POLITECNICO DI TORINO

Nanotechnologies for ICTs

Master degree thesis

A hardware-model-based simulator for Quantum Key Distribution systems employing photon polarization encoding

Advisors:
Prof. Maurizio Zamboni
Prof. Mariagrazia Graziano
Prof. Giovanna Turvani

Author:
Carlo Caputo

October 2021

A mio padre, per il cammino intrapreso.
Da lassù continua a guidare i miei passi.
A mia madre. A mio fratello.

Acknowledgments

I would like to thank my supervisors Prof. Maurizio Zamboni, Prof. Mariagrazia Graziano, and Prof. Giovanna Turvani who gave me the golden opportunity to do this master thesis on Quantum Key Distribution.

A special thanks also to Ph.D Giovanni Amedeo Cirillo and Ph.D Mario Simoni, for their continuous guidance and support throughout this project.

I would also like to thank Dr. Francesco Letizia and Dr. Luca Maggio for inspiring me with their interesting suggestions.

Finally, I would like to express my gratitude to my family and my dearest friends for their encouragement and support all through my studies.

Summary

The forthcoming release of quantum computers, as also the advances of classical computers, may put at risk most of the cryptosystems used today, in particular the asymmetric ones. Taking for example the widely used Rivest-Shamir-Adleman (RSA) algorithm, it can be easily broken using **Shor's factoring algorithm**, running on quantum computers and characterized by a polynomial computational complexity instead of exponential.

Although new and more secure cryptosystems can be developed, the best long-term solution is quantum cryptography. Nowadays, the first **Quantum Key Distribution (QKD)** systems are already on the market. They allow to exchange private keys between users through the transmission of single-photon pulses encoding the quantum information (qubits). QKD is usually employed in symmetric encryption schemes, like "one-time pad", and it ideally permits to obtain **unconditionally secure communications**, exploiting properties of quantum mechanics such as the **no-cloning theorem**.

In this work, a simulation framework for QKD systems based on photon polarization encoding is presented. It is composed by two elements: a **MATLAB simulator**, used to analyze the optical system where the photons are exchanged, and a **Verilog-A simulator for Single-Photon Avalanche Diodes (SPAD)**, able to predict the fundamental parameters of this kind of photon detectors, the most used in current QKD systems.

The treatment develops in six chapters: after an introduction about the fundamental concepts of QKD and quantum optics, the second chapter is centered on the theoretical model. This is based on the use of **coherent states** that are the most convenient choice to model the coherent light emitted by the attenuated lasers employed in current QKD systems. In fact, at present, efficient single-photon sources, which would be the most suitable solution, do not exist yet.
In the third chapter, the behaviour of the most common optical components is presented, as also their modeling. First, they are analyzed in their ideal form, and then losses are added in the treatment.

The fourth chapter is dedicated to single-photon optical detectors, one of the most critical parts of Quantum Key Distribution systems. After a brief overview on the newest and most suitable types of detectors for QKD, SPADs are analyzed in details, in particular the ones working in the near infrared, made of InGaAs/InP. Furthermore, a Verilog-A model for this kind of detectors is presented. Its non-trivial definition started with the theoretical study of SPADs, necessary to understand their functioning, with a focus on unwanted effects that cause dark counts. In fact, the generation of charge carriers due to thermal or tunneling effects, in addition to the release of trapped carriers after an avalanche (afterpulses), can lead to false detection events.
In the fifth chapter, the operation of the simulator is explained with a practical example.
In the last chapter, a real BB84 QKD system is analyzed to validate the proposed simulative methodology, evaluating its **Quantum Bit Error Rate (QBER)** and its **secure key rate**.

To sum up, the work presented in this thesis represents a necessary starting point for the development of a **simulation framework** for Quantum Key Distribution systems based on polarization encoding. With the correct improvements, for example exploiting the **density operators** formalism, enhancing the performance of the Verilog-A simulator, and integrating the MATLAB and Verilog-A simulators in a unified software infrastructure, a usefull design tool for QKD can be obtained.

Table of contents

Acknowledgments II

Summary III

1 Introduction **1**

1.1 Cybersecurity: a brief overview . . . 1
1.2 Quantum key distribution . . . 3
1.3 One-time pad . . . 4
1.4 Principles of quantum cryptography . . . 4
1.5 Two basic protocols . . . 7
1.5.1 BB84 protocol . . . 7
1.5.2 LM05 protocol . . . 10
1.6 A critical problem: PNS attack . . . 12
1.7 A fundamental improvement: the decoy state protocol . . . 14
1.8 Light sources: an overview . . . 15

2 Theoretical model **18**

2.1 Coherent states . . . 18
2.1.1 Glauber-Klauder-Sudarshan or Standard Coherent States . . . 22
2.1.2 Coherent states: an overcomplete basis . . . 23
2.1.3 Displaced vacuum states . . . 24
2.2 A brief recalling of polarization of light . . . 25
2.2.1 Polarization of light . . . 25
2.2.2 Jones calculus . . . 27
2.2.3 Displaced states considering polarization . . . 28
2.3 Propagation in quantum optics . . . 29
2.4 Limits of the model . . . 31

3 Analysis of the most common optical devices **32**
3.1 Attenuated laser . . . 32
3.2 Pockels cell . . . 33
3.3 Linear polarizer . . . 36
3.4 Mirror . . . 37
3.5 Beam splitter . . . 37
3.5.1 A general relation for creation and annihilation operators: the importance of vacuum state . . . 38
3.6 Polarizing beam splitter . . . 41
3.7 Quantum channel . . . 42
3.7.1 Optical fiber as quantum channel . . . 42
3.7.2 Open air as quantum channel . . . 46
3.8 Losses and deviations from ideality . . . 51
3.8.1 General considerations on the simulator and how errors and losses are taken in account . . . 52
3.8.2 Lossy Pockels cells, linear polarizers, and mirros . . . 53
3.8.3 Lossy Beam splitter . . . 53
3.8.4 Lossy Polarizing beam splitter . . . 53

4 Single-photon detectors **55**
4.1 Figure of merits of photon detectors . . . 55
4.1.1 Spectral range . . . 55
4.1.2 Photon detection efficiency (PDE) . . . 56
4.1.3 Noise equivalent power (NEP) . . . 56
4.1.4 Dark count probability . . . 56
4.1.5 Timing jitter . . . 56
4.1.6 Dead time . . . 57
4.2 An overview on the newest photon detectors for QKD . . . 57
4.2.1 Superconducting transition-edge sensors (TES) . . . 57
4.2.2 Superconducting nanowire single-photon detectors (SNSPD) . . . 58
4.3 Single-Photon Avalanche Diode (SPAD) . . . 58
4.3.1 Operating principle and semiconductor structure . . . 59

4.3.2 SPAD characterization and modelization . . . 62
4.4 Verilog-A model . . . 71
4.4.1 Reference SPAD . . . 71
4.4.2 Flowchart of the simulator . . . 71
4.4.3 Ports of the SPAD . . . 72
4.4.4 Circuital model . . . 72
4.4.5 Static and dynamic currents . . . 73
4.4.6 Current quenching . . . 75
4.4.7 Photon arrival . . . 76
4.4.8 Dark carrier generation . . . 79
4.4.9 Afterpulses . . . 80
4.4.10 Simulation and verification . . . 84

5 Detailed description of the simulator and MATLAB implementation 90
5.1 State representation and MATLAB operations . . . 90
5.2 Example of propagation . . . 91
5.3 Component libraries . . . 93
5.4 Analysis of a real QKD system . . . 93
5.4.1 Structure and operation . . . 94
5.4.2 Some real examples . . . 96
5.5 Overview of the complete simulation framework . . . 101

6 A detailed analysis of a real QKD system 103
6.1 Description of the QKD system . . . 103
6.2 MATLAB simulation . . . 105
6.3 Quantum bit error rate and secure key rate estimation . . . 106
6.3.1 Quantum bit error rate . . . 107
6.3.2 Secure key rate . . . 110

Conclusions and future perspectives 112

Bibliography 115

Chapter 1

Introduction

This thesis stems from the interest about quantum cryptography and, in particular, form the awareness that current cryptography standards will not be able to guarantee the security of users in the near future. In fact, the release of quantum computers, as also the development of best-performing classical computers, will make most of the current cryptography methods vulnerable. For this reason, it is necessary to study and develop quantum cryptography as soon as possible.

This thesis results the proper conclusion of my master degree "Nanotechnologies for ICTs", during which I consolidated my knowledge of physics and engineering applied to nanotechnologies and, in general, to information technologies. These knowledge were fundamental in developing this thesis were an hardware-model-based simulator for the analysis of polarization-encoding Quantum Key Distribution (QKD) systems will be presented.

1.1 Cybersecurity: a brief overview

Nowadays cybersecurity is a fundamental part of our life: all of our personal information are online, banks handle our money, which have become mostly digital. Even our memories and knowledge are entrusted to the network.
For these reasons, cryptography, the pillar of cybersecurity, must evolve to deal with the latest decryption methods. Most of the present cryptographic schemes used today are based on the difficulty of factorizing large numbers, from 2048 bits onwards. However, more powerful traditional computers and algorithms executable on quantum computers may put at risk most of these cryptography methods in a couple of decades, or even less.
The **Shor's algorithm** is the most famous example of such a kind of algorithm; it is used to decompose an integer number in its prime factors. Shor's algorithm is

similar to the classical factorization algorithm with the exception that one of the step must is a quantum algorithm [1]. Its peculiarity is that it is able to factorize integers in polynomial time [2]; this makes it extremely efficient in breaking ciphers.

The greatest weakness of current cryptography algorithms is that they are safe only for a "limited" time. For instance, the Rivest-Shamir-Adleman cryptosystem (RSA), whose safety relies on the difficulty of factorizing the product of two large prime numbers, is expected to be broken and completely useless with 50% probability within the 2032 (in its 2048 bits version) [3]. Moreover, since lots of other cryptosystems are similar to RSA, the trouble is concrete.

RSA is an example of **asymmetric encryption** where each user is associated with a **public key**, known to all. In addition, the user possesses a **private key** that nobody else must know. The adjective asymmetric stems from the presence of these two keys, one public and one private. For instance, if Alice wants to send a secure message to Bob, she can encrypt the message using the public key associated with him; in this way, only Bob can decrypt the message. Furthermore, asymmetric encryption methods allow the message authentication: senders can use their private key to encrypt the message, whereas receivers can use the associated public key to verify the identity of the sender. This is one of the advantages of asymmetric encryption, in addition to the fact that the exchange of private keys is not necessary. The main disadvantage is that public and private key are mathematically linked, consequently one can use the public key to crack the private key. For this reason the keys must be long enough to ensure an high resistance to attacks, although this makes communications slower [4].

Symmetrc encryption is the other category of cryptography methods. In this case, only a single, secret key is used to encrypt and decrypt information. The communications are faster, because smaller keys are used, and secure, on the condition that the secret key is not stolen. In fact, the hackers cannot use the public key to trace back to the private key as in asymmetric encryption, so inefficient and time-consuming brute-force attacks are the only solution to try to break these systems. However, the secret keys must be exchanged among the users. Therefore, if the transmission method is compromised, an eavesdropper can steal the key and consequently the message [4].

If a completely secure method to share the keys is used, symmetric encryption

methods will ensure an extremely high security with excellent performance.

1.2 Quantum key distribution

The best long-term solution is **Quantum Key Distribution**, that enables to exchange the private keys by exploiting quantum mechanical properties. The communication happens on a quantum channel where single photons, properly polarized or arranged to encode the key, are sent and received; this exchange method is extremely secure because the presence of an eavesdropper can be easily detected, as it will be clearer in the next sections.

The quantum channel can be an optical fiber, working in correspondence of one of the optical communication windows, or even the open air; the latter paves the way to establish satellite quantum communication and so global quantum communication networks.
Currently, using optical fibers and some tricks such as decoy states which will be analyzed later, a secure communication up to 166 km can be performed [5].

With regards to the encoding of information through single photons, several solutions are possible. The most common are:

- Polarization-encoding: the bit value corresponds to the direction of the polarization;
- Phase-encoding: a Mach-Zehnder interferometer is used to encode the information by changing the optical phase in the two arms of the interferometer;
- Temporal-encoding: the single photon is sent by Alice with a variable delay with respect to a reference clock;
- Multidimensional-encoding: given that photons can carry both spin and orbital angular momenta (SAM and OAM), associated with polarization, the idea is to use both these photon characteristics to encode the information, enhancing at the same time the security [6].

1.3 One-time pad

QKD allows to establish secure communications because the exchange of the key is extremely secure. Consequently, applying symmetric encryption schemes, an eavesdropper has no chance to steal information.

One-time pad applied to quantum cryptography is an extremely secure cryptosystem. In fact, if the following four rules are applied, this chiper results to be unbreakable [7]:

1. the key is at least as long as the message;
2. the key is completely random;
3. only two copies of the key exist: one for the sender and one for the receiver;
4. the keys are used only once.

QKD permits to distribute a new private key for every message, ensuring that only sender and receiver know it. Therefore, respecting the other three rules, the communication results to be unconditionally secure.

Once that the private key is exchanged, the sender can convert his message into a binary string, then he adds the private key to the message and he sends it to the receiver. The receiver only has to subtract the key from the encoded message to recover the message [8]. Another possibility to encrypt the message is to add the key to the message bitwise modulo 2, i.e. performing the operation $i \oplus j$. In order to decrypt the message, the receiver just has to add the key bitwise again since $(i \oplus j) \oplus j = i$ [1].

1.4 Principles of quantum cryptography

Quantum Key Distribution (QKD) is used to share secret keys between two users, traditionally called Alice and Bob. A primary objective is to prevent an eavesdropper (Eve) to interfere and subtract the keys. In order to detect the presence of Eve, it is necessary to give up classical communication, where signals are made by a great deal of photons, otherwise Eve can subtract some of them without being detected,

using a simple beam splitter and an optical amplifier as shown in Figure 1.2.

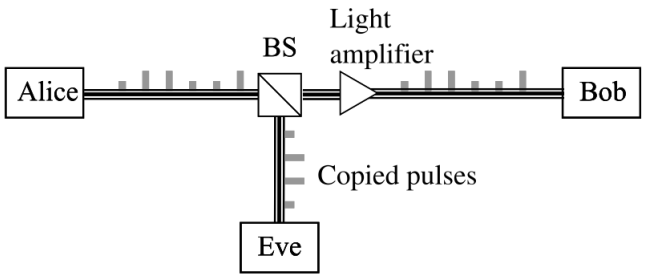

Figure 1.1: Eve can subtract part of the photons of the stream using the beam splitter. Then, using the amplifier, she can hide her presence restoring the initial signal intensity [8].

Instead, if single photon signals are used, the security of the communication is ensured by the **no-cloning theorem** which states that it is impossible to create an independent and identical copy of a generic quantum state [9]. To better understand how this theorem applies to QKD systems, some simple examples will be analyzed. For the moment it is assumed that Alice has got an ideal single photon source, impossible to be realized with current technologies.

Starting from a naif case: Alice and Bob decide to encode the information on photons using only horizontal and vertical polarization, the so-called {H,V} basis: horizontal polarization corresponds to "0" while vertical polarization to "1". Eve can easily barge in the quantum channel and measure the polarization of the photon using a polarizing beam splitter coupled with two photon detectors. After that, she sends to Bob a photon with the same polarization just measured. The presence of Eve seems to be completely hidden and the hopes for a secure communication seem to be fading.

Proceeding to a more concrete case: Alice is not limited to encode the information only in {H,V} basis, but she uses also other directions, for example the diagonal and anti-diagonal ones, the so-called {A,D} basis. However, she could also use right-hand and left-hand circular polarizations. In principle, the photon is in a superposition

of states:

$$|\psi\rangle \;=\; \cos\theta\;|\updownarrow\rangle \;+\; \sin\theta\;|\leftrightarrow\rangle\,, \tag{1.1}$$

where the {H,V} basis has been used. But it can be equivalently expressed using the {A,D} basis:

$$|\psi\rangle \;=\; \cos\gamma\;|\nwarrow\rangle \;+\; \sin\gamma\;|\nearrow\rangle\,. \tag{1.2}$$

Since Eve cannot know a priori the encoding basis used by Alice, she has to choose a random basis measurement: if she chooses the wrong one, she obtains a completely random outcome, erasing the qubit value. In fact, it is important to remember that **a quantum measurement is totally different from a classic one**: without going into detail, after a measurement, the system collapses into a particular eigenstate of the measurement apparatus [10]. Choosing the wrong basis is equivalent to choose the wrong configuration of the measurement apparatus that forces the photon wavefunction to collapse in an improper eigenstate.
Therefore, the most reasonable thing Eve can do is to send a photon to Bob in the same basis and with the same value she obtained with the measurement. It is clear that this outgoing photon is not the copy of the incoming one, and the information delivered to Bob is very different from the one sent by Alice.

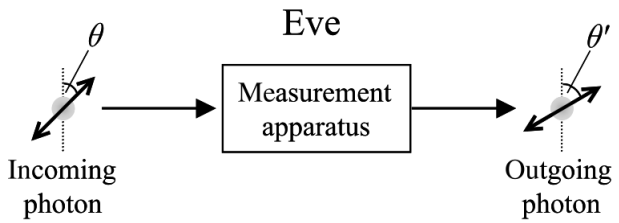

Figure 1.2: Eve measures the incoming photon in a random basis. If she chooses the wrong one, she obtains a completely random outcome, erasing the qubit information. As a result, the bogus photon sent to Bob will be completely different from the incoming one [8].

From these examples, it is clear that **Eve can be easily put in trouble using more than one basis**, and her presence can be easily detected. Alice and Bob can use a classic channel to confront part of the data exchanged: if there were any inconsistencies, they would be evidence of Eve's presence. Obviously, in real systems

imperfections, losses, and noise complicate the situation, allowing Eve to partially hide her presence.

1.5 Two basic protocols

In this section two basic QKD protocols will be analyzed: BB84 and LM05. BB84 is one of the first proposed protocol, while LM05 is a more recent proposal, based on a closed loop optical system.

1.5.1 BB84 protocol

BB84 protocol was proposed in 1984 by Charles H. Bennet and Gilles Brassard. In its polarization-encoding version, it is based on the use of two polarization basis set: the {Horizontal, Vertical} basis, also represented as $\oplus$, and the {Anti-diagonal, Diagonal} one, represented as $\otimes$.

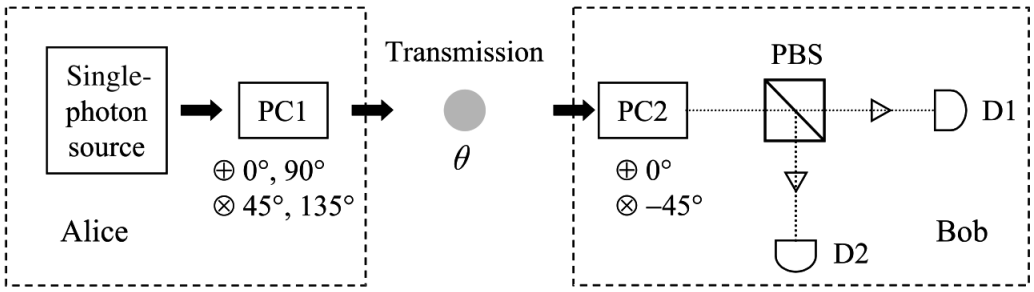

Figure 1.3: Schematic representation of a BB84 system. The polarization of photons generated by Alice's apparatus can be rotated using a set of Pockels cells, depicted as PC1. Bob uses a second Pockels cell to rotate again the polarization of 0° or −45° in order to select the measurement basis. The polarizing beam splitter (PBS) coupled with two single photon detectors constitutes the **measurement apparatus** [8].

The convention used to encode the information on the polarization state is the following:

- **Basis** $\oplus$: binary 1 corresponds to vertical polarization, while 0 to horizontal one;

- **Basis** $\otimes$: 1 corresponds to diagonal polarization ($\theta = 45°$ from vertical axis), while 0 corresponds to anti-diagonal polarization ($\theta = -45°$ from the vertical axis)

The protocol is divided in four phases: the "quantum transmission", the "public discussion", the "privacy amplification", and the "error reconciliation" : qubits are transmitted using the quantum channel, then the users compare some of them using the classical channel to test the security, and at the end, if no-one interfered, algorithms of privacy amplification and error reconciliation are applied to obtain a safer key.

Schematically, Alice apparatus consists of a single-photon source, which generates photons in vertical polarization (but the concepts apply equally if they come out horizontally polarized), and a set of Pockels cells used to change the polarization direction to encode "0" or "1" in one of the two basis.
A quantum channel (an optical fiber or the open space) links Alice and Bob equipments. Alongside, there is a classic channel used to exchange service information necessary to verify the security and synchronize the communication.

Bob apparatus consists of a Pockels cell and a measurement system. When the Pockels cell is activated, it rotates photon polarization of $\theta = -45°$ to measure in the {Anti-diagonal, Diagonal} basis, whereas, when de-activated, measurement happens in the {Horizontal, Vertical} basis.
Then a polarizing beam splitter directs vertically polarized photons to detector D1 and the horizontally polarized photons to detctor D2. So, PBS coupled with the photon detectors constitute the **measurement system** [8]. A block scheme of the system is given in Figure 1.3.

Hypotizing that Alice wants to send to Bob $4N$ qubits, she chooses randomly the polarization basis for each of them and she sends them without saying beforehand her base choices to Bob. He receives the photons and measures them randomly in one of the two basis. At the end of the quantum communication, Alice uses the classical channel to report to Bob the sequence of basis she used (**basis reconciliation**).

Bob choses the right basis in the 50% of cases so, on average, $2N$ qubits are correct whereas the other $2N$ must be discarded.

Alice sends	0	1	0	0	1	1	0	1	0	0	1	0	...
Alice's code	(1)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	(1)	...
Bob's code	(1)	(2)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	...
Bob reads	0	1	?	?	1	?	?	?	?	0	?	0	...

Figure 1.4: Example of exchanged qubits, with the corresponding basis used by Alice and Bob [1].

In order to verify the security of this communication, Alice and Bob compare half of the bits for which they used the same basis [8]. Therefore they compare N qubits randomly: if they all match (apart from a small and predictable error due to the instrumentation) the communication was secure and the remaining N bits form the **sifted key**.
On the contrary, if an eavesdropper interfered, a much larger error would be find during the comparison of the N bits, due to the aforementioned **no-cloning theorem**. The problem is that Eve does not know the encoding basis used by Alice, so she obtains a random outcome in the 50% of her measurements. As a result, there are cases (the ones highlighted in red in Figure 1.5) where Alice and Bob choose the same basis but they obtain a different result. At the moment of comparison of the N bits, Alice and Bob find that, on average, $\frac{N}{4}$ bits are wrong: this is an error much larger than the instrumental one, proof that someone interfered. In this case the communication is interrupted immediately.

Alice sends	0	1	0	0	1	1	0	1	0	0	1	0	...
Alice's code	(1)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	(1)	...
Eve's code	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	...
Eve reads	0	1	0	0	?	?	?	?	?	0	1	?	...
Bob's code	(1)	(2)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	...
Bob reads	0	1	?	?	?	?	?	?	?	0	?	?	...

Figure 1.5: Effect of Eve on the communication [1]

On the contrary, if the Quantum Bit Error Ratio (QBER) is less than a certain security threshold, Alice and Bob can post process the data using techniques called **error correction** and **privacy amplification** to obtain a shorter but more secure

key, with minimal information known by the eavesdropper [11]. Privacy amplification is the last but not least operation, used to distill the corrected raw key in order to obtain a final key which is secure, even if Eve stole some information during the communication on the quantum channel or during the post-processing carried out on the classical channel [12, 13].

Implementing this protocol in real systems, the non ideality of the light source must be taken in account. In fact, at present, only **quasi single-photon sources** are available and consequently not every signal pulse is made by a single photon. Hence, Eve can take advantage of this, by splitting the communication beam and subtracting information while remaining undetected, as she can do in classical communication systems.

To deal with this problem it is convenient to send pulses of different intensities, in addition to the signal ones: they are called **decoy states**, and they are used only for security purposes. Comparing the reception rates of signal and decoy states, it is possible to easily reveal the presence of Eve also in real systems, as will be shown in section 1.7.

Researches and experiments show that, using BB84 protocol without decoy states, a secure connection up to 120 km can be established using optical fibers as quantum channel [14, 15, 16], whereas, in free space, the maximum distance is about 25 km [17, 18]. Conversely, using decoy states, communications in fiber up to 200 km can be established [19], as well satellite quantum communications, with a feasible distance in the order of 720 km [20].

1.5.2 LM05 protocol

LM05 is an example of polarization-based, closed-loop QKD system, where two sets of orthogonal bases are used, as in BB84 protocol. In this case, the single-photon source is at the Bob side, who sends a string of photons, each of which in one of the four possible polarization states.

In order to encode the information, Alice uses the so-called **Universal equatorial gate**, made by two Pockels cells, able to flip the information encoded in the photon, preserving the basis previously fixed [21].

The Pockels cells are a fundamental part in a QKD system, especially in that based on polarization-coding. They are voltage-controlled waveplates made of birefringent materials, capable of altering the polarization of light [8]. The effects may be different, depending on the structure of the cell, as will be explained in the successive chapters. Half-wave plates are the most interesting in QKD because they changes the orientation of polarization vector, acting on linearly polarized light.

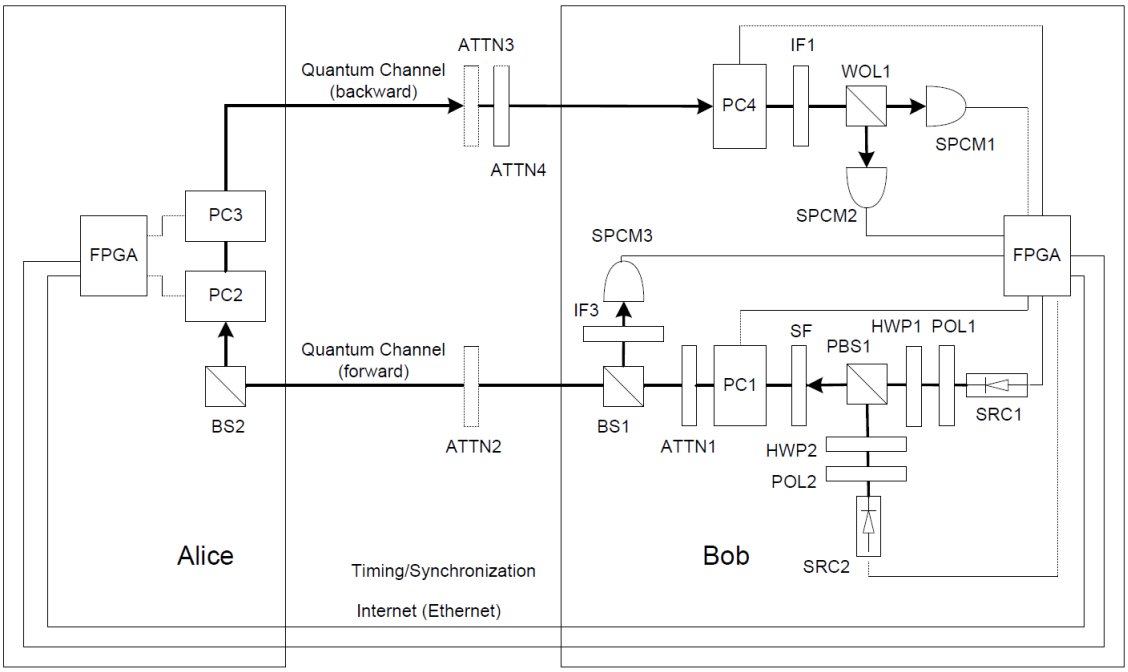

Figure 1.6: Example of LM05 communication setup: Bob uses two lasers (SRC1 and SRC2) coupled to polarizers (POL1 and POL2) to generate horizontally and vertically polarized photons respectively. Then, he uses a polarizing beam splitter (PBS1) to merge this photon in the same optical path. A spatial filter (SF) improves the mode quality. The first Pockel cell (PC1) encode the photons in the {A,D} basis, when active. A variable optical attenuator (ATTN1) reduces the intensity of the pulse down to signal or decoy level, verified using a beam splitter (BS1) and a photon detector (SPCM3). After the quantum channel, the photon pulse reaches Alice receiver, where she uses two Pockels cells (PC2 and PC3) to encode the information. The measurement part in the Bob side is made by a Pockels cell (PC4), coupled to PC1, to measure in the same sending basis, a Wollaston prism (WOL1), analogous of a polarizing beam splitter, and two photon counting modules (SPCM1 and SPCM2) [21].

As can be seen in Figure 1.6, Bob uses Pockels cell one (PC1) to pass from {H,V}

to {A,D} basis. Without knowing the basis used by Bob, Alice encodes a logic 1 activating her set of Pockels cells, the universal equatorial gate M_{23}, which acts in this way:

$$\begin{aligned} M_{23}\,|H\rangle &= |V\rangle \\ M_{23}\,|V\rangle &= |H\rangle \\ M_{23}\,|A\rangle &= |D\rangle \\ M_{23}\,|D\rangle &= |A\rangle \end{aligned} \tag{1.3}$$

On the contrary, when inactive, the state of polarization (SOP) of the photon remains untouched (M_{23} becomes the identity matrix), encoding the 0. Alice then sends the qubit back to Bob who uses the PC4 to measure in the same sending basis.

Unlike BB84, being a closed-loop system, LM05 does not require the basis reconciliation phase; the raw key measured by Bob coresponds to the sifted key. So they can directly proceed to error reconciliation and privacy amplification [21].

1.6 A critical problem: PNS attack

The theoretical basis of QKD assumes the usage of single photon signals; unfortunately, actual single photon sources have not been realized so far. In fact, the most common light sources are lasers attenuated to single photon level, as in the LM05 protocol example. Obviously, the resulting light beam is not a single photon, but a coherent state whose photon number follows a Poisson distribution.

$$\mathcal{P}_\lambda(x) = \frac{\lambda^x}{x!} e^{-\lambda}, \tag{1.4}$$

where λ is the mean photon number of a pulse.

An eavesdropper can take advantage of this weakness subtracting some photons from the pulse, without revealing its presence: this is the **photon number splitting attack** (PNS).

