMD) is the presence of two different group velocities for two orthogonal states. In an ideal fiber, the core would have a perfectly circular symmetry. In this case, any of the two orthogonal polarization states would propagate at the same speed. In real fibers, there are always imperfections which break that symmetry. Because of them, the states will propagate at different speeds, causing the pulse to spread and overlap. These imperfections are random, so the spread of the pulse is modeled as a statistical distribution of delays δ_τ . For long enough fibers, this delay is directly related with the fiber length l , the mean coupling length h (the length over which the maximum power is transferred from one mode to the other), and the mean birefringence B as follows [48]:

$$PMD = \sqrt{\langle\langle \delta_\tau^2 \rangle\rangle} = Bh\sqrt{l/h} = D_{PMD}\sqrt{l} \quad (6.1)$$

where D_{PMD} is a parameter of the fiber measured in $\frac{ps}{\sqrt{km}}$. PMD can cause depolarization, fortunately, it has an easy remedy for quantum applications. It suffices to use a source with a larger time coherence than the delay δ_τ . This is not a problem when using lasers as sources, however, imposes great limitations when using photons generated by parametric down conversion.

Polarization dependent losses

This is another kind of loss, intrinsic to any optical device, which attenuates the light depending on its polarization [48]. In fibers, this effect is negligible. However, in some optical components can be significant, since some devices have such a high attenuation for some polarization modes that they behave almost as polarizers. Combined with the effect of birefringence, PMD produces random polarization outcomes.

6.1.2 Chromatic dispersion

Chromatic dispersion is the presence of different propagation velocities depending on the frequency. This is an important problem when using phase coding schemes (see section 6.1.3), which requires photons arriving at well defined times. As any real pulse has some bandwidth (thus, different frequencies) which propagate at different velocities, chromatic dispersion always causes a spread in the pulse.

In order to overcome this feature, photons of small bandwidth must be used, or the system should be operated in a wavelength where the fiber chromatic dispersion is close to zero. Fortunately, this wavelength is the second telecommunication window (1330 nm), where the attenuation of the fiber is low (0.35 dB/km). There also exists some fibers known as dispersion-shifted, with a refractive index such as the chromatic dispersion goes to zero at the third telecommunication window (1550 nm), where the losses are even lower (0.2 dB/km).

6.1.3 Codifying information

For implementing QKD systems, different kind of codifications can be used. So far, only the photon polarization has been explained, since it is the most natural and easiest system. Nevertheless, there exists some other kind of codification schemes which may be more advantageous depending on the case.

Polarization coding

Polarization coding was widely explained in chapter 4, so here it will not be discussed again. Yet, it is important to emphasize the limitations of this kind of coding because of the polarization effects in optical fibers. The issues are not very important at a laboratory experiment level, however, in a real application, where optical fiber will have a length of hundreds of kilometers, these effects will become much higher, making the coding unfeasible. On the other hand, all these issues are not important for free space links, because the atmosphere does not change the photon polarization. This is why it is the main codification scheme used for this kind channel [48].

Phase coding

Phase coding is another kind of coding scheme more appropriate for optical fibers, since the information is coded in the phase difference of two paths. Before introducing how this can be done, it is necessary to introduce first the Mach-Zehnder interferometer in quantum mechanics [25]. A scheme of it can be found in figure 6.2.

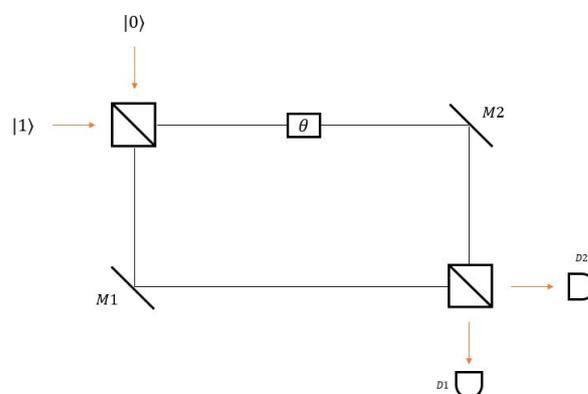


Figure 6.2 A Mach-Zehnder interferometer with a single-photon input.

As in classical physics, this interferometer can be used for constructing interference patterns, however, in this case only one photon is sent across the interferometer. This might sound counter-intuitive since one could ask how a single photon could interfere with itself. Nevertheless, it must be remembered that a photon, as a quantum particle, is represented by its wave function. This will propagate along the two different ways, and if one is larger than the other, interference at the output can be found.

Mathematically, a single photon ($|1\rangle$) is introduced for one of the beam splitters inputs, the vacuum is introduced for the other input since this field is always present in quantum optics (see section 3.2.2). After the beam splitter, the input is transformed as follows [25]:

$$|0\rangle|1\rangle \rightarrow^{BS_1} \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + i|1\rangle|0\rangle) \quad (6.2)$$

The phase shifter (θ), which could be implemented with just a larger path, cause a phase change in the first component:

$$\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + i|1\rangle|0\rangle) \rightarrow^\theta \frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle|1\rangle + i|1\rangle|0\rangle) \quad (6.3)$$

Mirrors contribute with a common factor of $e^{i\pi/2}$ for both path, so it can be omitted. Finally, after the second beam splitter:

$$\frac{1}{\sqrt{2}}(e^{i\theta}|0\rangle|1\rangle + i|1\rangle|0\rangle) \rightarrow^{BS_2} \frac{1}{2}((e^{i\theta} - 1)|0\rangle|1\rangle + i(e^{i\theta} + 1)|1\rangle|0\rangle) \quad (6.4)$$

Hence, the probability of the state $|0\rangle|1\rangle$ is detected is:

$$P_{01} = \frac{1}{2}(1 - \cos \theta) \quad (6.5)$$

Analogously, the probability of the state $|1\rangle|0\rangle$ is detected is:

$$P_{10} = \frac{1}{2}(1 + \cos \theta) \quad (6.6)$$

P_{01} represents the probability of detecting the photon at detector $D1$, and P_{10} represents the probability of detecting the photon at detector $D2$. Manipulating this path difference, it is possible to implement an equivalent of the BB84 protocol, with the system represented in figure 6.3

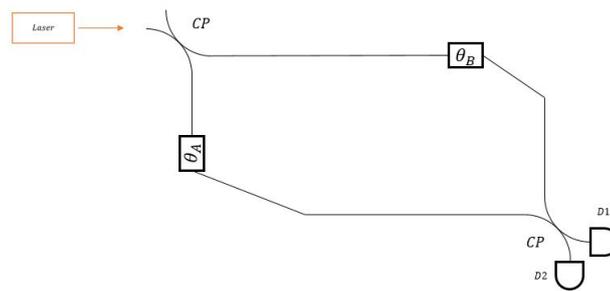


Figure 6.3 An interferometer for implementing the BB84 protocol.

In this scheme, Alice's system would be the laser, the first coupler (the equivalent to the beam splitter) and the θ_A phase shifter, while Bob's system would be the detectors, the second coupler and the θ_B phase shifter. The BB84 protocol could be implemented then, codifying the information as in table 6.1, where $\theta = \theta_A - \theta_B$.

Frequency coding

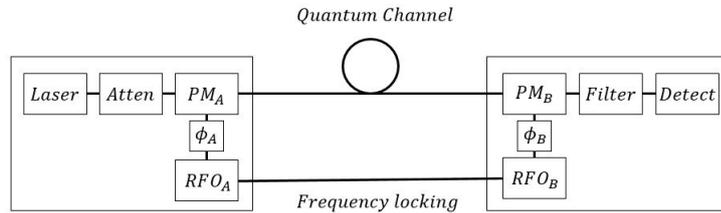
The problem of the previous system is that it is very difficult to implement when the two paths are long, because maintaining the phase stabilized during long paths is complex. For overcoming this issue, several

Table 6.1 The BB84 codification when using the phase coding scheme.

Alice		Bob		
Bit Value	θ_A	θ_B	$\theta_A - \theta_B$	Bit Value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$?
0	$\pi/2$	0	$\pi/2$?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$?
1	$3\pi/2$	$\pi/2$	π	1

modifications has been proposed [4]. However, in 1995, Prof. Goedgebuer and his team proposed a new kind of codification based on frequency [15].

