Experimental study of the integration of continuous-variable quantum key distribution into a silicon photonics device

Mauro Persechino

NNT : 2017SACLO013

THESE DE DOCTORAT
DE L'UNIVERSITE PARIS-SACLAY

préparée à

L'INSTITUT D'OPTIQUE GRADUATE SCHOOL

ÉCOLE DOCTORALE N°572
Ondes et Matière (EDOM)

Spécialité de doctorat : Physique

par

Mauro PERSECHINO

Experimental study of the integration of continuous-variable quantum key distribution into a silicon photonics device

Thèse présentée et soutenue à Palaiseau, le 19 Décembre 2017

Composition du jury :

M Fabio Sciarrino	Rapporteur	Università "Sapienza", Rome
M Sébastien Tanzilli	Rapporteur	CNRS, LPMC, Nice
M Jean-François Roch	Président du jury	LPQM, Orsay
Mme Sara Ducci	Examinateur	LMPQ, Paris
M Laurent Vivien	Examinateur	C2N, Orsay
M Philippe Grangier	Directeur de thèse	IOGS, Palaiseau
Mme Eleni Diamanti	Co-Directeur de thèse	LiP6, UPMC, Paris

Acknowledgments

This work would not be possible without my supervisors Philippe Grangier and Eleni Diamanti, forming a complete leading team, helping me to carry out this thesis: I thank them for having accepted me as PhD student and finally led me to this goal. I will make treasure of the lessons I learnt from them, directly or indirectly thought, as Philippe's scientific rigour, Eleni's formidable spirit, both fundamental characteristic of a scientist. It has been thank to the combined efforts of the two of them that me and the experiment passed through the long days and weeks of disorientation, where there is apparently no clue to come out of the fog of inconsistent results. In this context Eleni always had the right words to motivate and Philippe the right idea to see some light in the dark.

This project has been developed in collaboration with the Silicon Photonics group at C2N, working closely with Delphine Marris-Morini, Laurent Vivien and Paul Crozat, who I want to thank for the incredible experience and knowledge he tried to share with me, while I was doing my best to catch every insights and hints he was giving me.

Despite half of the three PhD years I have spent alone in the lab, the other half I shared it with two amazing people. During my first months at the Institute I had the pleasure to work alongside with Melissa who, as a post-doc fellow, introduced me to the real world of the experimental research. Similarly I cannot forget the big help I received from Luis during the last year, for his professionalism, kindness and insight of the field...and because he can speak Italian! Having a partner in the lab with whom I could exchange doubts and ideas helped me to infinitely speed up, in terms of both results and deeper comprehension of the subject.

A very special thank goes to André Villing, always present, nice, irreplaceable presence at the Institut d'Optique (not only a magician of electronics).

The everyday life at work would have been horrible without the other guys of the lab: Imam, Martin, all the Quantum Optics group and the football team. I want to thank Sylvie Lebrun and Hervé Sauer for giving me the opportunity to teach as assistant in their TD classes. A special thank goes to the Institut d'Optique in all its members, from the administration people to the technicians.

Among the many things that one does during a PhD thesis, I also had the chance to be part of the organisation of the first YQIS conference in 2015. This is why I want to thank Antoine Browaeys, Sébastien Tanzilli, Thierry Lahaye and Alain Aspect for giving me this task, shared with my friend Martin Bouillard and the other

guys like Bruno and Djelan: it's been an amazing and enlightening experience.

Then I would like to thank all the jury members, in particular Fabio Sciarrino and Sébastien Tanzilli for having accepted to be referees for my thesis.

Concerning scientific texts, as a physics thesis is, it is peculiar how they could mean so much and be so full of emotions, since for its same reason to be, their words must hide the sweat and the joy, the excitement and the lack of motivation, the growth and steadiness, the start, the trip, the end (for a new start). All this moments are often related to someone or some place.

The start, the trip and the end are, without any doubt, my father Ivano, my mother Patrizia, my brother Pierdavide and my sisters Elisabetta and Sara, or in other words the higher expression of love I've experienced so far. I will never be as thankful as they deserve I should be. Along with them come the brothers and sisters in law which have increased the range of this love even further.

Here in France two families made me live this same atmosphere, even if my own family was in Rome: that is why I want to thank Clément and Maria an their Romain, Maxime and Agnès, along with Mathieu and Claire, with the little Charlotte and Antoine, for welcoming me in their families.

I thank the fate or whatever works in its stand for the friends I have, as brothers they are. I was 10 ten when I met Valerio, Paolo and Roberto: I will never forget the long talks and walks with Valerio from high school to present, never getting tired of sharing thoughts, laughs and knowledge. With Stefano and Lorenzo we enjoy life and share passions, playing music and being both stupid and deep in thoughts. When I came to France I found a real friend in Ben, who could be part of a very nice trio with the previous two guys: ir mat, frate! Then I had the sheer dumb luck to meet Luca, who is my companion of so many adventures and discoveries, whose friendship completely changed my life in France.

I want to thank TTC ("paga TTC!") and The Dark Side Of The Lun for the music and the fun. I could not avoid mentioning the football club I played with during the past two years, with special thanks to Ben, Clém and Thomas: allez TUVB! I should write an entire chapter on the only thing that really allows to breath some Roman air to people like me who are homesick of the most wonderful city in the world, Roma, Caput Mundi, so I will just scream a huge "Forza Roma" to thank the Roma Club Parigi (RcP) and every one of the crazy Romans, French, English (or whatever their nationality is) people supporting AS Roma in Paris. They probably think I've forgotten them, but one should know that nothing is possible without "le ragazze del XV", one can just love them all!

I finally need to thank AA for making me a better man through love and pain, Äme for teaching me that there is always the chance for a new start.

Contents

Acknowledgements iii

Table of contents v

List of Figures xi

List of Tables xiii

Introduction 1

I Theoretical and experimental tools for integrated CVQKD 5

1 Bits and qubits: classical and quantum information 7
1.1 Classical information theory . . . 7
1.1.1 What is *Information* . . . 7
1.1.2 Elements of Information Theory . . . 8
1.2 A brief summary of Quantum Mechanics . . . 12
1.2.1 The Quantum state: evolution and measurement . . . 13
1.2.2 Quantum mechanics postulates . . . 15
1.3 Quantum Information with qubits . . . 19
1.3.1 The Qubit and the Bloch sphere . . . 19
1.3.2 The quantum copying machine . . . 23
1.3.3 Von Neumann entropy . . . 23

2 Quantum optics with continuous variables 25
2.1 Quantum states of light for CV communication . . . 25
2.1.1 Single-mode quantum optics . . . 26
2.1.2 Phase-space representation of the e.m. field . . . 26
2.1.3 Gaussian states . . . 27
2.1.4 Examples of quantum states of light . . . 29
2.2 The homodyne detection . . . 34
2.2.1 The beam splitter . . . 34

2.2.2 Optical scheme of the homodyne detection . . . 38
2.2.3 Theoretical details . . . 38
2.2.4 Homodyne detection balancing . . . 40

3 Key Distribution and Quantum Continuous Variables 43
3.1 From classical to quantum cryptography . . . 43
3.1.1 First cryptographic protocols . . . 44
3.1.2 The one-time pad and the problem of the key . . . 46
3.2 QKD with Continuous Variable . . . 47
3.2.1 Quantum mechanics to solve the KD problem . . . 47
3.2.2 The first (DV) protocols . . . 48
3.2.3 Advantages of CV . . . 50
3.3 The GG02 protocol . . . 51
3.3.1 Information theory for Gaussian states . . . 51
3.3.2 The protocol: reverse reconciliation . . . 52
3.3.3 Excess noise and key extraction through noisy channels . . . 53