As depicted in Figure 1.8, Eve can use a beam splitter to separate the signal in two parts, then she performs a Quantum Nondemolition measurement (QND) on one of these, by which she measures only if there is at least a photon. If so,

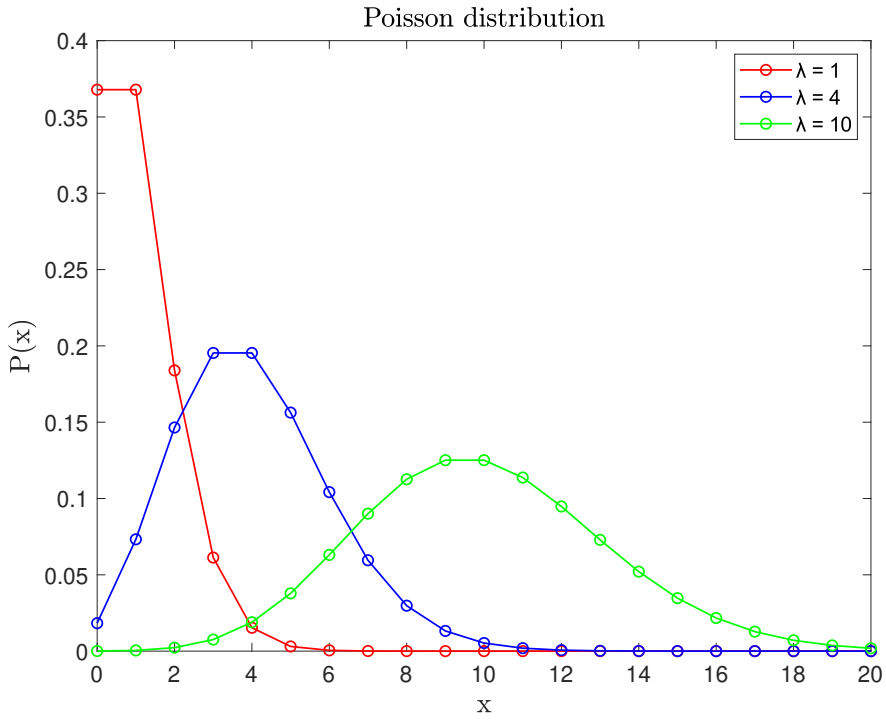

Figure 1.7: Poisson distribution with three different mean photon number λ. P(x) is the probability to find x photons in a pulse.

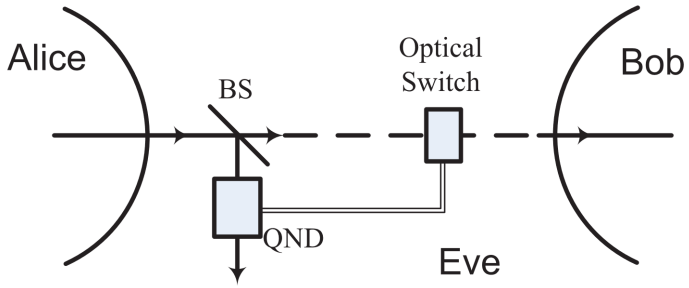

Figure 1.8: Schematic of the components necessary to perform a PNS attack [22].

she stores it in a quantum memory, otherwise she stops the communication with an optical switch. In this way all the single photons sent by Alice are blocked, while all the other qubits are possessed by both Eve and Bob [22]. At the moment of basis reconciliation, Eve can properly measure the photons stored in the memory, obtaining the final key.

Since for Alice and Bob the blocked photons are completely indistinguishable

from photons lost due to systems imperfections, the PNS only slightly increases the QBER. Obviously Eve has to properly choose the transmission coefficient of the beam splitter in order to not alter excessively the raw key rate and the QBER, remaining undetected [22, 23].

Leaving aside this example, it is clear that the current impossibility to use a real single-photon source is a serious weakness for QKD systems. Fortunately, the implementation of decoy states or the usage of different QKD protocols resistant to PNS, such as Measurement-Device Independent or Continuous Variable protocols [23], allow to overcome this problem.

1.7 A fundamental improvement: the decoy state protocol

As aforementioned, decoy states are a countermeasure against PNS attacks and, in general, are useful to improve the security of the communication. In a decoy state protocol Alice sends photon pulses at different intensity levels, in addition to signal pulses. The most implemented decoy protocols use three different types of states: signal, decoy, and vacuum states.
Signal states are the only ones that carry information, and they are usually light pulses with 0.6 mean photon number (MPN).
Decoy states can be weaker, made for example by 0.2 MPN pulses [23], or stronger, made for example by 1 MPN pulses [24].
Vacuum states, as suggested by their name, take place when Alice does not send photons at all. In these cases, the detection events obtained at Bob's side are linked only to background and errors.

It is important that signal and decoy states only differ in the mean photon number and are equal for wavelength, duration, and pulse shape: they must be completely indistinguishable for the eavesdropper. In fact, as explained in the previous section, during a PNS attack, the eavesdropper tries to block all single photon pulses. Since signal and decoy states have a different mean photon number, a PNS attack influences differently their yields, where the yield is the ratio between the states detected by Bob and those emitted by Alice. There are two cases:

1. Using weak decoy states, Eve significantly reduces the decoy states efficiency, due to their lower MPN [23];

2. Using strong decoy states, Eve reduces the signal efficiency.

Therefore, comparing the yield for signal and decoy states, it is possible to reveal the presence of the eavesdropper.

1.8 Light sources: an overview

As emerged from this brief introduction, the light source is a fundamental part of a QKD system. In fact the PNS attack takes advantage of its imperfections.

In general, a classical source emits light pulse in which the photon number follows a Poisson distribution, id est $\Delta n = \sqrt{\bar{n}}$ (**Poisson statistics**), where Δn and $\bar{n}$ are the photons variance and the photons mean number respectively. In other cases the emitted light has $\Delta n > \sqrt{\bar{n}}$ (**super-Poissonian statistics**). On the other hand, single-photon sources emit light with a lower variance, so $\Delta n < \sqrt{\bar{n}}$ (**sub-Poissonian statistics**) [8]. As it is clear, for quantum information applications, sub-Poissonian light is the most desirable, having a lower variance so resulting less vulnerable to PNS attacks.

In order to define the quality of a single photon source, the **second-order correlation function** $g^2(\tau)$ is used. It quantifies the intensity fluctuations in time (whereas the first-order correlation function $g^1(\tau)$ quantifies the electric field fluctuations), and it is given by the following formula [8]:

$$g^{(2)}(\tau) = \frac{\langle \mathcal{E}^*(t)\mathcal{E}^*(t+\tau)\mathcal{E}(t+\tau)\mathcal{E}(t)\rangle}{\langle \mathcal{E}^*(t)\mathcal{E}(t)\rangle \langle \mathcal{E}^*(t+\tau)\mathcal{E}(t+\tau)\rangle} = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle\langle I(t+\tau)\rangle}, \tag{1.5}$$

where $\mathcal{E}$ and $I(t)$ are the electric field and intensity of the light beam at time t. The symbol $\langle ... \rangle$ indicates the time average.
All classical light is characterized by the following properties:

$$\begin{aligned} g^2(0) &\geq 1 \\ g^2(0) &\geq g^2(\tau). \end{aligned} \tag{1.6}$$

In particular, perfectly coherent light has $g^2(\tau) = 1$ for all τ, whereas chaotic light, for example that emitted by a discharge lamp, has $g^2(0) > 1$ [8].
Conversely, ideal single photon sources emit only one photon at a time, therefore they have

$$\begin{aligned} g^2(0) &= 0 \\ g^2(\tau) &= 1 \end{aligned} \tag{1.7}$$

for $\tau \to \infty$ [25].

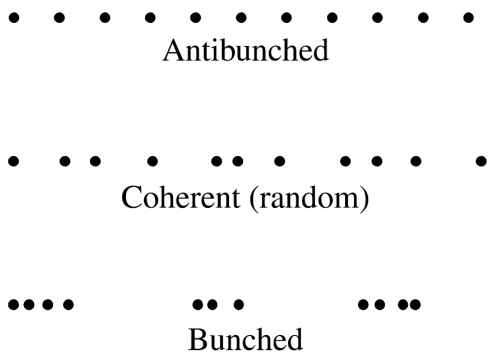

Figure 1.9: Comparison of the photon arrangement in antibunched, coherent, and bunched light [8].

Furthermore, the concepts of bunching and antibunching are really usefull to define the type of light emitted by the source. The classification is based on $g^2(0)$ and is the following [8]:

- **antibunched light**: $g^2(0) < 1$, it is a purely quantum optical phenomenon without classical counterparts. The photons spread out with regular intervals between them;
- **coherent light**: $g^2(0) = 1$, the time interval between two subsequent photons is completely random;
- **bunched light**: $g^2(0) > 1$, the photons clump together in bunches. This is typical of classical light sources.

Figure 1.9 clarifies this classification.

Nowadays, two types of single photon sources are the most investigated for quantum information applications: sources of single photons and sources of pairs of entangled photons. Most of them are based on parametric down-conversion [25], that consists in the use of nonlinear birefringent crystals to convert a photon in a pair of photons of lower energy [26].
Unfortunately they are too much immature to be implemented in commercial systems. For this reason, most of the current QKD systems use coherent light sources (lasers or diodes) attenuated to quasi-single-photon level.

Chapter 2

Theoretical model

In this chapter, a possible theoretical model to describe QKD systems will be explained. This model rises from the Heisenberg picture of quantum physics: the idea is to propagate the initial state generated by the light source across the structure, evolving the operators applied to the state vector.
Since the light source is often a laser attenuated to quasi single-photon levels, coherent states can correctly model these signals. Then, considering that a general coherent state can be written using the **displacement operator** $\hat{D}(\alpha)$ acting on the vacuum state $|0\rangle$, it is possible to propagate the initial state across every component of the system evolving the creation and annihilation operators contained in the displacement operator. Furthermore, using this model, it is possible to take in account also more than one optical path, a very useful feature when studying complex optical systems.

2.1 Coherent states

The theory of coherent states was introduced by Schrödinger in 1926 and was first used in quantum optics by Glauber in 1963, who understood that an electromagnetic wave in a box can be seen as a countably infinite superposition of harmonic oscillators [8, 27]. The choerent states representation fits very well to the description of quantized electromagnetic fields, and so in the cases of quasi single-photon light. In Dirac notation, they are represented as $|\alpha\rangle$, where α is a dimensionless complex number. Matematically, they are eigenstates of the annihilation operator:

$$\hat{a}\,|\alpha\rangle \;=\; \alpha\,|\alpha\rangle \tag{2.1}$$

In the number or Fock state representation, the annihilation operator $\hat{a}$ and

the creation operator $\hat{a}^\dagger$, its adjoint, are related to position $\hat{Q}$ and momentum $\hat{P}$ operators as follows:

$$\hat{a} = \frac{1}{\sqrt{2\hbar m\omega}}(m\omega\hat{Q} + i\hat{P}), \quad \hat{a}^\dagger = \frac{1}{\sqrt{2\hbar m\omega}}(m\omega\hat{Q} - i\hat{P}), \tag{2.2}$$

and acting on a Fock state they give:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \quad \hat{a}^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \tag{2.3}$$

in practice they add or remove a quantum from the system. Their action on the vacuum state is:

$$\hat{a}|0\rangle = 0, \quad \left(\hat{a^\dagger}\right)^n|0\rangle = \sqrt{n!}|n\rangle. \tag{2.4}$$

As aforementioned, in general α is a complex number because the annihilation operator is not Hermitian. Separating it in amplitude and phase:

$$\alpha = |\alpha|e^{i\phi}. \tag{2.5}$$

From this expression it is clear the possibilty to represent coherent states in the phasor space. To better understand the significance of α, it is possible to think about a linearly polarized mode of angular frequency ω enclosed in a cavity of volume V. It is possible to represent α using the dimensionless quadratures of field in the cavity [8], X_1 and X_2:

$$\alpha = X_1 + iX_2 \tag{2.6}$$

with

$$|\alpha| = \sqrt{X_1^2 + X_2^2}, \tag{2.7}$$

where the quadrature operators are by definition:

$$\begin{aligned} \hat{X}_1 &= \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right) \\ \hat{X}_2 &= \frac{1}{2i}\left(\hat{a} - \hat{a}^\dagger\right) \end{aligned} \tag{2.8}$$

which are used to re-write the electric field operator. Considering the x-component

of the electric field propagating along the z direction, the operator is:

$$\hat{E}_x = \mathcal{E}_0 \left(\hat{a}e^{-i\omega t} + \hat{a}^\dagger e^{i\omega t}\right) \sin(kz), \tag{2.9}$$

where $\mathcal{E}_0$ is the electric field amplitude, ω the angular frequency, and $k = 2\pi/\lambda$ is the wave vector [8]. It can be rewritten as:

$$\hat{E}_x(t) = 2\mathcal{E}_0 \sin(kz) \left[\hat{X}_1 \cos(\omega t) + \hat{X}_2 \sin(\omega t)\right], \tag{2.10}$$

where the quadrature operators $\hat{X}_1$ and $\hat{X}_2$ are associated with the oscillations of the electric field, shifted of 90°, so they are in quadrature [28].
Recalling the connection between light and harmonic oscillators, which comes from the wave nature of light, starting from the quantum uncertainty relation for harmonic oscillators:

$$\Delta q \, \Delta p_q \geq \frac{\hbar}{2} \tag{2.11}$$

where Δq is the uncertainty on position, Δp_q the uncertainty on momentum, and $\hbar$ the reduced Planck's constant; it is possible to find for coherent states:

$$\Delta X_1 = \Delta X_2 = \frac{1}{2} \tag{2.12}$$

understanding that they are minimum uncertainty states [8].

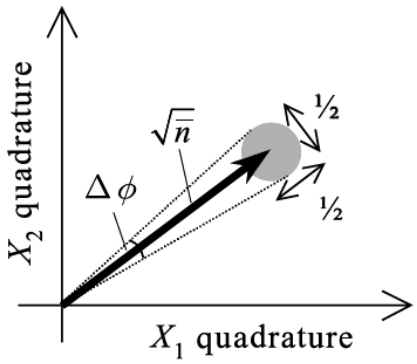

Figure 2.1: Phasor diagram of a coherent state, where the uncertainty circle is shown in grey [8].

Taking in account this uncertainty, the phasor diagram of a coherent state is reported in Figure 2.1. Phasor diagrams are very useful in quantum optics to represent the light state; any state is an area centered around the point $(\langle X_1\rangle,\langle X_2\rangle)$ for that state. The circle in grey represents the quantum uncertainty on photon number and phase, and it has an area related to the variance $\langle \Delta X_1^2\rangle$ and $\langle \Delta X_2^2\rangle$. For a coherent state, it has a diameter of $\frac{1}{2}$. Furthermore, it is interesting to note that the uncertainty area has a constant dimension, independent of the α parameter of the coherent state, and that two states are distinguishable only if they are separated at least by $\langle \Delta X_1^2\rangle$. This sets a limit for the measurement precision [29]. The amplitude of α can be related to the electric field amplitude $\mathcal{E}_0$ associated with the electromagnetic wave [8]:

$$|\alpha| = \sqrt{\frac{\epsilon_0 V}{4\hbar\omega}}\,\mathcal{E}_0 \tag{2.13}$$

where ϵ_0 is the electric permittivity of free space and V the mode volume, and also to the mean photon number [8, 30]:

$$|\alpha| = \sqrt{\bar{n}}\,. \tag{2.14}$$

Now, it is interesting to compute the variance of α. First of all, the **number operator** $\hat{n}$ shall be introduced:

$$\hat{n} \triangleq \hat{a}^\dagger \hat{a}. \tag{2.15}$$

The fluctuations of the photon number are computed as:

$$\Delta n = \sqrt{\langle \hat{n}^2\rangle - \langle \hat{n}\rangle^2}\,. \tag{2.16}$$

As reported in Equation 2.14, the expectation value of $\hat{n}^2$ is:

$$\bar{n} = \langle \alpha|\hat{n}|\alpha\rangle = |\alpha|^2 \tag{2.17}$$

while the expectation value of n^2 is:

$$\left\langle \hat{n}^2 \right\rangle = \left\langle \alpha \left| \hat{n}^2 \right| \alpha \right\rangle = \left\langle \alpha \left| \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} \right| \alpha \right\rangle = \left\langle \alpha \left| a^\dagger a^\dagger \hat{a} \hat{a} + \hat{a}^\dagger \hat{a} \right| \alpha \right\rangle = |\alpha|^4 + |\alpha|^2 = (\bar{n})^2 + \bar{n} \tag{2.18}$$

therefore:

$$\Delta n = \sqrt{\langle n^2 \rangle - \langle n \rangle^2} = \sqrt{\bar{n}} = |\alpha| \,. \tag{2.19}$$

In practice the variance of the photon number is equal to the mean photon number itself: this is typical of Poisson distributions. Hence, coherent states follow the Poisson distribution; in fact the probability to find n photons in the beam is [28] :

$$P_n \;=\; |\langle n|\alpha\rangle|^2 \;=\; e^{-|\alpha|^2} \cdot \frac{|\alpha|^{2n}}{n!} = e^{-\bar{n}} \cdot \frac{\bar{n}^n}{n!}. \tag{2.20}$$

Returning to fundamental properties, coherent states are also eigenbra of creation operators, with eigenvalue α^*:

$$\langle \alpha | \hat{a}^\dagger = \langle \alpha | \alpha^*. \tag{2.21}$$

2.1.1 Glauber-Klauder-Sudarshan or Standard Coherent States

It is possible to write the coherent states using the Fock basis. Let's start writing a generic coherent state as superposition of Fock states:

$$|\alpha\rangle \;=\; \sum_{n=0}^{\infty} A_n |n\rangle \,. \tag{2.22}$$

Applying the annihilation operator:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle = \sum_{n=0}^{\infty} A_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} A_n |n\rangle \tag{2.23}$$

giving:

$$A_n \sqrt{n} = \alpha A_{n-1} \tag{2.24}$$

and iterating:

$$|\alpha\rangle = A_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{2.25}$$

After the trivial normalization [30]:

$$\langle\alpha|\alpha\rangle = 1 = |A_0|^2 \sum_m \sum_n \frac{\alpha^m \alpha^n}{\sqrt{m!n!}} \langle m|n\rangle = |A_0|^2 \sum_n \frac{|\alpha|^{2n}}{n!} = |A_0|^2 e^{|\alpha|^2} \,, \tag{2.26}$$

at the end, one arrives at:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{2.27}$$

which is the normalized or standard representation of a coherent state.

2.1.2 Coherent states: an overcomplete basis

Unlike Fock states, coherent states are not orthogonal. In fact:

$$\begin{aligned} \langle \beta \mid \alpha \rangle &= e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{(\beta^*)^n \alpha^m}{\sqrt{n!m!}} \langle n \mid m \rangle \\ &= e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2} \sum_{n=0}^{\infty} \frac{(\beta^* \alpha)^n}{n!} \\ &= e^{-\frac{1}{2}|\alpha|^2 - \frac{1}{2}|\beta|^2 + \beta^* \alpha} \\ &= \exp\left[\frac{1}{2}\left(\beta^* \alpha - \beta \alpha^*\right)\right] \exp\left[-\frac{1}{2}|\beta - \alpha|^2\right] . \end{aligned} \tag{2.28}$$

The first term is just a complex phase so it is obvious that:

$$|\langle \beta \mid \alpha \rangle|^2 = e^{-|\beta - \alpha|^2} \neq 0 \,, \tag{2.29}$$

as shown in [28]. This last expression shows that coherent states becomes nearly orthogonal when $|\beta - \alpha|$ increases.
Furthermore, coherent states are overcomplete so there are more than enough states available to express a generic coherent state [28], as shown by the completeness

relation

$$\int |\alpha\rangle\langle\alpha| \, \mathrm{d}^2\alpha = \pi \, I, \tag{2.30}$$

where I is the identity matrix. This can be considered a direct consequence of the non-ortoghonality of coherent states shown in Equation 2.28.

2.1.3 Displaced vacuum states

The **displacement operator** is extremely powerful given that a coherent state can be obtained as a displaced vacuum state [28]:

$$|\alpha\rangle \; = \; e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \, |0\rangle \; = \; \hat{D}(\alpha) \, |0\rangle. \tag{2.31}$$

This operator is unitary, so $\hat{D}(\alpha)\hat{D}(\alpha)^\dagger = \hat{D}(\alpha)^\dagger\hat{D}(\alpha) = I$. Its Hermitian conjugate is a displacement operator of opposite magnitude $\hat{D}(\alpha)^\dagger = \hat{D}(-\alpha)$. From the Baker-Campbell-Hausdorff formula one obtains that, for the product of two displacement operators [30]:

$$\hat{D}(\alpha)\hat{D}(\beta) = e^{\frac{1}{2}(\alpha\beta^* - \alpha^*\beta)}\hat{D}(\alpha+\beta) \, . \tag{2.32}$$

To better understand the action of displacement operator given in 2.31, it is necessary to re-write this operator by exploiting the well-known Kermack-McCrae identity, also known as disentangling theorem [28]:

$$e^{\mathrm{A}+\mathrm{B}} = \begin{cases} e^{-\frac{1}{2}\mathrm{C}} \cdot e^{\mathrm{A}} e^{\mathrm{B}} & : \quad \text{AB-ordered} \\ e^{+\frac{1}{2}\mathrm{C}} \cdot e^{\mathrm{B}} e^{\mathrm{A}} & : \quad \text{BA-ordered} \end{cases} \tag{2.33}$$

valid when the operators $\hat{A}$ and $\hat{B}$ commute with their commutator $\hat{C} = [\hat{A},\hat{B}]$, with $\hat{C} \neq 0$. By placing $\hat{A} = \alpha\hat{a}^\dagger$ and $\hat{B} = -\alpha^*\hat{a}$, $\hat{C} = [\hat{A},\hat{B}] = |\alpha|^2$, one can find that [28, 30]:

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}. \tag{2.34}$$

After the trivial demonstration that:

$$e^{-\alpha\hat{a}} \; |0\rangle \; = \; |0\rangle \; , \tag{2.35}$$

starting from the standard representation of coherent states, it is easy to demonstrate

that:

$$\begin{aligned} |u\rangle &= e^{-\frac{|u|^2}{2}} \sum_{n=0}^{+\infty} \frac{u^n}{\sqrt{n!}} |n\rangle \\ &= e^{-\frac{|u|^2}{2}} \sum_{n=0}^{+\infty} \frac{u^n}{n!} (\hat{a}^\dagger)^n |0\rangle \\ &= e^{-\frac{|u|^2}{2}} e^{u\hat{a}^\dagger} |0\rangle \\ &= e^{-\frac{|u|^2}{2}} e^{u\hat{a}^\dagger} e^{-u^*\hat{a}} |0\rangle \\ &= \hat{D}(u)|0\rangle \end{aligned} \tag{2.36}$$

In the next sections, the propagation of the initial state will be carried out by the propagation of the displacement operator, component by component.

2.2 A brief recalling of polarization of light

Before entering the core of the model, some concepts about polarization of light and the basis of Jones calculus will be recalled.

2.2.1 Polarization of light

Polarization is a property that describes the orientation of oscillation of electric and magnetic fields associated with light. By convention, the polarization of electromagnetic waves refers to the direction of the electric field: it can be linear, if the electric field oscillates along a single direction, or elliptical (in particular cases circular), if the field rotates in a plane. In this last case it is distinguished in right or left circular polarization, depending if the field rotatets in the right or left sense hand respect to the propagation direction of the electromagnetic wave.
In general, the electric field has the following expression:

$$\begin{aligned} \vec{\mathbf{E}}(t) = &\mathcal{E}_{x0} \cos(\omega_0 t + \varphi_x)\, \hat{\mathbf{x}} \\ &+ \mathcal{E}_{y0} \cos(\omega_0 t + \varphi_y)\, \hat{\mathbf{y}} \\ &+ \mathcal{E}_{z0} \cos(\omega_0 t + \varphi_z)\, \hat{\mathbf{z}} \end{aligned} \tag{2.37}$$

which can be re-written as:

$$\vec{\mathbf{E}}(t) = \mathrm{Re}\left\{\left(\mathcal{E}_{x0}\mathrm{e}^{\mathrm{i}\varphi_{\mathrm{x}}}\hat{\mathrm{x}} + \mathcal{E}_{\mathrm{y}0}\mathrm{e}^{\mathrm{i}\varphi_y}\hat{\mathbf{y}} + \mathcal{E}_{\mathrm{z}0}\mathrm{e}^{\mathrm{i}\varphi_z}\hat{\mathbf{z}}\right)\mathrm{e}^{\mathrm{i}\omega_0\mathrm{t}}\right\} = \mathrm{Re}\left\{\vec{\mathbf{E}}\mathrm{e}^{\mathrm{i}\omega_0\mathrm{t}}\right\}, \tag{2.38}$$

where $\vec{\mathbf{E}}$ is the phasor associated with the field. The phasor is a complex vector, and so, in the tridimensional space, it is made by six components, three real and three imaginary. Therefore, it can be separated as:

$$\vec{\mathbf{E}} = \vec{\mathbf{E}}' + i\,\vec{\mathbf{E}}'', \tag{2.39}$$

where

$$\vec{\mathbf{E}}' = \mathcal{E}_{x0}\cos\varphi_x\hat{\mathbf{x}} + \ldots, \quad \vec{\mathbf{E}}'' = \mathcal{E}_{x0}\sin\varphi_x\hat{\mathbf{x}} + \ldots. \tag{2.40}$$

Now, re-writing Equation 2.38 as:

$$\vec{\mathbf{E}}(t) = \mathrm{Re}\left\{\left(\vec{\mathbf{E}}' + i\vec{\mathbf{E}}''\right)(\cos\omega_0 t + i\sin\omega_0 t)\right\} = \vec{\mathbf{E}}'\cos\omega_0 t - \vec{\mathbf{E}}''\sin\omega_0 t, \tag{2.41}$$

it can be shown that, in general, this equation describes an elliptical plot in the $\vec{\mathbf{E}}'$-$\vec{\mathbf{E}}''$ polarization plane, as shown in Figure 2.2. The time dependent electric field

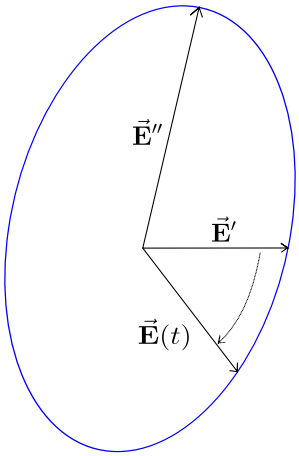

Figure 2.2: Plot of a generic elliptical polarization. The sense of rotation is from $\vec{\mathbf{E}}'$ to $-\vec{\mathbf{E}}''$

vector $\vec{\mathbf{E}}$ rotates from $\vec{\mathbf{E}}'$ to $-\vec{\mathbf{E}}''$ and its tip describes the blue plot.
In general this plot is an ellipse, called **elliptical polarization**. Depending on magnitude and relative direction of these two vectors, particular types of polarizations can be described:

- **linear polarization** when $\vec{\mathbf{E}}' \times \vec{\mathbf{E}}'' = 0$, so the vectors are parallel or one of them is 0;
- **circular polarization** when $\left|\vec{\mathbf{E}}'\right| = \left|\vec{\mathbf{E}}''\right|$ and $\vec{\mathbf{E}}' \cdot \vec{\mathbf{E}}'' = 0$

Another way to distinguish polarization types is to define an x-y cartesian reference frame on the polarization plane. So, the phasor has x and y components and can be re-written as follows:

$$\vec{\mathbf{E}} = E_x\,\hat{\mathbf{x}} + E_y\,\hat{\mathbf{y}} = |E_x|e^{i\phi_x}\,\hat{\mathbf{x}} + |E_y|e^{i\phi_y}\,\hat{\mathbf{y}} \tag{2.42}$$

- if the phase difference $\delta = \phi_x - \phi_y$ is 0 or π the polarization is linear;
- if $\delta = \pm\frac{\pi}{2}$ and $|E_x| = |E_y|$ the polarization is circular [31].

2.2.2 Jones calculus

To study the polarization of light and its transformations, it is often convenient to use the Jones calculus, formalized by R. C. Jones in 1942 [32]. The state of polarization of light is represented by a vector, whereas the optical components are described by 2×2 matrices. When light interacts with an optical component, the output polarization state is given by the product of the initial light vector with the matrix associated with the component.

A Jones vector contains the complex components of the electric field phasor:

$$\begin{pmatrix} |E_x|\,e^{i\phi_x} \\ |E_y|\,e^{i\phi_y} \end{pmatrix}, \tag{2.43}$$

where the reference system is choosen to align electric field polarization with the x-y plane. The fundamental Jones vectors are reported in Table 2.1, with their relative ket notation:

Polarization	Jones vector	Dirac notation	Bit value
Horizontal polarization, parallel to x axis	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\|H\rangle$	0
Vertical polarization, parallel to y axis	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\|V\rangle$	1
Antidiagonal polarization, oriented at -45° with respect to x axis	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$	$\|A\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	0
Diagonal polarization, oriented at 45° with respect to x axis	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\|D\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	1
Left-hand circular polarization	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	Not defined
Right-hand circular polarization	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	Not defined

Table 2.1: Summary of the possible light polarization states, together with their Jones vectors, their Dirac notation, and the corresponding usual bit value.

As an example, one of the simplest optical component, the linear polarizer, is represented by the following matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.44}$$

with horizontal transmission axis [33].

2.2.3 Displaced states considering polarization

A widely used characteristic of the displacement operator is that it can take in account also the state of polarization of the coherent state [34, 35, 36, 37]. For example, considering a coherent light pulse diagonally polarized, oriented at +45° from the horizontal axis, it can be expressed as:

$$|\alpha_{+45}\rangle = \hat{D}(\alpha_{+45^\circ})\,|0_H,0_V\rangle = \exp\left(\frac{\alpha}{\sqrt{2}}(\hat{a}_H^\dagger + \hat{a}_V^\dagger) - \frac{\alpha^*}{\sqrt{2}}(\hat{a}_H + \hat{a}_V)\right)|0_H,0_V\rangle\ , \tag{2.45}$$

where the horizontal-vertical basis has been used, and $|0_H,0_V\rangle$ is the vacuum state in the two-mode polarization Fock space [38].

This last expression is really evocative: modifying the creation and annihilation operators contained in $\hat{D}$, it is possible to describe the evolution of the coherent state across a generic structure.

2.3 Propagation in quantum optics

In order to propagate the state across the structure, unitary transformations are used to describe the interaction with every optical component. These unitary transformations are modeled by unitary operators $\hat{U}$ which preserve the inner product in the Hilbert space and respect the relation $\hat{U}^\dagger = \hat{U}^{-1}$ [29].