In this system (see figure 6.4), Alice generates short classical pulses of monochromatic waves with an angular frequency ω_S . Then, the first modulator PM_A , which is controlled by a radio-frequency oscillator RFO_A , will modulate the signal with a frequency $\Omega \ll \omega_S$, generating two sidebands at $\omega_S \pm \Omega$, and introducing a phase ϕ_A . After an attenuation, the pulses are sent to Bob, who will modulate the pulses again with the same frequency ω_S applied by PM_B , which is controlled by RFO_B , which is synchronized with RFO_A , and introducing another phase ϕ_B . After this second modulator, the pulses will contain the original frequency ω_S , the sidebands generated by Alice and the sidebands generated by Bob. These sidebands are mutually coherent, and they interfere among them. Hence, if the difference between phases is 0, the interference will be constructive and Bob will record a photon in his detector. On the other hand, if the phase difference is π , Bob will not record a photon in his detector, and this could be counted as a loss or a wrong basis selection. With this scheme, it is easy to understand how the protocols such as B92 could be implemented.

**Figure 6.4** Scheme for a frequency based coding in QKD applications.

6.2 Free space

Because of the reasons given in section 6.1.1 and 6.1.2, the losses in optical fibers are too high currently for QKD real applications. Some experiments had been successfully performed over distances of roughly 400 km [12], however, the resulting key rates were too low. Nowadays, for getting high enough key rates, the maximum distance for a system is about 100 km, something not enough for commercial applications. This is the reason why, the interest in free space links is raising, since they offer much lower losses and the possibility of constructing a QKD network in the near future. This section will introduce the free space links.

6.2.1 Free space links

Free space links offer two major advantages against optical fibers. First, it has much lower losses at a wavelength of 770 nm, where detectors are very efficient. It is possible to achieve an attenuation of 0.07 dB/km at 2400 m above the sea-level, with higher attenuation at lower levels, and a negligible attenuation

above the atmosphere [26]. Second, the atmosphere is not birefringent, so the polarization of the photons is maintained.

On the other hand, there are some problems which optical fibers do not have. For instance, while in the fibers the light was guided and localized, in the atmosphere the light spreads out. Moreover, the daylight or even the light from the moon can be detected, causing higher QBERs in the systems. This is specially important during the day, although it can be decreased using spacial filters and timing discrimination [48]. Finally, there is a great dependence on the atmospheric conditions, which will determine the performance of the system.

There exists some issues concerning the sources as well. The most important one is the transmission of wave through a turbulence medium. The atmospheric turbulence (small random fluctuations of the dielectric constant of the atmosphere) cause wave form distortion, a decrease in the spatial coherence, a wander in the beam, etc [42]. Because of them, the pointing between the transmitter and the receiver can introduced several losses (over 20 dB). Fortunately, the rate of changing of this turbulence is small compared with the speed of light, so a first pulse can be sent as a reference in order to compensate the effects of the atmospheric turbulence.

Finally, another problem is the beam divergence, which forces the receptor to be larger in order to be able to detect all the light. Nevertheless, this issue can be kept small taking advantage of larger optics.

6.2.2 Satellite QKD

Because of the problems with optical fibers and the advantages of free space links, a QKD scheme based on satellite is increasing in popularity lately [26]. In this scenario, satellites would orbit the Earth, enabling a wireless network for maintaining quantum communications and sharing secret keys. Most of the proposed schemes consider the satellites trusted-nodes, which would carry out operations with ground stations on the Earth.

These topologies have some security advantages. Although the satellite must be trusted, ground stations can be subject to constant surveillance, so they can be supposed to be secure. Moreover, attacks that require access to the channel would face higher difficulties since the channel would be constantly moving. Finally, denial-of-services attacks would not be an issue if the satellite is the transmitter, although they could be important whenever the satellite would be the receiver.

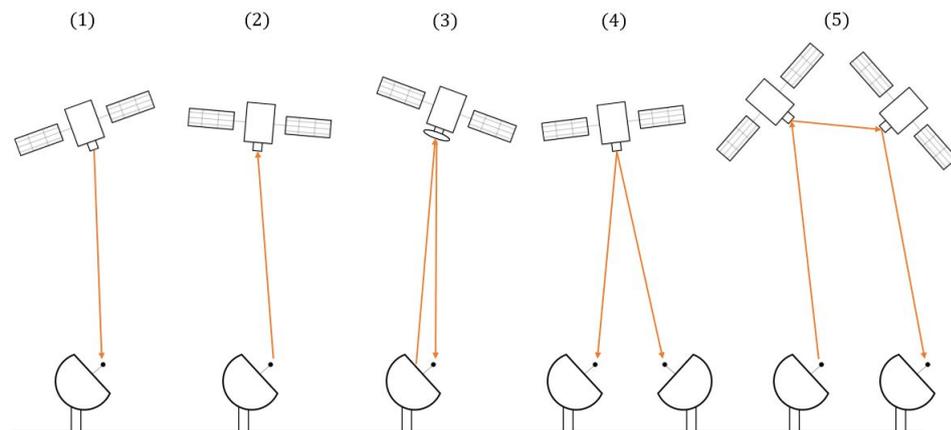


Figure 6.5 Different scenarios for satellite QKD.

Satellite QKD can be classified either as uplinks or as downlinks, as it is illustrated in figure 6.5. For every configuration there are advantages and disadvantages. However, the most common scenario, and the only one that has been demonstrated yet, is the downlink (1). This is because downlinks always have lower losses due to the beam only suffers the atmospheric turbulence almost at the receiver, which cause the beam to be most accurate. The main advantages for uplinks (2) is that there is not need to locate a complex quantum source in

the satellite. Another scenario for downlinks is the use of retro-reflectors on the satellite (3), where the ground station could send a powerful beam to the satellite and then, this would modulate the signal to send it back to the ground station. Option (4) allows satellite QKD to perform entanglement based protocols, for doing so, an entangled photon pair source is located on the satellite, this configuration was recently demonstrated by the Chinese Micius satellite [13]. In this scenario the satellite would not require to be trusted. Finally, satellite QKD could be used in a more advanced stage to build complex QKD networks around the world (5).

Depending on the orbit altitude, satellites are classified also in three categories: Low Earth orbit (LEO), between 600 to 3000 km, Medium Earth orbit (MEO), between LEO and GEO, and Geostationary orbit (GEO), with an altitude of 35,786 km. LEO and GEO are the most suitable options for satellite QKD. A satellite in LEO would take advantages of its low altitude, reducing losses due to beam diffraction. On contrary, because of its high speed it would be difficult to point it accurately, as well as the fact that QKD would only be able to perform during the flyover time. GEO satellite could run continuously, at the expense of much higher losses.

7 Receivers

This dissertation has already discussed about sources and the channel. This chapter will finally introduce the last entity in a communication system: the receiver. As it was the case for sources, the receiver can be very complex. Nevertheless, only its main component will be discussed here: the single-photon detectors, since they are ideal for QKD systems. There are a few kind of technologies for them, however, the most important one currently are the avalanche photo diodes (APD). Therefore, this chapter will be focused on them mainly.

The chapter is organized as follows: the first section (7.1) will give an introduction of APD, starting from its basis, the p-n junction (section 7.1.1), going through some general concepts of semiconductor diodes in section 7.1.2, an introduction of the APD in section 7.1.3, and finally, talking about the specific implementation used in QKD, in sections 7.1.4 and 7.1.5, and the main technologies and their current development in section 7.1.6. During section 7.2, some other detector will be briefly introduced to give a bigger picture of the state of art of detectors in QKD systems.

7.1 Avalanche photo diodes

Avalanche photo diodes are a photodetector semiconductor technology. Semiconductors are special materials which can have the electrical properties of a conductor or an insulator, depending on the conditions. They are typically doped with other atoms to add some impurities to form n-type or p-type crystals. Then, they are joined between in order to form pn junctions with unique characteristics.

This technology has several applications, and it has entailed a huge revolution in the electronic devices (the most important one may be the transistor). It is also very important in optic communications, specially for building sources and detectors. During this section, the most interesting kind of semiconductor detector for QKD systems (the avalanche photo diode) will be presented from its basis to the current development.

7.1.1 The p-n junction

Diodes are made of the junction of an electrical neutral donor-doped semiconductor material (which has more electrons than holes, also called a n-type semiconductor) and an electrical neutral acceptor-doped semiconductor material (which has more holes than electrons, also called a p-type semiconductor), separated by a narrow transition zone, called the metallurgical junction. It is also called the p-n junction and it is the most important zone of a semiconductor [24]. because of its properties.

When a n-type semiconductor and a p-type semiconductor are joined, at the beginning, there is a concentration of electrons n_{n0} and holes p_{n0} in the n-type region, as well as there is a concentration of electrons n_{p0} and holes p_{p0} in the p-type region. However, in the n-type region there are much more electrons than holes, while in the p-type region there are much more holes than electrons. This difference in the carriers makes the electrons in the n-type move to the p-type region and holes in the p-type to move to the n-type region because of diffusion currents [31]. Yet, this flux of carriers will not be indefinite, since ions next to the junctions will not be electrical neutral any longer. Hence, the net positive and negative charges induce an electrical field in the direction from the n to the p region. These regions are shown in figure 7.1, the two regions free of

carriers are called the **space charge region** or the **depletion region**. The electric field will establish balance conditions within the semiconductor, together with the 'diffusion forces', so the semiconductor will reach an stable state in a thermal equilibrium.