4 Introduction to Silicon Photonics 61
4.1 Main physical effects . . . 62
4.1.1 Pockels and Kerr effects . . . 62
4.1.2 Franz-Keldysh effect (FKE) and Quantum-confined Stark effect (QCSE) . . . 63
4.1.3 Plasma dispersion effect . . . 64
4.1.4 Thermo-optic effect . . . 64
4.2 Optical structures . . . 64
4.2.1 Waveguides . . . 65
4.2.2 Phase shifters . . . 65
4.2.3 Mach-Zehnder interferometer . . . 66
4.2.4 Multimode interference (MMI) couplers . . . 67
4.2.5 Grating couplers . . . 68
4.3 Electrical structures . . . 68

II On-chip integration of the GG02 protocol 73

5 Introduction to the experiments 75
5.1 Standard implementation of CVQKD protocols . . . 75
5.2 Basic requirements for integrated CVQKD . . . 77
5.2.1 Some conditions that need to be fulfilled . . . 77
5.2.2 Some design criteria . . . 78

6 All in one chip: a proof of principle for CVQKD 79
6.1 Overview . . . 80
6.1.1 Grating couplers . . . 81
6.1.2 Beam splitters or MMI . . . 82
6.1.3 Fast modulation devices . . . 82

6.1.4 Photodetectors . . . 85
6.2 Acquisition and control systems . . . 86
6.2.1 Electrical support for the silicon chip . . . 87
6.3 Electrical and optical approach . . . 91
6.3.1 From electrical probes to wire bonding . . . 91
6.3.2 Optical coupling . . . 92
6.4 A complete integrated CVQKD system . . . 93
6.4.1 Setup description . . . 94
6.4.2 Insertion losses and extinction ratios . . . 95
6.5 Standard homodyne detection calibration . . . 96
6.6 A new method for the detection calibration . . . 98
6.6.1 Phenomenological model for the OpSIS chip . . . 99
6.6.2 Shot Noise Limited slope . . . 102
6.7 Conclusion . . . 103

7 Separation of Alice and Bob for real communication 105
7.1 Overview and devices testing . . . 106
7.1.1 Grating couplers . . . 106
7.1.2 Beam splitters or MMI . . . 107
7.1.3 Fast modulation devices . . . 108
7.1.4 Slow Attenuation . . . 110
7.1.5 Photodetectors . . . 111
7.2 Calibration of the homodyne detection . . . 112
7.2.1 Overview . . . 112
7.2.2 Balanced homodyne fetection for SNL behavior . . . 112
7.2.3 Detection stability . . . 115
7.3 Integrated detection for hybrid GG02 . . . 115
7.3.1 Parameter evaluation . . . 117
7.3.2 Deviations from standard GG02 . . . 120
7.3.3 Measuring α, ξ, and ρ . . . 121
7.3.4 Value of the secret key rate . . . 125
7.3.5 Conclusion . . . 127
7.4 Work in progress . . . 128
7.4.1 Alice's modulation chip . . . 128
7.4.2 Bob 2.0: the Heterodyne detection . . . 129

III Conclusion 131

IV Appendices 135

A Quantum model of the detection and η evaluation 137

B Acquisition card (PCI and USB) 143
B.0.3 Triggering the system . . . 149

C Holevo's key rate 153

D The control software 157

Bibliography 161

V Abstract 165

Résumé 167

Abstract 170

List of Figures

1.1 Shannon binary entropy as a function of the probability p. 9
1.2 A qubit $|\psi\rangle$ represented in the Bloch sphere 20

2.1 The vacuum state and the coherent state in phase-space 31
2.2 Squeezed vacuum and squeezed coherent states in phase-space. . . . 33
2.3 The beam splitter schematic. 35
2.4 Quantum beam splitter schematic. 36
2.5 Optical scheme of the homodyne detection. 39
2.6 The homodyne detection measurement in phase-space. 41

3.1 Examples of ancient cryptographic systems. 44
3.2 The *Tabula Recta* used for the Vigenère cipher. 45

4.1 (a) Semiconductor band-gap structure at equilibrium and (b) FKE; (c) Quantum well band-gap structure and (d) QCSE [1]. 63
4.2 Different waveguide structures: (a) thin-film, (b) strip, (c) rib or ridge, (d) strip loaded and (e) buried strip waveguides [2] 65
4.3 MMI: (a) main structure and (b) self-image reproduction scheme [2]. 67
4.4 Star coupler-based beam splitter [2] 68
4.5 Grating coupler [2] 69
4.6 The PN junction [2] 69
4.7 The PIPIN structure [2] 70

5.1 Overview of the optical setup in bulk configuration. The different parts of the setup are discussed in the text. 76
5.2 The optical setup in the on-chip configuration. 78

6.1 OpSIS chip: overview of the design. 80
6.2 OpSIS chip: GC. On the left the coupling test structures with one input and one output. On the right the coupling structures for a CVQKD system: the light is split in two and a part is taken out to evaluate the coupling losses. 81
6.3 OpSIS chip: GC. IN/OUT transmission for different couplers on the same chip [3]. 82
6.4 OpSIS chip: directional couplers spectral analysis of the transmission 83

6.5 OpSIS chip: **(a)** PIN test structures. From top: 1.3mm MZI, 1.0mm MZI, 1.3mm phase shifter, 0.7mm phase shifter, 0.3mm phase shifter. **(b)** Induced phase shift vs. induced losses 84
6.6 OpSIS chip: 0.7mm phase shifter. Normalized transmission dependence on the (a) current and on the (b) voltage [3]. 84
6.7 OpSIS chip: test (a) 1.3mm MZI and (b) 1.0mm MZI. Normalized transmission vs applied current. 85
6.8 OpSIS chip: Photodiodes. The straight and dashed lines represent the two different photodiodes on the same chip. 86
6.9 Schematic of the acquisition and control system. The various parts are highlighted by arrow of different colours. 87
6.10 The multi-layer PCB support design. 87
6.11 Acquisition system: multi-layer PCB structure with fiber-attached chip. 88
6.12 The box for Alice's chip. 89
6.13 Details of the electronic circuit. 89
6.14 Electronics detail: photodiode's current extraction. 90
6.15 Electrical probes 91
6.16 CVQKD system: detail. 94
6.17 Electronic configuration of the photodiodes. 95
6.18 CVQKD system: losses scheme. 96
6.19 Electrical noise amplification circuit: scheme. 98
6.20 Spectral analysis: peak at 500kHz. From picture (a) to picture (b) we measure a $CMRR \simeq -52dB$. 98
6.21 AMod1: photocurrent (proportional to the transmission) vs the applied voltage. 101
6.22 VAT1: output voltage vs applied voltage. 101
6.23 VAT1: output voltage vs applied voltage when AMod 1 is attenuating. 102
6.24 OpSIS chip: SNL. 103
6.25 OpSIS chip: detectors. Study of the influence of photodiode bias voltage on the linearity. 104

7.1 LETI chip: overview. 106
7.2 LETI: coupling test 107
7.3 LETI chip: Phase shifter losses (in dB) vs injected current (in mA). 108
7.4 LETI chip: PIPIN MZI attenuation using arm 1(left) and arm 2 (right). 109
7.5 LETI: test structures for VOA. 110
7.6 LETI chip: Thermal MZI attenuation using arm 1(left) and arm 2 (right). 110
7.7 LETI chip: homodyne detection photodiode I-V curves depending on the input channel. The dark current I-V curve is plotted as well. 111
7.8 LETI chip: The homodyne detection 112
7.9 Unbalanced and balanced detection [4] 113
7.10 LETI chip: SNL slope 114

7.11 The optical configuration for the communication with the integrated LETI homodyne detection. 116
7.12 The scheme of a beam splitter with current losses in our system. . . 119
7.13 Normalized variance at Bob's versus the digital variance $\bar{V}_A$ generated by Alice. 122
7.14 Normalized variance at Bob's versus Alice's generated variance in SNU. 123
7.15 The correlations ρ versus Alice's generated variance in SNU. 124
7.16 Ξ versus Alice's generated variance in SNU. 125
7.17 Key rate in terms of bit/pulse and bit/sec vs. the losses in the channel. The distance that the communication can reach is evaluated for standard fibers connection (0.2 dB/km). The different curves are taken for different ξ values, while η is fixed. $\beta = 0.95$ for general LDPC codes under collective attacks. 126
7.18 Key rate in terms of bit/pulse and bit/sec vs. the losses in the channel. The distance that the communication can reach is evaluated for standard fibers connection (0.2 dB/km). The different curves are taken for different η values, while ξ is fixed. $\beta = 0.95$ for general LDPC codes under collective attacks. 127
7.19 Alice's modulation chip. 129
7.20 Bob's heterodyne detection chip. 130
7.21 SNL comparison between the two chip designs: OpSIS (left) vs LETI (right). 134