In order to describe the evolution of a quantum state, two equivalent pictures are employed: the Schrödinger and the Heisenberg ones.
The Schrödinger picture puts its roots in the homonymous and famous equation, from which the **temporal evolution of the state** can be computed:

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle , \tag{2.46}$$

where $\hat{H}$ is the Hamiltonian of the system. Considering a time-invariant Hamiltonian, the solution is:

$$|\psi(t)\rangle = \exp\left\{-\frac{i\hat{H}t}{\hbar}\right\} |\psi(0)\rangle = \hat{U}(t) |\psi(0)\rangle , \tag{2.47}$$

where $|\psi(0)\rangle$ is the initial state of the system.
On the contrary, in the Heisenberg picture, the states of the system are temporal independent, whereas **the operators are temporal dependent**. The evolution of the observable $\hat{O}$ can be computed as follows:

$$\left\langle \psi(t) \left| \hat{O} \right| \psi(t) \right\rangle = \left\langle \psi(0) \left| e^{\frac{i\hat{H}t}{\hbar}} \hat{O}\, e^{-\frac{i\hat{H}t}{\hbar}} \right| \psi(0) \right\rangle = \left\langle \psi_H \left| e^{\frac{i\hat{H}t}{\hbar}} \hat{O}\, e^{-\frac{i\hat{H}t}{\hbar}} \right| \psi_H \right\rangle . \tag{2.48}$$

So, in the Heisenberg picture, the operator evolves according to the following relation:

$$\hat{O}' = e^{\frac{i\hat{H}t}{\hbar}} \hat{O}\, e^{-\frac{i\hat{H}t}{\hbar}} = \hat{U}^\dagger \hat{O} \hat{U}. \tag{2.49}$$

Obviously the two pictures are equivalent, i.e. the expectation values are equal in the two pictures [29]:

$$\left\langle \psi' \middle| \hat{O} \middle| \psi' \right\rangle = \left\langle \psi \middle| \hat{U}^\dagger \hat{O} \hat{U} \middle| \psi \right\rangle = \left\langle \psi \middle| \hat{O}' \middle| \psi \right\rangle, \tag{2.50}$$

where $|\psi'\rangle$ represents the time-dependent state in Schrödinger picture whereas $|\psi\rangle$ is the temporal independent state in the Heisenberg representation.

In quantum optics, the Heisenberg representation appears very useful in dealing with coherent states. In fact, thanks to canonical quantization, the equations that describe the evolution of creation and annihilation operators are identical to those of the classical complex amplitudes of the electric field [29, 34, 35, 39].

Therefore, in general, if an optical component is modeled with a Jones matrix $J_{component}$, such that its action on the Jones vector is:

$$\begin{pmatrix} E_x^{\,out} \\ E_y^{\,out} \end{pmatrix} = J_{component} \begin{pmatrix} E_x^{\,in} \\ E_y^{\,in} \end{pmatrix}, \tag{2.51}$$

it is possible to obtain the quantum description of the component passing to creation (or similarly annihilation) operators:

$$\begin{pmatrix} \hat{a}_H^{\,out} \\ \hat{a}_V^{\,out} \end{pmatrix} = J_{component} \begin{pmatrix} \hat{a}_H^{\,in} \\ \hat{a}_V^{\,in} \end{pmatrix}. \tag{2.52}$$

This relation is the core of the theoretical model because it allows to propagate the coherent state from the input to the output of an optical device, modifying the creation and annihilation operators which appears in the displacement operators. The relations for creation operators can be easily obtained computing the conjugate transpose of this last expression.

2.4 Limits of the model

Using this semi-classical approach based on coherent states is an optimum trade-off to simulate most of the current QKD systems, which use lasers as light source, maintaining the model "simple" and consequently obtaining a pretty fast simulator.

The limitations are that QKD protocols where entangled photons are employed cannot be simulated, as also systems where non-classical light sources are used. In fact, the light emitted by sub-Poissonian sources or effective single-photon sources is conceptually distant from a coherent state, therefore it must be modeled in a different way.

The solution to solve this limitations is the passage to **density matrices** to describe the light state, that allow one to obtain a more complex and universal model.

Chapter 3

Analysis of the most common optical devices

In this chapter, the most used optical components in quantum key distribution systems will be analyzed. The physics of the device will be presented, together with its quantum mechanical relations, necessary to build the simulating framework. To simplify the treatment, first the components will be analyzed in their ideal form, then losses and non-idealities will be inserted in the model.
A separate chapter will be dedicated to optical detectors, given their complexity and importance.

3.1 Attenuated laser

As aforementioned in section 1.8, most of the current QKD systems use lasers as light sources. In some configurations, only a single laser is used to produce the initial photon that is properly polarized in one of the four possible states of polarization afterwards, according to the qubit to be sent to Bob, as in [40, 41, 42]. In other setups, multiple lasers, activated one at a time, are used to produce photons already polarized in the correct polarization state, as in [43, 44, 45].
Obviously the emitted light must be properly attenuated to reach a quasi-single-photon level; the attenuation can be carried out just after the laser or at the end of Alice's subsystem.

The initial light state produced by the laser can be easily represented using the bi-dimensional vector, analogous of the Jones vector. For example, if the laser produces a light pulse vertically polarized with a mean photon number equal to two,

the coefficient of the coherent state will be $\alpha = \sqrt{2}$. Formally, the state is:

$$|\Psi\rangle \;=\; D(\alpha_V = \sqrt{2})\;|0\rangle \;=\; \exp\left(\sqrt{2}\,\hat{a}_V^{\dagger} - \sqrt{2}\,\hat{a}_V\right)\;|0\rangle\,, \tag{3.1}$$

while the vectorial representation is:

$$V \;=\; \begin{pmatrix} 0 \\ \sqrt{2} \end{pmatrix} \tag{3.2}$$

3.2 Pockels cell

The polarization of light can be modified using waveplates, also called retarders, made up of **birefringent materials**, in which the refractive index depends on polarization and propagation direction of light. This characteristic comes from the anisotropy in the binding force of the electrons shells that surround the atoms of the crystal. As a result, one component of the polarization is retarded with respect to the other; according to this retardation and to the input polarization, the effect of the waveplate is different.
Pockels cells are voltage controlled waveplates, widely used in QKD systems both for modifying the logical value of the qubit in polarization-coding systems, both for compensating unwanted polarization deviations.

Birefringent crystals are characterized by two axes: ordinary, with refractive index n_0, and extraordinary, with refractive index n_e. Light polarized along ordinary axis moves with a speed equal to $v_0 = \frac{c}{n_0}$, while light (or the component of light) polarized parallel to extraordinary axis moves at $v_e = \frac{c}{n_e}$. When $n_e < n_0$, as in calcite, the ordinary axis is called **slow axis** and the extraordinary **fast axis**.
The **retardation** describes the phase shift between the two polarization components, which is given by the following expression:

$$\theta \;=\; \frac{2\,\pi}{\lambda_0}\,d\,|n_0 - n_e|, \tag{3.3}$$

where λ_0 is the wavelength in vacuum and d is the thickness of the plate [46].

Depending on this retardation, different types of waveplates can be identified:

- if $\theta \;=\; 2\,\pi$ the device is called **full-waveplate** or **full-wave retarder** and it

has not visible effect for light at λ_0;

- if $\theta = \pi$ the device is an **half-waveplate** (HWP). If linearly polarized light enters the pockles cell oriented with an angle θ with respect to the fast axis, it comes out with the polarization vector rotated of 2θ. For this reason HWPs

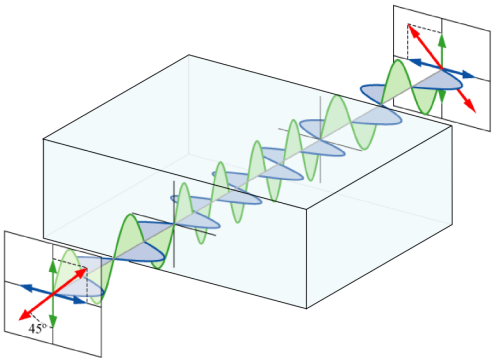

Figure 3.1: Representation of the effect of an half-waveplate on linearly polarized light [47].

  are also called **polarization rotators**: they rotate linearly and elliptically polarized light. In addition they flip the handedness of circularly and elliptically polarized light, from right to left or vice-versa [46].

- if $\theta = \frac{\pi}{4}$ the retarder is called **quarter-waveplate**. Linear light oriented at 45° from the fast axis comes out circularly polarized. Similarly, incoming circular light comes out linearly polarized [46].

Using the Jones calculus, if the retarder has the fast axis parallel to the vertical axis, it is described by the following matrix [34]:

$$J_{retarder(\theta)} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(-i\theta) \end{pmatrix}, \tag{3.4}$$

where θ is the retardation. To properly change the polarization, the retarder must be rotated with respect to the vertical axis. This operation is represented by the following rotation matrix:

$$U_{(\delta)} = \begin{pmatrix} \cos\delta & \sin\delta \\ -\sin\delta & \cos\delta \end{pmatrix}, \tag{3.5}$$

where δ is the rotation angle. Therefore, the retarder is described by the following Jones matrix:

$$J_{retarder(\theta,\delta)} = U^{\dagger}_{(\delta)} \begin{pmatrix} 1 & 0 \\ 0 & \exp(-i\theta) \end{pmatrix} U_{(\delta)} \tag{3.6}$$

$$= \begin{pmatrix} \cos^2(\delta) + \sin^2(\delta)\exp(-i\theta) & \cos(\delta)\sin(\delta) - \cos(\delta)\sin(\delta)\exp(-i\theta) \\ \cos(\delta)\sin(\delta) - \cos(\delta)\sin(\delta)\exp(-i\theta) & \sin^2(\delta) + \cos^2(\delta)\exp(-i\theta) \end{pmatrix}. \tag{3.7}$$

To conclude, its quantum mechanical relation is:

$$\begin{pmatrix} \hat{b}_H \\ \hat{b}_V \end{pmatrix} = J_{retarder(\theta,\delta)} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix}, \tag{3.8}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators at input and output ports respectively.

As a further remark, retarders are distinguished in three types [46]:

1. **zero-order**: the retarder has the minimum thickness necessary to obtain the wanted effect. Even if they are fragile and expensive, they have a large field-of-view (also called acceptance angle, is the maximum angle to proper inject a light ray in an optical device [48]);

2. **multiple-order**: the retarder gives a phase shift equal to the required one plus multiples of $2\,\pi$. They are cheaper but more sensitive to wavelength, temperature, and they have a narrow field-of-view;

3. **compound zero-order**: they are used in order to compensate temperature dependence. They are obtained combining two multiple-order retarders, aligning the fast axis of one with the slow axis of the other.

In QKD systems, the most used are half-waveplate Pockels cells ($\theta = \pi$) because they act as polarization rotators. For example, a Pockels cell oriented at 45° from the vertical axis is described by the matrix:

$$M = J_{retarder(\theta=\pi,\delta=\frac{\pi}{4})} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{3.9}$$

and so, when properly activated, it acts in the following way:

$$\begin{pmatrix} \hat{b}_H \\ \hat{b}_V \end{pmatrix} = M \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix}, \tag{3.10}$$

and so:

$$\begin{cases} \hat{a}_H = \hat{b}_V \\ \hat{a}_V = \hat{b}_H \end{cases}. \tag{3.11}$$

In practice, it flips the logic value of the qubit in the {H,V} base, transforming horizontal light in vertical light, and vice-versa. Using the displaced states representation, its action is the following one. If the initial state is:

$$|\Psi\rangle = \exp\left(\alpha\, \hat{a}_H^\dagger - \alpha^*\, \hat{a}_H\right) |0_H,0_V\rangle\,, \tag{3.12}$$

it becomes vertically polarized at the output:

$$|\Psi\rangle = \exp\left(\alpha\, \hat{c}_V^\dagger - \alpha^*\, \hat{c}_V\right) |0_H,0_V\rangle\,. \tag{3.13}$$

3.3 Linear polarizer

Linear polarizers are ordinary optical components, used to linearly polarize light. In general they are divided in absorptive and beam splitter polarizers. The former are often based on dichroism while the latter on birefringence or reflection at Brewster's angle.
Their Jones matrix is [33]:

$$J_{polarizer(\theta)} = \begin{pmatrix} \cos^2(\theta) & \cos(\theta)\sin(\theta) \\ \cos(\theta)\sin(\theta) & \sin^2(\theta) \end{pmatrix}, \tag{3.14}$$

where θ is the orientation of the transmission axis with respect to the horizontal axis.

3.4 Mirror

For normal incidence a mirror has the following Jones matrix:

$$J_{mirror} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{3.15}$$

in accordance with Fresnel's equations. In practice, it has the same matrix of an half-waveplate oriented with its fast axis parallel to the horizontal axis [34, 49].

A noticeable effect of mirror is to change the handedness of circularly polarized light, from left-handed to right-handed and vice-versa. For example right handed polarized light becomes left-handed polarized, shifted of π, as shown in the following eqation:

$$J_{mirror} \, |R\rangle = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} = - \, |L\rangle \tag{3.16}$$

3.5 Beam splitter

Beam splitters are essential components in optical experiments, as also in QKD systems. For example, they are used to joint in a single optical path light beams coming from different sources or they are used in the detection sub-systems, to randomly select photons and consequently the measurement basis [29]. In classical

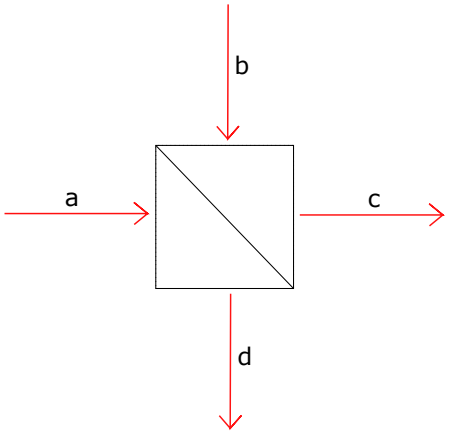

Figure 3.2: Naming convention for beam splitter ports.

electrodynamics, neglecting light polarization, the complex amplitudes of the fields

respect the following relation:

$$\begin{pmatrix} E_c \\ E_d \end{pmatrix} = \begin{pmatrix} t_0 & r_1 \\ r_0 & t_1 \end{pmatrix} \begin{pmatrix} E_a \\ E_b \end{pmatrix}, \tag{3.17}$$

where the ports follow the nomenclature shown in Figure 3.2. The matrix is unitary (in the ideal case), and it has complex elements which are transmission and reflection coefficients [50].
As already shown, it is possible to substitute electric field amplitudes with annihilation or equivalently creation operators to find the quantum-mechanical relation.

3.5.1 A general relation for creation and annihilation operators: the importance of vacuum state

At this point, it is convenient to introduce a relevant concept useful to analyze every optical component.

In order to respect **energy conservation**, the creation and annihilation operators must respect the following commutators [28, 50]:

$$\begin{aligned} \left[\hat{a}_i, \hat{a}_j^\dagger\right] &= \delta_{i,j} \\ \left[\hat{a}_i, \hat{a}_j\right] &= 0 \\ \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right] &= 0 \end{aligned} \tag{3.18}$$

where i and j label the ports of the component. From these relations it is easy to demonstrate the relevance to take in consideration all possible input and output ports of an optical element, even if they do not have any input state. From a classical point of view, it seems useless to consider unused ports because they do not affect the output state. However, in a quantum-mechanical picture, the vacuum states at the unused ports must be considered; as well known, the fluctuations of vacuum can have important physical effects [28], surprising in some cases as in Casimir effect.

As a demonstration, it is possible to wrongly study a beam splitter neglecting an input port, the "b" port in Figure 3.2. From Equation 3.17, passing to annihilation

operators, it is possible to write that:

$$\hat{d} = r\,\hat{a}\,, \hat{c} = t\,\hat{a} \quad \text{with}\,|r|^2 + |t|^2 = 1 \tag{3.19}$$

Now, calculating the commutators, it is easy to see that this transformation does not respect the physics of fields:

$$\begin{aligned}\left[d\,, d^\dagger\right] &= r\hat{a}r^*\hat{a}^\dagger - r^*\hat{a}^\dagger r\hat{a} = |r|^2\,\left[\hat{a}\,, \hat{a}^\dagger\right] = |r|^2\,\mathrm{I}\\ \left[c\,, c^\dagger\right] &= |t|^2\,\left[\hat{a}\,, \hat{a}^\dagger\right] = |t|^2\,\mathrm{I}\\ \left[d\,, c^\dagger\right] &= r\,t^* \neq 0,\end{aligned} \tag{3.20}$$

and similarly for the other pairs. The last relation is an evidence that this transformation does not respect energy conservation.
To sum up, it is always necessary to consider the vacuum state as input of unused ports in order to obtain a coherent description of the system [28].

After this important remark, it is possible to return to the correct modelling of a beam splitter. For an ideal beam splitter, the commutation relations give:

$$|t_0|^2 + |r_0|^2 = 1 \tag{3.21}$$

$$|t_1|^2 + |r_1|^2 = 1 \tag{3.22}$$

$$t_0^*\,r_1 + r_0^*\,t_1 = 0. \tag{3.23}$$

From the last expression, a relation for the phases at the ports of the beam splitter can be found:

$$\phi_{t_0} + \phi_{r_0} - \phi_{t_1} - \phi_{r_1} = \pm\,\pi, \tag{3.24}$$

as confirmed in [28, 50]. The conventional choice for a cube beam splitter is:

$$\phi_{t_0}\,, \phi_{r_0}\,, \phi_{t_1} = 0 \tag{3.25}$$

$$\phi_{r_1} = -\,\pi \tag{3.26}$$

As a result, the relations for the annihilation operators of a cube beam splitter,

neglecting the polarization, are [29]:

$$\begin{cases} \hat{c} = t\,\hat{a} - r\,\hat{b} \\ \hat{d} = r\,\hat{a} + t\,\hat{b} \end{cases} . \tag{3.27}$$

If the beam splitter is constructed as a single dielectric layer, reflected and transmitted beams will differ in phase by a factor $\exp\left(\pm i\,\frac{\pi}{2}\right) = \pm i$ and so the relations become [28, 29]:

$$\begin{cases} \hat{c} = t\,\hat{a} + i\,r\,\hat{b} \\ \hat{d} = i\,r\,\hat{a} + t\,\hat{b} \end{cases} . \tag{3.28}$$

As it is clear, these are only two examples of possible beam splitter relations. The proper one can be obtained with a detailed characterization of the component that is expected to be used in the optical system. In this thesis, the convention shown for the cube beam splitter is adopted.

After having developed a rigorous scalar model for beam splitters, it is now possible to **include the polarization in the treatment**. Sticking to the conventional choice of a cube beam splitter, it is possible to write:

$$\begin{cases} \hat{c}_j = t\,\hat{a}_j - r\,\hat{b}_j \\ \hat{d}_j = r\,\hat{a}_j + t\,\hat{b}_j \end{cases} \tag{3.29}$$

where the subscript j can stand for H or V, as confirmed in [51].

Finally, combining the Jones vectors of inputs and outputs in four dimensional vectors and defining an "expanded" 4×4 Jones matrix for the beam splitter, the relation for annihilation operator including the polarization is:

$$\begin{pmatrix} \hat{c}_H \\ \hat{c}_V \\ \hat{d}_H \\ \hat{d}_V \end{pmatrix} = \begin{pmatrix} t_H & 0 & -r_H & 0 \\ 0 & t_V & 0 & -r_V \\ r_H & 0 & t_H & 0 \\ 0 & r_V & 0 & t_V \end{pmatrix} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \\ \hat{b}_H \\ \hat{b}_V \end{pmatrix} , \tag{3.30}$$

analogous to the expressions shown in [51].

3.6 Polarizing beam splitter

Using birefringent materials, it is possible to obtain optical elements able to split the input beam in two output beams, where one is completely TE polarized, while the other is TM polarized. Transverse electric (TE) polarized light has the electric field polarized perpendicularly to the incidence plane, and so it is also known as s-polarization ("senkrecht" means perpendicular in German). Similarly, transverse magnetic (TM) light has the magnetic field polarized perpendicularly to this plane, so it is also called p-polarization because the electric field is parallel to the incidence plane. The incidence plane is by definition the plane identified by the propagation vector of the incoming light and a vector perpendicular to the surface of incidence. TE and TM are normal modes and so they form a basis for the electromagnetic waves. Hence, it is possible to decompose any plane wave in its TE and TM components, as shown in the following relations:

$$\mathbf{E}(\mathbf{r}) = E_x(\mathbf{r})\hat{\mathbf{x}} + E_y(\mathbf{r})\hat{\mathbf{y}} + E_z(\mathbf{r})\hat{\mathbf{z}} \tag{3.31}$$

$$\mathbf{H}(\mathbf{r}) = H_x(\mathbf{r})\hat{\mathbf{x}} + H_y(\mathbf{r})\hat{\mathbf{y}} + H_z(\mathbf{r})\hat{\mathbf{z}}, \tag{3.32}$$

where the blue terms are related to TE polarization, while black ones to TM (assuming that x-z is the incidence plane). An example of polarizing beam splitter is the **Wollaston prism** that, as shown in figure Figure 3.3, splits light in its TE and TM components. It is made joining together two calcite crystals, using optical cement. The optic axes of the two parts are orthogonal. The deviation angle δ ranges from 5° to 45° [52].

Another example of polarizing beam splitter is the **Glan-Focault prism**, which is based on total internal reflection, or rather, on the fact that the reflectance at the crystal-air interface is dependent on polarization [46].

Assuming an ideal polarizing beam splitter that is able to completely split incoming light in two separate beams, the quantum-mechanical relations are [35]:

$$\begin{cases} \hat{a}_H &= \hat{c}_H \\ \hat{a}_V &= \hat{d}_V \\ \hat{b}_H &= \hat{d}_H \\ \hat{b}_V &= -\hat{c}_V \end{cases} \tag{3.33}$$

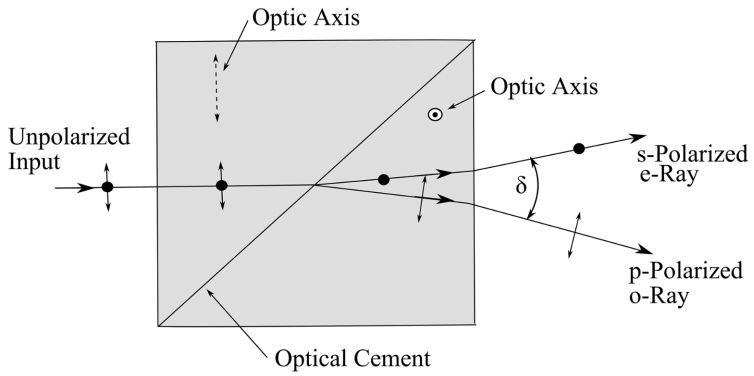

Figure 3.3: Wollaston prism. e-Ray means that the vector of polarization is parallel to extraordinary axis, whereas in o-Ray light is polarized parallel to ordinary axis [52].

where the nomenclature for ports is the same as in Figure 3.2. To clarify, these relations derive from the analysis of a Glan-Focault prism where TE component is totally internal reflected and TM is transmitted.

3.7 Quantum channel

The quantum channel is the link between Alice and Bob that allows to exchange the qubits. The two most used solutions are optical fibers and the open air, both with advantages and disadvantages. In the last years, also quantum channels established underwater have been studied; unfortunately the high water attenuation forces them to be long only few hundreds of meters [53].

3.7.1 Optical fiber as quantum channel

The usage of optical fiber as quantum channel has several advantages; it has a low and pretty constant attenuation, slightly dependent on temperature and mechanical vibrations. It also allows to establish quantum communication systems where an infrastructure already exists.
The principle drawback is the Polarization Mode Dispersion (PMD) effect which scrambles the state of polarization of the photons. PMD occurs due to a birefringence of the fiber that is caused by the unavoidable fiber imperfections, which make

the fiber core not perfectly circular and cause microbends or microtwists [54]. The PMD effect also fluctuates as a result of temperature variations and mechanical vibrations [29].
In time domain, depending on input polarization, a different arrival time of photons is observed, while, in frequency domain, a change in polarization happens. In order to describe PMD, a parameter called called Differential Group Delay (DGD) is used; it is the difference between the maximum and minimum delays observed in time domain. DGD ranges from 1 to 50 ps in a 500 km long fiber [54].

PMD must be carefully considered when a long-distance QKD system is designed, in particular for polarization-coding systems. Actually, this problem is not unique for polarization based systems, in fact also phase-coding and time-coding systems are affected by PMD [55].

Fortunately, modern optical fibers, in particular single-mode ones, have very low DGD, in the order of $0.06\,\mathrm{ps}/\sqrt{\mathrm{km}}$ [56]: the particular unit $\sqrt{\mathrm{km}}$ derives from the fact that PMD is a diffusive process, such as random walk [57]. Furthermore, DGD time must be compared with the coherence time of the source: if the latter is larger than the polarization mode delay, as it often happens, the effect of PMD on polarization is faint [57, 58].

To conclude this analysis on PMD, it is appropriate to specify that this effect spreads the signal pulse width in time, causing problems to high bit rate communication systems. However, in QKD, the bit rate is quite low, almost always under the GHz, so the primary issue is the effect on polarization.

In order to reduce the QBER caused by PMD, in long-distance QKD systems, active compensation devices are employed. These are usually Pockels cells, pairs of liquid crystal retarders (LCR) [59] (analogous to Pockels cells), or wavelength-division-multiplexed (WDM) polarization controllers [60]. At regular intervals, qubits are sent in a predetermined basis in order to verify the entity of PMD and to adjust properly the compensators.
This process can be fully automated and it ensures a great reduction of the QBER. As an example, in the QKD system developed by Lijun Ma et al. in [59], the compensation happens every fifteen minutes using a Polarization auto-Recovery and Auto-Compensation (PRAC) system based on piezoelectrics or liquid crystals. In

both cases, the QBER remains constant in time, as it can be inferred from Figure 3.4, in contrast to the case where compensators are not used. Better to say,

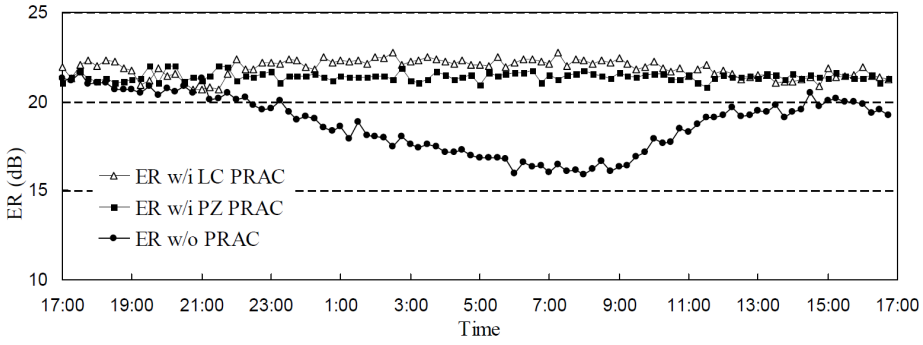

Figure 3.4: Comparison of extinction ratio with and without PRAC. Compensation and measurements of ER happen every 15 minutes [59].

they used extinction ratio as error parameter, defined as "the ratio of the counts in compatible detection bases to the counts in incompatible detection bases" [59]. In fact, the PMD alters the state of polarization of photons that, in some cases, are erroneously directed towards the erroneous detector.

In light of this, in the simplified model presented in this thesis, PMD effect is neglected, but obviously, when simulating a system, the compensators are taken in consideration. In fact, PMD models already exist: they are based on the PMD-Manakov equation, a nonlinear partial differential equation, where nonlinear effects are taken in account using the Fourier transform to study them in time-domain [61]:

$$\frac{\partial \mathbf{E}(z,\omega)}{\partial z} = D[\mathbf{E}(z,\omega)] + \mathrm{Im}\{N[\mathbf{E}(z,t)]\}, \tag{3.34}$$

where D and N are a linear and a non-linear operator acting on the electric field, respectively.

Ignoring PMD, the fiber effect is only to reduce the intensity of the light beams. Hence its quantum-mechanical relation is:

$$\begin{pmatrix} \hat{b}_H \\ \hat{b}_V \end{pmatrix} = 10^{-\frac{Attenuation_{dB} \cdot \mathrm{length}}{20}} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix}, \tag{3.35}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators at input and output ports respectively. This relation was obtained starting from the attenuation coefficient of the fiber, called $Attenuation_{dB}$ in the previous expression, defined as:

$$\alpha = -\frac{10}{z}\log\left(\frac{P(z)}{P(0)}\right), \tag{3.36}$$

where z is the fiber length and P the power. Equivalently:

$$P(z) = 10^{-\frac{\alpha}{10}z}P(0). \tag{3.37}$$

Knowing that the power carried by the wave is proportional to the Poynting vector, which is calculated as follows for an electromagnetic wave propagating in the $\hat{s} = \hat{z}$ direction [31]:

$$P(z) \propto S(z) = \frac{1}{2}\frac{|E_0|^2}{Z}\hat{s}, \tag{3.38}$$

where $Z = \sqrt{\frac{\mu}{\epsilon}}$ is the wave impedance. Therefore, it can be stated that the complex electric field amplitudes follow this relation:

$$|E(z)| = 10^{-\frac{\alpha}{20}z}|E(0)| \tag{3.39}$$

Employing the analogy bewtween fields and annihilation operators which has been used many times so far, it is possible to affirm that the quantum-mechanical relation for the optical fiber is the one shown in Equation 3.35.

3.7.2 Open air as quantum channel

QKD in open air has several advantages, such as the freedom to establish a communication without having to set-up an optical fiber; quantum based satellite communication is a striking example of this. Ground-to-satellite and satellite-to-satellite quantum communication are essential to establish global quantum networks, by exploiting the loss-free and distorsion-free communication in space [62]. In fact, not surprisingly, European Space Agency, in accordance with European Commission, is developing a pan-European quantum communication infrastructure based on satellites [63]. Then, considering that polarization noise is practically absent [64], it is clear that the usage of open air as quantum channel is beneficial in every type of QKD protocol.

The principal drawback is that atmospheric attenuation is often higher than the one achievable with a fiber and, at sea level, it fluctuates constantly due to atmospheric conditions or pollution.

From Table 3.1, it is clear that atmospheric attenuation is strongly dependent

Visibility (km)	**dB/km at 785 nm**	**dB/km at 1550 nm**	**Weather**
0.05	315	272	Fog
0.2	75	60	
0.5	29	21	
1	14	9	
2	7	4	Haze
4	3	2	
10	1	0.4	Clear
23	0.5	0.2	

Table 3.1: Atmospheric attenuation in dB/km as function of visibility [65].

on meteorological conditions, and it is lower at 1550 nm in all cases [65]. A good parameter to estimate the attenuation is the **visibility**, defined as the distance where light power decreases to 2% of its starting value [65, 66].