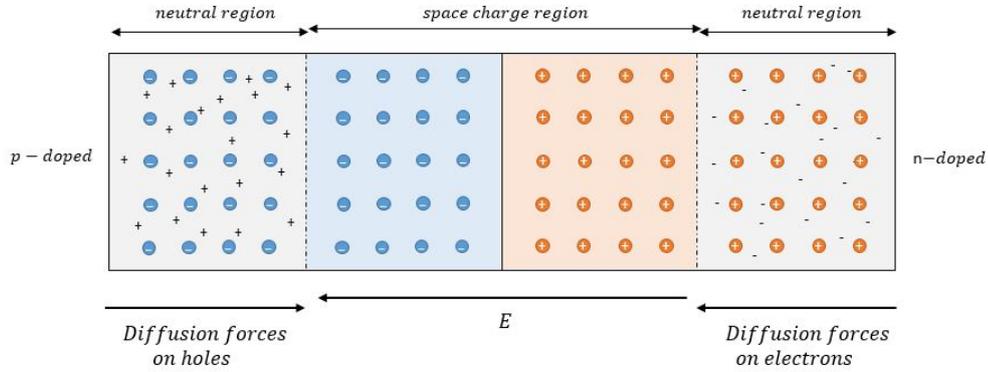


Figure 7.1 A representation of the concentration of electrons and holes in pn junction.

Because of the electric field, there will exit a difference of potential V_0 between the regions n and p. Therefore, an electron in the p-region will have a greater potential than an electron in the n-region a quantity equal to qV_0 , applying the same for holes in the n-region. Moreover, because the system is in a thermal equilibrium, the Fermi level must be the same in the whole semiconductor [24]. These considerations make the representation of the energy bands in the figure 7.2 possible. When the junction is connected to two metallic connectors, the device is called a diode. The connector at the p-region is called the anode, while the connector at the n-region is called the cathode.

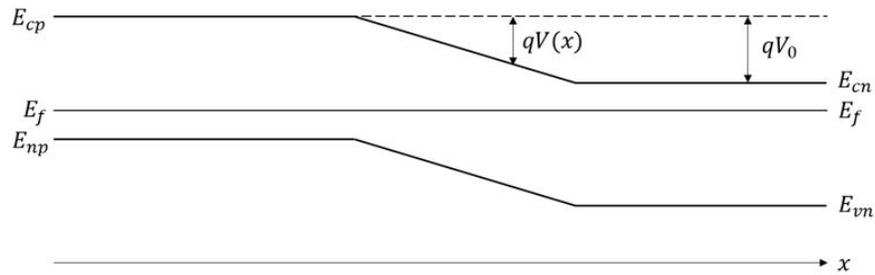


Figure 7.2 The energy bands in pn junction with no electric field applied and under thermal equilibrium conditions.

The electron and holes concentrations in the conduction and valance band respectively can be expressed as [31]:

$$n_0 = N_c e^{-\frac{E_{cn}-E_f}{kT}} \tag{7.1}$$

$$p_0 = N_c e^{-\frac{E_{cp}-E_f}{kT}} \tag{7.2}$$

where N_c is the effective density of states, E_{cn} and E_{cp} are the minimum allowed energies for the conduction band in the n and p region respectively, E_f is the Fermi level, k is the Boltzmann constant and T the temperature.

The potential V_0 is defined as:

$$V_0 = \frac{kT}{e} \ln \frac{N_a N_d}{n_i^2} \quad (7.3)$$

where N_a and N_d are the impurities concentration at the n and p region respectively, and $n_i^2 = n_0 \cdot p_0$.

Knowing this density, it is possible to deduce the electric field E and the potential energy V integrating them:

$$E(x) = \frac{1}{\epsilon_s} \int_{-x_p}^{x_n} \rho(x) dx \quad (7.4)$$

$$V(x) = - \int_{-x_p}^{x_n} E(x) dx \quad (7.5)$$

Figure 7.3 shows the typical density charge distribution (ρ) in a pn junction, its electric field and the potential.

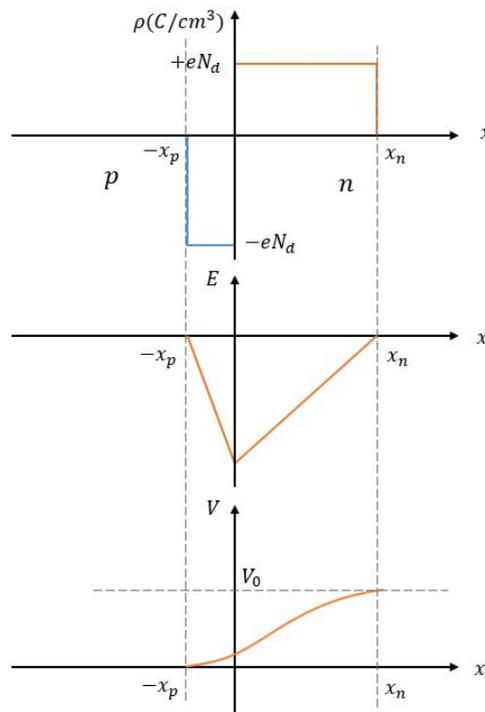


Figure 7.3 Density charge distribution, electric field and electric potential for a generic pn junction.

The biased p-n junction

When a potential (V_D) is applied between the anode and the cathode, the behavior of the device changes. If the potential difference is positive, the potential energy of the electrons in the n region will increase with respect of the electrons in the p region. Hence, the potential difference between the two regions will decrease to $q(V_0 - V_D)$. Otherwise, if the potential difference is negative, the potential energy of electrons in region n will decrease with respect to the electrons in the region p. Hence, the potential difference between the two regions will increase to $q(V_0 + V_D)$ [24]. The new energy bands are represented in figure 7.4.

Because of the reasons mentioned above, a p-n junction with a direct (positive) bias will behave as a good conductor, while if it has a reverse (negative) bias the device will behave as a good insulator. The latter is the configuration used for photodetectors, the devices we are interested in.

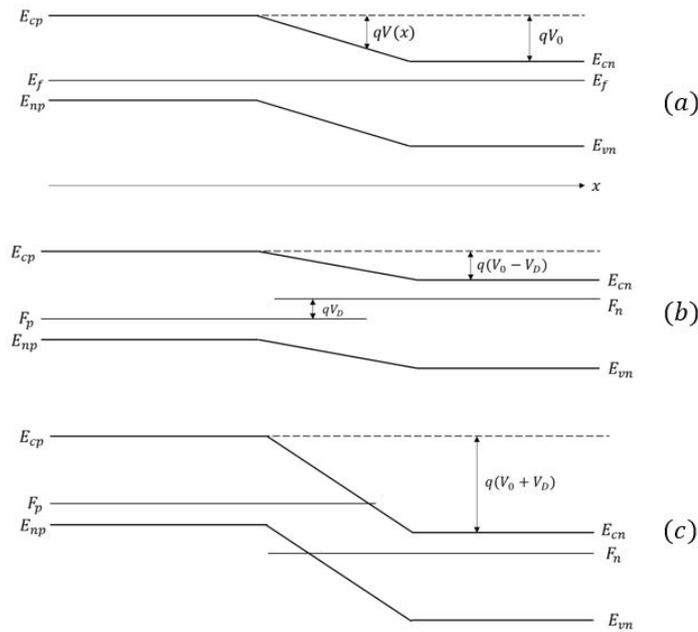


Figure 7.4 The energy bands in pn junction under thermal equilibrium conditions with: (a) no electric field applied, (b) a direct polarization, (c) a reverse polarization.

7.1.2 Photodetectors

Photodetectors are mainly build nowadays with the pn junction technology, if so, they are known as semi-conductors photodetectors. Specifically, the most important ones are the diodes with a reverse bias. These devices have similar characteristics than the insulators: no current will go through them if there is not an excitation in the system. However, if a photon illuminates the device, and if it is absorbed (because of the stimulated absorption process) an electron-hole pair will be generated within the p-n junction. The pair will be dragged by the electric field and, if it was absorbed in a region where it takes longer to be reabsorbed before it reaches the depletion zone, the electron and/or the hole will, with high probability, cross the junction because of the electric field. An electron or a hole traversing the transition zone will contribute a charge e to the current flow in an external circuit. Therefore, with these devices, it is possible to detect photons [31].