A.1 Model of the detection 137

B.1 FFT: frequency range 0-250 kHz 144
B.2 Noise of the card 145
B.3 Card + circuit (off) 145
B.4 FT noise analysis in working conditions (1): high frequencies 146
B.5 The teeth at f_{C1} andf_{C2} 147
B.6 Zoom in 147
B.7 FT noise analysis in working conditions (3): Noise of the card . . . 148
B.8 FT noise analysis in working conditions (3): Card + circuit (off) . . 149
B.9 Homodyne detection output seen by the two acquisition cards . . . 150
B.10 The triggering system. The delays are checked visually on the oscilloscope and measured with the control system 151
B.11 Bulk setup with the PCI card: the SNL slope (proportional to the gain) changes with the delay 151
B.12 LETI chip with USB card: the variance changes with the delay . . . 152

C.1 The GG02 protocol with an EPR source, with Alice, Bob and Eve [5] 154

D.1 The structure of a block of data. Above the voltage generated by Alice for the two modulators, below the corresponding homodyne output measured by Bob 159

List of Tables

3.1 Vigenère code: example. 45
3.2 *XOR* truth table. 47
3.3 Comparison between DV and CV. 50

6.1 Available complete systems listed by homodyne (HoD) or heterodyne (HeD) detection and by PIN or thermal + ring resonators (Th+r) based modulation. 93
6.2 Set of V_0 values for the signal attenuation 102

7.1 Photocurrents measured injecting classical light alternatively into one of the two BS inputs and respective transmission-to-reflection ratio considering two identical photodiodes. Channels refer to the scheme of figure A.1. 119
7.2 Alice's chip grating couplers purpose, numbered from left to right following figure 7.19b. 129

B.1 $\frac{q}{m}$ ratio vs. the trigger delay 152

Introduction

The ability to communicate is a hallmark of human or animal societal life. Nature provides many different levels and types of communication, and in any of them we can find a common structure: there is a *language*, an ensemble of different *words* and messages that have a specific meaning; these meanings must be implemented into something *physical* (a state) to be transmitted from one individual to another through a *channel*. The other individual, the receiver, must have the ability to read and comprehend (*detect and analyze*) the message sent to him. This scenario pictures the *how to communicate*.

Coming back to societal life, a specificity of humanity compared to the rest of the species is a very high level communication system. The natural selection process has continued also within human kind itself, leading to a hierarchical society system. Since ancient times it has been clear that knowledge and information were the basis of political and economical power: being informed about the situation before others puts in a position of advantage. So the abilities to elaborate sophisticated information and to share it are the building blocks of fast evolution.

When an important information is held by someone, two possibilities are opened to him: share it, to increase the knowledge of a friend party, or keep it secret, to take an advantage over an adversary. All sensitive data (where “sensitive" refers to data that must be kept secret) must be protected both when stored and when transmitted. For obvious reasons, politics and economics have been very strong incentives to find methods for safe communication. The first evidences of systems suitable for information encryption are more than 2000 years old: Greek and Romans came up with simple strategies, changing the orders of the letters or replacing them, following a predetermined strategy. Confidentiality was already important during these times, but now it has to be present everywhere: we live in the so-called *information era*, where secrecy is fundamental for the never-ending race for wealth and power, but also for simple individual privacy issues.

Taking into account what has been said about evolution, politics, economics and philosophy, and the many different points of view involved, the subject of keeping and sharing secrets is not just important, it is also very interesting and fascinating. We are of course interested in exploring how these procedure can be studied and implemented from a scientific aspect, that lies in the structured mechanism of the list of action that the sender and the receiver should have done to encrypt and decrypt the message.

The branch of science that studies the procedures (protocols) to perform to hide (encrypt) a message is called *Cryptography*. Cryptography is only a part of the bigger field of *Information and Communication Theory*. Despite a long history, cryptography has rapidly evolved only from the 20th century, when it has been approached scientifically for the first time. It must be clarified that cryptography studies how to communicate safely, but it also how to break this security i.e. the art of eavesdropping. These two sides of the same coin evolve together: if a protocol is thought (or demonstrated) to be not breakable by any known eavesdropping strategy, any imperfection in the implementation of such protocol opens the way to eavesdropping. In this critical scenario where the reality of the world shift the balance towards the eavesdropping, quantum mechanics plays a fundamental role: it can be demonstrated that if part of the communication is performed using quantum states, the protocol cannot be broken by any eavesdropping strategy, constrained only the laws of physics. Thereby *quantum cryptography* surpasses classical cryptography and gives us the chance to access safe communication.

More precisely, Alice, the sender, and Bob, the receiver, can communicate safely by using quantum states for exchanging a *secret key*, to be used later for encryption/decryption of the message: this is known as Quantum Key Distribution, or QKD. The rules of quantum physics, such as the *no-cloning theorem* discussed later on, allow them to detect the presence of an eavesdropper, Eve, and determine if the amount of knowledge she can extract is enough to reconstruct the key. When this is not the case, Alice and Bob share a totally secret key and can use it to encrypt (Alice) and decrypt (Bob) the actual message.

Several kinds of quantum states and encoding of the key can be used to this purpose. They can be regrouped in two main categories, based on the detection scheme rather than on the quantum states themselves. If detectors for single quanta (photon counters) are used, one speaks about *discrete variable quantum key distribution* (DVQKD). If coherent detectors are used (homodyne or heterodyne detection) one speaks about *continuous variable quantum key distribution* (CVQKD). Both DV and CV QKD systems already exist on the market, and this work will focus on CVQKD, that has the important advantage of avoiding the use of photon counters.

To introduce further the present work, another very important aspect of modern technology is *miniaturization*. A smaller device has less consumption of both energy and space and it is consequently much more efficient and, sometimes, less expensive. Electronics and computers have successfully stepped into this process, and integrated circuits have already reached nano-scale dimensions. Optics embarked on the same journey, and the first step was to create so-called *fibered* devices. Optical elements were not made by blocks of crystals anymore, macroscopic pieces of materials with particular optical properties: the same functionalities could be obtained by smaller systems embedded in an optical fiber-like device. One further step, crucial for the present work, is to miniaturize the devices into something comparable to the electronics miniaturization, so that both optics and electronics could work together. The advantage would be huge: the small dimensions (and consumption and costs) will be coupled with the higher speed of light communication, with respect to the electrical streams of data.

The aim of this thesis is to implement CVQKD protocols based on integrated optical circuits, made using silicon photonics elements. The advantage of such devices is that they properly work at room temperature and they are able to satisfy all requirements needed for CVQKD, as it will be explained below. We want therefore to demonstrate that this technology is in principle ready to be chosen as the basis for CVQKD integration.

The work is divided in two parts: in the first one we will present some theoretical and experimental basic tools needed for this work, ranging from a theoretical introduction about quantum cryptography, to basic facts about silicon photonics. The second part is focused on the experiments that we have carried out, including the procedures and results. More precisely, the contents of the chapters is as follows:

Part I The first part gives an overview of the background to the experimental work carried out for this thesis. Presentations of the quantum communication part and the silicon photonics part are included in this general overview.

Ch.1 In the first chapter an introduction of quantum mechanics and quantum information is given. Since quantum information theory developed from information theory and quantum mechanics combined together, in this chapter it will be introduced in the same way.