The transmission in open air obeys Lambert-Beer law that gives the transmittance τ at distance x [65, 67]:

$$\tau(x) = \frac{P_x}{P_0} = e^{-\sigma x}, \tag{3.40}$$

where σ is the attenuation or total extinction coefficient. Both absorption and scattering events given by molecules and aerosol particles present in the air, labeled respectively with α and β in the following equation, contribute to the attenuation coefficient [67, 68].

$$\sigma = \alpha_m + \alpha_a + \beta_R + \beta_M + \beta_{NS}. \tag{3.41}$$

Molecular absorption (α_m) is caused essentially by N_2, O_2, H_2, H_2, CO_2, O_3: a peak of absorption happens when the molecules of these gases start to resonate after the interaction with the light wave [68]. Similarly, absorption can be caused by aerosol particle (α_a) such as droplets of water, salt-crystal in maritime regions or human-made aerosol in urban regions [68].

Using wavelengths that fall in the transmission windows of atmospheric absorption spectra, so 758 nm, 850 nm and especially 1550 nm, absorption can be avoided, and the dominant effect is scattering. Depending on the light wavelength and on the radius of scattering particles, different types of scattering can be identified. The size parameter, used to distinguish the different scattering regions, is defined as follows [65]:

$$\alpha = \frac{2\pi\, r}{\lambda} \tag{3.42}$$

where r is the radius of the particle and λ the laser wavelength.

The three scattering types are [68]:

- Rayleigh (β_R): particles are smaller than the wavelength. This is the effect responsible of the blue colour of sky. Since its scattering coefficient is proportional to λ^{-4}, Rayleigh coefficient is negligible for telecommunication wavelengths;

- Mie (β_M): the radius of the particles is larger than the wavelength. It is dominant in lower portions of the atmosphere where large particles are more abundant. **This is the dominant effect to be considered in telecommunications**;

- Non-selective or geometrical (β_{NS}): particles are much larger than wavelength

so the scattered radiation can be studied by geometrical optics. It is called non-selective because the scattering coefficient is independent from the wavelength.

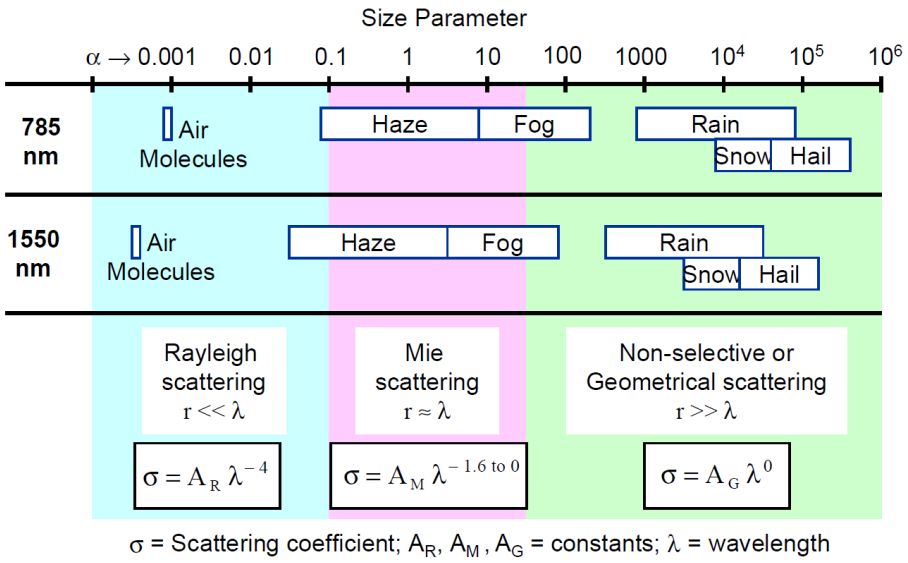

Figure 3.5: Regions for Rayleigh, Mie and Non-selective scattering as function of the size parameter.

As aforementioned, visibility is a measurement of the quantity of fog, dust, and attenuating particles present in the air. So, it is possible to find a relation between attenuation and visibility; the most famous one is called Kruse-Kim relation [69]. Given that this model underestimate the attenuation for low and medium visibility [66], nowadays a modified version is usually employed in telecommunication [65, 70]. According to this, the total attenuation coefficient is:

$$\sigma = \frac{3.91}{V}\left(\frac{\lambda}{550\,\mathrm{nm}}\right)^{-q} \tag{3.43}$$

with V the visibility in km, λ the wavelength in nm and q a parameter which is

related to the size distribution of scattering particles:

$$q = \begin{cases} 0 & \text{for V} < 500\,\text{m (Fog)} \\ V - 0.5 & \text{for } 500\,\text{m} < \text{V} < 1\,\text{km (Mist)} \\ 0.16V + 0.34 & \text{for } 1\,\text{km} < \text{V} < 6\,\text{km (Haze)} \\ 1.3 & \text{for } 6\,\text{km} < \text{V} < 50\,\text{km (Clear)} \\ 1.6 & \text{for V} > 50\,\text{km (Very high visibility)} \end{cases} \tag{3.44}$$

This total attenuation coefficient σ can be used in the Lambert-Beer equation.

$$\tau(x) = \frac{\mathrm{P_x}}{\mathrm{P_0}} = \mathrm{e}^{-\sigma \mathrm{x}}. \tag{3.45}$$

However, it is convenient to convert this attenuation coefficient in dB/km to use it in the canonical formula for attenuation used in telecommunication:

$$\frac{\mathrm{P_x}}{\mathrm{P_0}} = 10^{-\frac{\sigma_{dB}}{10}\mathrm{x}}. \tag{3.46}$$

By comparison, one finds that:

$$\sigma_{dB} \;=\; -10\,\log_{10}\left(e^{-\sigma}\right). \tag{3.47}$$

The plot of the attenuation coefficient as a function of visibility is reported in Figure 3.6.
The discontinuity observable at 50 km comes from the discontinuity in the q parameter, and it is widely accepted in literature.

Once the attenuation coefficient in dB/km has been obtained, it is possible to write the quantum-mechanical relation for the air quantum channel, analogous to that for the optical fiber:

$$\begin{pmatrix} \hat{b}_H \\ \hat{b}_V \end{pmatrix} = 10^{-\frac{Attenuation_{dB}\cdot \text{length}}{20}} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix}. \tag{3.48}$$

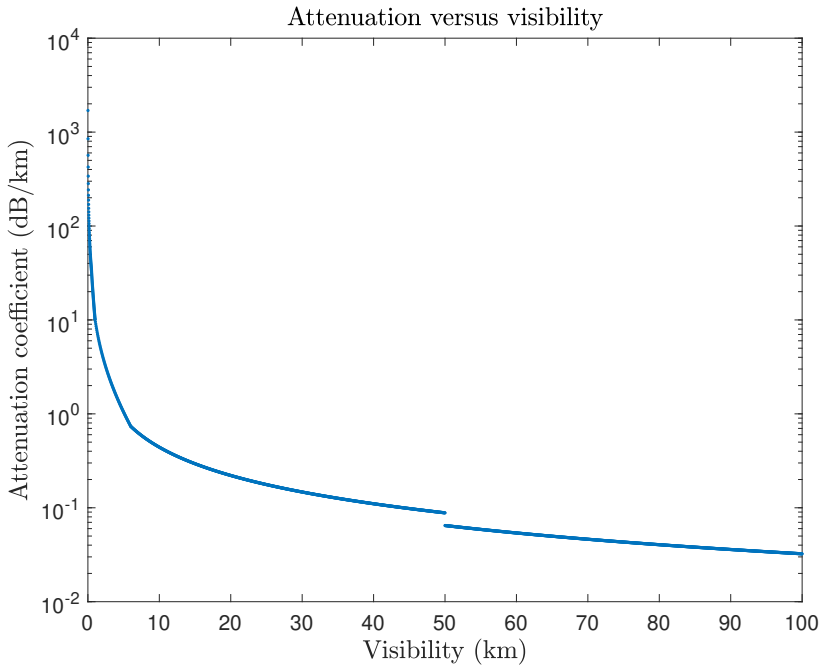

Figure 3.6: Plot of attenuation (dB/km) versus visibility.

3.8 Losses and deviations from ideality

In the previous sections, the most used optical components have been analyzed neglecting losses and imperfections, except for the quantum channels because their effect is simply to attenuate the light beam intensity.
In general, to consider losses, relations between input and output operators must be modified introducing the **Langevin operators** $\hat{F}$, also called noise operators [71]. For example, considering a beam splitter, the relations become :

$$\begin{cases} \hat{c} = t\,\hat{a} - r\,\hat{b} + \hat{F}_1 \\ \hat{d} = r\,\hat{a} + t\,\hat{b} + \hat{F}_2 \end{cases} \tag{3.49}$$

The Langevin operators respect the following commutators with the input annihilation operators [71]:

$$\left[\hat{a}\,,\hat{F}_1\right] = \left[\hat{a}\,,\hat{F}_2\right] = \left[\hat{a}\,,\hat{F}_1^\dagger\right] = \left[\hat{a}\,,\hat{F}_2^\dagger\right] = 0\,, \tag{3.50}$$

and similarly for $\hat{b}$. Being a noise, their averages vanish [71]:

$$\left\langle \hat{F}_1 \right\rangle = \left\langle \hat{F}_2 \right\rangle = \left\langle \hat{F}_1^\dagger \right\rangle = \left\langle \hat{F}_2^\dagger \right\rangle = 0. \tag{3.51}$$

Fortunately, in the case of coherent states the treatment of losses can be simplified. In fact, passing through linear components, coherent states remain coherent states [29]. In other words, the input and output relations for creation (or annihilation) operators are the same of the ideal case, but the reflection and transmission coefficients have a reduced amplitude due to losses [71], in order to take in account energy dissipation.

3.8.1 General considerations on the simulator and how errors and losses are taken in account

The emerging simulator is aimed to analyze a QKD system based on polarization-encoding, estimating fundamental parameters such as the sifted Key Rate and the Quantum Bit Error Rate (QBER), and comparing them by varying the used components. Therefore it is fundamental to describe each of these components in the best possible way, using the information available in the datasheets.

As it will be clear in the next chapters, the MATLAB simulator works in an **aggregate** way, not iterative. In practice the user "describes" the system component after component, respecting the paths of light. After that, he can simulate how a coherent state propagates from Alice to Bob, following a particular light path. For example, when Alice sends a "0" to Bob in the {Horizontal, Vertical} basis, the user can understand the mean photon number reaching the correct and incorrect measuring detectors, **by running only once the simulation**. After that, using also the information about the photon detectors used in the system, the key rate and the QBER can be estimated. A detailed analysis of detectors will be made in the next chapters.

As aforementioned, the non-idealities of the components are taken in account in the transmission and reflection coefficients. The producers of the devices report in the datasheets only the average values of the parameters, rarely indicating also the associated standard errors. Furthermore, the simulator works in aggregate way, not simulating the passage of every single light pulse; so, it is not possible to estimate the parameters of the components by simulating the dynamics of a stochastic process.
Consequently, only the average values for the parameters are used. Obviously, information on the errors, such as the variance, is not provided. Nevertheless, the most important parameters of a QKD system can be correctly evaluated, as it will be shown in the final chapters; this is more than satisfactory from an engineering point of view.

After these significant considerations, the lossy relations for Pockels cells, linear polarizers, mirrors, beam splitters and polarizing beam splitters will be presented.

The lossy relations for quantum channels were already presented in section 3.7, so they will not be repeated.

3.8.2 Lossy Pockels cells, linear polarizers, and mirros

To take in account losses in these devices it is sufficient to multiply their matrices by the transmission coefficient (or reflection coefficient in the case of the mirror). Since datasheets usually report transmittance calculated as the ratio between transmitted and incident optical power, the square root appears in the formula. For example, for a Pockels cell, it is trivial to modify its quantum relation shown in Equation 3.8 obtaining:

$$\begin{pmatrix} \hat{b}_H \\ \hat{b}_V \end{pmatrix} = \sqrt{t}\, J_{retarder(\theta,\delta)} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix}, \tag{3.52}$$

where t is the aforesaid transmittance. For polarizers and mirrors the considerations are the same.

3.8.3 Lossy Beam splitter

In the case of beam splitters, producers usually provide transmittance and reflectance for p and s polarization. Orienting the beam splitter so that horizontal transmittance coincides with that for p-polarization ($t_H = t_p$), and vertical transmittance to that for s-polarization ($t_V = t_s$), one can use the relation shown in 3.30 inserting transmittance and reflectance under square roots:

$$\begin{pmatrix} \hat{c}_H \\ \hat{c}_V \\ \hat{d}_H \\ \hat{d}_V \end{pmatrix} = \begin{pmatrix} \sqrt{t_H} & 0 & -\sqrt{r_H} & 0 \\ 0 & \sqrt{t_V} & 0 & -\sqrt{r_V} \\ \sqrt{r_H} & 0 & \sqrt{t_H} & 0 \\ 0 & \sqrt{r_V} & 0 & \sqrt{t_V} \end{pmatrix} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \\ \hat{b}_H \\ \hat{b}_V \end{pmatrix}. \tag{3.53}$$

3.8.4 Lossy Polarizing beam splitter

For real polarizing beam splitters, in addition to the use of real transmittance and reflectance coefficients, it is necessary to consider also their extinction ratio. In fact, a real polarizing beam splitter does not perfectly separate horizontal and vertical

polarization; therefore part of the incoming s-polarized light is partially transmitted even if it should be totally reflected (in the case of Glan-Focault prism). For this reason, it is necessary to use the following quantum mechanical relation:

$$\begin{pmatrix} \hat{c}_H \\ \hat{c}_V \\ \hat{d}_H \\ \hat{d}_V \end{pmatrix} = \begin{pmatrix} \sqrt{t_H} & 0 & -\sqrt{r_{H,u}} & 0 \\ 0 & \sqrt{t_{V,u}} & 0 & -\sqrt{r_V} \\ \sqrt{r_{H,u}} & 0 & \sqrt{t_H} & 0 \\ 0 & \sqrt{r_V} & 0 & \sqrt{t_{V,u}} \end{pmatrix} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \\ \hat{b}_H \\ \hat{b}_V \end{pmatrix}, \tag{3.54}$$

where the subscript u stands for unwanted. The unwanted transmittance and reflectance can be easily calculated from the extinction ratio, id est the ratio between the wanted and unwanted transmittance (or reflectance).

Chapter 4

Single-photon detectors

The photon detectors are the last link in the chain of a QKD system; they accomplish the essential task of measuring the photons received by Bob. For this reason they are a crucial part of these systems.

These detectors must sense single-photon pulses, not an easy task due to intrinsic limitations in photon detection, such as a low quantum efficiency, or noise. In fact, considering that a single near-infrared photon carries an energy in the order of 10^{-19} J, these detectors must be extremely sensitive, which makes them particularly subject to noise.

After a brief overview on the parameters used to characterise photon detectors, the most suitable ones for QKD will be introduced. Single-Photon Avalanche Diode (SPAD), the most used, will be analyzed in detail. A Verilog-A model for InGaAs-InP device will be presented; it allows the simulation of these types of SPADs providing in output important parameters to be used in the analysis of a QKD system.

4.1 Figure of merits of photon detectors

Before entering into the core of this chapter, it is convenient to peruse the figure of merits of photon detectors, in order to understand the most important characteristics they must have.

4.1.1 Spectral range

The spectral range identifies the photon spectral region where the detector is sensible. It is linked to the material used to build the detector. For the QKD purposes, a

wide spectral range is unnecessary because the wavelength operation region is fixed and defined at the design stage.
As seen in the previous chapter, the best working region is the near-infrared, in particular 1550 nm, which corresponds to the lowest lossy region for communication in optical fibers and open air [72].

4.1.2 Photon detection efficiency (PDE)

Photon detection efficiency (PDE) is the ratio between detected photons and impinging ones. As it is clear, detection efficiency must be the highest possible in order to ensure high key rate, low QBER and a greater resistance to PNS attacks.

4.1.3 Noise equivalent power (NEP)

Noise equivalent power (NEP) is the incident signal power which gives signal-to-noise ratio equal to 1. The NEP is the smallest detectable signal, hence it must be as low as possible for the photo counting applications.

4.1.4 Dark count probability

This is the probability of registering a detection event without illumination [73]. It is caused by the dark carrier generated in the device and by afterpulses which happen after an avalanche. To reduce this effect, SPAD's rarely works in free-running mode; they often work in gated mode, synchronizing the active state of the detector with the expected arrival time of the photon, and leaving the SPAD inactive for the rest of the time.

4.1.5 Timing jitter

Timing jitter is the variation in the time interval between the arrival of a photon and the generation of the electrical response pulse [72].

4.1.6 Dead time

Dead time is the time interval after a detection event during which the detector is unable to detect a new photon. Along with timing jitter, it fixes the maximum count rate.

4.2 An overview on the newest photon detectors for QKD

After a detailed analysis, the most suitable detectors for QKD are Superconducting transition-edge sensors (TES), Superconducting nanowire single-photon detectors (SNSPD), and Single-Photon Avalanche Diode (SPAD). The first two are the newest one, with great performance but with the need to work at ultra-low temperatures. SPADs are the most frequently used today, and they will be analyzed in a dedicated section.

4.2.1 Superconducting transition-edge sensors (TES)

Superconducting transition-edge sensors consist of a thin metal layer electrically biased to maintain the metal in the superconducting state, really close to the phase transition [74]. In such a way, also a single photon has enough energy to heat the material causing the transition from superconducting to normal state of at least a part of the film. The steep resistive transition causes a fluctuation in the current which flows in the film, easily measurable with a SQUID amplifier [72, 75]. The signal is proportional to the energy carried by the photons so TESs can be also used for photon counting application. Considering their extremely high PDE, close to the 95% at 1550 nm, and the absence of dark counts [72], the interest for TESs in quantum optics is obvious. Their principal drawbacks are a long timing jitter (100 ns), a long dead time (up to 1 µs), and their extremely low working temperature of about 100 mK [72]. This last drawback is really constrictive because it obliges to use expensive cooling systems.

4.2.2 Superconducting nanowire single-photon detectors (SNSPD)

The active element of these detectors is a 100 nm wide nanowire operating well below the superconducting transition edge temperature but biased just below its critical current (Figure 4.1 (i)). The impinging photons have enough energy to break hundreds of Cooper pairs generating an **hotspot** (Figure 4.1 (ii)). Consequently the supercurrent will start to flow around this resistive region (Figure 4.1 (iii)) but, in doing so, the current density at the edges of the nanowire increases so much that new resistive regions are formed (Figure 4.1 (iv)). This increase in resistivity causes a measurable voltage pulse across the structure (Figure 4.1 (v)) [76].

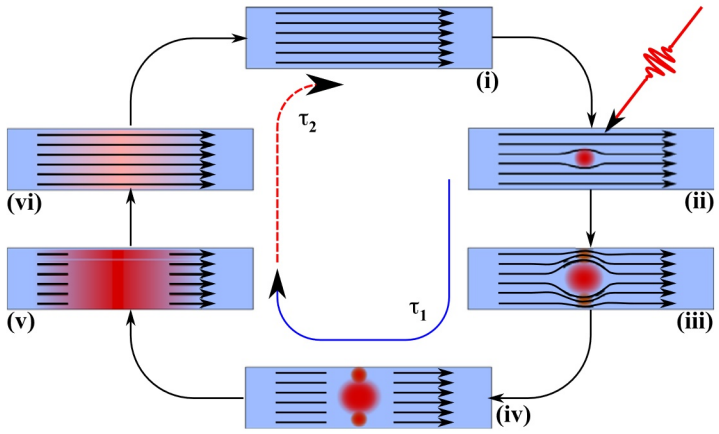

Figure 4.1: Detection cycle of a SNSPD detector [76].

Integrating these detectors in small cavities allows to reach PDE of about 57%. Furthermore SNSPDs have a very low timing jitter (tens of picoseconds) and a low dead time [72]. These characteristics make them very attractive, except for their low operating temperature, but still greater than that of TESs.

4.3 Single-Photon Avalanche Diode (SPAD)

Single-Photon Avalanche Diodes are still the most used photon detectors in QKD systems. Nevertheless, they have photon detection efficiency and maximum count

rate lower than the newest superconductive detectors. The reason is clear: the technology to produce Silicon or Indium-Gallium-Arsenide/Indium-Phosphide diodes is well known and so the production costs are low. Furthermore, SPADs are easily compatible with optical fibers. Another significant advantage is the working temperature; SPADs have adequate performance working at about 220 K, in contrast, superconducting detectors work below 4 K, so expensive coolers are needed.

Si SPADs allow the detection of photons in the spectral range 400-1100 nm [77], while InGaAs/InP SPADs work between 1 µm and 1.7 µm [78].
Si SPADs are used in QKD systems with optical fiber as quantum channel, working with photons in the near-infrared (780 nm [79], 850 nm [80]); even if at these wavelengths the attenuation of the fiber is higher, Si SPADs have great performance, in particular an higher photon detection efficiency (up to the 63% [72, 77, 81, 82]) compared to InGaAs/InP SPADs. This is not surprising considering that Silicon is one of the material with the highest quantum efficiency, equal to approximately 90% at about 650 nm.
Nevertheless, modern InGaAs/InP SPADs have adequate performance; A. Tosi et al. showed in [83] an InGaAs/InP SPAD with 30% PDE at 1550 nm, a timing jitter of about 87 ps Full Width at Half Maximum (FWHM) and moderate afterpulses. Then, considering that InGaAs/InP SPADs are the best to work at telecommunication wavelength (1550 nm), from now on, the discussion will be focused on them. However analogous considerations can be done for Silicon SPADs.
Moreover, as foretold, a Verilog-A model for InGaAs/InP SPAD will be presented in the next sections. The SPAD developed by Tosi et al. presented in [83] will be used as benchmark for the theoretical estimations and Verilog-A simulations.

4.3.1 Operating principle and semiconductor structure

SPADs are photodiodes that exploit the avalanche effect in order to have an extremely high sensitivity. In fact, they have a peculiar structure for which, when they are inversely polarized above the breakdown voltage, a strong electric field occurs in a well defined region of the device, the **multiplication region**. This electric field is so high that carriers that pass through this region are able to acquire enough

energy to generate new electron/hole pairs, due to impact ionization. These generated carriers, in turn, are able to repeat this process; for this reason the avalanche is a **self-sustained mechanism**. As a result, also a single photon is able to generate a macroscopic electrical signal.

Since the avalanche is a self-sustained mechanism, it must be **quenched**, otherwise the current can dramatically increase, breaking the device. Quenching methods are divided in passive, active and hybrid and will be analyzed in section 4.3.2.

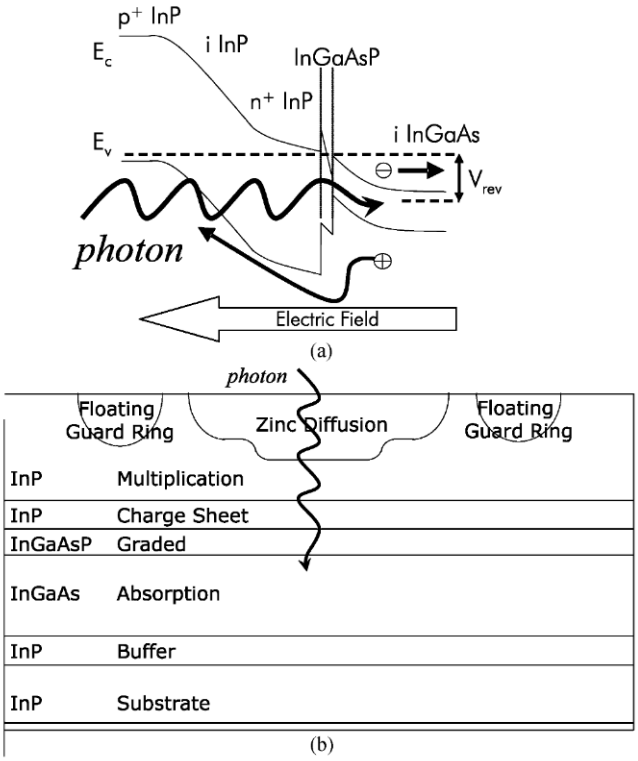

Figure 4.2: (a) Energy band diagram under reverse bias. (b) Schematic cross section of an InGaAs/InP SPAD [84].

The operating principle of the SPAD is shown in Figure 4.2: the 1550 nm photon passes through the InP layers, which has a wide bandgap, and is absorbed in the **InGaAs absorption layer**. The generated electron drifts towards the back contact while the hole is swept towards the **InP multiplication region**. Here the electric field is so high that the hole is able to generate an avalanche.

The thin InGaAsP layer, called **grading layer**, is used to flatten the valence band discontinuity between InGaAs and InP, to avoid an accumulation of holes at the heterojunction interface [84, 85].
Instead, the **InP charge layer** is used to shape the electric field, to increase it in the multiplication layer, and to decrease it in the absorption layer [83, 84, 85].
The **Zinc diffusion region** is often used in this type of SPAD in order to shape the high electric field in the multiplication region, decreasing the electric field amplitude at the edge of the device; in this way, both the PDE is increased and the tunneling dark carrier generation is reduced [83, 84].

Unfortunately, thermal carrier generation and tunnel effects caused by the strong electric field can generate electron/hole pairs able to produce new avalanches and so erroneous detections, known as **darkcounts**. **Afterpulsing** is another unwanted effect: during an avalanche some carriers get stuck in deep trap levels. After a certain time, these carriers are released and they risk to generate new avalanches and so other erroneous detections.

Carefully designing the structure of the diode, tunneling generations can be reduced, as also decreasing the temperature of the device is a solution to reduce the thermal carrier generation [83]. In order to reduce afterpulsing, it is convenient to maintain the SPAD inactive (gate-OFF or dead time) for a certain period after an avalanche in such a way that trapped carriers can be released without generating a new avalanche.

Therefore, instead of working in free running mode, a good solution is **Gated (Geiger) mode**: the SPAD is active in a short time window, the Gate-ON time, which corresponds to the expected arrival time of the photon. For the rest of the time, the SPAD is deactivated, and so dark carriers or released carriers cannot generate avalanches and so erroneous counts. The adjective Geiger comes from the fact that the detection process is analogous to Geiger counter, where an avalanche multiplication process followed by a dead time is used too [86].

4.3.2 SPAD characterization and modelization

In this section, the operating mechanisms of the SPAD will be analyzed in detail, as also the undesirable effects, such as dark carriers generation and afterpulsing.

Static and dynamic currents

To properly describe the behaviour of the SPAD in reverse bias, the model in figure Figure 4.3 is used. Below breakdown and when avalanche is not triggered, the static current is the reverse current I_s while, when avalanche starts, it is:

$$I_{\text{spad}} = I_s + \frac{V_n}{R_{\text{break}}} \ln\left(1 + e^{\frac{V_{\text{ex}}}{V_n}}\right) \tag{4.1}$$

where V_n is a normalization voltage and it is about 10 mV, R_{break} is a resistance of about 3.5 kΩ which takes in account the space-charge resistance and the resistance of the neutral regions crossed by the avalanche current [87], $V_{\text{ex}} = V_{\text{cath}} - V_{\text{anod}} - V_{\text{break}}$ is the excess bias, and V_{break} is the breakdown voltage [88].
To complete the model, the capacitive effects must be considered. Calling C_{j} the depletion capacitance, C_{cs} and C_{as} the stray capacitances with the substrate, the currents at cathode I_c and anode I_a are defined as follows:

$$I_c = I_{\text{spad}} + \frac{dQ_{\text{j}}}{dt} + \frac{dQ_{\text{c s}}}{dt}, \quad I_a = -I_{\text{spad}} - \frac{dQ_{\text{j}}}{dt} + \frac{dQ_{\text{a s}}}{dt}, \tag{4.2}$$

where these two currents flow into the Cathode and Anode nodes respectively, as shown in Figure 4.3 [88, 87].

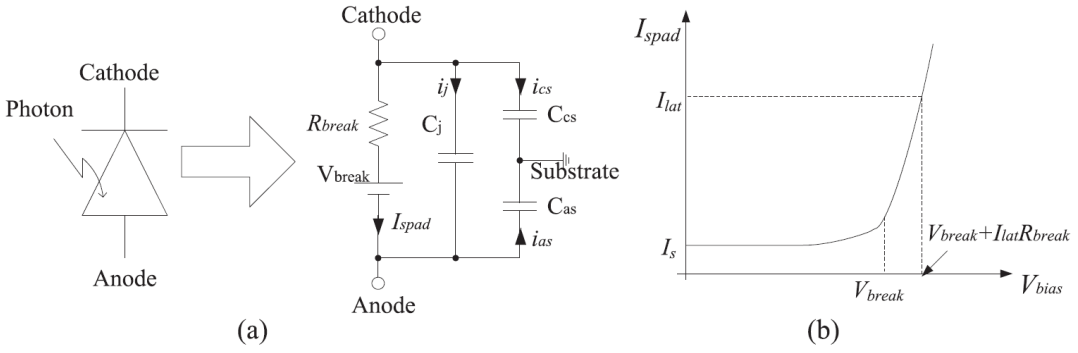

Figure 4.3: SPAD model and I-V curve in reverse bias [88].

Photon detection efficiency

The detection efficiency can be modeled considering the various steps which brings to the detection of a photon. First of all, the photon must be correctly absorbed in the InGaAs layer, then the generated hole has to reach the multiplication region where it can trigger an avalanche. So, PDE can be modeled as:

$$PDE = P_{coup} \cdot P_{abs} \cdot P_{inj} \cdot P_{tr}, \tag{4.3}$$

as confirmed in [85] and [89].
P_{coup} is the coupling efficiency of the SPAD and depends on insertion losses, reflectivity of the surface and the detection area [85].
P_{abs} is the absorption probability in InGaAs and can be modeled as follows:

$$P_{abs} = 1 - e^{-\alpha_{InGaAs} W_{absorption}}, \tag{4.4}$$

where α_{InGaAs} is the absorption coefficient of InGaAs. It is equal to $1 \times 10^4\,\mathrm{cm}^{-1}$ in $In_{0.47}Ga_{0.53}As$ [90], the most suitable choice to absorb photons near 1550 nm.
P_{inj} is the collection probability of photogenerated holes from absorption to multiplication layer.
P_{tr} is the avalanche triggering probability, usually computed as:

$$P_{tr} = 1 - e^{\frac{-V_{ex}}{\eta V_{break}}} \qquad (V_{ex} > 0) \tag{4.5}$$

η is the extracted exponential slope and is temperature dependent. Its dependence can be extracted from a fit of the avalanche triggering probability versus temperature but, anyway, a constant value give a good accuracy in the operating range, as it will be shown in the next sections. Obviously, when the excess bias is negative, the avalanche cannot begin and so P_{tr} is equal to zero.
InGaAs SPADs have a PDE of 30%, approximately, polarizing the SPAD with an excess voltage between 3 V and 7 V [83, 91, 92].