Photons can be absorbed in the p-region, the depletion zone or the n-region. The closer the photon is absorbed to the depletion zone, the more chances the photon has to cross it. This is why, most photodetectors include a high-resistivity (i or π) layer, sandwiched between the p and the n regions. The potential drop occurs mostly across this layer, and it can be made long enough to ensure that most of the absorption occur here.

Depending on how the detectors are build, they will present different characteristics, so it is important to define parameters in order to distinguish between them. An important one is the quantum efficiency (η), which is defined as the number of carriers generated per incoming photon. In a diode, an important fraction of the incoming photons will be reflected because of the sudden change in the refraction index. This is why, for achieving a quantum efficiency close to 100%, a good antireflection coating is needed. If the photon is not reflected, then it will have a greater probability to be absorbed in relation to the amount of distance it travels. This probability is directly related with the absorption coefficient α , which depends on the material and the frequency of the photon. Figure 7.5 represents this absorption coefficient for different semiconductors. Notice how for photon with lower energies, α goes to zero.

Others key parameters are the dark count rate (the number of electron-hole pairs generated for other processes rather than photons), and the dead time (the time it takes to a photodetector to generated a second electron-hole

pair after a the previous photon was absorbed). During next sections they will be explained deeper for the case of the APD.

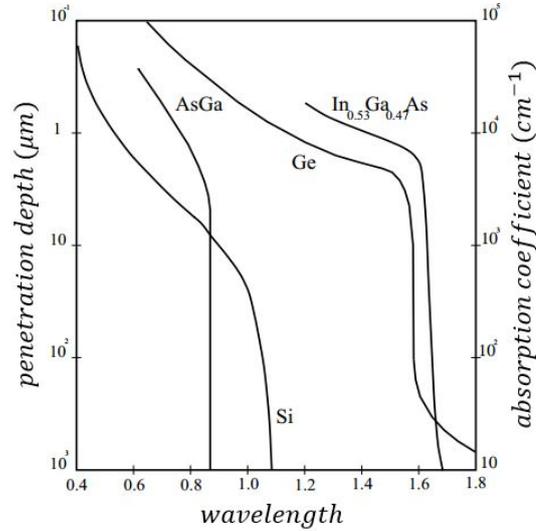


Figure 7.5 The absorption coefficient for different semiconductors [23].

7.1.3 Avalanche photo diode

When the reverse polarization applied to a diode is high enough, the electrons and holes which cross the depletion layer can gain a great kinetic energy. When these carriers hit a nucleus of the net, it can promote an electron to the conduction band or a hole to the valance band. These new electrons and holes can repeat the process, creating an avalanche effect. If the reverse voltage is below a certain value called the *breakdown voltage*, the current generated in the circuit will be proportional to the power of the incident light. If it is above, the APD will operate in the Geiger mode (see next subsection).

This carrier multiplication can be characterized by two ionization coefficient α and β , the former related with the electrons and the latter related with the holes [23]. They quantified the gain per unit of length. The gain of the APD, its noise and its dead time are directly related with these coefficients. There are two cases for real devices, either $\alpha \sim \beta$ or $\alpha \gg \beta$. For real applications, only the last option is acceptable, since the first one introduce to much noise and the response time is too high as well. This is because if $\alpha \sim \beta$, and an electron creates another electron-hole pair, the hole will cross the depletion zone backwards, generating another electron-hole pair and repeating the process. In this case it is much more difficult to know how many carriers will be generated and which will be the delay till the avalanche process stops. Hence, the delay and the noise are much worse.

Figure 7.6 shows the structure of an APD. Within the intrinsic zone (π) most of the photons are absorbed. Because of the electric field, electrons and holes are split apart. When the electron reaches the second pn junction, the electric field is so intense than they hit the nucleus with a high kinetic energy, causing the avalanche effect.

7.1.4 The Geiger mode

When a photodiode has a reverse bias higher than its avalanche breakdown, the APD will have a gain high enough for detecting single-photons. This mode of operation is called Geiger mode. In it, the APD is not considered an amplifier, but rather a digital detector, giving two possibles outputs: the OFF state with no current, and the ON state, when there has been an avalanche process and an electric current is generated because of it. These devices have the same principle than APDs, except that when the avalanche process has started, it is self-sustaining. Because of that, a quenching circuit is needed, which will have to decrease the reverse bias for stopping the avalanche, and to restore it above the breakdown voltage again. During this time,

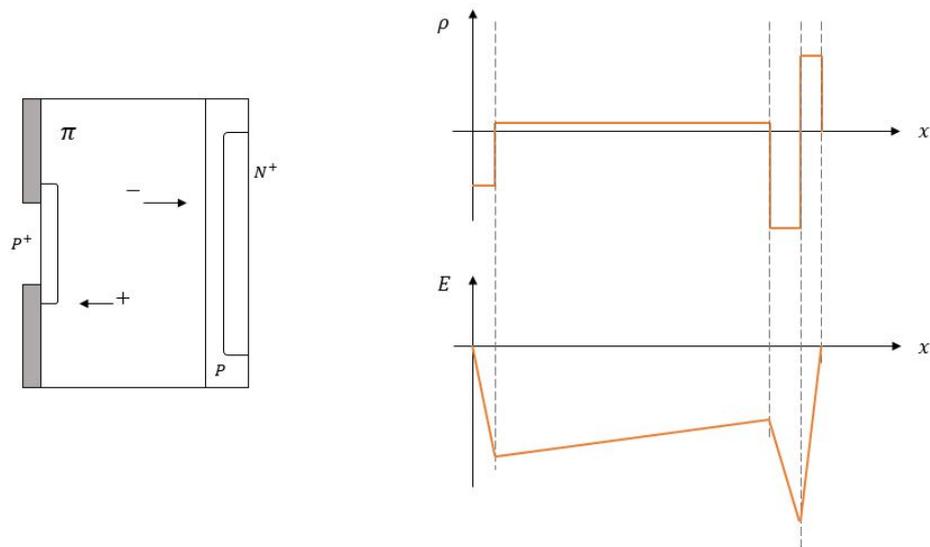


Figure 7.6 The structure of an avalanche photodiode.

the APD will not be able to detect any other photon, so the dead time for these detectors not only depends on the device itself, but also on the electronic of the quenching circuit. APDs in Geiger mode operate in a such a different way, that for avoiding confusion, they are usually called single-photon avalanche diode (SPADs).

The most important performance parameters and features of SPAD device to take into consideration are presented now briefly [39].

Photon detection efficiency

For a SPAD to detect a photon, not only it must be absorbed (generating a electron-hole pair), but also this pair must success triggering an avalanche. This avalanche-triggering probability increase with the excess bias voltage V_E (the voltage above the breakdown voltage), increasing linearly at low V_E and tending to saturate for higher V_E , as it is showed in figure 7.7

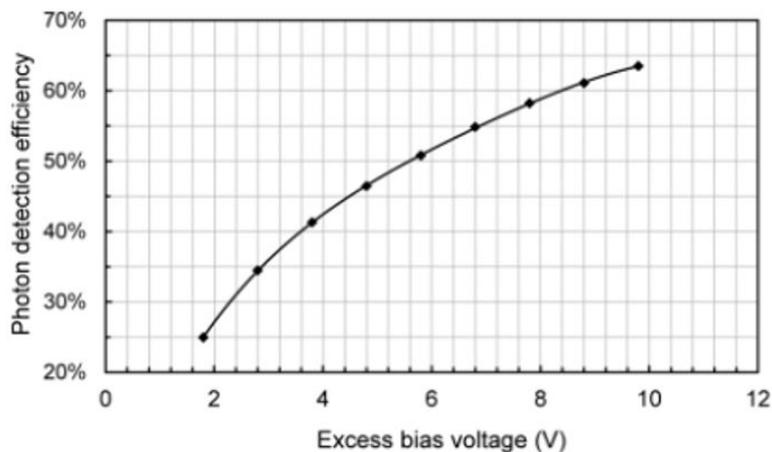


Figure 7.7 The probability for a photon to trigger an avalanche versus the excess bias voltage [39].