Ch.2 The second chapter is about quantum optics, focusing on the continuous variable approach. The phase space representation of the electromagnetic field and Gaussian states are introduced, and we discuss in detail the homodyne detection, that is fundamental to CVQKD.

Ch.3 Chapter 3 starts with an historical introduction to quantum cryptography and arrives to CVQKD as a natural evolution. In this section it will be stressed why quantum mechanics is fundamental for completely secure communication, replacing classical theories.

Ch.4 The fourth chapter, last of first part, is a brief introduction to silicon photonics. The main properties of integrated devices are exposed, based on the typical physical effects taking place into such systems.

Part II The second part treats the experimental work.It starts from an introduction of the general experimental implementation of the protocol and the it gets into the details of the actual on-chip implementation

Ch.5 This chapter gives an introduction about the experimental implementations of our CVQKD protocol, along with a general idea of how to perform the on-chip implementation.

Ch.6 The first approach is to build a simple proof-of-principle chip, reproducing an already working “bulk" optical setup onto the photonic circuit, with Alice and Bob onto the same physical support. This coexistence was meant to

make the implementation easier, since the communication channel and the distortions it induces are absent. On the other hand different properties and interactions arise, highlighting fundamental differences between the bulk and the integrated system. An overview on technical details about the optical and electrical access to the silicon photonics circuit is also given.

Ch.7 The difficulties encountered in the previous chapter lead us to use another architecture for a second chip generation. Differently from the all-in-one chip approach for a proof-of-principle experiment, the second chip is designed to work with two physically separated parties for Alice and Bob. The new conception and manufacturing allowed us to overcome some of the fundamental constraints we run into using the previous generation, and to increase the efficacy of the communication and giving us the possibility of a key extraction, even though for quite low key rates and distances.

Part I

Theoretical and experimental tools for integrated CVQKD

Chapter 1

Bits and qubits: classical and quantum information

In this chapter we shall define *communication* and *information*, on the basis that communication is the interaction designed to transfer information from the sender, who already knows, to the receiver, who in principle does not know yet. To do that, we first have to define and then quantify the concept of information; this is done in the first section of this chapter. Then in the second section we will briefly remind some basic features of quantum mechanics, useful for our purpose. Finally the third and last part of the chapter will show how information theory and quantum mechanics brought together can give birth to *Quantum Information Theory*.

1.1 Classical information theory

1.1.1 What is *Information*

We can identify the beginning of the study of information and communication as **sciences** with the famous paper of C.E. Shannon "A mathematical theory of communication" [6]. Following Shannon, we define an alphabet, a word and a language.

Definition 1.1. A finite, non-empty ensemble of symbols Λ is called *alphabet*.

Example 1.2. The binary alphabet is $\Lambda_{bin} = \{0, 1\}$, composed by two symbols.

Definition 1.3. Given an alphabet Λ, a *word* is a string x made of symbols of the alphabet.

Example 1.4. Using Latin alphabet with Arabic numerals, examples of words can be *Roma* or $er'gkj!\,g$ or 01010010011011110110110101100001.

Definition 1.5. An ensemble L of words created from an alphabet is called *language*.

At this stage the meaning (semantic) and the appearance and shape (morphology) of a word are not connected. The second word in example 1.4 has no meaning in any spoken language; on the other hand the string of numbers presented above can be translated using the ASCII code into the Latin word *Roma*.

Now we are ready to define information. Let us picture a standard communication scenario: Alice (say A) sends a message to Bob (say B) who, receiving the message, increases his knowledge. The knowledge (or information) gained by Bob is strictly related to his own ignorance about the message before getting it. It means that the quantification of Bob's lack of information about the message quantifies the amount of information that he would gain from it as well. Let us try with an example. If a person's vocabulary comprehends just one word and everybody knows that he can speak only that, the question is: how much ignorance we have about the message coming from him? How much information do we gain by receiving the message? The answer to these two questions is always zero.

So to describe information carried by a message we look for a quantity that depends on the probability to receive this given message (i.e. measures our ignorance about the message). The appropriate quantity has been proposed by Shannon:

Definition 1.6. A language L created on an alphabet Λ is given. A is sending words to B. If $p(w)$ is the probability with which Bob receives the word w, then the **information** associated to this word is

$$I(w) = -\log_2 p(w) \tag{1.1}$$

and

- it depends only on p, not on the specific choice of symbols of the alphabet;
- it is additive for independent events: $I(w_1 w_2) = I(w_1) + I(w_2)$;
- it is a smooth and infinitely derivable function.

From the definition above we see that we have some information in a message if the language has at least two words, otherwise a single word language will always produce the same word with probability 1, carrying zero information. This language can be reduced to the binary alphabet of example 1.2 from which we can extract the simplest and basic quantity of information, the bit, defined as follows.

Definition 1.7. The simplest unknown event has 2 possible equiprobable outcomes, known in literature as *0* and *1*. The occurrence of one of the two outcomes gives a BIT of information, where **BIT** stands for *B*inary digi*IT*.

For example the tossing of a coin can be resolved by assigning 0 to heads and 1 to tails. The tossing result will give a bit of information.

Extending the definition above, the word *bit* has also assumed the meaning of *letter of the dichotomic alphabet*: a bit can be one of the symbols *(0,1)* and the information the letter carries within itself.

1.1.2 Elements of Information Theory

Equation 1.1 is the starting point of all information theory, for both the classical and the quantum approach. We can now generalize it, and then introduce other very important notions as channel, noise, error and coding.

1.1.2.1 Shannon Entropy

We just saw what is the information related to a given word. Let us picture a more general scenario: we have an alphabet of n letters a_i and we look at the probability of the single letter to be sent. We call this probability $p(a_i)$. The average information that we can gain during the communication is known as *Shannon Entropy* and it is obviously related to the previous definition of information:

Definition 1.8 (Shannon Entropy). An alphabet $\Lambda = \{a_i\}_{i=1}^n$ is given. The *average information* or *Shannon Entropy* is

$$H(x) = -\sum_{i=1}^{n} p(a_i)\ \log_2 p(a_i) \tag{1.2}$$

A fundamental example is the *Shannon* ***binary*** *entropy* (figure 1.1), the entropy related to the dichotomic alphabet, i.e. the communication with bits of information. Assuming that 0 occurs with probability p, it is

$$H_2(x) = -p\ \log_2 p - (1-p)\ \log_2(1-p) \tag{1.3}$$

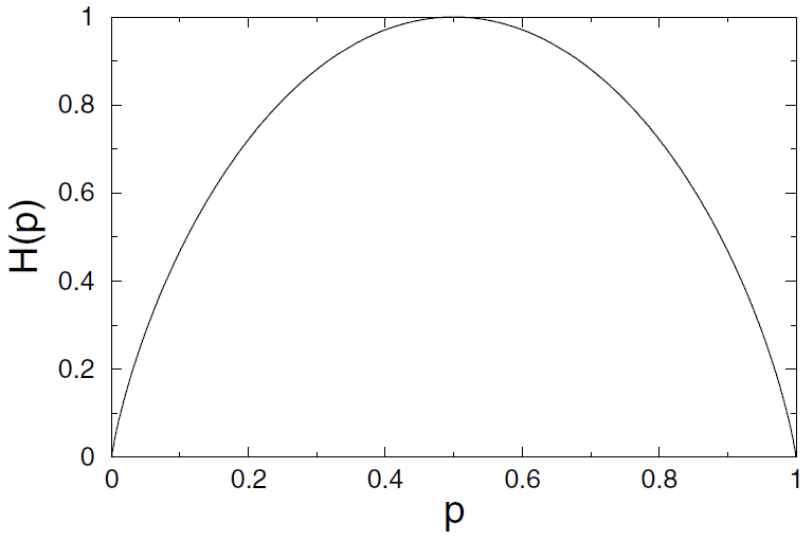


Figure 1.1: Shannon binary entropy as a function of the probability p.