Timing jitter

Timing jitter, in these SPADs, ranges from about 80 ps to 370 ps [72, 83, 93]. Modeling this time is not trivial; one should consider the diffusion time from absorption to multiplication region, the initial noise associated with the start of the avalanche process which is very irregular, and, once it is stable, the spread time of the avalanche [93]. For this reason, the timing jitter will be neglected in the Verilog-A model proposed in this thesis.

Dark carrier generation

Three effects are dominant and cause the generation of charge carriers able to produce avalanches and so erroneous detections. These three effects are:

1. **thermal generation (SRH)**: is dominant in the InGaAs absorption layer whereas it is negligible in InP, having a wider bandgap. It is modeled with Shockley-Read-Hall theory;

2. **band-to-band-tunneling (BTBT)**: due to the high electric field, valence and conduction bands are so bent that an electron in valence band can tunnel towards the conduction band without the assistance of a trap. The process for holes is analogous and opposite. The band gap acts as the potential barrier that carriers must cross [94];

3. **trap assisted tunneling (TAT)**: the carriers tunnel between conduction and valence bands passing through the traps, whose energy level falls in the band gap. As the previous one, it is prevalent in the InP multiplication layer where the electric field is very high: it can exceed the 4×10^5 V/cm [95].

The generation rate per unit of volume of SRH mechanism is:

$$G_{abs.SRH} \approx \frac{n_i}{\tau_e e^{\frac{-(E_t - E_i)}{kT}} + \tau_h e^{\frac{-(E_i - E_t)}{kT}}}. \tag{4.6}$$

The subscript "abs" indicates that this phenomena is dominant in the absorption layer. In fact, the parameters of InGaAs must be used: the temperature-dependent relation for the intrinsic carrier concentration n_i; the electron and hole lifetime

$\tau_e = 47.36\,\mu s$ [96], $\tau_h = 3\,\mu s$ [97]; and $E_t - E_i = 0.06\,eV$ (extracted from [98]), where E_t is the dominant trap level and E_i the intrinsic Fermi level. Using these values a good aproximation is obtained, as confirmed by the dark count rate in [83] where SRH generation is dominant.
The tunneling generation rates per unit area are [89, 99]:

$$G_{mult.BTBT} \approx \sqrt{\frac{2m_r}{E_{InP}}}\frac{q^2F^2}{4\pi^3\hbar^2}\exp\left(-\frac{\pi\sqrt{m_r E_{InP}^3}}{2\sqrt{2}q\hbar F}\right), \tag{4.7}$$

and

$$G_{mult.TAT} \approx \frac{\sqrt{\frac{2m_r}{E_{\mathrm{InP}}}}\frac{q^2F^2}{4\pi^3\hbar^2}N_{\mathrm{trap}}\ \exp\left(-\frac{\pi\sqrt{m_{lh}E_{B1}^3}+\pi\sqrt{m_c E_{B2}^3}}{2\sqrt{2}q\hbar F}\right)}{N_{v\,\mathrm{InP}}\exp\left(-\frac{\pi\sqrt{m_{lh}{E_{B1}}^3}}{2\sqrt{2}q\hbar F}\right)+N_{c\,\mathrm{InP}}\exp\left(-\frac{\pi\sqrt{m_c{E_{B2}}^3}}{2\sqrt{2}q\hbar F}\right)}. \tag{4.8}$$

To compute these two last generation rates per unit of area it is convenient to use the SI units, obtaining a generation rate in $s^{-1}m^{-3}$.
In this case the subscript "mult" indicates that these two phenomena are dominant in the multiplication region. Therefore, the parameters for InP must be used: m_r is the reduced mass of electrons and light holes, E_{InP} is the energy gap, F is the electric field in the multiplication region and it can be extracted by TCAD simulations, using for example "Sentaurus". To model the SPAD presented by Tosi et al. in [83], a value of $F = 3.2 \times 10^7\ Vm^{-1}$ is used, as suggested in [89] where the same SPAD is analyzed. N_{trap} is the trap concentration, E_{B1} and E_{B2} are the barrier heights for valence and conduction band respectively, and $N_{v\,\mathrm{InP}}$ and $N_{c\,\mathrm{InP}}$ are the effective density of states in valence and conduction band, respectively.
After calculating these three values, it is possible to compute the **mean carrier generation time** as follows:

$$t_{DCG} = \frac{1}{G_{abs.SRH}\,W_{abs}\,Area + (G_{mult.BTBT}+G_{mult.TAT})\,10^{-6}\,W_{mult}\,Area} \tag{4.9}$$

where the factor 10^{-6} multiplies the tunneling generation rates in order to use multiplication thicknesses and detector area in cm and cm^2 respectively.

Afterpulsing

As explained before, afterpulse events consist in the release of charge carriers trapped in deep levels during an avalanche. Improving deposition techniques used in fabrication processes can reduce the number of defects inside the material and so the afterpulse probability [85].

In order to characterize afterpulsing in SPAD, usually the afterpulse probability as a function of the delay from the last avalanche is measured.
A standard method often used to estimate afterpulsing is called double-pulse method [100]; it allows to measure the afterpulses reducing the effects of dark carrier generation. In practice the SPAD is operated in gated mode: first the SPAD is mantained below breakdown voltage for hundreds of microseconds, in order to empty the traps; then an avalanche is triggered using a pulsed laser during the first gate-ON window; after a certain dead time, the SPAD is re-activated in the second detection window, waiting for an afterpulse. These operations are shown in Figure 4.4. Repeating many times this operations and gradually changing the dead time, a statistically significant histogram is obtained [100, 101], and consequently the afterpulse probability similar to that in Figure 4.11.

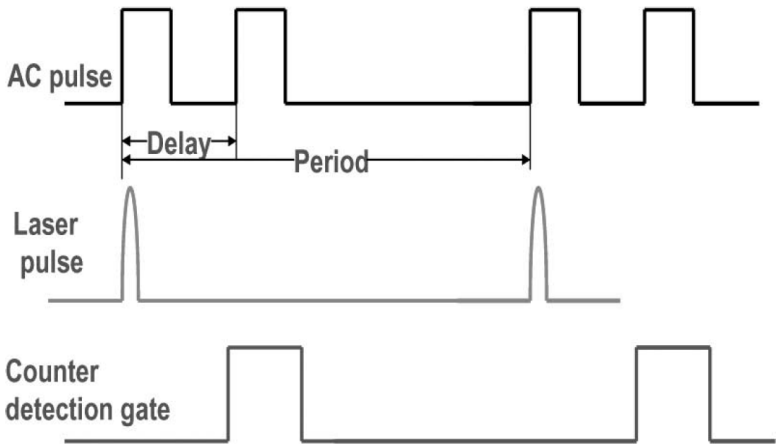

Figure 4.4: Measurement schematic of double-pulse method [101]

A unique and affirmed model to describe afterpulsing does not exist, in particular for InGaAs/InP SPADs. By contrast, Silicon SPADs are most-well studied, and an accurate model can be used. The latter is a simple trapping and de-trapping model

[88], linked to electron and hole capture coefficients in Silicon, which are well known. First of all, in order to obtain an accurate model, it is convenient to consider at least three trap levels, as confirmed in [102]. Then, as shown in [88], the trapping carrier rate for the i-level during an avalanche can be computed as:

$$R_{capture\_i} = r_{n\_i}\, n(t)\, N_{tn\_i}\, (1 - f_{tn\_i}), \tag{4.10}$$

where N_{tn_i} is the trap density in the forbidden band, $n(t)$ the electron density during an avalanche, and r_{n_i} is the electron capture coefficient for the i-th level and is given by:

$$r_{n\_i} = v_{th}\, \sigma_{n\_i}, \tag{4.11}$$

where v_{th} is the electron thermal velocity and σ_{n_i} the electron capture cross section. In order to obtain this cross section, a detailed analysis on traps of the material must be made; they are available for Si but not for InP.
The last term expresses the fraction of traps unoccupied by electrons and is calculated as follows:

$$1 - f_{tn\_i} = \frac{\exp\left[\frac{(E_g - E_{ai})}{2k_B T}\right]}{2\cosh\left[\frac{E_g - E_{ai}}{2k_B T}\right]}, \tag{4.12}$$

where E_{ai} is the activation energy of the i-th level and E_g is the energy gap. For de-trapping, the average release time from the i-th level is:

$$\tau_{cr\_i} = \frac{1}{r_{n\_i}\, N_c}\, e^{\frac{E_{ai}}{k_B T}} = \tau_{0i}\, e^{\frac{E_{ai}}{k_B T}}. \tag{4.13}$$

Here N_c is the state density in conduction band bottom.
Now, having the capture rate and the average release time, the differential equation for the total number n_{e_i} of electrons trapped in the i-th level can be written:

$$\frac{\mathrm{d}n_{e\_i}(t)}{\mathrm{d}t} = R_{capture\_i} - \frac{n_{e\_i}(t)}{\tau_{cr\_i}}. \tag{4.14}$$

The solution of this equation is:

$$n_{e\_i}(t) = r_{n\_i} \cdot \frac{C_j V_{ex}}{q} \cdot N_{tn\_i} \cdot (1 - f_{tn\_i}) \cdot e^{-\frac{t}{\tau_{cr\_i}}} \tag{4.15}$$

Now, having obtained the number of trapped electrons in time, the afterpulsing probability in a short time can be computed, and it is equal to:

$$dP_a = -P_{tr} \cdot dn_{e\_i}(t). \tag{4.16}$$

Similar calculations can be made for holes.

In order to reduce afterpulsing phenomena, it is convenient to work in Gated Geiger mode, and an efficient quenching method is also necessary, in order to stop the avalanche the fastest way possible.

Quenching methods and reset

The quenching circuit is a fundamental part of a SPAD detector; without this, the avalanche current would dramatically increase, breaking the device. Moreover, an efficient quenching circuit able to stop the avalanche as fast as possible makes the detector more efficient, because it reduces the trapped carrier and consequently the afterpulses. After quenching, it is also necessary to restore the detector in the original bias condition, to sense new photons: this is the reset phase.
The possible quenching methods are:

- **Passive quenching**: it is the simplest method of quenching, where a huge resistance (ballast resistance R_B) is connected to the anode or to the cathode of the SPAD: both solutions can be found in literature.

  When the avalanche current starts to flow, the voltage on this resistance increases. As a result, the excess voltage on the diode decreases, as also the avalanche current; when the current goes below a certain "latching current", the avalanche is no longer self sustained, and so it stops in a random time [104]. The level of this threshold current is not exactly defined, it is approximately 100 µA [103].
  The excess voltage decreases towards zero with a time constant equal to:

  $$\tau = C_P \left(R_S \| R_B\right) \tag{4.17}$$

  where C_P is the parasitic capacitance at SPAD anode or cathode, depending

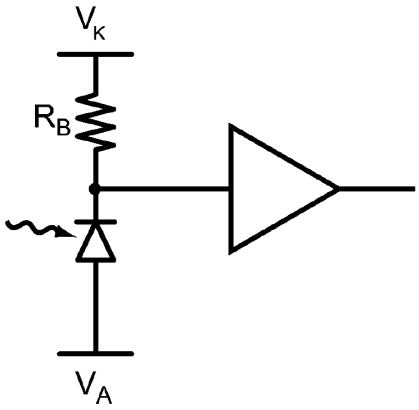

Figure 4.5: Simple passive quenching circuit [103]

on where ballast resistance is connected, and R_S is the SPAD's resistance [103]. The average quenching time can be estimated as follows:

$$t_Q = \tau \ln\left(\frac{I_0 - I_F}{I_{Threshold} - I_F}\right) \tag{4.18}$$

where I_0 is the peak current at the beginning of the avalanche, I_F the quenched current and $I_{Threshold}$ the latching current mentioned above [103].
In order to decrease this quenching time, a low time constant is required, and so it is convenient to connect the ballast resistor to the less capacitive terminal of the SPAD [103]. It is important to emphasize that this quenching time is random; this is one of the drawbacks of passive quenching. Another drawback is the long reset time [103]. Indeed, after quenching, the bias voltage returns slowly to its initial value (passive reset), with a time constant that is five or ten times bigger than the quenching time. Considering that the quenching time is in the order of tens of nanoseconds, the reset time can overcome 1 µs. It is a concrete problem because, during this time, some photons may generate too small currents, remaining undetected. Consequently, the dead time of the detector must be very long, limiting the working frequency.
Passive quenching has the advantages to be cheap, simple, and to occupy a small area.

- **Active quenching**: active quenching circuits are much more complex, so

they are more expensive and they occupy a larger area, but they have better performance, in particular in reset phase.
The avalanche is detected through a low impedance, and, using active components, the voltage on the diode is lowered below the breakdown. As a consequence, the avalanche is immediately blocked; this allows the reduction of power dissipation. Furthermore, an important advantage is that the quenching time is well defined.
The reset time is much faster than in passive systems, in the order of few nanoseconds or a few dozens of nanoseconds [103].
Commercial detectors rarely use pure active quenching systems because the delay from detection of avalanche and the quenching intervention can last tens of nanoseconds during which dissipation is high. Hence, the best solution is to use hybrid quenching systems.

- **Hybrid quenching**: this quenching method mixes active and passive quenching to get the advantages from both [105]. Active, passive or mixed quenching circuits combined with active, passive or mixed reset must be choosen depending on the specific application requirements. The most used combination is active-passive quenching with active reset [103]. In fact, the passive quenching allows the reduction of the current (and consequently the lowering of power dissipation and trapped carriers) before the active quenching comes into operation [103, 106].

Operation modes: free-running and gated

A SPAD can work in two different ways:

1. **free-running mode**: the SPAD is continuosly above the breakdown voltage, so capable to detect a photon. The principal drawback is that the detector can be continuously triggered by dark generated avalanches or afterpulses;

2. **gated mode**: the SPAD is maintained below the breakdown for most of the time, and it is activated for a small time window, the gate-ON time, synchronized with the arrival of a photon. This method allows one to strongly

decrease the dark counts caused by both dark generations and afterpulses because many of them "happen" when the SPAD is deactivated.

4.4 Verilog-A model

As suggested from the previous sections, the performance of a SPAD is strictly connected with its physical structure but also to the control circuit used to quench and reset the diode. Developing a Verilog-A model for the SPAD, it is possible to simulate its behaviour, studying how its performance varies using different control circuits or different operating conditions. In this way, it is possible to obtain usefull information that are essential to estimate the key rate and the QBER of a QKD system, such as the total dark count rate. A detailed estimation of these parameters for a real QKD system will be done in chapter 6.

4.4.1 Reference SPAD

The Verilog-A code is developed having as reference the aforementioned InGaAs/InP presented by Tosi et al. in [83], but this model is suited to simulate also Si SPADs. This detector has the usual physical structure of a InGaAs/InP SPAD, as depicted in Figure 4.6, where the scanning electron microscope image of its cross-section is shown. The role of each layer and each material has been already analyzed in subsection 4.3.1.

4.4.2 Flowchart of the simulator

The Verilog-A code was written and tested using "Cadence Virtuoso". The operation of the simulator is described by the flow chart in Figure 4.7: at the beginning of the simulation, the variables of the SPAD are initialized; after that, if the SPAD is properly biased, it can detect photons, whose interactions are simulated with an if-clause. Dark carriers generations and afterpuling are simulated using two distinct timers.

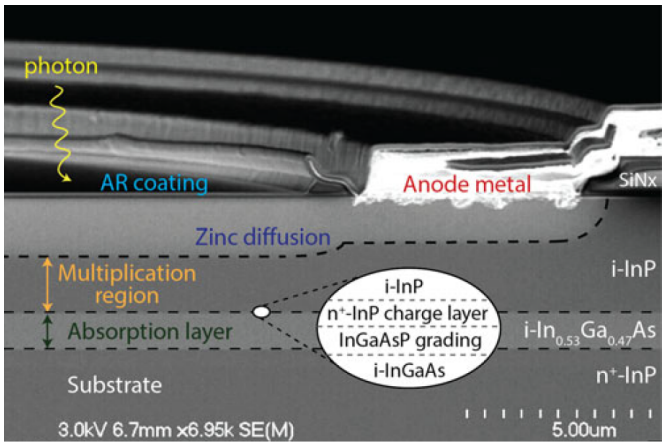

Figure 4.6: Scanning electron microscope image of the InGaAs/InP SPAD cross-section [83].

4.4.3 Ports of the SPAD

The SPAD is modeled as a three port device, two real and a fictitious one. Anode and cathode are the real ones while the third is called "photon": when the voltage at this port overcomes the value fixed in the variable "PhotonThreshold" the arrival of a photon is simulated.

4.4.4 Circuital model

The simplified circuital model is shown in Figure 4.8. Consequently, the SPAD structure is described at the beginning of the Verilog-A code in the following way:

```
module SPAD (a, k, photon);
inout a,k,photon;
electrical a, k, photon, gnd;
ground gnd;

branch (k,gnd) Kcap;
branch (a,gnd) Acap;
branch (k,a) Jcap, spad;
```

In practice "a", "k", and "photon" are the three ports, also called pins or nodes. The branches, defined as a single path between two nodes [107], are "Kcap" and

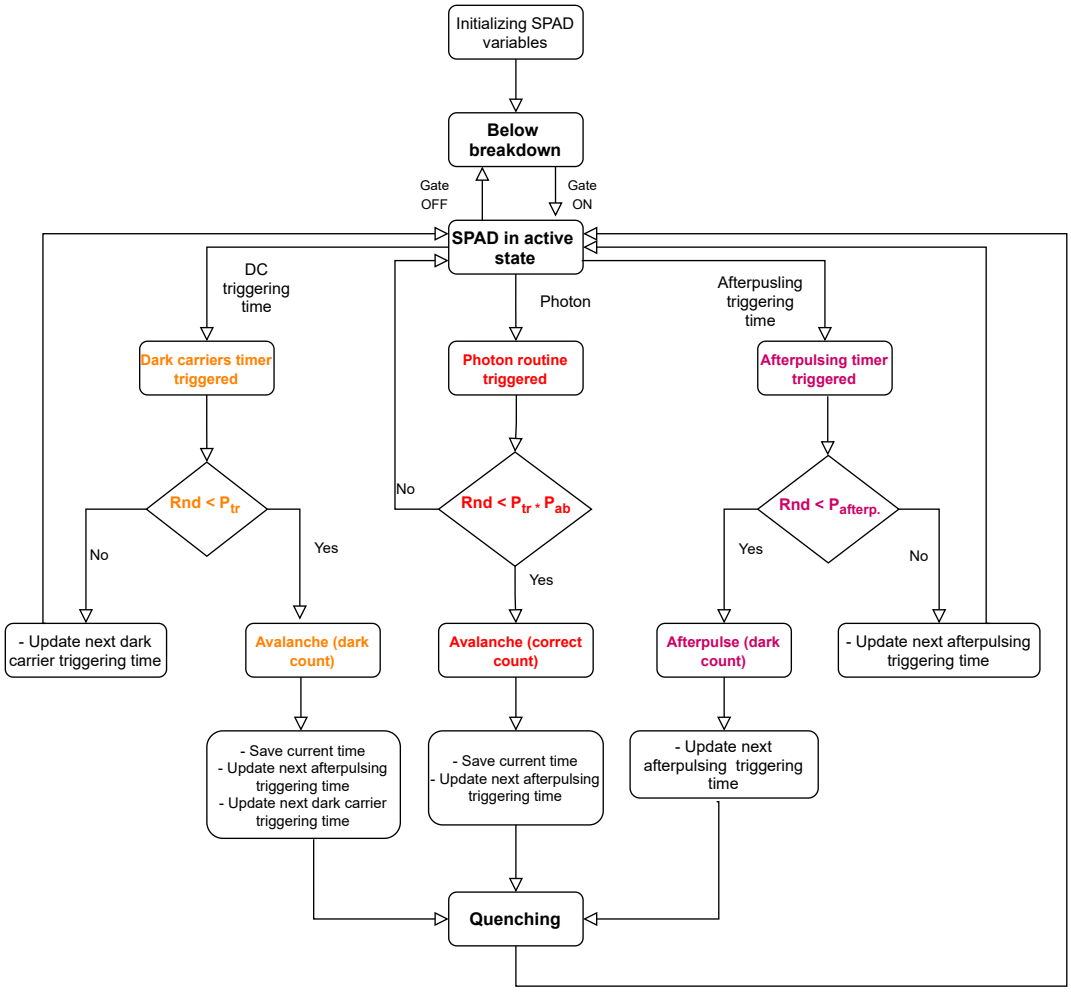

Figure 4.7: Flow chart that describes the operation of the simulator.

"Acap", which are the stray capacitances with the substrate; "Jcap", which models the depletion capacitance at the junction; and "spad", which is the static DC branch.

4.4.5 Static and dynamic currents

As explained in section 4.3.2, below breakdown and when avalanche is not triggered, the static current is the reverse current I_S while, when avalanche starts, it becomes [88]:

$$I_{spad} = I_s + \frac{V_n}{R_{\text{break}}} \ln\left(1 + e^{\frac{V_{ex}}{V_n}}\right) \tag{4.19}$$

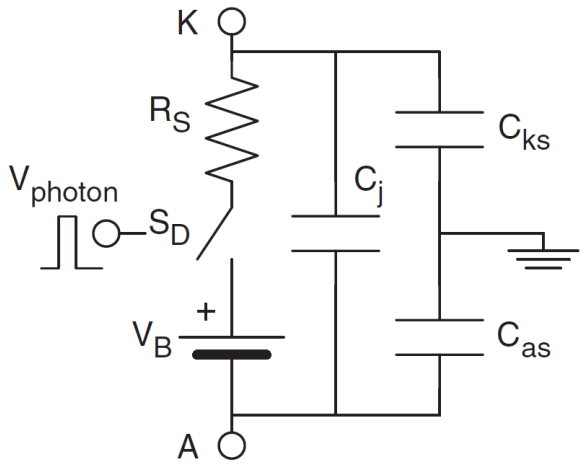

Figure 4.8: Circuital model of the SPAD [87].

Including also the capacitive effects given by the depletion region and the stray capacitances with the substrate, the total currents at cathode and anode are defined as follows [87, 88].:

$$I_c = I_{\text{spad}} + \frac{dQ_j}{dt} + \frac{dQ_{cs}}{dt}, \quad I_a = -I_{\text{spad}} - \frac{dQ_j}{dt} + \frac{dQ_{as}}{dt}, \tag{4.20}$$

The Verilog-A code for the current definition is the following one:

```
//////// Diode and excess voltages /////////
Vd=V(k)-V(a);
Vex=Vd-Vbreak;

//////// STATIC AND DYNAMIC BEHAVIOUR ////////
Qks=Cks*V(Kcap);
Qas=Cas*V(Acap);
Qj=A*Vbi*Cj0*pow((1+V(Jcap)/Vbi),(1-mj))/(1-mj);
Cj=A*Cj0*pow((1+V(Jcap)/Vbi),(1-mj))/(1-mj);
Curr_av=(Vn/Rbreak)*ln(1+exp(Vex/Vn));


////////// SETTING CURRENTS //////////
Curre=Is+avalanche*Curr_av;
```

```
I(Acap)<+ ddt(Qas);
I(Kcap)<+ ddt(Qks);
I(Jcap)<+ ddt(Qj);
I(spad)<+ Curre;
```

In the first lines, the voltage across the diode and consequently the excess voltage are calculated. Then the charge contained in the capacitive regions are computed using the expressions reported in [87], as also the variable "Curr_av", which is the static current when an avalanche is triggered. Obviously, the other variables present in these equations are previously initialized at the beginning of the simulation. This variable is used to obtain the current in the DC branch: when the SPAD is not in avalanche condition, the variable "avalanche" is 0 and consequently the current "I(spad)" in the DC branch is equal to the reverse current "Is", instead, when an avalanche is self sustained in the diode, the current is given by Equation 4.19.

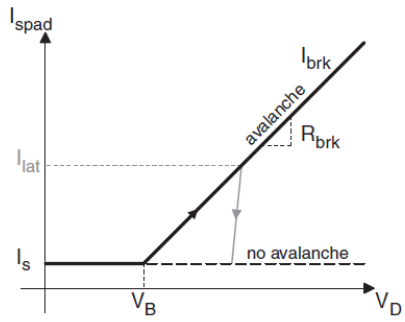

Figure 4.9: Simplified plot of the current that flows in the SPAD. The black dashed line shows the current without an avalanche, the black solid line shows the current during an avalanche or below breakdown. The latching current and the turn-off behavior are in grey [87].

4.4.6 Current quenching

As explained in section 4.3.2, the quenching circuit is necessary to stop the avalanche. In general, it simultaneously reduces both current and voltage on the SPAD. The avalanche ends when the current decreases below a certain threshold current, called "latching current", where the avalanche is not self-sustained anymore; this behaviour

is shown in grey in Figure 4.9. Furthermore, it may terminate if the diode voltage goes below the breakdown value, i.e. the excess voltage becomes lower than 0.
In the Verilog code, the shutdown of the SPAD is modeled by the following lines:

```
//////// STOPPING AN AVALANCHE ////////////
if (((avalanche==1.0) && (Vex<=0))||((avalanche==1.0) && (Curr<Ilatch)))
begin
avalanche=0.0;
$strobe("AVALANCHE STOPS!",  $abstime);
//Set a new latching current
Ilatch=$rdist_normal(seed_Ilatch,Ilatch_av,Ilatch_sig);
end
```

In practice, if an avalanche is active, it ends if "Vex" becomes negative or the static current "Curr" goes below the lathcing current.
The function "$strobe" is used to print in the log file the simulation time "$abstime" when the avalanche stops; the strobe function is very useful in Verilog-A because it allows to debug the code, showing the values of the variables during a certain simulation step.
The last line before the "end" which concludes the if clause is used to define a new latching current because, as already explained, this threshold current is not exactly defined. So, to make the simulation more realistic, the next latching current is calculated using a normal distribution that has mean value (Ilatch_av) equal to 20 µA and standard deviation (Ilatch_sig) equal to 1.5 µA [88]. The variable "seed_Ilatch" is an integer number used to initialize the pseudo-random number generation on the basis of the normal distribution.

4.4.7 Photon arrival

The arrival of a photon, simulated with a voltage signal at the pin "photon", is modeled with the following part of code:

```
//////// PHOTON ARRIVAL ///////////
if((V(photon)>PhotonThreshold))
begin
```

```
if (Vex>0)
begin
Ptr=1.0-exp(-Vex/(eta*Vbreak));

if($rdist_uniform(seed_Pphoton,0.0,1.0)<Ptr*Pab)
begin
avalanche=1.0;
$strobe("1) Avalanche occurs due to photon at time:",  $abstime);
DetectedPh=DetectedPh+1;
time_last_av=$abstime;

//schedule next afterpulse triggering time
tap=$abstime+20e-9;
end
end
end
```

So, when the voltage at the fictitious pin "photon" exceed the "PhotonThreshold", if the excess voltage is greater than 0 (i.e. the SPAD is active and potentially an avalanche could start), firstly the avalanche triggering probability "Ptr" is computed using Equation 4.5, where the exponential slope "eta" is assumed equal to 0.1707 as suggested in [89].
This probability is multiplied by the absorption probability "Pab" which takes in account the reflectivity of the surface, the absorption probability in InGaAs and the collection probability of holes, from absoprtion to multiplication region. In practice "Pab" contains the first three terms of Equation 4.3. Since an exact relation exists only for the absorption in InGaAs (Equation 4.4), the other two contributions are taken in account with a correction factor. The probability "Pab" is computed at the beginning of the simulation in the global event "@(initial_step)" as follows:

```
////////////// INITIAL STEP ///////////////
@(initial_step)
begin
 ...
```

```
//Computing photon absorption probability
Pab=(1-exp(-alpha_abs*Wab))*corr_fac_abs;
 ...
end
```

The correction factor is choosen in order to obtain a photon detection efficiency close to the real one:

$$PDE = P_{coup} \cdot P_{abs} \cdot P_{inj} \cdot P_{tr} \approx \text{Pab} \cdot \text{Ptr} \tag{4.21}$$

Choosing the right correction factor (0.63), the photon detection efficiency used in the simulator well reproduces the real one in the working temperature range, as depicted in Figure 4.10. In fact the modeled PDE line falls exactly in the middle

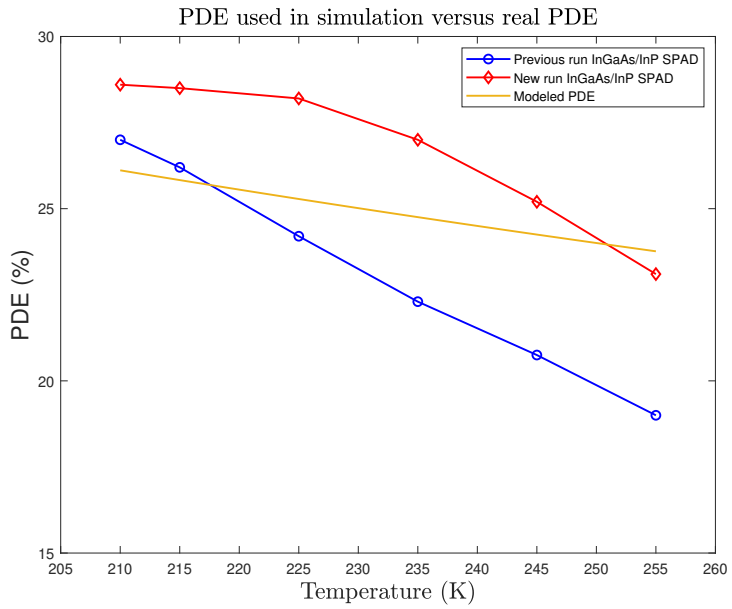

Figure 4.10: Comparison among the PDE used in the simulations (orange curve) and the real PDE efficiency of the SPAD. The blue curve is related to an older version of the SPAD, while the red one is the PDE in a newer and more efficient version of it [83].

of the two experimental curves. The blue one is related to an older version of the SPAD, while the red one is the PDE in a newer and more efficient version of it.