Since not all the absorbed photons will trigger the avalanche process in a SPAD, the overall photon detection probability is [9]:

$$P_d = \eta \frac{\bar{n}_c}{\bar{n}} = \eta P_{trig} \quad (7.6)$$

Being \bar{n}_c the number of photons that trigger the avalanche, and \bar{n} the number of photons absorbed. \bar{n} over an interval T , can be written as:

$$\bar{n} = \frac{\eta P_0 T}{hf} \quad (7.7)$$

where P_0 is the received optical power and hf is the photon energy. A signal to noise ratio might be defined as the ratio between the photons coming from the signal which trigger the avalanche, and all the other photons which also trigger the avalanche.

$$SNR = \frac{P_{trig} \bar{n}_s}{P_{trig} (\bar{n}_s + \bar{n}_{bg}) + \bar{n}_{dark}} \quad (7.8)$$

where \bar{n}_{bg} are the background photons and \bar{n}_{dark} are the dark counts. The probability of P_{trig} increases with the bias voltage, however, so does the dark count rate. Usually the dark count rate increases more than the P_{trig} so a compromise need to be found depending on the application.

Dark count rate (DCR)

Dark counts are due to electron-hole pair thermally generated. DCR is a source of noise for SPADs since it generates a current when no photon has reached the device. The dark count rate increases with the excess bias voltage as well. This raises is not only due to the increase in the avalanche-triggering probability, but also to the field enhancement of the carrier generation rate. Figure 7.8 shows how DCR increases with V_E .

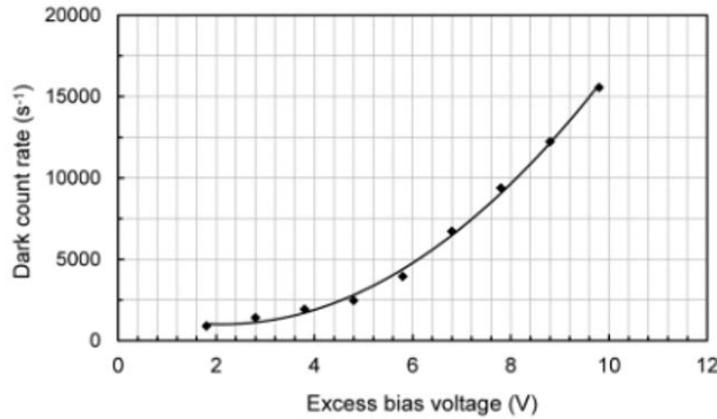


Figure 7.8 The dark count rate versus the excess bias voltage [39].

Afterpulsing

Afterpulsing is another source of noise for SPAD, which does not play any role in linear APDs. Afterpulsing occurs, because during an avalanche process, some carriers are trapped in deep levels located at intermediate energies. These trapped carriers may be released after a while, re-triggering the avalanche process. It is a non-linear effect of SPADs and it occurs randomly between 10^{-9} and 10^3 seconds after the first avalanche, although it happens mainly during the first microseconds.

Deep levels traps increases linearly with the charge that flows during an avalanche. Therefore, for reducing afterpulsing, the total avalanche charge should be reduced as much as possible. If not, using specific quenching circuits can be another solution.

Timing jitter

The time that takes since a photon is absorbed till the avalanche process is detected is not constant. Instead, it has statistical fluctuations, so even if the photons reach the detector equidistantly, there is an uncertainty on when the macroscopic current will be high enough. The time jitter quantified this uncertainty. It is usually quoted as the FWHM of the photon arrival time distribution

Crosstalk

When talking about SPAD arrays, absorbed photons within the active area of a pixel should only activate that pixel. However, in practice these events can cause detection in neighboring pixels, causing crosstalk.

Optical crosstalk

Silicon pn junction can emit photons when operating in avalanche regime. The probability of this emission is very low, but it can trigger an avalanche in another contiguous SPAD, causing a crosstalk again.

Electrical crosstalk

Finally, another kind of crosstalk occurs when carriers generated in a detector diffuse laterally, triggering the avalanche in a neighboring pixel. This crosstalk can be addressed by exploiting isolation techniques.

Fill factor

It is defined as the active area ratio to the total area of a pixel. It is a key figure of merit, especially for application involving SPAD arrays.

7.1.5 Quenching

For stopping self-sustaining avalanches in SPADs, quenching circuits are needed. These circuits have to detect the peak current of the avalanche process for reducing the bias voltage below breakdown level, and then restoring it till the initial level. There are three main methods for doing so: passive, active and gated quenching.

A scheme of the passive circuit quenching is illustrated in figure 7.9 [46]. In this circuit, when a photon hits the detector, the diode will change to the ON state, and the avalanche current will discharge the parasite capacitance of the SPAD. V_d and I_d will fall toward the values of V_f and I_f :

$$I_f = \frac{V_{dd} - V_{break}}{R_d + R_L} \cong \frac{V_{excess}}{R_L} \quad (7.9)$$

$$V_f = V_{break} + R_d I_f \quad (7.10)$$

where V_{break} is the breakdown voltage, R_d is the resistance of the diode and V_{excess} is the voltage above the breakdown voltage. The approximation in equation 7.9 is valid because typically $R_L \gg R_d$. If R_L is high enough to reduce the current below a few μA , the number of carriers will be very small and the probability of the interruption of the avalanche will be very high. After the avalanche has been quenched, the SPAD will start to charge slowly again. An evolution of the current and the voltage through the diode is also shown in figure 7.9. This recovery time can be a problem for applications where photons reach at higher frequencies. For this kind of circuits, it can be up to $\sim 1\mu$ [46], which is not very high.

For overcoming the drawbacks of passive quenching, an active quenching is needed. This kind of circuits were first proposed in 1975 [27]. The principle is simple: to sense the rise of the current and react changing the bias of the SPAD. Figure 7.10 shows an example circuit of this quenching. Whenever the comparator senses the avalanche, it will trigger a voltage driver to switch the bias below the breakdown voltage. After a controlled hold-off time, the diode is switched again to its initial voltage.

In gated quenching, the bias voltage is only increased above the breakdown level when the photon is expected. This is only possible when the arrivals of photons can be predicted. Fortunately, this is the case for QKD, since Alice will send photons periodically. Otherwise, if arrivals of photons can not be deduced, gated quenching is not feasible.

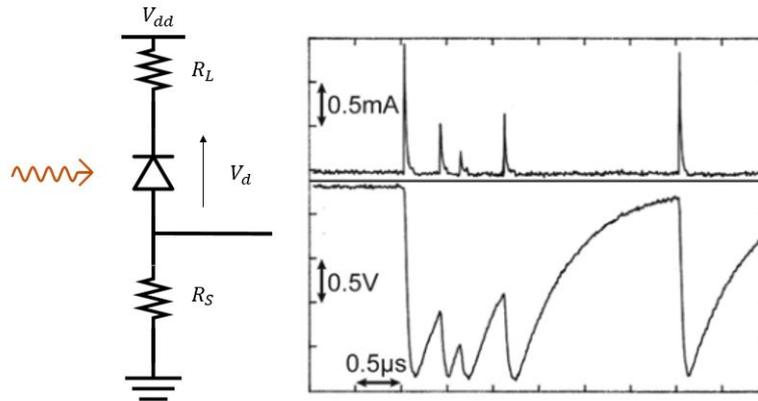


Figure 7.9 A scheme of a passive quenching circuit [39].

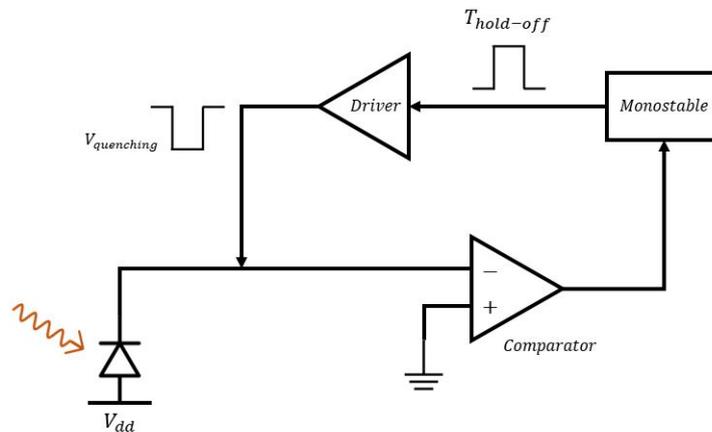


Figure 7.10 A scheme of an active quenching circuit.

7.1.6 Technologies

There are different semiconductor material options for building SPADs. Each of them is used for an specific wavelength, since their forbidden energy gap is different. This section will review the most widely used nowadays, giving a brief discussion on the future work.

Silicon

Silicon is one of the oldest technologies for semiconductors. Its detection efficiency is the best among all the semiconductors. Hence, it is the one used when working in the spectral region of 400-1000 nm (the wavelengths the silicon is sensible to).