We can deduce different interesting characteristics of this important quantity:

- $H = 0$ iff all the $p_i = 0$ but one, which is $p^\star = 1$. This corresponds to the example discussed in the previous section in which the same word is always used, so we have complete knowledge of the message before it has been sent;
- for a n-letter alphabet, $H = \log_2 n$ is the maximum value that the entropy can have and it corresponds to equiprobable letters, i.e. $p_i = \frac{1}{n}$. This is also quite

intuitive: if we have no clue about the next letter coming, since every letter has the same appearance probability, there is no scenario in which we are less ignorant (or uncertain) about the content of the message, so we gain the maximum information. Doing some easy calculations we obtain the relation

$$0 \leq H \leq \log_2 n; \tag{1.4}$$

- given two events a and b, respectively with m and n possibilities for which the joint probability of the i-th case for the first event and j-th for the second is $p(i,j)$, the entropy of the joint event, called the **joint entropy**, is

$$H(a,b) = -\sum_{i,j} p(i,j)\ \log_2 p(i,j). \tag{1.5}$$

Then the entropy of the event a is

$$H(a) = -\sum_{i,j} p(i,j) \log_2 \sum_{j'} p(i,j'). \tag{1.6}$$

and the entropy of b follows the same rule, but the second sum is performed over the index i' of the event a. It follows that

$$H(a,b) \leq H(a) + H(b); \tag{1.7}$$

In the same situation we define the **conditional entropy** of b

$$H(b|a) = -\sum_{i,j} p(i,j)\ \log_2 p(j|i) \tag{1.8}$$

where $p(j|i) = p(i,j)/\sum_{j'} p(i,j')$ is the conditional probability if j when i. Then

$$H(b|a) = H(a,b) - H(a) \quad or \quad H(a,b) = H(b|a) + H(a). \tag{1.9}$$

But the most important quantity we can derive from Shannon entropy is given by:

Definition 1.9 (Mutual Information). The quantity

$$I(a,b) = H(a:b) = H(a) - H(a|b) = H(b) - H(b|a) = H(a) + H(b) - H(a,b) \tag{1.10}$$

which evaluates the amount of information shared by a and b. Since $H(a,b)$ is symmetric, one also has $I(a,b) = I(b,a)$.

From now on, if not specified, we assume that the alphabet we are using is the binary alphabet $\Lambda_{bin} = \{0, 1\}$. Moreover since the logarithms are all written in base 2, the expression $\log_2$ will be replaced by log if not differently specified.

1.1.2.2 Channels and noise

A channel is defined as the medium through which the encoded information is sent (air, wires, etc.). In general every channel is subject to some noise. When the sent signal is different from the received one it means that it suffered a perturbation. We can distinguish two different kinds of perturbations:

- when every sent message undergoes the same transformation, this transformation is called *distortion*. If an inverse function exists we can apply it to retrieve the undisturbed signal;
- when the action of the channel is not predictable, it is called *noise*. The received message is a function of the input signal S and the noise N.

For transmission through a channel, the previous entropies $H(a)$ and $H(b)$ can be respectively associated with the sent and received data. Following this idea the rate of actual transmission, R, would be obtained by subtracting from the rate of production (i.e., the entropy of the source $H(a)$) the average rate of conditional entropy $H(a|b)$, which measures the average ambiguity of the received signal:

$$R = H(a) - H(a|b)$$

and thus it identifies with the mutual information as defined above. Then the capacity C of a noisy channel is defined as

$$C = Max[H(a) - H(a|b)] = Max[I(a : b)]$$

where a is the input and b the output. The maximization is over all possible information sources that might be used as input to the channel.

Quoting Shannon, "it may seem surprising that we should define a definite capacity C for a noisy channel since we can never send certain information in such a case. It is clear, however, that by sending the information in a redundant form (*this is known as "encoding"*) the probability of errors can be reduced. For example, by repeating the message many times and by a statistical study of the different received versions of the message the probability of errors could be made very small. One would expect, however, that to make this probability of errors approach zero, the redundancy of the encoding must increase indefinitely, and the rate of transmission therefore approach zero. **This is by no means true**. If it were, there would not be a very well defined capacity, but only a capacity for a given frequency of errors; the capacity going down as the error requirements are made more stringent. Actually the capacity C defined above has a very definite significance. It is possible to send

information at the rate C through the channel with as small a frequency of errors as desired by proper encoding. This statement is not true for any rate greater than C. Nature takes payment by requiring just that much uncertainty, so that we are not actually getting any more than C through correctly". This major insight leads to Shannon's fundamental theorem for a discrete channel with noise:

Theorem 1.10 (Noisy channel coding theorem). *Let a discrete channel have the capacity C and a discrete source the entropy per second H. If $H \leq C$ there exists a coding system such that the output of the source can be transmitted over the channel with an arbitrarily small frequency of errors. If $H > C$ there is no method of encoding which gives a value of the conditional entropy $H(a|b)$ smaller than $H - C$, so there are always errors in arbitrarily long messages.*

Notice that the theorem 1.10 does not specify how to encode the data, but only tells that under the right circumstances errorless encoding is possible. Finding efficient codes able to correct errors as close as possible to Shannon's capacity limit is a fundamental problem in coding theory, and as we will show it also plays a crucial role in the quantum cryptography protocols we will consider in the next chapters.

1.2 A brief summary of Quantum Mechanics

In this section we will highlight the most relevant features of Quantum Mechanics, for applications in Quantum Information and Quantum Cryptography. After a brief historical introduction to Quantum Mechanics, we will present how to define a quantum state, how to interact with it and measure it to extract information.

1.2.0.3 Historical introduction

Historically the first paper on Quantum Mechanics is *On the theory of the energy distribution law of the normal spectrum* by Max Planck in 1901 [7], in which the author explains that, to justify the finite amount of radiation energy of a black body, the energy must be discrete and not continuous as suggested by classical mechanics. This discretization is made by *quanta* of energy $h\nu$ where ν is the frequency of the radiation and $h = 6.62607004 \times 10^{-34} m^2 kg/s$ is the *Planck constant*.

A **quantum system** is a physical system described by quantum mechanics in terms of definition, evolution and measurement. The description of such a system is called its **quantum state**. The evolution in time of the quantum state can be calculated, and the results of any measurement performed on the system can be predicted. However quantum mechanics is *non-deterministic*, meaning that the theory cannot uniquely predict the evolution of the system into a single result, but it gives the probability distribution of the outcomes of a measurement.

1.2.1 The Quantum state: evolution and measurement

1.2.1.1 Quantum state

A physical quantum system is fully described by its quantum state, which can be either a **pure state** or a **mixed state**. A pure state is represented by a (normalized) vector in a Hilbert space, whereas a mixed state is defined as follows.

Definition 1.11. A **pure state** $|\psi\rangle$ is a *coherent superposition* of states living in the Hilbert space dedicated to the system. It can be written as

$$|\psi\rangle = \sum_{i=1}^{k} c_i |\alpha_i\rangle, \tag{1.11}$$

where the $\{|\alpha_i\rangle\}$ are a basis of the Hilbert space, and the complex numbers c_i are *quantum probability amplitudes*, with $\sum_{i=1}^{k} |c_i|^2 = 1$. The notion of superposition is the main feature that distinguishes a quantum state from a classical one.

Definition 1.12. A **mixed state** is the most general version of a quantum state, and it is described by a **density operator** $\hat{\rho}$:

$$\hat{\rho} = \sum_{k=1}^{l} p_k |\psi_k\rangle\langle\psi_k|, \tag{1.12}$$

where p_k are classical probabilities, and $|\psi_k\rangle\langle\psi_k|$ is the projector onto the pure state $|\psi_k\rangle$. The density operator is described by the **density matrix** with coefficients

$$\rho_{ij} = \langle i|\hat{\rho}|j\rangle \tag{1.13}$$

A pure state can be written as a density matrix 1.12 in which the only term in the sum is the projector on $|\psi\rangle$ with probability 1:

$$\hat{\rho} = |\psi\rangle\langle\psi| \tag{1.14}$$

The usual definition of the **trace operation Tr** on an operator $\hat{O}$ for a basis$\{|i\rangle\}$

$$Tr(\hat{O}) = \sum_{i} \langle i|\hat{O}|i\rangle. \tag{1.15}$$

allows us to easily distinguish between a pure and a mixed state, since it can be easily demonstrated that

$$Tr(\hat{\rho}^2) \begin{cases} = 1 & \rho \text{ is } pure \\ < 1 & \rho \text{ is } mixed \end{cases} \tag{1.16}$$

From now on the circumflex accent on operators will be omitted unless necessary to the comprehension of the text.