To determine if the impinging photon generates or not an avalanche, a random

number is extracted using the function "$rdist_uniform" that returns a pseudo-random-real number between 0 and 1 using a uniform distribution. If this random number is lower than the calculated photon detection probability (Pab · Ptr), the avalanche starts: the variable avalanche switches from 0 to 1, the avalanche start time is printed and saved in the variable "time_last_av", the counter for the correctly detected photons "DetectedPh" is incremented, and the triggering time for the next afterpulse is saved in the variable "tap". In practice, after 20 ns from an avalanche and for the next 150 µs, the simulator tests if an afterpulse occurs or not entering in a dedicated timer, as it will explained in subsection 4.4.9.

4.4.8 Dark carrier generation

Thermal, band-to-band-tunneling, and trap assisted tunneling generation rates per unit of volume can be easily calculated using Equation 4.6, 4.7, and 4.8. Subsequently the mean dark carrier generation time can be computed using Equation 4.9. Therefore this mechanism can be described in the Verilog-A model using this simple timer:

```
/////////Timer for DCG event ////////
@(timer(tdc,inf))
begin
if (Vex>0)
Ptr=1.0-exp(-Vex/(mu*Vbreak));
else
Ptr=0.0;

if($rdist_uniform(seed_dark,0.0,1.0)<Ptr)
begin
avalanche=1.0;
time_last_av=$abstime;
Ndcr=Ndcr+1;
$strobe("2) Dark generation generated an avalanche", Ndcr, $abstime);

//schedule next afterpulse triggering time
```

```
tap=$abstime+20e-9;
end

//schedule next dark carrier release
delta_tdc=$rdist_exponential(seed_tcg,tcg);
tdc=$abstime + delta_tdc;

end
```

First of all, it is convenient to recall how a Verilog-A timer is set: the first variable, in this case "tdc", fixes the first simulation time in which the timer is triggered; the second variable, in this case "inf" which stands for infinity, set the period of the timer. This timer is controlled only by the triggering time "tdc" that is set at the beginning of the simulation exactly equal to the mean dark carrier generation time. Then "tdc" is updated at every occurrence of the timer, as it will explained below.

Basically, when the simulator enters in this timer, firstly the avalanche triggering probability is computed. In a manner similar to what happens in the "Photon arrival" routine, a random number between 0 and 1 is extracted. If it is lower than the triggering probability an avalanche occurs: the variable "avalanche" is set to 1, the counter "Ndcr" for dark counts is updated, the starting time of the avalanche is saved and the variable "tap" to simulate afterpulses is updated.
Before going out this timer, the next dark carrier release time is set using an exponential distribution, even if the carrier release did not generate an avalanche. This escamotage is used in lots of Verilog-A model for SPADs [87, 88, 89] to make the simulation more realistic.

4.4.9 Afterpulses

The modeling of afterpulses was one of the most demanding task in developing this code; the first idea was to use the trapping-detrapping model shown in 4.3.2, using the data for trap levels in InP. To implement this model is necessary to have detailed data about both electrons and holes. Unfortunately these data are fragmentary in literature and strongly related to the deposition techniques, not mentioned by the designers of this SPAD. Furthermore, saving the trapping time of each carrier and

determining its releasing time is not trivial in Verilog.

After several non-working versions, it was decided to model this phenomenon by exploiting the afterpulse probability as a function of time from the last avalanche. This probability is obtainable with a simple characterization of the device, indeed it is frequently reported in the presentation papers of these devices. For this SPAD, the avalanche probability is shown in Figure 4.11; it was obtained using double pulse method [100] with a gate-ON time of 20 ns and an excess bias of 5 V. For this reason

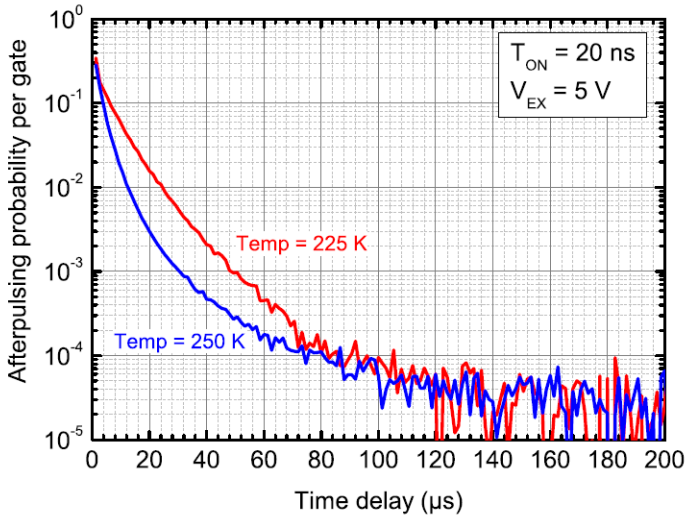

Figure 4.11: Afterpulse probability as a function of time from last avalanche measured with double pulse method, with $V_{EX} = 5\,V$ and T_{ON} =20 ns at 225 K and 250 K [83].

it is possible to model the afterpulses using a timer which is repeated every 20 ns for 150 µs, when the afterpulse probability in InGaAs/InP SPAD becomes negligible.

The code for afterpulsing is pretty similar to that for dark carriers, but here the afterpulse probability is computed in place of the avalanche triggering probability. The probability used in the simulation was obtained by a fit of the experimental curve of Figure 4.11 with a sum of three exponentials:

$$f(x) = A_1 e^{-\frac{t-t_0}{\tau_1}} + A_2 e^{-\frac{t-t_0}{\tau_2}} + A_3 e^{-\frac{t-t_0}{\tau_3}}, \tag{4.22}$$

where A_i are the exponential pre-factors and τ_i are the average lifetimes in the

trap levels. The fit with three exponential appears to be the best choice to obtain an accurate fitting expression for the afterpulse probability in InGaAs/InP SPADs [83, 89, 108].
The result of the interpolation, carried out using the software "Origin 2021", is reported in Figure 4.12.

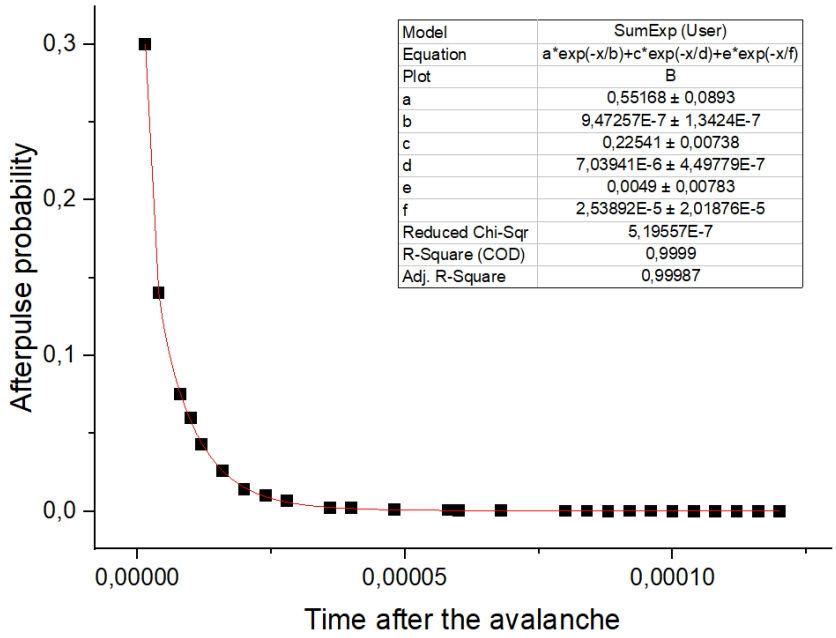

Figure 4.12: Experimental data (black dots) and curve fit (red) of afterpulse probability, obtained using "Origin 2021". The fitting equation and the calculated parameters are reported in the table.

The fit was made only for the experimental data at 225 K and $V_{EX} = 5\,V$ because this is the best operating condition for this device; consequently the afterpulsing results are accurate at this temperature and with this excess voltage. However, if one has more experimental data (and not only two plots as in this case), a relation for afterpulse probability which depends also on temperature and excess voltage will be obtainable.

The code for afterpulses is the following:

```
////////Timer for afterpulses////////
@(timer(tap,20e-9))
```

```
begin

if (Vex>0)
begin
P_afp_1=corr_fac_1*exp(-($abstime-time_last_av)/trel_1)
        +corr_fac_2*exp(-($abstime-time_last_av)/trel_2)
        +corr_fac_3*exp(-($abstime-time_last_av)/trel_3);
end
else
P_afp_1=0.0;

if($rdist_uniform(seed_aft_1,0.0,1.0)<P_afp_1)
begin
avalanche=1.0;
Naft=Naft+1;
$strobe("3) Afterpulse generated an avalanche with P_afp=",P_afp_1,
        "at time:",  $abstime,"Counter afp:", Naft);

//schedule next afterpulse triggering time
tap=$abstime+20e-9;
end

if ($abstime-time_last_av>150e-6)
begin
tap=1000;
end
end
```

Unlike the dark carrier generation routine, here the next triggering time "tap" of the timer is scheduled every 20 ns, without varying this interval with an exponential distribution. This decision was taken in order to not introduce new simulation errors in addition to those already given by the afterpulse probability characterization and accentuated by the fitting.

The last lines of this part of code fix the next triggering time "tap" at 1000 s (but every large amount of time would be fine) when 150 µs has passed from the last avalanche, effectively deactivating the timer. In fact, after 150 µs from an avalanche, the afterpulse probability becomes negligible.

4.4.10 Simulation and verification

In order to test the reliability of this Verilog-A code, the modeled SPAD was included in a passive quenching-and-reset circuit, operated in gated mode, shown in Figure 4.13.
The generator "V_{photon}" is used to simulate the incident photon, generating a 1 ns narrow pulse.
"V_{bias}" is used to fix the bias point of the diode during the gate-OFF period, 0.5 V below the breakdown voltage. Since the breakdown voltage is temperature dependent, this bias point is variable. This generator is connected to the cathode of the diode through a 50 Ω resistor.
"V_{gate}" is used to polarize the SPAD above the breakdown voltage during the gate-ON periods, fixing the excess bias voltage. It is connected through a 50 nF capacitor at the cathode of the diode.
The 100 kΩ resistance "R_B" connected to the anode is the ballast resistance, the essential part of this simple quenching circuit.

Primary dark count rate

The primary dark count rate (DCR), id est the erroneous detection events effectively caused by generated dark carriers, was simulated at three different temperatures (225 K, 250 K, 275 K) and with $V_{EX} = 5\,V$, in order to compare the results with the data shown in the paper, where a passive quenching circuit was used too. A very long dead time (100 µs) was used in order to minimize the effect of afterpulses, hence the adjective primary. The gate-ON time is irrelevant because the results are corrected using the following formula:

$$DCR = -\frac{1}{T_{ON}} \cdot \ln\left(1 - \frac{N_{\text{counter}}}{f_{GATE}}\right), \tag{4.23}$$

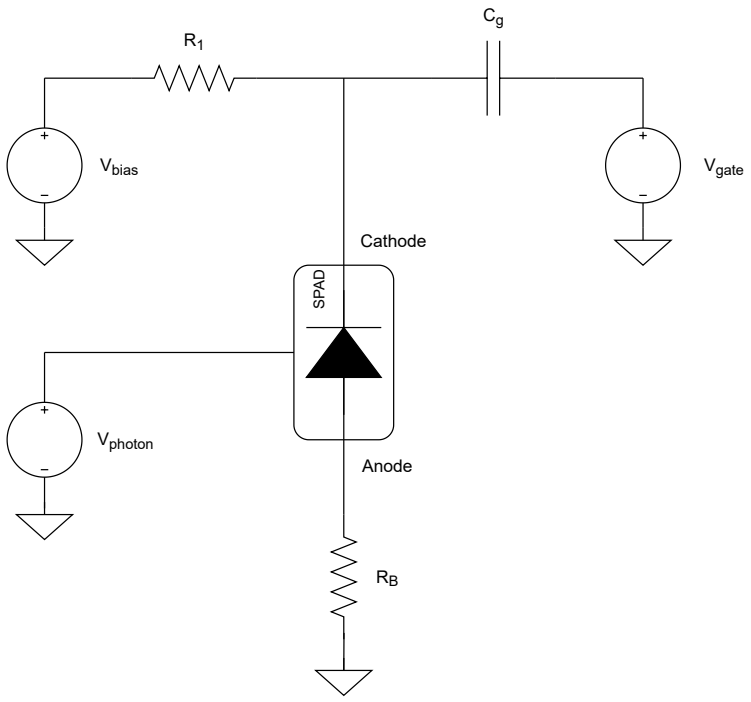

Figure 4.13: Passive quenching circuit used in the SPAD model simulations.

where $f_{GATE} = 1/(T_{ON} + T_{OFF})$ and $\mathrm{N_{counter}}$ is the measured/simulated avalanche rate [109]. Using this formula, it is possible to normalize the DCR making it independent from the gating periods; in practice, the calculated DCR is that of the device as if it works in free-running mode. Usually, the dark count rate is expressed in counts per seconds (cps).

The comparison between experimental and simulated DCR is shown in Figure 4.14; the primary dark count rate is very-well simulated across the entire temperature range, in fact the simulated values fall exactly between the ones relative to a newer and an older version of this SPAD.
The dominant phenomenon is thermal generation, as in the real case [83]. This is demonstrated in Figure 4.15 where all the contributions to dark count rate, theoretically computed, are reported. In this plot also the simulated values for the DCR are shown (red asterisks), the same of Figure 4.14: they correctly follows the theoretical primary DCR. This is evidence of the goodness of the simulation.

From these results, it is easy to understand that dark counts are a limiting factor for the sensibility of a SPAD, and, consequently, the importance to work in gated mode.

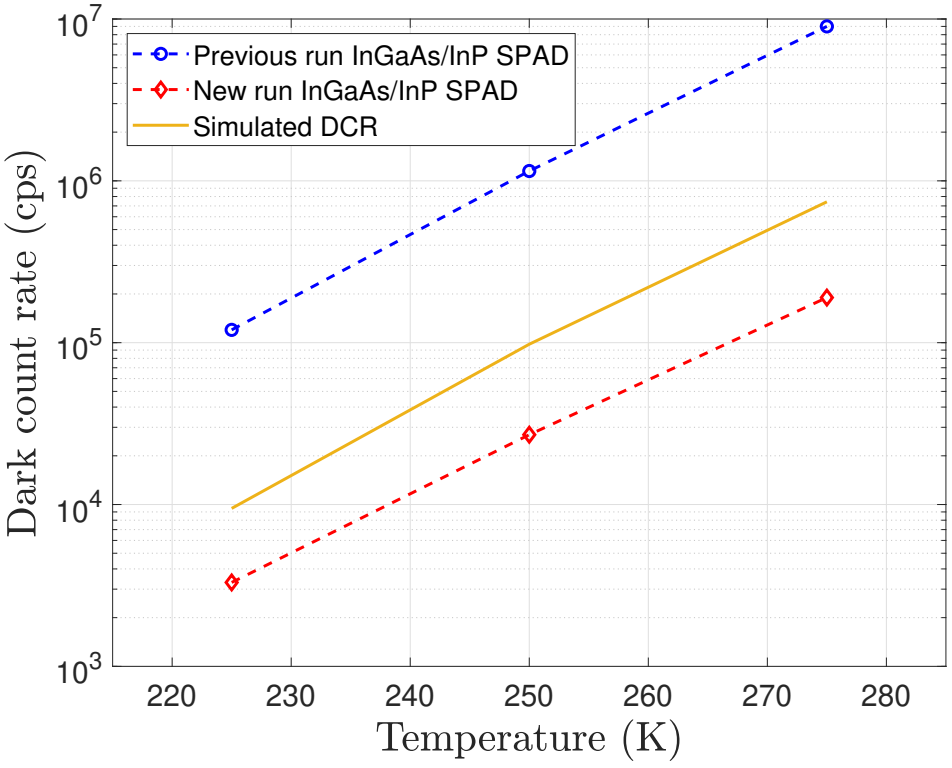

Figure 4.14: Comparison between the experimental primary dark count rate (dashed lines) and the simulated one (orange solid lines), both obtained with 5 V of excess bias and with T_{OFF} =100 µs. The values are reported in counts per seconds (cps). As in Figure 4.10, the blue curve is related to an older version of the SPAD, while the red one is the DCR in a newer and more efficient version of it [83].

Afterpulsing and total dark count rate

After having computed the primary dark counts, it is necessary to understand how afterpulses affect the total dark count rate. To do this, the previous simulations were repeated but the dead time was progressively reduced, until it becomes so small that some trapped carriers are released during a gate-ON time window.

This simulation method for afterpulses proposed in this thesis allows an excellent accuracy when the excess bias is equal to 5 V, well reproducing the experimental

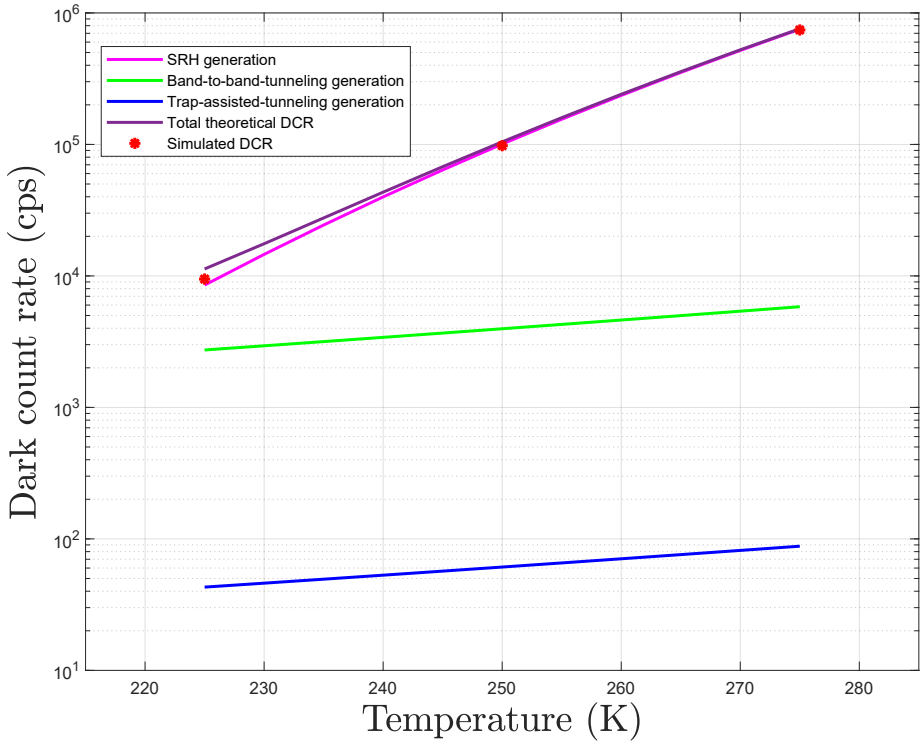

Figure 4.15: Theoretical DCR and simulated one with 5 V of excess bias and T_{OFF} =100 µs. The values are reported in counts per seconds (cps). In addition to the total theoretical DCR (dark purple), all the contributions to DCR are reported: Shockley-Read-Hall (fuchsia), band-to-band-tunneling (green), and trap-assisted-tunneling (blue).

results, as shown in Figure 4.16.
On the other hand, the total DCR is slightly overestimated when the excess bias is fixed to 3 V. These results were largely predictable because the afterpulse probability was obtained with V_{EX} = 5 V; in this condition a larger current flows in the diode, therefore more carriers are trapped, and the afterpulses are more frequent compared to when V_{EX} = 3 V is applied. Similarly, it is reasonable to expect an underestimation of afterpulses when an higher excess bias is applied.

In order to correct the model ensuring a better simulation accuracy in all the operating conditions, a more detailed afterpulsing characterization would be necessary. In this manner, an afterpulse probability function dependent also on excess bias and

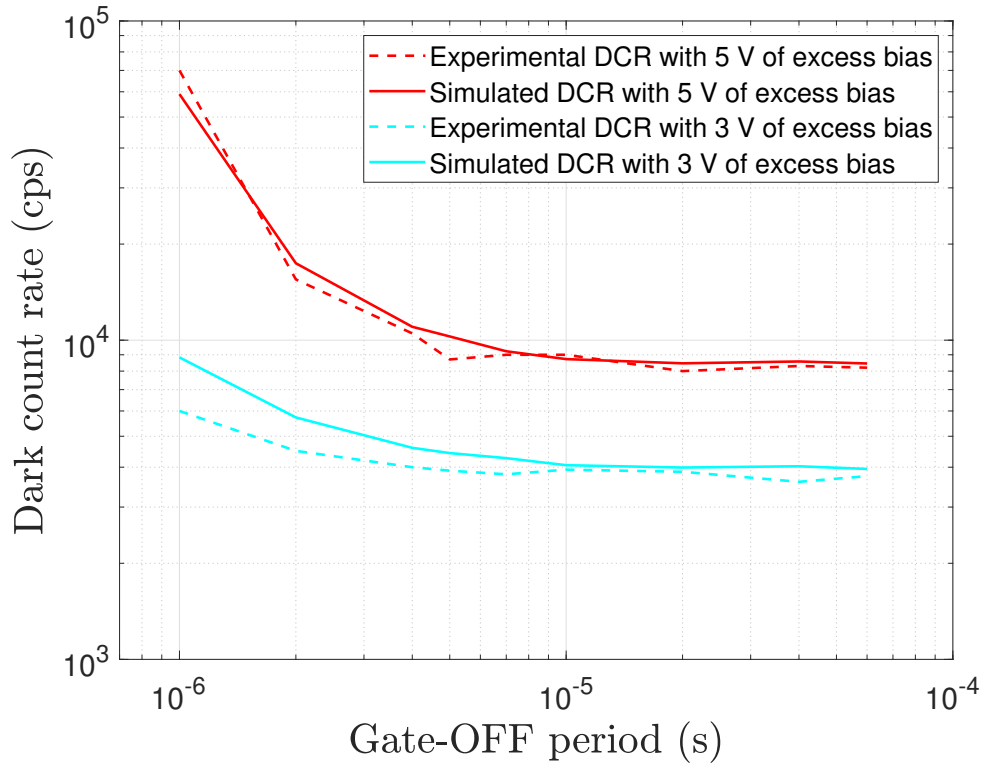

Figure 4.16: Comparison between experimental total dark count rates (dashed lines) and the simulated ones (solid lines), as a function of gate-OFF time. The simulations where repeated with two different excess bias, 5 V (red curves) and 3 V (cyan curves). In the simulation temperature was set to 225 K and the gate-ON time to 20 ns, as in the experiments.

temperature could be obtained. Another solution is to recover all the parameters for trap levels in InP, necessary to implement the trapping-detrapping model explained before. In fact this is the most used solution to simulate Si SPADs, for which these parameters are widely investigated.

Returning to the simulation results, it is evident how the number of total dark counts is quite constant for gate-OFF delays greater than 10 µs, linked almost only to generated dark carriers. For gate-OFF times smaller than 10 µs, the total dark count rate strongly increases due to the effect of afterpulses. Now it is clear why a long and appropriate gate-OFF time is necessary to decrease the dark detections. With a lower excess bias the DCR is lower also at higher operating frequency, but the photon detection efficiency is lower too.

To sum up, it is necessary to find the most convenient trade-off among all the operating parameters of a SPAD, from the temperature to the gating periods, passing through the excess bias voltage.

Chapter 5

Detailed description of the simulator and MATLAB implementation

After having analyzed all the components that may be encountered in a QKD system, it is now possible to show in detail how the simulator works. A series of MATLAB functions have been developed to easily describe and simulate a generic QKD system, but, in principle, it is possible to study any optical experiment. The explanation will be supported by the analysis of a real QKD system.
As a remark, this model is intended to simulate QKD systems based on polarization encoding, when coherent light sources are used, for example an attenuated laser. Nowadays, this is the most common solution in QKD systems. Anyway, this is a necessary starting point to build more complex models for systems where exotic light sources or entanglement-based protocols are employed.

5.1 State representation and MATLAB operations

As seen in the previous chapters (section 2.3), the propagation of a coherent state can be studied representing the state as a bi-dimensional vector, formed by its creation (or annihilation) operators coefficients, analogous of the Jones vector. Looking at the displaced vacuum state representation, the coefficients for the horizontal and vertical creation (or annihilation) operators are the components of this vector. For example, an antidiagonal-linearly polarized coherent state:

$$|\alpha\rangle \;=\; \exp\!\left(\frac{\alpha}{\sqrt{2}}\left(\hat{a}_H^{\dagger}-\hat{a}_V^{\dagger}\right)-\frac{\alpha^*}{\sqrt{2}}\left(\hat{a}_H-\hat{a}_V\right)\right)|0_H,0_V\rangle\,, \tag{5.1}$$

can be equivalently represented using the coefficients for creation or annihilation operators with the following vector:

$$V_\alpha = \frac{\alpha}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{5.2}$$

By doing so, the previous quantum mechanical relations seen in chapter 3 can be used to propagate the state across the optical system in MATLAB. It is important to note that the Horizontal/Vertical basis has been used to represent the states in the MATLAB scripts and functions.

5.2 Example of propagation

As an example, the propagation through a non-polarizing beam splitter is considered. If the state defined in Equation 5.1 enters in the "a" port of a beam splitter while the other port "b" is left unused, the input state for the beam splitter is:

$$|\alpha\rangle_a \, |\text{vacuum}\rangle_b = \exp\left(\frac{\alpha}{\sqrt{2}}(\hat{a}_H^\dagger - \hat{a}_V^\dagger) - \frac{\alpha^*}{\sqrt{2}}(\hat{a}_H - \hat{a}_V)\right)_a |0\rangle_a \, |0\rangle_b \,, \tag{5.3}$$

where the vacuum state $|0_H,0_V\rangle$ is represented only with $|0\rangle$ to lighten the notation, and the subscripts a and b indicate the input ports. Their associated vectors to be used in MATLAB are:

$$V_a = \frac{\alpha}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \; V_b = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{5.4}$$

In order to calculate by hand the output state of the beam splitter, it is necessary to invert the relation shown in Equation 3.30, in order to obtain the input annihilation operators as a function of the annihilation operators at output ports. Labeling the transmittance and reflectance of the beam splitter as t and r, the

inverted relation is:

$$\begin{pmatrix} \hat{a}_H \\ \hat{a}_V \\ \hat{b}_H \\ \hat{b}_V \end{pmatrix} = \begin{pmatrix} \sqrt{t_H} & 0 & \sqrt{r_H} & 0 \\ 0 & \sqrt{t_V} & 0 & \sqrt{r_V} \\ -\sqrt{r_H} & 0 & \sqrt{t_H} & 0 \\ 0 & -\sqrt{r_V} & 0 & \sqrt{t_V} \end{pmatrix} \begin{pmatrix} \hat{c}_H \\ \hat{c}_V \\ \hat{d}_H \\ \hat{d}_V \end{pmatrix}. \tag{5.5}$$

Here the square roots come from the fact that transmittance and reflctance coefficients reported in datasheets are referred to the ratio of transmitted and reflected optical power [110], and not to the electric field amplitudes.
Now, substituting the expressions for $\hat{a}_H$ and $\hat{a}_V$ in the displacement operator of Equation 5.3, and assuming in the ideal case of a 50:50 non-polarizing beam splitter where $t_H = t_V$ and $r_H = r_V$, the output state results to be:

$$\begin{aligned} |\beta\rangle_c |\beta\rangle_d = \exp &\left(\frac{\alpha\sqrt{t}}{\sqrt{2}} \left(\hat{c}_H^\dagger - \hat{c}_V^\dagger \right) - \frac{\alpha^*\sqrt{t}}{\sqrt{2}} \left(\hat{c}_H - \hat{c}_V \right) \right)_c \\ \cdot \exp &\left(\frac{\alpha\sqrt{r}}{\sqrt{2}} \left(\hat{d}_H^\dagger - \hat{d}_V^\dagger \right) - \frac{\alpha^*\sqrt{r}}{\sqrt{2}} \left(\hat{d}_H - \hat{d}_V \right) \right)_d |0\rangle_c \, |0\rangle_d , \end{aligned} \tag{5.6}$$

where the subscripts c and d indicate the output ports of the beam splitter. In practice, the input state has been separated in two antidiagonal output states, as expected.
The vectorial representation of the output states is:

$$V_c = \frac{\alpha\sqrt{t}}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \; V_d = \frac{\alpha\sqrt{r}}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \tag{5.7}$$

easily obtainable using the following MATLAB function:

```
[V_c,V_d]=beamsplitter(V_a, V_b , transmittance, reflectance)
```

This is the basic version of the function, where the user manually enters the value of transmittance and reflectance of the optical component. This function takes the vectors associated with the coherent states at the input ports of the beam splitter, and it calculates the output vectors, using Equation 3.30.

Finally, from the vectors of Equation 5.7, one can easily calculate the mean photon number contained in each of the two output states, by squaring the components

of these vectors, and summing them together.

5.3 Component libraries

In order to simplify the simulations, a dedicated MATLAB function has been created for each type of component. The function contains the matrix expression of the component plus a sort of library where the user can add the list of parameters necessary in the simulation. In this way, the commercial component can be quickly inserted in the simulation of a QKD system by its name, without having to rewrite its parameters every time.
For example, to use the beam splitter function as in the previous example, one can write:

```
[V_c,V_d]=beamsplitter_known(V_a, V_b , BS_Name)
```

where "BS_Name" recalls one of the saved beam splitters.
As a further example, the function for a Pockels cell is:

```
V_out=pockels_cell_known(V_in, PC_name, Orientation,
      Active/Inactive_state)
```

In general, the user puts as arguments of the function the input state (or the input states in the case of four ports device such as beam splitters), the name of the commercial component, and the working conditions of the device such as the orientation of the Pockels cell and if it is active or inactive.

5.4 Analysis of a real QKD system

In this section, the system presented in [111] is considered. Here a modified version of the BB84 protocol is applied but the structure is the same as an ordinary BB84 system. The experimental setup is shown in Figure 5.1.