There are two kind of Si-SPAD: thick and thin junction [8]. The main difference between them is the length of the depletion layer where the absorption takes place. For the thick junction, this length is a few tens of μm , while for the thin junction is only a few μm . Because the depletion layer is thinner for the thin junction, its detection efficiency is generally lower than the thick junction, and the latter also works better near the infrared for the same reasons. Thin junctions have a peak of detection efficiency 52% at 525 nm, while the thick junction has a peak of 70% at 800 nm

In contrast, thin junction has a lower time jitter, in the order of 20 ps FWHM. Thick junction generally exhibit a time jitter of the order of 500 ps FWHM. Finally, the dark count rate is also lower for the thick junction. It is a function of the temperature and the diameter of the active area. However, for a temperature of $-25\text{ }^\circ\text{C}$

with an active area of $200\ \mu\text{m}$, the dark count rate of the thin junction has a value about 1500 counts per second, while a thick junction has about 300 counts per second.

Germanium

Germanium is one of the semiconductors sensible to the infrared spectral region from 1000 nm to 1500 nm [8]. It was commercially available in the mid-1990s. They have a peak of detection efficiency of about 10% at 1450 nm, with a time jitter of 100 ps. Their main problem is the high dark count rate they suffer, although it can be reduced by cryogenic cooling, another important issue is the high level of afterpulsing. Germanium detectors are not used nowadays, since the InGaAs/InP (see below) SPADs has become dominant for single-photon detection in these wavelengths. However, it is important in a promising technology where hetero-structures are used. Specifically, silicon germanium single-photon detectors promise that will have a better performance than InGaAs/InP SPADs.

Indium-phosphide-based

InGaAs/InP photodetectors are the most widely used SPADs at near-infrared wavelength. The technology is relatively new for SPADs, because most of the progress was made for this kind of detectors operating at the linear mode, but almost any was made at geiger mode till this last decade [32].

All InGaAs/InP photodetectors are based on the separate absorption and multiplication regions. Figure 7.11 shows the schematic of the geometry of these detectors. The InGaAs layer is where the photons are absorbed, while the high-field InP is the layer where the multiplication takes place. The electric field in the multiplication layer is high enough to provide a desirable avalanche probability, while it is low enough in the absorption layer to minimize field-induced leakage currents. The inclusion of the charged layer is designed for having this high and low electric field profile. The grading layer is important to reduce hole trapping effects that results from the valance band discontinuity, so it provides a graded step for the holes to traverse.

The main issues for this detector are the time jitter and the afterpulsing. Time jitter has been demonstrated for being less than 50 ps for an excess bias of 7 V [21]. However, this high bias voltage also increase the dark count rate and afterpulsing. For a bias voltage of 3.5 V the time jitter is around 100 ps. Afterpulsing is a major problem for these detectors, and almost only gated quenching circuits are possible for avoiding them, with a gating rate up to 1 GHz. Some active quenching has been demonstrated as well at 210 K.

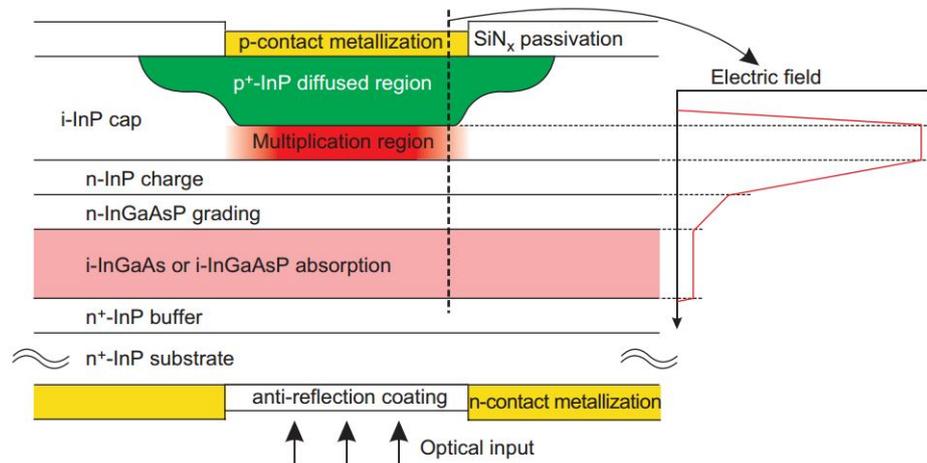


Figure 7.11 The typical InGaAs/InP structure for single-photon detection [32].

Future work

Future work related with the improving of SPADs will be focus on the advance of the detector parameters, as well as the quenching circuits [32]. The former requires researching in the structure design, optimization, high-quality material growth and fabrication technology. Apart from that, there are some potential candidates based on silicon for single-photon detection at the near-infrared wavelength which could improve the parameter of the InGaAs/InP. Some examples are Ge/Si and InGaAs/Si, although their dark count is still to high. The

latter will be focused on inventing new quenching techniques and optimizing the current ones. Finally, for the case of InGaAs/InP photodetectors, the challenge is the development of integrated circuits for the present techniques, something that was achieved for Si SPADs over a decade ago.

7.2 Other receivers

SPADs are not the only technology used for detecting single photons, although it is one of the most promising. This section will give a brief introduction to some other technologies which are being developed currently.

7.2.1 Photomultiplier tubes

Photomultiplier tubes were invented in 1934 by an RCA group based in Harrison. These kind of detectors are very sensitive for the wavelengths used in QKD. They can multiply the current produced by a single photon by million of times due to the photoelectric effect, making them a suitable candidate for single-photon detection [8].

These devices consist on a photocathode, followed by a series of dynodes, and ending in an anode. When a photon hits the photocathode, up to one electron is emitted. This electron will be accelerated towards the first dynode, collapsing with it. After the collision, more electrons are released, which are accelerated towards the next dynode again, repeating the process till electrons reach the anode. Each dynode is charged to a higher positive potential than the previous one, in order to point accuracy the electrons.

Compared them to the SPADs, these devices have higher internal gain. For N dynodes, each with a gain of α , the total internal gain M will be:

$$M = \alpha^N \quad (7.11)$$

Another advantage of them is its active area, which is much greater than the APD's ones. In contrast, photomultiplier tubes require to be contained in bigger packages, higher voltages and they have a bad mechanical stability. Besides, their photon detection efficiency is very poor and their time jitter are typically around 1 ns. Hence, all these factors make photomultiplier tubes a worse choice in more demanding systems.

7.2.2 Hybrids

Hybrid detectors (HPDs) combine avalanche photo diodes with photomultiplier tubes. The APD is placed inside the vacuum tube with the photocathode as the input [8]. The electrons emitted by the photocathode are focused onto the APD, which will produce a detectable current pulse. With this technique, the time taken by the electrons to spread is much lower, and hence the dead time. These devices are particularly suitable for applications which require large detection areas.

7.2.3 Quantum dots

Quantum dots can also be used for detecting singles photon, as well as they could be used for generating them (see chapter 5). For doing so, a field effect transistor (FET) is used [8]. This FET is doped with a quantum dot layer. When a photon hits on the device, it will generate an electron which will be absorbed by the quantum dots. This will cause a change in the electric field in the FET, and hence, a measurable change in the source-drain current of the FET. This kind of devices have a photon detection efficiency of 0.9%, quite far yet from APD or photomultiplier tubes.

7.2.4 Superconductors

Superconductors are materials which can support an electrical current without any resistance and any loss of energy under certain conditions. These materials only present this behavior under extremely low temperatures. The superconductivity was first discovered by Heike Kamerlingh Onnes in 1911. Since then, several progresses have been made to develop applications for them.

One of these applications is the use of superconductors for single photon detection [8]. Being the transition edge sensor (TES) one of these technologies. This device is an incredibly sensitive calorimeter, a device which can measure the heat generated by a physical process. The materials use for these detectors are characterized by their sharp transition between the temperature in which they behave as superconductor and the temperature

in which they do as normal conductors. The TES is cooled down below the superconducting transition and a bias voltage is applied so it gets a temperature where a small variation in it will cause a big variation in the resistance. When a photon is absorbed, the electron generated will heat up the device, causing a measurable variation in its resistance, being able to detect a single photon then.

7.2.5 Up-conversion

This technique is the reverse of the parametric down-conversion saw in chapter 5. Up-conversion is used in conjunction with detectors suitable for short wavelengths in order to detect photons with higher wavelengths [8]. In this method the photons incident a non-linear crystal, together with a pump beam. Because of the conservation of energy, the frequency in the output must be the sum of the two frequencies in the input. For instance, incident photons at a wavelength of 1550 nm together with a pump laser at 980 nm will be up-converted to a wavelength of 630 nm. These resulting photons can be detected now by silicon SPADs, taking advantages of their characteristics.

8 Conclusions

The following are the conclusions that have been drawn from the study carried out on the state of the art of quantum cryptography.

Quantum cryptography is taking its last steps toward a commercial explosion that will revolutionize the world of computer security.