1.2.1.2 Evolution and measurement in Quantum Mechanics.

If in a pure state, a physical system S at a given time t is fully described by the vector $|\psi(t)\rangle$ living in the Hilbert space $\mathcal{H}_S$. Then one has to describe how this state changes in time, and this is governed by the

Definition 1.13. Time-dependent Shrödinger equation

$$\imath\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = H|\psi(t)\rangle, \tag{1.17}$$

where H is the *Hamiltonian* or *Energy operator* of the system.

If H does not depend on time, we can easily derive that

$$|\psi(t)\rangle = e^{-\imath\frac{Ht}{\hbar}}|\psi(0)\rangle = U|\psi(0)\rangle, \tag{1.18}$$

where $U = e^{-\imath\frac{Ht}{\hbar}}$ is the unitary **evolution operator**. The next important definition is about physical quantities, also called "observables", and one has:

Definition 1.14. An **observable** A is represented by a hermitian operator $\hat{A}$.

The eigenvalues of the operator are the possible outcomes of the measurement of the observable A. Since $\hat{A}$ is hermitian, its eigenvalues are real, and the set of eigenvectors is a basis of the Hilbert space, so any state can be written as a linear combination of these eigenvectors. Moreover, if $\{a_i\}$ and $\{|a_i\rangle\}$ are the eigenvalues and eigenvectors of A, with $\hat{A}|a_i\rangle = a_i|a_i\rangle$, then the observable is

$$\hat{A} = \sum_i a_i|a_i\rangle\langle a_i| \tag{1.19}$$

This is called the *spectral decomposition* of the operator. Finally one has:

Definition 1.15. Say that after performing $\hat{A}$ the result of the measurement is a particular a_n. The state, after the measurement, will change to

$$\frac{P_n|\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}}, \tag{1.20}$$

where P_n is the projector on the eigenspace associated with the eigenvalue a_n.

The **expectation value** (or mean value) of the operator will be

$$\langle A\rangle = \langle\psi|A|\psi\rangle = \langle\psi|\sum_i a_i P_i|\psi\rangle = \sum_i a_i\langle\psi|P_i|\psi\rangle \tag{1.21}$$

These notions can be extender from a pure state to the density matrix, as detailed below for the free time evolution and (projective) measurements.

Definition 1.16. Von Neumann equation

$$\imath\hbar\frac{d}{dt}\hat{\rho}(t) = [H, \hat{\rho}(t)]\,, \tag{1.22}$$

where the *time dependent density matrix* evolves as $\hat{\rho}(t) = U\hat{\rho}_0 U^\dagger$.

It can be easily demonstrated that the mean value of an operator is

$$\langle A\rangle = Tr(\rho A) = \sum_i \langle i|\rho A|i\rangle \tag{1.23}$$

and after a measurement the outcome n will be the result with a probability

$$p_n = Tr(\rho P_n). \tag{1.24}$$

If the state is $|\psi\rangle$ pure, it will collapse to $|\psi'\rangle$ seen in equation 1.20. If the initial state is ρ, knowing the result of the measurement, the final state will be

$$\rho_n = \frac{P_n \rho P_n}{Tr(\rho P_n)} \tag{1.25}$$

If the result is not known, then the final state will be a mixture of all the possible outputs weighted by their classical probabilities p_i

$$\rho_{out} = \sum_i p_i \rho_i. \tag{1.26}$$

1.2.2 Quantum mechanics postulates

We have seen in the previous section how differently a quantum state behaves (is created, evolves and is measured) with respect to a classical one. Still we want to understand how quantum mechanics can open new ways for processing information, in particular for quantum cryptography. For this purpose we will now discuss five important features of QM that are specific to the quantum world and cannot be experienced classically. The first and second ones, the *superposition principle* and *entanglement*, are relative to quantum states, whereas the other three apply to measurements: the *Heisenberg inequalities*, the *perturbation due to an action* on a quantum state and the *no-cloning theorem*, crucial for quantum cryptography.

1.2.2.1 The quantum superposition

Physically the superposition principle is related to interference, which also appears classically: it allows us to explain the interference of two light sources and to predict their combined light intensity distribution pattern knowing their properties.

From a quantum point of view we already said that a pure state $|\psi\rangle$ is a *coherent superposition* of states living in the Hilbert space dedicated to the system. This feature is related to the Shrödinger equation 1.17 which is a linear equation: if there are two different quantum states satisfying the equation, then any linear combination of them will be a solution as well.

A usual example of superposition is the spin state of an electron: the electron can have a spin up $|\uparrow\rangle$ or $|\downarrow\rangle$ (*up* or *down*), and the state $|\uparrow\rangle + |\downarrow\rangle$ is also acceptable. In fact if we can easily see the intensity peaks and deeps of an interference pattern it is more difficult to imagine that *something* can be *at the same time* in two orthogonal states. It is a a bit like looking right *and* left at the same time!

In quantum information this is crucial: one can consider a two-state system involving the bit states 0 and 1, properly encoded in the quantum state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.27}$$

giving rise to the concept of *qubit*, an arbitrary superposition of $|0\rangle$ and $|1\rangle$.

1.2.2.2 Entanglement

The entanglement is a completely quantum property of two or more systems. To explain entanglement we must first define the concept of *separability*.

Definition 1.17. The (pure) quantum state of a two-partite system is *separable* when it can be factorized into states for the two subsystems.

For example: suppose the systems $\mathcal{S}_1$ and $\mathcal{S}_2$ are in some state and the composite system is $\mathcal{S}_{12}$. The system is separable if the state $|\psi\rangle_{12}$ can be written as a tensor product of two states, one living completely in $\mathcal{H}_1$ and the other in $\mathcal{H}_2$:

$$|\psi\rangle_{12} = |\phi\rangle_1|\xi\rangle_2 \tag{1.28}$$

For example, if the first system can be in the state $\alpha|A\rangle_1 + \beta|B\rangle_1$ and the second system in the state $\gamma|C\rangle_2 + \delta|D\rangle_2$ then the state

$$|\psi\rangle_{12} = \alpha\gamma|A\rangle_1|C\rangle_2 + \alpha\delta|A\rangle_1|D\rangle_2 + \beta\gamma|B\rangle_1|C\rangle_2 + \beta\delta|B\rangle_1|D\rangle_2$$

for the joint system is obviously separable.

A pure state is **entangled** if it is not separable, and a simple example is

$$|\phi\rangle_{12} = |A\rangle_1|C\rangle_2 + |B\rangle_1|D\rangle_2 \tag{1.29}$$

It follows that, as soon as a measurement is performed on one subsystem, say the first, the second system will collapse on the state correlated to the measured one in the first system. Using the state $|\phi\rangle_{12}$ as an example, if the measurement on the system 1 gives the result a corresponding to the state $|A\rangle$, the system 2 will collapse instantaneously on the state $|C\rangle$ even if the systems are separated. The physical nature of these correlations between systems 1 and 2 have been matter of study since the early years of quantum mechanics, leading to two different approaches:

- the *hidden variable* idea, inspired by Einstein, Podolsky and Rosen [8] (*EPR*) who claimed that quantum mechanics is local, but incomplete: there are still-unknown (hidden) variables that will transform QM in a better theory;
- quantum mechanics as we know it, which is considered complete, and obeys relativistic causality, but has some non-local features.