The objective of this example is to show how a QKD system based on polarization encoding works and how it is described in the model. It is not taken as benchmark for the model because the employed light source does not generate coherent states. It is made by a laser coupled to a Periodically Poled Lithium Niobate (PPLN),

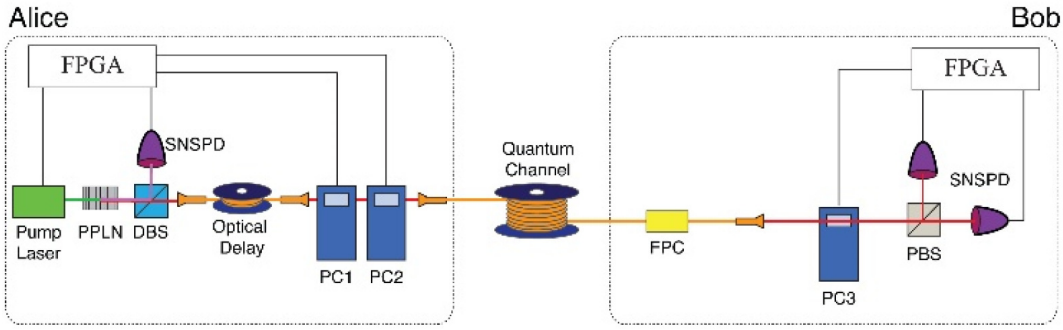

Figure 5.1: Experimental setup. The light source is formed by a laser and a Periodically Poled Lithium Niobate (PPLN) crystal. A dichroic beam splitter (DBS) is used to split the light pulse and monitor it through a SNSPD. Pockels cells PC1 and PC2 are used to encode the single-photons. The quantum channel is the optical fiber SMF28e. FPC is a fiber polarization controller used to compensate PMD. PC3 is used by Bob to select the measurement base. The polarizing beam splitter (PBS) coupled with two SNSPD form the measurement unit [111].

an highly efficient crystal used for non-linear conversion process [112]. The light generated is characterized by a second order correlation function of 0.048, therefore the generated light states have a smaller variance than a coherent state, which has a second order correlation function equal to 1.

5.4.1 Structure and operation

As just mentioned, the light source is formed by a pump laser coupled to a PPLN, which uses the spontaneous parametric down-conversion (SPDC) to produce quasi-single photon pulses with a second order correlation function of 0.048. The PPLN emits idler photons at 782 nm and signal photons at 1550 nm. A dichroic beam splitter (DBS) is used to separate signal and idler photons; the latter are detected by a superconductor nanowire single photon detector to monitor the operation of the light source.

On the other hand, the signal photon passes first in an optical delay, which can be neglected in this analysis, and then in two Pockels cells. These two cells work as half-waveplate and are used to encode the qubits value. It is worth recalling the encoding scheme used in these types of systems: binary “1” corresponds to vertical

or diagonal photons, whereas binary "0" corresponds to horizontal or anti-diagonal photons. The state of polarization of the vertically polarized photons emitted by the laser is modified as follows:

1. the first Pockels cell has its fast axis oriented at 45° with respect to the vertical axis and consequently, if properly activated, vertically polarized photons become horizontally polarized. Its action on annihilation operators is:

$$\begin{cases} \hat{a}_H = \hat{c}_V \\ \hat{a}_V = \hat{c}_H \end{cases} \tag{5.8}$$

   where a and c label input and output ports respectively.

2. the second one is oriented at $-22.5°$ with respect to the vertical axis, and so, when activated, vertically polarized photons become diagonally polarized (plus a phase shift of π), while horizontal ones become anti-diagonally polarized. In practice this second Pockels cell is used to pass from {H,V} to {A,D} basis. In fact its action on annihilation operators is:

$$\begin{cases} \hat{a}_H = \frac{1}{\sqrt{2}} (\hat{c}_H - \hat{c}_V) \\ \hat{a}_V = -\frac{1}{\sqrt{2}} (\hat{c}_H + \hat{c}_V) \end{cases} \tag{5.9}$$

Transmitter and receiver are linked through a single-mode optical fiber (SMF28e) that has a low attenuation (0.2 dB/km) and very low DGD value ($0.06\,\mathrm{ps}/\sqrt{\mathrm{km}}$). However, an unspecified fiber polarization controller is used anyway.

Bob's subsystem is very simple; it contains a Pockels cell oriented at $-22.5°$ with respect to the vertical axis, used to select the measurement basis. This Pockels cell, coupled with a polarizing beam splitter and two SNSPD, forms the detection unit, that works in this way:

- assuming that Bob receives horizontally or vertically polarized photons, if he turns off his Pockels cell, he measures in the correct {H,V} basis. In fact, photons surpass undisturbed the Pockels cell, and then the polarizing beam splitter directs horizontally polarized photons towards one detector, while vertical photons to the other one (except for small errors due to imperfections of

the PBS);

- similarly, if he receives horizontally or vertically polarized photons, but he activates his Pockels cell in order to measure in {A,D} basis, the photons arrive diagonally or anti-diagonally polarized to the PBS, and so they are randomly directed towards the detectors. As a result, the measurement is totally random, triggering in the 50% of the cases one or the other detector, regardless on the initial qubit value;

- likewise, when he receives diagonally or anti-diagonally polarized photons, if he activates the Pockels cell, photons arrive horizontally or vertically polarized at the PBS, which directs them correctly;

- conversely, if he does not activate the Pockels cell, the diagonally or anti-diagonally polarized photons arrive in this state to the PBS, which splits them randomly.

5.4.2 Some real examples

Now that the operation of the system is clear, some real situations are analyzed. The coherent state will be propagated by hand, neglecting the losses of the components, while, simultaneously, the vectorial representation of the state will be used to propagate the state using the MATLAB script, including losses and non-idealities of the components.

The system is simplified joining the laser and the PPLN in a block called light source and neglecting the optical delay and the fiber polarization controller. The simplified scheme is reported in Figure 5.2. For simplicity, the light source is assumed to emit coherent states with mean photon number equal to 1, hence the α coefficient of the initial state is equal to 1 too. Commercial optical components are used for the Pockels cells and the polarizing beam splitter, whereas the optical fiber is the SMF28e used in the paper. In particular the Pockels cell is the "1147-6" from "Lasermetrics" with transmittance equal to 0.98 [113], while the polarizing beam splitter is the "PBS1005-FY" from "Precision photonics" with transmittance and reflectance higher than the 98% and an extinction ratio of 1000:1 [114]. As a remark, the extinction ratio is the "ratio of maximum to minimum transmissivity

of a sufficiently linearly polarized input" [115], in particular, for the aforementioned beamsplitter, the ratio between transmissivity for p-polarized light and s-polarized light.

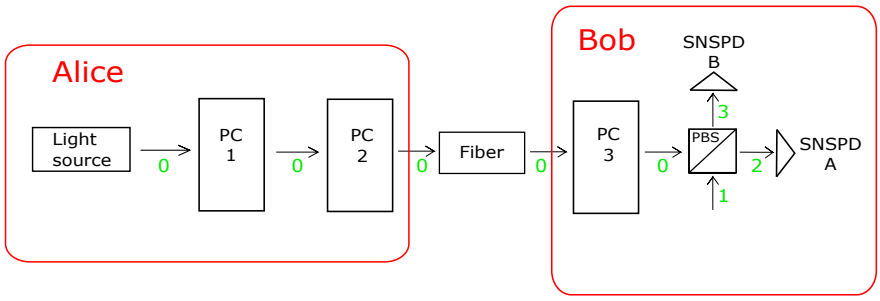

Figure 5.2: Simplified structure of the system. The light paths are labeled in green.

Case 1

In this first example, the case where Alice sends a "0" in {A,D} basis to Bob, who measures in this same basis, is analyzed.
The emitted photons are vertically polarized, so the initial state is:

$$|\Psi\rangle_0 \;=\; D(\alpha = 1_V)_0\;|0\rangle_0 \;=\; \exp\left(\hat{a}_V^\dagger - \hat{a}_V\right)_0\;|0\rangle_0\,, \tag{5.10}$$

where the subscript 0 indicates the first light path, as shown in green in Figure 5.2. The associated state vector is:

$$V_0 \;=\; \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{5.11}$$

Alice activates the first Pockels cell in order to encode the binary "0", polarizing the photon horizontally. Applying the relations shown in section 3.2, it is easy to find that, after the pockels cell, the state becomes:

$$|\Psi\rangle_0 \;=\; D(1_H)_0\;|0\rangle_0 \;=\; \exp\left(\hat{b}_H^\dagger - \hat{b}_H\right)_0\;|0\rangle_0\,. \tag{5.12}$$

Here the symbol b is used instead of a to identify the creation and annihilation

operators only to underline that this is the output state of this Pockels cell. The alphabetical order will be followed in the next steps. Using the MATLAB script, which implements the relation for a lossy Pockels cell shown in Equation 3.52, the state vector is:

$$V_0 = \begin{pmatrix} 0.9899 \\ 0 \end{pmatrix}. \tag{5.13}$$

The horizontal coefficient is not 1 anymore because the MATLAB script takes in account the losses of the Pockels cell.

The second Pockels cell is activated because Alice wants to encode the qubit in the {A,D} basis. For this reason the state becomes anti-diagonally polarized:

$$|\Psi\rangle_0 = D(1_A)_0 \, |0\rangle_0 = \exp\left(\frac{1}{\sqrt{2}}\left(\hat{c}_H^\dagger - \hat{c}_V^\dagger\right) - \frac{1}{\sqrt{2}}\left(\hat{c}_H - \hat{c}_V\right)\right)_0 |0\rangle_0 \,. \tag{5.14}$$

The state vector calculated with MATLAB is:

$$V_0 = \begin{pmatrix} 0.6930 \\ -0.6930 \end{pmatrix}. \tag{5.15}$$

Neglecting losses in the calculation by hands, the fiber has no effect on the state, thus this remains the same as before:

$$|\Psi\rangle_0 = D(1_A)_0 \, |0\rangle_0 = \exp\left(\frac{1}{\sqrt{2}}\left(\hat{d}_H^\dagger - \hat{d}_V^\dagger\right) - \frac{1}{\sqrt{2}}\left(\hat{d}_H - \hat{d}_V\right)\right)_0 |0\rangle_0 \,. \tag{5.16}$$

In reality, the light intensity is strongly attenuated by the 30 km long optical fiber, as shown by the state vector computed using MATLAB:

$$V_0 = \begin{pmatrix} 0.3595 \\ -0.3595 \end{pmatrix}. \tag{5.17}$$

Bob wants to measure in the correct {A,D} basis, so he activates the third Pockels cell. The state of polarization of the photon returns to be horizontal:

$$|\Psi\rangle_0 = D(1_H)_0 \, |0\rangle_0 = \exp\left(\hat{e}_H^\dagger - \hat{e}_H\right)_0 |0\rangle_0 \,, \tag{5.18}$$

as shown also by its vectorial form:

$$V_0 = \begin{pmatrix} 0.5033 \\ 0 \end{pmatrix}. \tag{5.19}$$

As a consequence, the light state can be correctly separated in two path by the polarizing beam splitter. In fact, considering that the input state of the PBS is:

$$|\Psi\rangle_0 \, |\text{vacuum}\rangle_1 = D(1_H)_0 \, |0\rangle_0 \, |0\rangle_1 = \exp\left(\hat{e}_H^\dagger - \hat{e}_H\right)_0 |0\rangle_0 \, |0\rangle_1 , \tag{5.20}$$

the output state can be easily computed using Equation 3.33:

$$|\Psi\rangle_2 \, |\Psi\rangle_3 = D(1_H)_2 \, |0\rangle_2 \, |0\rangle_3 = \exp\left(\hat{f}_H^\dagger - \hat{f}_H\right)_2 |0\rangle_2 \, |0\rangle_3 . \tag{5.21}$$

In practice the photons are completely transmitted towards light path 2 and they can be correctly detected by "detector A" associated with the horizontal polarization or, better to say, with the qubit value "0". Using the MATLAB function for the PBS which implements the Equation 3.54, the vector for the coherent state in path 2 is:

$$V_2 = \begin{pmatrix} 0.4957 \\ 0 \end{pmatrix}, \tag{5.22}$$

whereas for path 3:

$$V_3 = \begin{pmatrix} 0.0152 \\ 0 \end{pmatrix}. \tag{5.23}$$

Path 3 has non-zero components because of the limited polarization contrast of the used PBS, which mistakenly reflect a small part of horizontal incoming photons. These imperfections can lead to erroneous detections.

Case 2

This second case is equal to the previous one, except for the fact that Bob tries to measure in the {H,V} basis, obtaining a random detection. The state encoding in Alice's subsystem and the propagation in the fiber are the same as before, so Bob receives the coherent state shown in Equation 5.16, equivalently represented by the vector in Equation 5.17. In this case, Bob does not activate his Pockels cell, so the

state remains unchanged after it:

$$|\Psi\rangle_0 \;=\; D(1_A)_0\,|0\rangle_0 \;=\; \exp\left(\frac{1}{\sqrt{2}}\left(\hat{e}_H^{\dagger}-\hat{e}_V^{\dagger}\right)-\frac{1}{\sqrt{2}}\left(\hat{e}_H-\hat{e}_V\right)\right)_0 |0\rangle_0\,, \tag{5.24}$$

except for the intensity attenuation, calculable with the MATLAB function:

$$V_0 \;=\; \begin{pmatrix} 0.3559 \\ -0.3559 \end{pmatrix}. \tag{5.25}$$

Consequently, anti-diagonal photons arrive at the PBS, which splits them randomly. In fact the input state of the PBS is:

$$|\Psi\rangle_0\,|\text{vacuum}\rangle_1 = \exp\left(\frac{1}{\sqrt{2}}\left(\hat{e}_H^{\dagger}-\hat{e}_V^{\dagger}\right)-\frac{1}{\sqrt{2}}\left(\hat{e}_H-\hat{e}_V\right)\right)_0 |0\rangle_0\,|0\rangle_1\,, \tag{5.26}$$

which gives at the output:

$$|\Psi\rangle_2\,|\Psi\rangle_3 = \exp\left(\frac{1}{\sqrt{2}}\left(\hat{f}_H^{\dagger}-\hat{f}_H\right)\right)_2 \exp\left(\frac{1}{\sqrt{2}}\left(\hat{g}_V^{\dagger}-\hat{g}_V\right)\right)_3 |0\rangle_2\,|0\rangle_3\,. \tag{5.27}$$

In practice, the initial light intensity is equally divided in the two output paths; as a result, a single photon is randomly directed towards one of the two detectors. In other words, in the 50% of the cases the "detector A" will be triggered, measuring "0", while in the other 50% of the cases the photons will reach "detector B", measuring "1".
Using the MATLAB model, the vector state in path 2 is:

$$V_2 \;=\; \begin{pmatrix} 0.3505 \\ -0.0107 \end{pmatrix}, \tag{5.28}$$

whereas in path 3:

$$V_3 \;=\; \begin{pmatrix} 0.0107 \\ -0.3557 \end{pmatrix}. \tag{5.29}$$

From the comparison between the theoretical calculations and the MATLAB simulations, it is evident how real optical components influence photons propagation, leading to erroneous propagation and imbalances. For this reason, it is important

to properly choose high quality components to reduce the errors and consequently to limit the QBER and increase the key-rate.

5.5 Overview of the complete simulation framework

Now that the functioning of both the MATLAB functions and the Verilog-A SPAD code is clear, it is possible to understand how the complete simulation framework works. The flow chart in Figure 5.3 represents the series of processes that allow to analyse a QKD system, starting from the details of the employed hardware to arrive at the fundamental parameters which describe the quality of the system.

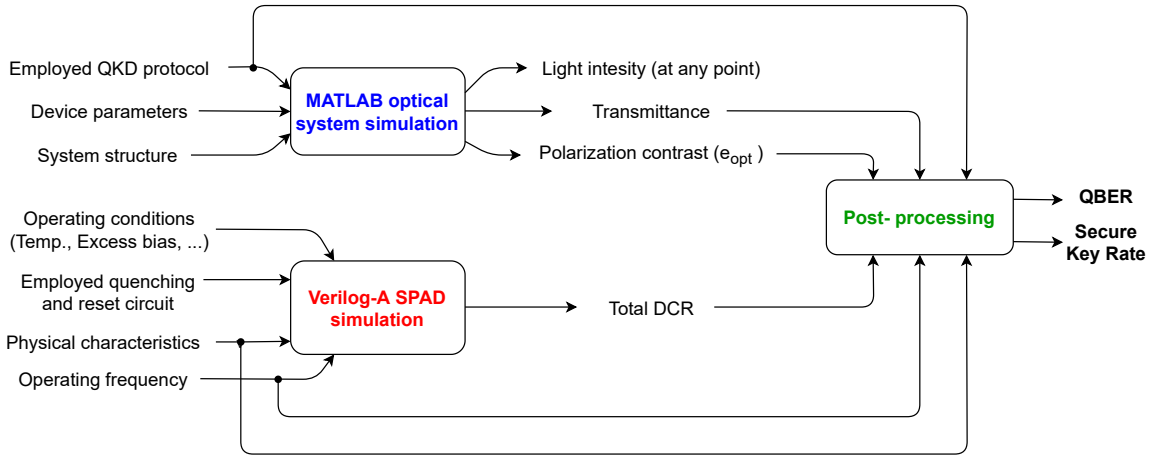

Figure 5.3: Flow chart of the simulation framework.

The MATLAB scripts simulate the propagation of the qubits, namely the photon pulses, through the optical system. This must be described respecting the optical paths and inserting the optical devices in their proper positions. Obviously, also the peculiarity of the employed QKD protocol must be considered, for example the mean photon number sent by Alice in a signal pulse. The MATLAB simulation allows to obtain the light intensity at every point of the structure, the transmittance through any optical path as also the polarization contrast, i.e. the probability that the photon hits the erroneous detector. Furthermore, this hardware based model

allows to understand if a qubit sent by Alice is correctly detected by Bob when he employs a certain measurement basis.

To perform the Verilog-A SPAD simulation, first of all, it is necessary to define the physical characteristics of the diode in the code. Then, the SPAD is ready to be actually tested by setting the operating conditions, as for example the working temperature and the excess bias. In fact, inserting the SPAD model in the quenching circuit which one plans to use, the total dark count can be obtained as a function of the operating gating frequency.

Combining the information derived by the MATLAB and Verilog simulators, the user can perform simple calculations in order to obtain the Quantum Bit Error Rate and the Secure Key Rate of the system, as explained in the next chapter. The advantage of this simulator is that one can easily observe how these parameters vary changing the optical devices, the operating conditions of the SPAD or even rearranging the optical structure of the system. With improvements, this simulation framework could be implemented effectively in a professional software to design QKD systems based on polarization encoding.

Chapter 6

A detailed analysis of a real QKD system

In this chapter, the simulative approach will be validated analyzing a real polarization-coding BB84 systems has been analyzed. The system presented in [116] was selected. In this example, classic and quantum channel coincide in the same optical fiber. Classic communication happens using 32 channels modulated with a 16-QAM format. Wavelengths range from 1535.7 nm to 1559.7 nm. The synchronization signal between the QKD transmitter and the receiver is a photon signal at 1570 nm, multiplexed on the same fiber. The wavelength of the quantum signal is 1310 nm.

6.1 Description of the QKD system

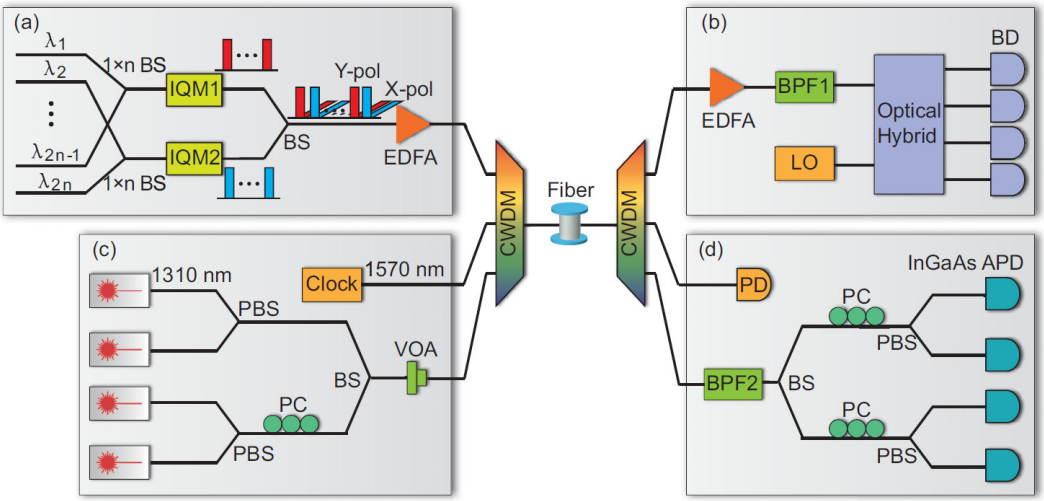

Figure 6.1: Experimental setup. (a) and (b) are the classic transmitter and receiver, respectively. (c) and (d) form the quantum sub-system [116].

The system is depicted in Figure 6.1, where the elements (c) and (d) represent the QKD sub-system.
Starting from the Alice transmitter, the four nonorthogonal states are generated by four different laser sources. Their light is properly polarized using the polarizing beam splitters, obtaining Horizontal or Vertical states. The light coming from the two lower lasers passes through a Pockels cell in order to generate Antidiagonal or Diagonal states. Then the light coming from these two optical paths is combined in the same path using a beam splitter.
Then, the intensity of the light pulse is adjusted using a Variable Optical Attenuator (VOA).
In Bob's side, a 100 GHz bandpass filter at 1310 nm is used in order to suppress the noise added by the classical communication, in particular caused by Raman scattering. In fact the photon-phonon interaction can cause the change in wavelength of the classical photons. The photon can be de-excited or excited during the interaction with the material; de-excited when it loses energy generating a phonon (Stokes event), excited when it absorbs a phonon (Anti-stokes event). Scattering with acoustic phonons (Brillouin scattering) is negligible because they have small energy, while interactions with optical phonons (Raman scattering) can cause wavelength shifts in the order of 100 nm at 1550 nm [117]. As a result photons used for classical communication can interfere with quantum communication.
The measurement basis is randomly selected by a 50:50 beam splitter. If the "single-photon" goes to the upper detectors it is measured in the {H,V}, while, if it goes to the other two, it is measured in {A,D} basis.
The polarization controllers are used to compensate the state of polarization, altered by imperfections or by the fiber.
The InGaAs/InP SPADs have an efficiency of 10% and a dark count probability of 1×10^{-6} in a gate-ON cycle. The dead time of the detector is set to 200 ns, when a detection event occurs, in order to reduce the afterpulsing probability.
The decoy state method is employed with the purpose of increasing the security of the communication; Alice sends signal states, weak-decoy states, and vacuum states with a ratio of 6:1:1. The average photon number of signal and weak-decoy states are 0.6 and 0.2, respectively.

6.2 MATLAB simulation

In order to simulate this QKD system, the following components have been selected and inserted in the "library" of components:

- the "PCBS-OC" from "Spectral Products";
- the 5 mm, 1100-1620 nm, 50/50, Non-Polarizing Cube Beamsplitter from "Edmund Optics";
- the "DPZ-8-IM": 8 mm, half-wave-Pockels cell, with an activation voltage of 3200 V, from "Qioptiq".

The researches, as always, do not mention the used components so this simulation can give only an estimation of the parameters of the QKD system, and not exact results.
The attenuation of the VOA is choosen in order to obtain the signal and decoy states mean photon number required. The attenuation of the filter at Bob's side is fixed at -0.5 dB, as indicated in the paper.

The structure is described component after component in the MATLAB script. First of all, the laser states (path_A, path_B, path_C, path_D) are initialized, as also the vacuum state.
Then the Alice's subsystem is described as follows:

```
%_______ALICE TRANSMITTER_________
if strcmp(Laser_ON,'A')
    path_1=P_beamsplitter_known(path_A,vac,PBS_name);
    path_2=vac;
elseif strcmp(Laser_ON,'B')
    path_1=P_beamsplitter_known(vac,path_B,PBS_name);
    path_2=vac;
end

if strcmp(Laser_ON,'C')
    path_2=P_beamsplitter_known(path_C,vac,PBS_name);
    path_1=vac;
```

```
elseif strcmp(Laser_ON,'D')
    path_2=P_beamsplitter_known(vac,path_D,PBS_name);
    path_1=vac;
end

%Pockels cell to pass in AV basis, always active (true)
path_2=pockels_cell_known(path_2,PC_name,-pi./8,true); %Passing from
%HV basis to AV;

[path_3,dis]=beamsplitter_known(path_1,path_2,BS_name);
%Variable optical attenuator VOA
disp('At Alice transmitter output the state is:')
path_3=10.^((-attenuation_VOA)./(20)).*path_3;
out_Alice=path_3;

%_____________________________________________
```

Depending on the qubit value the user wants to send, a different laser generates the light pulse. In the simulation it can be choosen using the variable "Laser_ON". Path_1 and path_2 are the combined light paths, output of the first two polarizing beamsplitters. Path_2 passes through a Pockels cell, necessary to transform horizontal or vertical light in antidiagonal or diagonal light. Then path_1 and path_2 are combined in path_3 using a beam splitter.
At the end of Alice's subsystem the VOA is used to have the desired mean photon number for signal and weak-decoy states. The rest of the system is described in a similar way.

6.3 Quantum bit error rate and secure key rate estimation

After having described the system in the MATLAB script, it is possible to calculate the parameters which define the efficiency of the system.

6.3.1 Quantum bit error rate

First, the quantum bit error rate (QBER) must be calculated because it is necessary to evaluate the secure key rate.

Before introducing the expression for the QBER, it is convenient to define some usefull concepts. First of all, the **yield** Y_i of a light pulse made by i-photons is the probability of detection at Bob's side, given that Alice sends an i-photon pulse [118]. When Alice sends a vacuum state, i.e. she does not send photons to Bob, the yield Y_0 is linked to dark counts, hence to the background noise (such as Raman noise in this case) and especially to the dark counts of the photon detectors. Now it is clearer why in section 4.3 SPAD detectors were extensively analysed and in section 4.4 a Verilog-A model for them was presented; their behaviour, and in particular primary dark counts and afterpulsing, which combined together give the total dark count rate, must be well known to design a QKD system. For a generic i-photon state, the yield is [118, 119]:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \cong Y_0 + \eta_i, \tag{6.1}$$

where η_i is the transmittance of the i-photon state, which is given by:

$$\eta_i = 1 - (1 - \eta)^i. \tag{6.2}$$

η is the overall transmittance, obtained considering the power attenuation caused by the quantum channel, the optical components at Bob's side and also the photon detection efficiency of the detector [116]. The overall transmittance for every optical path is easily obtainable in the MATLAB simulator: assuming Alice sends to Bob a photon vertically polarized, it is sufficient to make the ratio between the mean photons number reaching the correct detector and the mean photons number leaving Alice's apparatus, multiplied by the photon detection efficiency:

$$\eta = PDE \cdot \frac{\text{path\_det}(1)^2 + \text{path\_det}(2)^2}{\text{path\_Alice}(1)^2 + \text{path\_Alice}(2)^2} \tag{6.3}$$

where path_X^2 are the components of the state vector used to calculate the mean photons number in horizontal (1) and vertical (2) polarization states.

Returning to the QBER, its expression in BB84 QKD systems, widely used in literature [116, 118, 119], is the following one:

$$E_\mu = \frac{1}{Q_\mu}\left[e_{\text{vac}}Y_0 + e_{\text{opt}}\left(1 - Y_0\right)\left(1 - e^{-\eta\mu}\right)\right], \tag{6.4}$$

where:

- Q_μ: the probability of a detection event when Alice sends a signal state. It is also called signal gain, and it is equal to:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}, \tag{6.5}$$

  where μ is the signal mean photon number. In general, the aforesaid Y_0 can be easily obtained by the Verilog-A SPAD simulation, but, in this case, also the Raman noise contributes to Y_0. Not having information on the used detectors, Y_0 is assumed equal to 2.45×10^{-6}, considering the dark count probability per clock cycle of the used detector (equal to 1×10^{-6}) plus the Raman noise probability reported in the paper. The transmittance η is computed using the simulator;

- e_{vac}: the error rate of the background. Dealing with the BB84 protocol, it is usually considered completely random, consequently e_{vac} is assumed equal to 0.5 [118];

- e_{opt}: the probability that the photon hits the erroneous detector, due to a finite polarization contrast. It fixes the QBER at small communication lengths. In this system setup, it is mostly caused by the polarizing beam splitter.
  This parameter can be easily computed from the simulator; it is sufficient to divide the light intensity reaching the wrong detector by the total light intensity reaching the pair of detectors:

$$e_{\text{opt}} = \frac{\text{path\_inc}(1)^2 + \text{path\_inc}(2)^2}{\text{path\_cor}(1)^2 + \text{path\_cor}(2)^2 + \text{path\_inc}(1)^2 + \text{path\_inc}(2)^2}, \tag{6.6}$$

  where the subscripts "inc" and "cor" stay for incorrect and correct detectors,

respectively.

Unfortunately, no details are given regarding the optical components used; this parameter is obtained by the fit of the theoretical QBER plot shown in the paper, which gave $e_{\text{opt}} = 1.2$. In general this parameter is independent from the quantum channel length, and it ranges between 0.5 and 3.3 [118], therefore the fitted value is reasonable.

The comparison of simulated and experimental values is shown in Figure 6.2; the simulations slightly underestimate the experimental QBER. This discrepancy is attributable to the fact that the optical components used in this system are not mentioned. In particular the parameter e_{opt}, connected to the quality of the optical components used, strongly influence the QBER fixing its minimal value when the quantum channel length tends to zero.

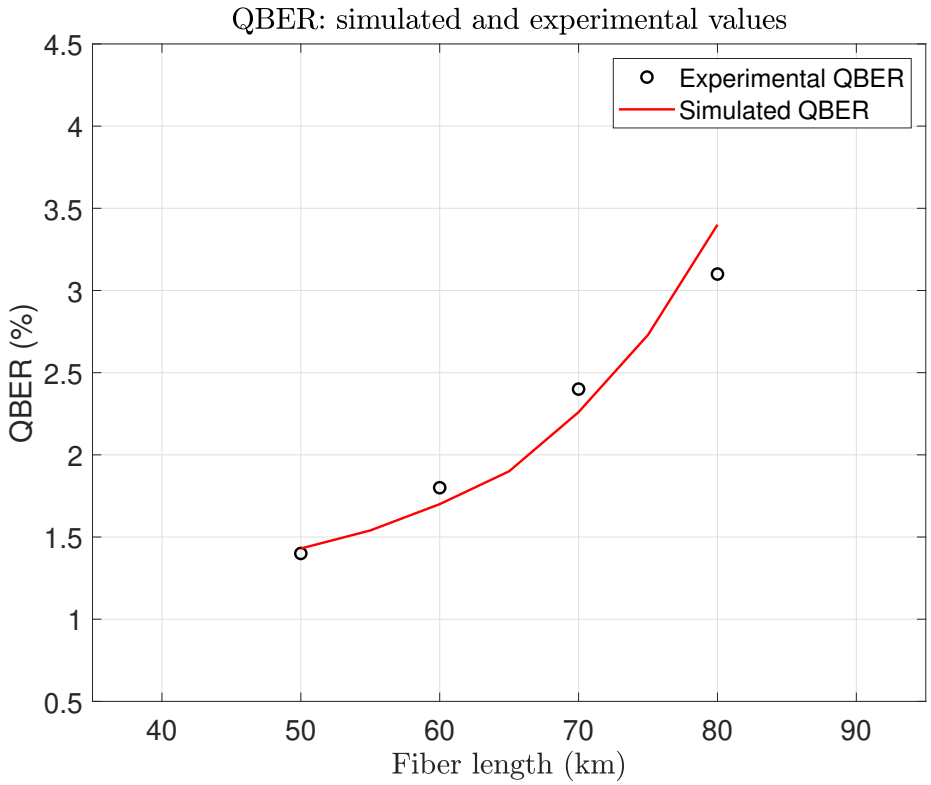

Figure 6.2: Comparison between the experimental QBER and the simulated values.