The entity that still needs further evolution is the source. Specifically, single photon sources have not yet been developed with an adequate performance, and this means that there is still big room for improvements in the systems.

Until repeaters and quantum amplifiers are developed, optic fibers does not seem to be able to offer many more improvements, so these communications are beginning to develop through free space links. In particular, satellite communications seem to be very promising.

The receivers are the most developed devices of all this technology, being in a mature state in which the improvements that continue to be made are already small compared to the early stages of the development of any device.

Appendix A

A complete BB84 system

The protocol BB84 was the first quantum key distribution protocol proposed. It supposed the beginning of a whole new and revolutionary field, which promises to bring the first direct quantum application for the real world. Apart from its originality, it is remarkable how simple the protocol is. Nevertheless, from an engineering point of view, the system is much more complex, since the devices used are never perfect. Therefore, this appendix will present a possible real implementation of the BB84 protocol [26] with the current technology, according to what has been discussed along the whole dissertation.

Figure A.1 shows this feasible implementation for the protocol. Alice's system will be composed of a pulse generator, four lasers (L), three beam splitters (BS), an aperture (A), a filter (F), a lens (L) and an attenuator (At). Each laser will generate photons in each polarization needed for the BB84 protocol. The activation of the lasers will be random and stimulated by the fast pulse generator, so each time, only one laser emits one pulse. The beam splitters will point the pulse to the output of the system. This output will be composed of an aperture and a lens which will point the pulse to Bob. A filter will eliminate the not desired frequencies, while the attenuator will reduce the mean photons by pulse to the typical values for these applications (see chapter 5).

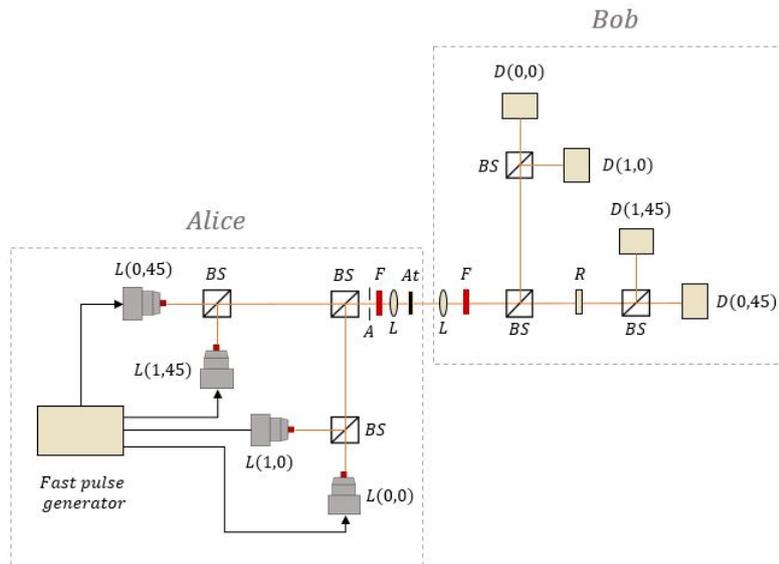


Figure A.1 An example of a real implementation for implementing the BB84 protocol.

Bob's system will contain a lens (L), a filter (F), three beam splitters (BS), a wave plate (R) and four detectors (D). After the beam reaches Bob's system, it will be pointed and filtered again to minimize the losses it may

have suffer while crossing the channel, and to eliminate new not desired frequencies. The first beam splitter will simulate Bob's basis decision, and it will be random. If the beam is deflected, it is assumed Bob is measuring in the horizontal basis. If this was the basis of the photon sent by Alice, the behavior of the second beam splitter will be deterministic, if not, it will be random. For each case, only one detector will be fired. On the other hand, if the first beam splitter does not deflect the beam, then it is assumed Bob will measure in the diagonal basis. A wave plate will rotate the polarization of the photon 45° and the second beam splitter will work as in the previous case.

As it is showed, with this system, a full implementation of the BB84 protocol can be executed. Even so, there is an issue for this scheme which has no solution currently: the randomness of Alice's source. Currently, random number generators are not really random, since they use algorithms which makes them pseudo-random. This drawback could be exploited for Eve to gain some information about the system (although this might be quite difficult, it is possible in principle). Hence, for the system being perfectly secure, really quantum random number generators must be developed (however, as single photon sources, these devices still need a lot of investment and researching).

List of Figures

1.1	The Caesar cipher is named after the roman emperor, who was the first in using it	1
1.2	An artistic representation of the cryptography field [1]	2
1.3	An artistic representation of quantum mechanics [2]	3
1.4	The dependences among the chapters of the dissertation	4
2.1	An example of a wave function Ψ versus the position x	6
2.2	A representation of a wave function after it has just collapsed	6
2.3	The Harmonic oscillator scheme for an object with mass m	8
2.4	A representation of some Hydrogen orbitals in 2D [38]	12
2.5	The angular momentum states of an atom with the quantum number $l = 2$	13
2.6	Different total angular momentum depending on the sum of l and s	15
2.7	An example of a periodic potential suffer by an electron within a solid	16
2.8	The band structure of a solid. Different allowed energy bands, separated each of them by a forbidden band where electrons can not exit	17
2.9	An illustration of the absorption and stimulated emission processes	19
2.10	An illustration of the spontaneous emission process	20
3.1	A single-mode electric field confined in a cavity	24
3.2	Allowed energy levels for a single-mode electromagnetic field	26
3.3	Phasor diagram for a coherent state	28
3.4	Phasor diagram for a classic coherent state	30
3.5	Phasor diagram for the vacuum field	30
3.6	Phasor diagram for three different squeezed states	30
3.7	The Hanbury Brown-Twiss experiment scheme	31
3.8	The Hanbury Brown-Twiss experiment with photons scheme	32
3.9	The shot noise caused by the intensity fluctuations of the intensity due to the uncertainty on the number of photons arriving	34
3.10	Photon bunched vs. coherent light vs. photon antibunched	34
4.1	A vertically polarized photon in the vertical-horizontal and in the diagonal basis	39
4.2	A beam going through two polarized filters, one vertically polarized and the other horizontally polarized	40
4.3	A beam going through three polarized filters, the first vertically polarized, the second polarized along 45° axis, and the last horizontally polarized	40
4.4	The EPR experiment	41
4.5	Bell's generalization for the EPR experiment	41
4.6	The basis used for measuring in the E91 protocol	44
4.7	The BB84 states (a) versus the B92 states (b)	45
4.8	The limit for the intercept-resend attack	47
4.9	The scheme used by Eve to perform a feasible attack	49
5.1	Scheme for a weak coherent pulse source	51
5.2	The probability of finding n photons in a pulse with mean equal to μ	52

5.3	The scheme for a two level atom system as a single photon source	53
5.4	Comparison among the different kind of quantum confinement	54
5.5	An example of a single photon source triggered with electric pulses	54
5.6	The cascade decay for generating a pair of entangled photons within a calcium atom	55
6.1	Structure of an optical fiber [3]	58
6.2	A Mach-Zehnder interferometer with a single-photon input	59
6.3	An interferometer for implementing the BB84 protocol	60
6.4	Scheme for a frequency based coding in QKD applications	61
6.5	Different scenarios for satellite QKD	62
7.1	A representation of the concentration of electrons and holes in pn junction	66
7.2	The energy bands in pn junction with no electric field applied and under thermal equilibrium conditions	66
7.3	Density charge distribution, electric field and electric potential for a generic pn junction	67
7.4	The energy bands in pn junction under thermal equilibrium conditions with: (a) no electric field applied, (b) a direct polarization, (c) a reverse polarization	68
7.5	The absorption coefficient for different semiconductors [23]	69
7.6	The structure of an avalanche photodiode	70
7.7	The probability for a photon to trigger an avalanche versus the excess bias voltage [39]	70
7.8	The dark count rate versus the excess bias voltage [39]	71
7.9	A scheme of a passive quenching circuit [39]	73
7.10	A scheme of an active quenching circuit	73
7.11	The typical InGaAs/InP structure for single-photon detection [32]	74
A.1	An example of a real implementation for implementing the BB84 protocol	79

List of Tables

2.1	The selection rules for electron transitions	20
3.1	Properties of the second-order correlation function for classical light	32
4.1	Qbits representation in BB84 protocol	43
6.1	The BB84 codification when using the phase coding scheme	61