A major progress was obtained by J.S. Bell [9]: assuming the existence of local hidden variable, he derived *Bell's inequalities* which contradict quantum mechanics. This opened an experimental way to decide between the two options above, and experimental work was launched to check whether nature agrees or not with these inequalities. In these attempts there are so-called *loopholes* to be avoided:

- the *locality loophole*, occurring if the choices of the measurements are not space-like separated. This requires that the distance between the two systems is large enough, and was first addressed by Alain Aspect and coworkers in the 1980's. The results were in perfect agreement with QM, and thus in contradiction with Bell's inequalities.
- the *detection loophole*, occurring if only a small fraction of the prepared systems are actually detected. This requires in particular very high detection efficiencies, and was first addressed with pairs of trapped ions, at the beginning of the 2000's. Again the results were in perfect agreement with QM, and in contradiction with Bell's inequalities.
- finally, closing these loopholes together, with some other ones such as the *memory loophole*. This was done by three different experiments in 2015, and one more in 2017, again in perfect agreement with QM.

A free online review (https://physics.aps.org/articles/v8/123) is presented by Alain Aspect in [10], entitled "Closing the Door on Einstein and Bohr's Quantum Debate". Quoting him, "by closing two loopholes at once, three experimental tests of Bell's inequalities remove the last doubts that we should renounce local realism. They also open the door to new quantum information technologies."

1.2.2.3 Heisenberg inequalities

In physics the precision with which a measurement can be performed plays a key role, and its evaluation lies at the heart of the scientific method. In classical physics, given an appropriate experimental setup and instrumentation, the measurement

error can be reduced under a given threshold $\varepsilon > 0$, for all relevant quantities. In QM this is no anymore the case: even if the measurement precision for any given physical quantity can be made as good as desired, the dispersion of results for all possible measurements for a given quantum state cannot be arbitrarily small.

This is related to the fact that quantum observables are described by operators, that do not always commute: for two operators $\hat{A}$ and $\hat{B}$, the commutator $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ can be non-zero. If two observables commute, they can be simultaneously given arbitrarily precise values, and are said to be *compatible*. Correspondingly, classical observables are always compatible. On the other hand, if two observables do not commute, the product of their dispersion for a given quantum state is bounded by the Heisenberg inequalities [11, 12]

$$\Delta\hat{A}\Delta\hat{B} \geq \frac{1}{2}|\langle[\hat{A}, \hat{B}]\rangle| \tag{1.30}$$

These inequalities have major consequences and we will discuss later the ones relevant for quantum cryptography.

1.2.2.4 Perturbative nature of quantum measurement

We have already seen in equation 1.20 that the state after a measurement is given from the initial one by a projection operator; this deeply changes the state, unless it is an eigenstate of the measured observable.

Correspondingly, measuring sequentially non-commuting observables will produce random results. For instance, measuring $\hat{A}$ with result a_n, then $\hat{B}$ with $[\hat{A}, \hat{B}] \neq 0$, then $\hat{A}$ again will generally not recover a_n again. We note that this scenario of sequential measurements is different from the Heisenberg inequalities discussed above, which deals with the dispersion of non-commuting observables, all measured on the same initial state. On the other hand, the two situations are related by the commutation rules, that play an essential role in both cases.

1.2.2.5 No-cloning Theorem

The *no-cloning theorem* [13] applies to the situation where we want to duplicate a state $|\psi\rangle$ onto an already existing state $|\phi\rangle$. The initial state is

$$|E\rangle \otimes |\psi\rangle \otimes |\phi\rangle, \tag{1.31}$$

where $|E\rangle$ describes the state of other systems, usually called "the environment". The cloning operator should be a unitary U such that the final state will be

$$U(|E\rangle \otimes |\psi\rangle \otimes |\phi\rangle) = |E\rangle \otimes |\psi\rangle \otimes |\psi\rangle. \tag{1.32}$$

It can be demonstrated by using either linearity or unitarity of QM that such an operator does not exist [13].

We emphasize that this theorem applies to a single sample of the input state. If many samples are available the state can be determined (this is called quantum tomography), and then reproduced. For instance, if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, one can perform a very large (in principle infinite) amount of measurements on many replicas to actually know them. This is probably the most important QM feature for cryptography: if an eavesdropper wants to clone a single sample, keeping a copy for her and sending out the other one, the output cannot be identical to the input. This can be detected by errors (or increased noise) in the communication, showing the presence of the eavesdropper. We will get into details in chapter 2.

1.3 Quantum Information with qubits

When information theory joins quantum mechanics, a new field of study is created: *quantum information*. In this section we will expose how the main properties that we found in the classical regime change in the quantum regime.

1.3.1 The Qubit and the Bloch sphere

Classically the information is stored into two separate states corresponding to the bit value 0 or 1. In the quantum world the information is stored in the **QUBIT** (*qu*antum *b*inary dig*it*), a two level system living in a Hilbert space $\mathtt{H}^2$. In this space we can choose the simplest orthonormal basis that is called the *computational basis*:

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.33}$$

Thanks to the superposition principle, the general form of a pure qubit is a coherent superposition of these two quantum states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.34}$$

As discussed before, if classically we can send a 0 *or* a 1, in the quantum regime we are able to send any superposition of them. The two probability amplitudes α and β completely characterize the qubit state and the phase relation between $|0\rangle$ and $|1\rangle$. The two coefficients obey the normalization relation

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.35}$$

A general qubit state can be represented by a density matrix

$$\hat{\rho} = \sum_{k=1}^{l} p_k |\psi_k\rangle\langle\psi_k| \tag{1.36}$$

as we discussed in equation 1.12. So a pure qubit state as well can be written this way with its matrix representation:

$$\hat{\rho} = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^\star \\ \alpha^\star\beta & |\beta|^2 \end{bmatrix} \tag{1.37}$$

The diagonal terms are the *populations* of the states $|0\rangle$ and $|1\rangle$, while the off-diagonal terms are the *coherences* and they are what makes a qubit a quantum state, since there is no corresponding in the classical world.

Since state vectors are defined up to a global face, we can also write equation 1.34 as

$$|\psi\rangle = cos\frac{\theta}{2}|0\rangle + e^{\imath\phi}sin\frac{\theta}{2}|1\rangle = \begin{bmatrix} cos\frac{\theta}{2} \\ \\ e^{\imath\phi}sin\frac{\theta}{2} \end{bmatrix} \tag{1.38}$$

with $0 \leq \theta < \pi$, $\quad 0 \leq \phi < 2\pi$.

1.3.1.1 The Bloch sphere

A qubit quantum state can be geometrically represented in the **Bloch sphere** (figure 1.2). The Bloch sphere has a radius $r = 1$. A general quantum state living

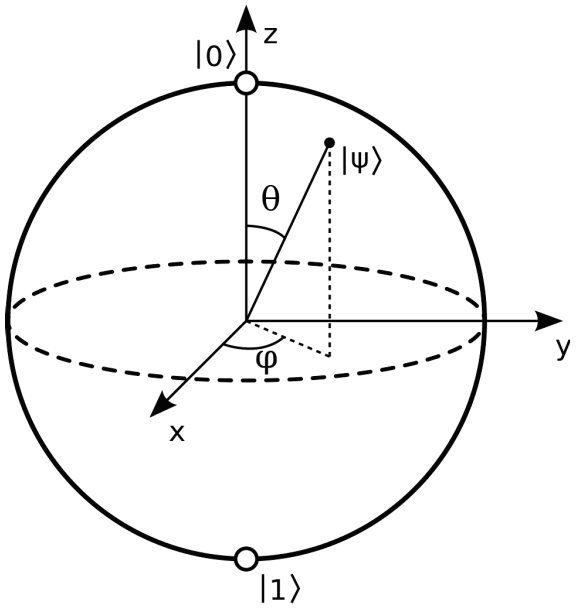


Figure 1.2: A qubit $|\psi\rangle$ represented in the Bloch sphere

in $\mathbb{H}^2$ can be represented by an arrow vector whose origin is in the center of the sphere (and origin of axis) and whose tip is a point inside the sphere (surface included). From the Bloch sphere we can visualize the expression 1.38, since running θ and ϕ we can span all the surface of the sphere if ($x = \cos\phi\,\sin\theta$, $y = \sin\phi\,\sin\theta$, $z = \cos\theta$) are the Cartesian coordinates in the sphere.