6.3.2 Secure key rate

The secure key rate per clock cycle in a BB84 protocol can be calculated as follows [23, 116, 120]:

$$R = q\left\{-Q_\mu f \cdot H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right] + Q_0\right\}. \tag{6.7}$$

The parameters in the formula are:

- q: is the probability that Alice emits a signal state (0.75) and Alice and Bob choose the same basis (0.5), so $q = 0.75 \times 0.5$;
- f: the inefficiency of the error correction, which is 1.25 in this system;
- H_2: the binary entropy function, equal to:

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{6.8}$$

- E_μ: the QBER of the system;
- Q_1 and Q_0: are the fraction of detection events that are due to single-photons or vacuum components of a signal state. Their values are calculated using Equation 6.5 and the simulated transmittance;
- e_1: the quantum error rate due to single photon. It can be estimated with the following formula:

$$e_i = \frac{e_{vac}Y_0 + e_{\text{opt}}\,\eta_i}{Y_i}. \tag{6.9}$$

The simulated Secure key rate is shown in Figure 6.3. The black dots are linked to the experimental values. The simulated curve, in red, tends to overestimate the key rate also because the previously calculated QBER was lower than the experimental one. Nevertheless, the trend is the same of experimental values; this proves the goodness of the model.

Considering the few information given by the researchers, the presence of Raman noise, and the simplifications introduced by this simulator, the results are still satisfactory. Probably, having a more detailed description of the system, better results would be obtained.

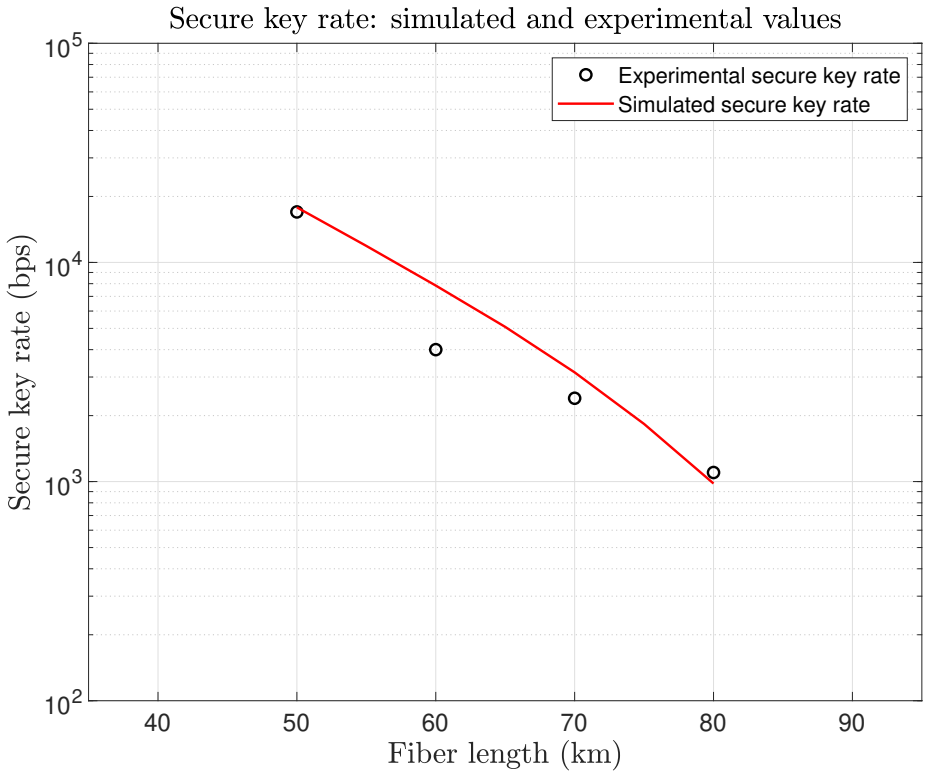

Figure 6.3: Comparison between the experimental secure key rate and the simulated values.

Conclusions and future perspectives

The work presented in this thesis represents a necessary starting point for the development of a simulation framework for Quantum Key Distribution systems based on polarization encoding.

The first stages of this work were related to the study of the fundamentals of quantum optics, which are partially presented in the first three chapters, required for the formalization of the theoretical model based on coherent states, that constitutes the basis of this simulator.

Considering a future perspective, this theoretical model should be evolved, abandoning the semi-classical approach in view of an effective quantum model. Obviously, this model is much more complicated but it allows to analyze all the types of QKD systems, including those based on entanglement or those where non-coherent light sources are going to be used. This evolved model would be based on the use of the **density matrix** formalism. For example, a generic phase-randomized coherent state can be represented as follows:

$$\hat{\rho} = \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} |\alpha\rangle \langle\alpha| = \sum_n \frac{\mathrm{e}^{-\mu}\mu^n}{n!} |n\rangle \langle n| , \tag{6.10}$$

where the single photon state $|n\rangle$ is a Fock state [121]. The use of the density matrix, also called **density operator**, is very useful because it allows to study also entangled systems, and, as a consequence, to rigorously analyze the interaction of photons with the environment [122].

The time evolution of the state, corresponding to the evolution of the density matrix, can be calculated according to the Von Neumann or Liouville equation [122, 123]:

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{\rho} = \frac{1}{i\hbar}\left[\hat{H}(t),\hat{\rho}\right], \tag{6.11}$$

where $\hat{H}(t)$ is the Hamiltonian of the system.
Another advantage of this formalism is that it permits to describe decoherence phenomena. This can be done with Kraus' operators M_i, which change the density matrix according to the following equation:

$$\hat{\rho}_{out} = \mathcal{E}(\hat{\rho}_{in}) = \sum_i \hat{M}_i \, \hat{\rho}_{in} \, \hat{M}_i^\dagger \,, \tag{6.12}$$

with $\sum_i \hat{M}_i \, \hat{M}_i^\dagger = \hat{I}$. In general, transformations can be studied with a **quantum channel** $\mathcal{E}$ that maps density operators to density operators by using a series of Kraus' operators [124].

After having defined the theoretical model, the matrix expressions for each optical component were investigated. For a given device, the study started from the analysis of its physical structure, in order to understand its operating mechanisms; then its Jones matrix was obtained. Finally, the losses were inserted into the model. Throughout these phases, MATLAB was steadily used, first to test the ideal model, and then to automate the computation of the propagated states, including losses.
Several MATLAB functions are currently available, one for each component analyzed in this thesis. Moreover, small libraries with some commercial components are included in the infrastructure. The user can use them to describe and simulate the QKD system as shown in chapter 5 and chapter 6. Obviously, the MATLAB simulator can be improved creating a user-friendly application with a graphical interface, currently missing, where the user can "draw" the optical system component after component. A ready to use solution would be to exploit the MATLAB-Simulink programming environment. Another upgrade of the simulator would consists in the inclusion of PMD effect, currently neglected, when the communication is performed on an optical fiber.

In a second phase, the optical detectors were analyzed, focusing on the SPAD, which are the most used detectors at present. First, the theoretical study was necessary to understand the functioning of these detectors and their unwanted effects like dark counts.
The development of the Verilog-A code was nontrivial, also because of the missing

experience with this particular hardware description language. As aforementioned, the simulation of afterpulses was the most complex part, due to the absence of clear data about the trap levels in InP and to the difficulty to schedule absorption and release of trapped carriers. The adoption of the afterpulse probability permitted to obtain simulation results compatible with the experimental ones.
In order to improve this Verilog code in future, one could modify the afterpulsing simulation, as already explained in section 4.4. Another secondary improvement would be the introduction of the timing jitter in the code. Moreover, it would be very useful to integrate the Verilog simulator into the MATLAB scripts in order to create a unified simulation tool.

In light of this, the simulation environment mapped out in this thesis can be improved and enlarged in order to gain in reliability and universality, so that it can simulate also future QKD systems. In fact, it is reasonable to expect a rapid evolution of quantum cryptography in the next years that will bring to the use of new protocols, modern optical devices, and certainly exotic light sources.

The more interesting and appropriate field of application for this simulator would be the free-air QKD based on polarization encoding. This types of quantum-cryptosystems are very promising because they are the basis for the satellite QKD. In fact, considering the "limited" communication distance reachable today with optical fibers (in the order of 200 km [19]), satellite QKD is the fastest way to establish a worldwide QKD infrastructure in the short term.

By the way, a simulator like the one proposed in this thesis, possibly integrated with a network simulator, would certainly ensure a huge advantage in designing new QKD systems.

Bibliography

[1] Tetsuo Ohmi Mikio Nakahara. *Quantum computing, from linear algebra to physical realizations*. CRC Press, 2008.

[2] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124â134. doi:10.1109/sfcs.1994.365700.*

[3] Michele Mosca. Cybersecurity in an era with quantum computers. will we be ready? *IEEE Security Privacy*, pages 38–41, September/October 2018.

[4] *https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption.*

[5] J. W. Harrington P. R. Rice N. Dallman K. T. Tyagi K. P. McCabe S. Nam B. Baek R.H. Hadfield R.J. Hughes D. rosenberg, C. G. Peterson and J.E. Nordholt. Practical long-distance quantum key distribution system using decoy levels. *New Journal of Physics*, pages 1–9, April 2009.

[6] Ivan B. Djordjevic and Yequn Zhang. Photon angular momentum based multidimensional quantum key distribution. *IEEE*, 2014.

[7] Marek LeÅniewicz Mariusz Borowski. Modern usage of âoldâ one-time pad. *IEEE, Military Communications and Information Systems Conference (MCC)*, October 2012.

[8] Mark Fox. *Quantum optics, an introduction.* Oxford.

[9] V. Buzzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *The American Physical Societ*, September 1996.

[10] Michael Danos and T.D. Kieu. Measurement in quantum physics.

[11] Michael Danos and T.D. Kieu. Quantum key distribution over 122 km of standard telecom fiber. *American Institute of Physics*, April 2014.

[12] Bang-Ying tang et al. High-speed and large-scale privacy amplification scheme for quantum key distribution. *Nature: scientific reports*, 2019.

[13] Yodai Watanabe. Privacy amplification for quantum key distribution. *J. Phys. A: Math. Theor. 40*, 2007.

[14] C. Marand and P. D. Townsend. Quantum key distribution over distances as long as 30 km. *Opt. Lett. 20*, 1995.

[15] O. Guinnard G. Ribordy H. Zbinden D. Stucki, N. Gisin. Quantum key distribution over 67 km with a plugplay system. *New Journal of Physics 4,41*, 2002.

[16] Z. L. Yuan C. Gobby and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Appl. Phys. Lett. 84, 3762*, 2004.

[17] D. Derkacs C. G. Peterson R. Hughes, J. E. Nordholt. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics 4, 43*, 2002.

[18] M. Halder Ph. M. Gorman P. R. Tapster J. G. Rarity H. Weinfurter C. Kurtsiefer, P. Zarda. Long-distance free space quantum cryptography. *Proceedings of SPIE Vol. 491*, 2002.

[19] Yang Liu et al. Decoy-state quantum key distribution with polarized photons over 200 km. *OPTICS EXPRESS 8587*, April 2010.

[20] Sheng-Kai Liao et al. Space-to-ground quantum key distribution using a small-sized payload on tiangong-2 space lab. *Chinese Phys. Lett. 34 090302*, 2017.

[21] Mohd Fared bin Abdul Khir et al. Implementation of two way free space quantum key distribution. *Optical Engineering*, August 2011.

[22] Lin-Mei Liang Wei-Tao Liu, Shi-Hai Sun and Jian-Min Yuan. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution. *American Physical Society*, 2011.

[23] Logan O. Mailloux, Michael R. Grimaila, Douglas D. Hodson, Ryan Engle, Colin McLaughlin, and Gerald Baumgartner. Modeling, simulation, and performance analysis of decoy state enabled quantum key distribution systems. *Appl. Sci. 2017, 7, 212. https://doi.org/10.3390/app7020212.*

[24] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *PhysRevLett.91.057901*, August 2003.

[25] J Fan JC Bienfang A Migdall, SV Polyakov. Single-photon generation and detection: physics and applications. *Academic press*, 2013.

[26] S.PÃ¡duab P.H.Souto Ribeiro S.P.Walborna, C.H.Monkenb. Spatial correlations in parametric down-conversion. *Physics Reports, https://doi.org/10.1016/j.physrep.2010.06.003.*

[27] Jean-Pierre Gazeau. *Coeherent States in Quantum Physiscs.* WILEY-VCH, 2009.

[28] Christopher C. Gerry and Peter L. Knight. *Introductory Quantum Optics*. CAMBRIDGE, 2005.

[29] Hans-A. Bachor and Timothy C. Ralph. *A Guide to Experiments in Quantum Optics*. WILEY-VCH Verlag GmbH Co. KGaA, Weinheim, 2004.

[30] Nicolas Wheeler. Harmonic oscillator-revisited: Coherent states. December 2012.

[31] Renato Orta. *Lecture notes on Electromagnetic Field Theory*. October 2017.

[32] R.Clark Jones. A new calculus for the treatment of optical systems. iv. *J.O.S.A.*, August 1942.

[33] G. Fowles. *Introduction to Modern Optics (2nd ed.)*. 1989.

[34] Petr KUCERA. Quantum description of optical devices used in interferometry. *RADIOENGINEERING, VOL. 16, NO. 3*, September 2007.

[35] Arpita Maitra and Suvra Sekhar Das. Generalized theoretical approach for analysing optical experiments. *arXiv:1905.01112v1 [quant-ph]*, May 2019.

[36] M. Curty et al. Passive preparation of bb84 signal states with coherent light. *Progress in informatics, No. 8*, 2011.

[37] N.I. Miklin M.V. Fedorov S.V. Vintskevich, D.A. Grigoriev. Passive preparation of bb84 signal states with coherent light. *arXiv:1812.11462v3 [quant-ph]*, May 2019.

[38] N.I. Miklin M.V. Fedorov S. V. Vintskevich, D.A. Grigoriev. Entanglement of multiphoton two-mode polarization fock states and of their superpositions. *arXiv:1812.11462v3*.

[39] S. Prasad et al. A quantum description of the beam splitter. *Optics communications - Elsevier*, May 1987.

[40] Youn-chang jeong et al 2014 laser phys. lett. 11 095201.

[41] A. muller et al 1996 epl 33 335.

[42] J chen et al 2009 new j. phys. 11 065004.

[43] J. C. Bienfang et al. Quantum key distribution with 1.25 gbps clock synchronization. *Optics express, Vol. 12 No. 9*, 2011.

[44] Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Barry Hershman, Joshua Bienfang, Ronald F. Boisvert, Charles Clark, and Carl Williams. High speed fiber-based quantum key distribution using polarization encoding. 5893:326 – 334, 2005.

[45] Sheng-kai liao et al 2017 chinese phys. lett. 34 090302.

[46] Eugene Hecht. *Optics, fourth edition*. Addison Wesley, 2002.

[47] *CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=760346*.

[48] https://www.rp-photonics.com/field_of_view.html.

[49] Natale C. Pistoni. Simplified approach to the jones calculus in retracing optical circuits. *Applied Optics Vol. 34, Issue 34*, pages 7870–7876, 1995.

[50] R. Loudon. *The Quantum Theory of Light*. Oxford University Press, 2000.

[51] G. Weihs and A. Zeilinger. Photon statistics at beam splitters: an essential tool in quantum information and teleportation.

[52] Polarization properties of prisms and reflectors, https://spie.org/samples/pm200.pdf.

[53] YA XIAO YUAN SHEN YONG-JIAN GU SHI-CHENG ZHAO, XIN-HONG HAN and WEN-DONG LI. Performance of underwater quantum key distribution with polarization encoding. *Journal of the Optical Society of America, Vol. 36, No. 5*, May 2019.

[54] J. P. Gordon and H. Kogelnik. Pmd fundamentals: Polarization mode dispersion in optical fibers. *PNAS, vol. 97 u no. 9*, page 4541â4550, April 2000.

[55] A. Duplinski et al. Low loss qkd optical scheme for fast polarization encoding. *Optical Society of America*, November 2017.

[56] *Corning SMF-28e, Optical Fiber Product Information*.

[57] A. Muller et al. Quantum cryptography over 23 km in installed under-lake telecom fibre. *EPL 33 335*, 1996.

[58] Yang Liu et al. Decoy-state quantum key distribution with polarized photons over 200 km. *OPTICS EXPRESS 8587, Vol. 18, No. 8*, April 2010.

[59] Xiao Tang Lijun Ma, Hai Xua. Polarization recovery and auto-compensation in quantum key distribution network. *Proc. of SPIE Vol. 6305 630513-1*.

[60] Lothar Moller. Wdm polarization controller in plc technology. *IEEE PHOTONICS TECHNOLOGY LETTERS, VOL. 13, NO. 6*, June 2001.

[61] Andrea Carena Dario Pilori, Mattia Cantono and Vittorio Curri. Ffss: The fast fiber simulator software. *IEEE*, 2017.

[62] Laszlo Bacsardi and Sandor Imre. Analyzing the quantum based satellite communications. *Procedia Computer Science Volume 7*, pages 256–257, 2011.

[63] *https://www.esa.int/Applications/Telecommunications_Integrated_Applications/European_quantum_communications_network_takes_shape*.

[64] D Elser et al. Feasibility of free space quantum key distribution with coherent polarization states. *New J. Phys. 11 045014*, 2009.

[65] Eric J. Korevaar Isaac I. Kim, Bruce McArthur. Comparison of laser beam-propagation at 785 nm and 1550 nm in fog and haze for optical wirelesscommunications. *Proc. SPIE 4214, Optical Wireless Communications III*, February 2001.

[66] Vaclav Kvicera Martin Grabner. Experimental study of atmospheric visibility and optical wave attenuation for free-space optics communications.

[67] P. F. Szajowski et al. 2.4 km free-space optical communication 1550 nm transmission link operating at 2.5 gb/s - experimental results. *SPIE Vol. 3532*, November 1998.

[68] Alberto Carrasco-Casado; Veronica Fernandez; Natalia Denisenko. *Optical Wireless Communications*. Springer, 2016.

[69] M. Khan M. T. Mushtaq R. Khan, R. W. Khattak. Analysis of optical attenuation from measured visibility data in islamabad, pakistan. *Mehran University Research Journal of Engineering and Technology, Mehran University of Engineering and Technology, Jamshoro, Pakistan*, pages 269–278, 2018.

[70] I. I. Kim et al. Measurement of scintillation and link margin for the terralink laser communication system. *SPIE Vol. 3232*.

[71] John Jeffers Stephen M. Barnett and Alessandra Gatti. Quantum optics of lossy beam splitters. *The American Physical Society*, March 1998.

[72] Robert H. Hadfield. single-photon detectors for optical quantum information applications. *Nature photonics — VOL 3*, December 2009.

[73] Quantum key distribution (qkd); component characterization: characterizing optical components for qkd systems. *ETSI GS QKD 011 V1.1.1*, May 2005.

[74] K. D. Irwin D. R. Schmidt D. S. Swetz, D. A. Bennett and J. N. Ullom. Current distribution and transition width in superconducting transition-edge sensors. *APPLIED PHYSICS LETTERS 101, 242603*, page http://dx.doi.org/10.1063/1.4771984, 2012.

[75] Joel N Ullom and Douglas A Bennett 2015. *Supercond. Sci. Technol. 28 084003*.

[76] Chandra M Natarajan et al 2012. *Supercond. Sci. Technol. 25 063001.*

[77] Andreas Bulter. Single-photon counting detectors for the visible range between 300 and 1,000 nm. *Springer Ser Fluoresc, doi: 10.1007/4243_2014_63*, 2014.

[78] A. Ruggeri C. Scarcella, G. Boso and A. Tosi. Ingaas/inp single-photon detector gated at 1.3 ghz with 1.5% afterpulsing. *IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 17-22*, May/June 2015, Art no. 3800306, doi: 10.1109/JSTQE.2014.2361790.

[79] Youn-Chang Jeong et al. An experimental comparison of bb84 and sarg04 quantum key distribution protocols. *Laser Phys. Lett. 11 095201*, 2014.

[80] Ma Lijun Mink Alan Nakassis Anastase Hershman Barry et al. Tang, Xiao. High speed fiber-based quantum key distribution using polarization encoding. *Proc. of SPIE Vol. 5893*, 2005.

[81] Mario Stipčevič, Daqing Wang, and Rupert Ursin. Characterization of a commercially available large area, high detection efficiency single-photon avalanche diode. *Journal of Lightwave Technology*, 31(23):3591–3596, 2013.

[82] H. Hofer M. Lopez and S. Kuck. Detection efficiency calibration of single-photon silicon avalanche photodiodes traceable using double attenuator technique. *Journal of Modern Optics, 62:20, 1732-1738, DOI: 10.1080/09500340.2015.1021724.*

[83] M. Sanzaro A. Tosi, N. Calandri and F. Acerbi. Low-noise, low-jitter, high detection efficiency ingaas/inp single-photon avalanche diode. *IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 20, NO. 6*, November/Decmber 2014.

[84] Lionel J. J. Tan Jo Shien Ng Andrey B. Krysa Kristian Groom John P. R. David Sergio Cova Michael J. Robertson Sara Pellegrin, Ryan E. Warburton and Gerald S. Buller. Design and performance of an ingaasâinp single-photon avalanche diode detector. *IEEE JOURNAL OF QUANTUM ELECTRONICS, VOL. 42, NO. 4*, April 2006.

[85] Hugo Zbinden Jun Zhang, Mark A Itzler and Jian-Wei Pan. Advances in ingaas/inp single-photon detector systems for quantum communication. *Light: Science Applications, doi:10.1038/lsa.2015.59*, 2015.

[86] Armin kolb et al 2010 phys. med. biol. 55 1815.

[87] R. Mita G. Giustolisi and G. Palumbo. Behavioral modeling of statistical

phenomena of single-photon avalanche diodes. *Int. J. Circ. Theor. Appl.*, page DOI: 10.1002/cta.748, 2011.

[88] Ding Li Yue Xu, Tingchen Zhao. An accurate behavioral model for single-photon avalanche diode statistical performance simulation. *Superlattices and Microstructures*, 2017.

[89] Junting Liu Sheng Xie and Fan Zhang. An accurate circuit model for the statistical behavior of inp/ingaas spad. *Electronics, doi:10.3390/electronics9122059*, December 2020.

[90] M. R. Islam A. G. Bhuiyan M. S. Alam, M. S. Rahman and M. Yamada. Refractive index, absorption coefficient, and photoelastic constant: Key parameters of ingaas material relevant to ingaas-based device performance. *IEEE*, 2007.

[91] Alberto Tosi, Sergio Cova, Franco Zappa, Mark A. Itzler, and Rafael Ben-Michael. Ingaas/inp single photon avalanche diode design and characterization. pages 335–338, 2006.

[92] Carmelo Scarcella, Gianluca Boso, Alessandro Ruggeri, and Alberto Tosi. Ingaas/inp single-photon detector gated at 1.3 ghz with 1.5% afterpulsing. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):17–22, 2015.

[93] R. Carmona-Galan J. M. Lopez-Martinez and A. Rodriguez-Vazquez. Photon-detection timing-jitter model in verilog-a.

[94] J. T. Teherani. Band-to-band tunneling in silicon diodes and tunnel transistors. June 2010.

[95] F. Zappa S. Cova M.A. Itzler X. Jiang A. Tosi, A. Dalla Mora. Ingaas/inp single-photon avalanche diodes show low dark counts and require moderate cooling. *SPIE OPTO: Integrated Optoelectronic Devices*, 2009.

[96] S. Johnston R. K. Ahrenkiel, R. Ellingson and M. Wanlass. Recombination lifetime of ingaas as a function of doping density. *Appl. Phys. Lett. 72, 3470*, 1998.

[97] Alexandre W. Walkera and Mike W. Denhoff. Heavy and light hole minority carriertransport properties in low-doped n-ingaaslattice matched to inp. *Applied Physics Letters, Volume 111, Issue 16*, August 2017.

[98] Yue Xu Hengjing Tang Xue Li HaiMei Gong Bo Shen Xuelin Yang Ping Han Xiaoli Ji, Baiqing Liu and Feng Yan. Deep-level traps induced dark currents

in extended wavelength inxga1âxas/inp photodetector. *Journal of Applied Physics 114, 224502*, 2013.

[99] Xudong Jiang, Mark A. Itzler, Rafael Ben-Michael, and Krystyna Slomkowski. Ingaaspâinp avalanche photodiodes for single photon detection. *IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 13, NO. 4*, JULY/AUGUST 2007.

[100] IEEE A . Lacaita Member IEEE Sergio Cova, Senior Member and G. Ripamonti. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE ELECTRON DEVICE LETTERS, VOL. 12, NO. 12.*, December 1991.

[101] Mingguo Liu; Chong Hu; Xiaogang Bai; Xiangyi Guo; Joe C. Campbell; Zhong Pan; Mark M. Tashima. High-performance ingaas/inp single-photon avalanche photodiode. *IEEE Journal of Selected Topics in Quantum Electronics (Volume: 13, Issue: 4, July-aug. 2007), DOI: 10.1109/JSTQE.2007.903855.*

[102] IEEE Xiaoqing Zheng Student Member IEEE Darek Palubiak Member IEEE M. Jamal Deen Fellow IEEE Zeng Cheng, Student Member and IEEE Hao Peng, Member. A comprehensive and accurate analytical spad model for circuit simulation. *IEEE TRANSACTIONS ON ELECTRON DEVICES*, April 2006.

[103] Ivan Rech Andrea Gallivanoni and Massimo Ghioni. Progress in quenching circuits for single photon avalanche diodes. *IEEE TRANSACTIONS ON NUCLEAR SCIENCE, VOL. 57, NO. 6*, December 2010.

[104] Joe C. Campbell Zhong Pan Mingguo Liu, Chong Hu and Mark M. Tashima. Reduce afterpulsing of single photon avalanche diodes using passive quenching with active resetmingguo liu, chong hu,. *IEEE JOURNAL OF QUANTUM ELECTRONICS, VOL. 44, NO. 5*, May 2008.

[105] A. Lacaita C. Samori S. Cova, M. Ghioni and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *APPLIED OPTICS @ Vol. 35, No. 12*, April 1996.

[106] Sergio Cova Carlo Samori Franco Zappa, Massimo Ghioni and Andrea Carlo Giudice. An integrated active-quenching circuit for single-photon avalanche diodesfra. *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 49, NO. 6*, December 2000.

[107] Verilog-a reference manual. *Agilent Technologies*, September 2004.

[108] Chong Hu et al. Mingguo Liu. High-performance ingaas/inp single-photon avalanche photodiode. *IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 13, NO. 4*, July/August 2007.

[109] F. Zappa S. Cova M.A. Itzler X. Jiang A. Tosi, A. Dalla Mora. Ingaas/inp single-photon avalanche diodes show low dark counts and require moderate cooling. *Proc. of SPIE Vol. 7222, 72221G.*

[110] https://www.rp-photonics.com/transmittance.html.

[111] Changho Hong Hee Su Park Youn-Chang Jeong, Se-Wan Ji and Jingak Jang. Deterministic secure quantum communication on the bb84 system. *Entropy 2020, 22, 1268; doi:10.3390/e22111268.*

[112] https://www.thorlabs.com/catalogpages/693.pdf.

[113] http://www.fastpulse.com/pdf/1147.pdf.

[114] http://52ebad10ee97eea25d5e-d7d40819259e7d3022d9ad53e3694148.r84.cf3.rackcdn.comuk_prc_ppc-polarizing-beamsplitter-cubes_ds.pdf.

[115] https://www.thorlabs.de/newgrouppage9.cfm?objectgroup_id=739.

[116] Wei Sun Yingqiu Mao Yi-Xiao Zhu Hua-Lei Yin Qing Chen Yong Zhao Fan Zhang Teng-Yun Chen Liu-Jun Wang, Kai-Heng Zou and Jian-Wei Pan. Long-distance copropagation of quantum key distribution and terabit classical optical data channels. *PHYSICAL REVIEW A 95, 012301*, page DOI: 10.1103/PhysRevA.95.012301, 2017.

[117] P Eraerds et al 2010. *New J. Phys. 12 063027.*

[118] Yi Zhao Xiongfeng Ma, Bing Qi and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *DOI: 10.1103/PhysRevA.72.012326.*

[119] Xiongfeng Ma, Chi-Hang Fred Fung, Frédéric Dupuis, Kai Chen, Kiyoshi Tamaki, and Hoi-Kwong Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *PHYSICAL REVIEW A 74, 032330 (2006)*, DOI: 10.1103/PhysRevA.74.032330.

[120] Sheng-kai liao et al 2017 chinese phys. lett. 34 090302.

[121] Feng-Yu LU Zhen-Qiang YIN Shuang WANG-Guang-Can GUO Guan-Jie FAN-YUAN, Wei CHEN and Zheng-Fu HAN. A universal simulating framework for quantum key distribution systems. *Science China Press and Springer-Verlag GmbH Germany, part of Springer Nature 2020, https://doi.org/10.1007/s11432-020-2886-x.*

[122] F Laloe-B Dui C Cohen-Tannoudji, B Diu. *Quantum Mechanics (2 vol. set).* WILEY-VCH, 2006.

[123] Petrosyan David Lambropoulos Peter. *Fundamentals of Quantum Optics and Quantum Information.* Springer.

[124] John Preskill. Physics/computer science 219 a at caltech: Quantum computation, lecture 4: Quantum channels, complete positivity, channel state duality.