Bibliography

- [1] <http://www.engineersjournal.ie/2013/09/19/encryption-is-less-secure-than-we-thought-say-maynooth-researchers/>.
- [2] <http://www.portoalegre.travel/wallpapers/quantum-mechanics-wallpaper/>.
- [3] <https://www.newport.com/t/fiber-optic-basics>.
- [4] CHARLES H. BENNETT, *Quantum cryptography using any two nonorthogonal states*, Physical review letters **68** (1992), no. 21, 3121.
- [5] S STRAUF; N G STOLTZ; M T RAKHER; L A COLDREN; P M PETROFF; D BOUWMEESTER, *High-frequency single-photon source with polarization control*, Nat. Photonics **1** (2007), no. 12, 704.
- [6] CHARLES H. BENNETT; GILLES BRASSARD, *Quantum cryptography: Public key distribution and coin tossing*, International Conference on Computers, Systems & Signal Processing (1984), pp 175–179.
- [7] MICHAEL A. NIELSEN; ISAAC L. CHUANG, *Quantum computation and quantum information*, 10th anniversary ed., Cambridge, 2010.
- [8] GERALD S. BULLER; RJ COLLINS, *Single-photon generation and detection*, Measurement Science and Technology **21** (2009), no. 1.
- [9] XIAOLI SUN; FREDERIC M. DAVIDSON, *Photon counting with silicon avalanche photodiodes*, Journal of lightwave technology **10** (1992), no. 8.
- [10] ROBERT EISBERG, *Quantum physics of atoms, molecules, solids, nuclei, and particles*, 2nd ed., John Wiley & Sons, 1958.
- [11] ARTUR K EKERT, *Quantum cryptography based on bell's theorem*, Physical review letters **67** (1991), no. 6, 661.
- [12] H. L YIN; et al., *Measurement-device-independent quantum key distribution over a 404 km optical fiber*, Phys. Rev. Lett. **117** (2016), no. 19, 190501.
- [13] J YIN. et al., *Satellite-based entanglement distribution over 1200 kilometers.*, Science **356** (2017), no. 6343, 1140–1144.
- [14] et al. F STEINLECHNER, *A high-brightness source of polarization-entangled photons optimized for applications in free space.*, Opt. Express **20** (2012), no. 9, 9640–9649.
- [15] P.C SUN; Y. MAZURENKO; Y. FAINMAN, *Long-distance frequency-division interferometer for communication and quantum cryptography*, Opt. Lett. **20** (1995), no. 9, 1062.
- [16] MARK FOX, *Quantum optics, an introduction*, 2nd ed., Oxford, 2006.
- [17] HELLE BECHMANN-PASQUINUCCI; NICOLAS GISIN, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography*, Physical Review A. **59** (1999), no. 6, 4238.

- [18] VALERIO SCARANI; ANTONIO ACÍN; GRÉGOIRE RIBORDY; NICOLAS GISIN, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations*, Physical Review A. **73** (2004), no. 1.
- [19] DAVID J. GRIFFITHS, *Introduction to quantum mechanics*, 2nd ed., Pearson Education International, 2005.
- [20] WY HWANG, *Quantum key distribution with high loss: toward global secure communication*, Physical Review Letters **91** (2003), no. 5.
- [21] M. A. ITZLER; R. BEN-MICHAEL; C. F. HSU; K.SŁOMKOWSKI; A. TOSI; S. COVA; F. ZAPPA; R. ISPASOIU, *Single photon avalanche diodes (spads) for 1.5 μm photon counting applications*, J. Mod. Opt **54** (2007), no. 2-3, 283–304.
- [22] et al. J YIN, *Satellite-based entanglement distribution over 1200 kilometers.*, Science **356** (2017), no. 6343, 1140–1144.
- [23] C JANER, *Dispositivos activos y componentes pasivos para sistemas dwdm*, Course Material, 2009.
- [24] F COLODRO; J GARCÍA; C. JANER, *Dispositivos de unión pn*, Course Material, 2012.
- [25] CHRISTOPHER C. GERRY; PETER L. KNIGHT, *Introductory quantum optics*, 1st ed., Cambridge, 2005.
- [26] ROBERT BEDINGTON; JUAN MIGUEL ARRAZOLA; ALEXANDER LING, *Progress in satellite quantum key distribution.*, npj Quantum Information **3** (2017), no. 1, 30.
- [27] P ANTOGNETTI; S COVA; A LONGONI, *A study of the operation and performances of an avalanche diode as a single-photon detector.*, Proc. 2nd ISPRA Nuclear Electronics Symp. (Stresa, Italy) (1975), 453–6.
- [28] et. al. M JOFRE, *Fast optical source for quantum key distribution based on semiconductor optical amplifiers*, Optics express **19** (2011), no. 5, 3825–3834.
- [29] XIONGFENG MA, *Quantum cryptography: from theory to practice*, PhD. Thesis, University of Toronto, 2008.
- [30] CHARLES H. BENNETT; GILLES BRASSARD; N DAVID MERMIN, *Quantum cryptography without bell's theorem*, Physical review letters. vol. **68** (1992), no. 5, 557.
- [31] DONALD A. NEAMEN, *Semiconductor physics and devices*, 4th ed., Mc Graw Hill, 2012.
- [32] JUN ZHANG; MARK A. ITZLER; HUGO ZBINDEN; JIAN-WEI PAN, *Advances in ingaas/inp single-photon detector systems for quantum communication*, Light: Science & Applications **4** (2015), no. 5, e286.
- [33] FRANCISCO J. PAYAN, *Tratamiento de la información en comunicaciones digitales: Tema 1. información y entropía*, Course Material, 2018.
- [34] ———, *Tratamiento de la información en comunicaciones digitales: Tema 2. información mutua y desigualdad de fano*, Course Material, 2018.
- [35] ———, *Tratamiento de la información en comunicaciones digitales: Tema 4. teorema de codificación de canal*, Course Material, 2018.
- [36] VALERIO SCARANI; HELLE BECHMANN-PASQUINUCCI; NICOLAS J CERF; MILOSLAV DUSEK; NORBERT LÜTKENHAUS; MOMTCHIL PEEV, *The security of practical quantum key distribution*, Reviews of modern physics. **81** (2009), no. 3, 1301.
- [37] A. PERES, *Quantum theory: Concepts and methods*, 1st ed., Kluwer Academic Publisher, 1997.
- [38] PoorLeno, *Hydrogen density plots*, https://en.wikipedia.org/wiki/Atomic_orbital#/media/File:Hydrogen_Density_Plots.png.

- [39] SERGIO COVA; MASSIMO GHIONI; MARK A. ITZLER; JOSHUA C. BIENFANG; ALESSANDRO RESTELLI, *Single-photon generation and detection: Chapter 4. semiconductor-based detectors*, 1st ed., Academic Press, 2013.
- [40] P M INTALLURA; M B WARD; O Z KARIMOV; Z L YUAN; P SEE; A J SHIELDS; P ATKINSON; D A RITCHIE, *Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm* , *Appl. Phys. Lett* **91** (2007), no. 16, 161103.
- [41] NICOLAS GISIN; GRÉGOIRE RIBORDY; HUGO ZBINDEN; DAMIEN STUCKI; NICOLAS BRUNNER; VALERIO SCARANI, *Towards practical and fast quantum cryptography*, arXiv preprint quant-ph/0411022 (2004).
- [42] T HANADA; K FUJISAKI; M TATEIBA, *Theoretical analysis of effects of atmospheric turbulence on bit error rate for satellite communications in ka-band*, InTech (2010).
- [43] THOMAS M. COVER; JOY A. THOMAS, *Elements of information theory*, 1st ed., John Wiley & Sons, 1991.
- [44] G VEST; M RAU; L FUCHS; G CORRIELLI; H WEIER; S NAUERTH; A CRESPI; R OSELLAME; H WEINFURTER, *Design and evaluation of a handheld quantum key distribution sender module*, *IEEE journal of selected topics in quantum electronics* **21** (2015), no. 3, 131–137.
- [45] H WEIER; T SCHMITT-MANDERBACH; N REGNER; C KURTSIEFER; H WEINFURTER, *Free space quantum key distribution: Towards a real life application*, *Fortschr. Phys.* **54** (2006), no. 8–10, 840–845.
- [46] S COVA; M GHIONI; A LACAITA; C SAMORI; F ZAPPA, *Avalanche photodiodes and quenching circuits for single-photon detection*, *Applied optics* **35** (1996), no. 12, 1956–1976.
- [47] G. RIBORDY; J. BRENDEL; J.D. GAUTIER; N. GISIN; H. ZBINDEN, *Long distance entanglement based quantum key distribution*, *Phys. Rev. A* **63** (2001), no. 1, 012309.
- [48] NICOLAS GISIN; GRÉGOIRE RIBORDY; WOLFGANG TITTEL; HUGO ZBINDEN, *Quantum cryptography*, *Reviews of Modern Physics* **74** (2008), no. 1, 145.