Since the length of the vector is the modulus of the average spin vector, we see that a pure state lies on the surface of the sphere while a mixed state in the inner

part; the center of the sphere corresponds to a randomized spin. Every point of the sphere, inner part and surface, is reachable starting from a point of the surface. In principle we could get from the inside to the surface as well, but it is only a geometric process that does not have a physical counterpart, as it will soon be clear.

Moving a point around the sphere surface means applying a general rotation that can be decomposed into 2 rotations around 2 of the axes. A rotation of θ around the axes are represented by the operators

$$R_k(\theta) \;=\; e^{-\imath\frac{\theta}{2}\sigma_k} \qquad k = x, y, z$$

If an operator A is such that $A^2 = I$, then $e^{-\imath\frac{\theta}{2}A} = cos\theta\, I \;+\; \imath sin\theta\, A$. Since Pauli matrices (see below) satisfy this property, we can use them to represent the rotations around the Bloch sphere axes:

$$R_x(\theta) = cos\frac{\theta}{2}\, I \;-\; \imath sin\frac{\theta}{2}\, \sigma_x = \begin{bmatrix} cos\frac{\theta}{2} & -\imath sin\frac{\theta}{2} \\ -\imath sin\frac{\theta}{2} & cos\frac{\theta}{2} \end{bmatrix} \tag{1.39a}$$

$$R_y(\theta) = cos\frac{\theta}{2}\, I \;-\; \imath sin\frac{\theta}{2}\, \sigma_y = \begin{bmatrix} cos\frac{\theta}{2} & -sin\frac{\theta}{2} \\ sin\frac{\theta}{2} & cos\frac{\theta}{2} \end{bmatrix} \tag{1.39b}$$

$$R_z(\theta) = cos\frac{\theta}{2}\, I \;-\; \imath sin\frac{\theta}{2}\, \sigma_z = \begin{bmatrix} e^{-\imath\theta/2} & 0 \\ 0 & e^{\imath\theta/2} \end{bmatrix} \tag{1.39c}$$

1.3.1.2 Measuring a qubit

To know $|\psi\rangle$ we must evaluate the two complex numbers α and β, equivalent to 4 real numbers. Since $|\psi\rangle$ is defined up to a global phase and represented on the Bloch sphere, this is equivalent to the evaluation of the three parameters x, y, z which correspond to the expectation values of the matrices σ_x, σ_y, σ_z over $|\psi\rangle$:

$$\begin{aligned} \langle\psi|\sigma_x|\psi\rangle &= x \ , \\ \langle\psi|\sigma_y|\psi\rangle &= y \ , \\ \langle\psi|\sigma_z|\psi\rangle &= z \ , \end{aligned}$$

which we can obtain by projective measurements in the computational basis. The three σ matrices are the so-called **Pauli Matrices**:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.40}$$

and they satisfy $\sigma_i^2 = I, \quad \sigma_j\sigma_k = i \cdot \varepsilon_{jkl}\sigma_l$.

Indeed, from equation 1.38, applying σ_z we obtain the output $+1$ corresponding to $|0\rangle$ with probability p_0 and the output -1 corresponding to $|1\rangle$ with probability

p_1. If we have an infinite amount of copies of the state to measure, then the frequencies of the outputs ± 1 will be exactly the probabilities p_0, p_1. Then the expectation value z is actually the difference between the two probabilities:

$$z = p_0 - p_0.$$

We access the values of x and y by rotating the state with proper unitaries so that the measurements of σ_z on the rotated states are equivalent to the measurements of σ_x, σ_y on the original states. This is obtained by action of the two unitaries:

$$U_y = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \qquad U_x = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -\imath \\ -\imath & 1 \end{bmatrix}$$

which correspond to a 90° rotation respectively around around the y and x axes.

1.3.1.3 Quantum errors on a qubit

During classical communication an error can occur and the bit can be flipped. But a qubit state can suffer different errors during communication since the state is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The bit could flip, the phase between $|0\rangle$ and $|1\rangle$ could change and we can have loss of information by mixing of the state or interaction with the environment. In general when a qubit passes through a noisy channel, it is said to be affected by *decoherence* (in its broader meaning). The different decoherence effects can happen all at the same time, but they can be seen singularly as some particular channel acting on the qubit and inducing the error. They define all the operations that can be made on a qubit state:

- The *bit-flip channel* flips $|0\rangle$ to $|1\rangle$ and vice-versa with a probability p that describes the strength of the flipping channel. A perfect bit-flip channel correspond to the action of a σ_x;
- The *phase-flip channel* flips the phase between $|0\rangle$ and $|1\rangle$ sending $|1\rangle$ to $-|1\rangle$ and vice-versa with a probability p. A perfect phase-flip channel correspond to the action of a σ_z;
- The *bit-phase-flip channel* is the channel performing both bit and phase flips;
- The *depolarizing channel* merges the state with the maximally mixed state I. It corresponds to an isotropic contraction in the Bloch sphere, i.e. a combined action of the 3 Pauli matrices;
- The *amplitude damping* is comparable to the decay of $|1\rangle$ onto $|0\rangle$ by the interaction with the environment (ex. spontaneous emission);
- The *phase damping* is the *decoherence* process in its strict meaning, since it is the loss of the off-diagonal terms of the matrix representation of the state.

1.3.2 The quantum copying machine

Thanks to the no-cloning theorem we know that we cannot efficiently copy a quantum state. This does not prevent us from making an approximate copy of a state, even though we have just one-shot measurement to perform.

The accuracy of the copying process or, more in general, the degree of similarity between the unknown ρ and the comparison state $|\psi\rangle$ is measured by the **fidelity**

$$F \;=\; \langle\psi|\,\rho\,|\psi\rangle \tag{1.41}$$

with $0 \;\leq\; F \;\leq\; 1$ and 1 corresponds to a perfect match.

The optimal copy ρ of the state $|\psi\rangle$ will give the upper bound for the fidelity of the copying process:

$$F_{opt} \;=\; \langle\psi|\,\rho_{opt}\,|\psi\rangle \;=\; \frac{5}{6} \tag{1.42}$$

meaning that the optimal copy can be written as

$$\rho_{opt} \;=\; \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^{\perp}\rangle\langle\psi^{\perp}| = \;\frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}I, \tag{1.43}$$

where $|\psi^{\perp}\rangle$ is the state orthonormal to $|\psi\rangle$ and $I = (|\psi\rangle\langle\psi|+|\psi^{\perp}\rangle\langle\psi^{\perp}|)/2$ is the completely mixed state.

1.3.3 Von Neumann entropy

The Von Neumann entropy is the quantum analogue of the Shannon entropy. A quantum system described by the density matrix ρ has a Von Neumann entropy

$$S(\rho) \;\equiv\; -Tr(\rho\,\log\,\rho). \tag{1.44}$$

Let assume that Alice has an alphabet $\mathcal{A} = \{\rho_1, ..., \rho_n\}$ to which is associated the set of probabilities p_i. Before the measurement the state to Bob is $\rho \;=\; \sum_i \; p_i\rho_i$ whose Von Neumann entropy is

$$S(\rho) \;=\; -\lambda_i\,\log\,\lambda_i \;=\; H(\lambda_1, ..., \lambda_n), \tag{1.45}$$

where H is the classical Shannon entropy and the set of λ_i is the set of eigenvalues of ρ. The Von Neumann entropy satisfies these properties:

- for a pure state $S(\rho) = 0$;
- $S(\rho) = 0$ is invariant under unitary transformations: $S(\rho) = S(U\rho U^{\dagger})$. This means that Von Neumann entropy is invariant unitary temporal evolutions;
- if $S(\rho) = 0$ acts on a N-dimensional space, then $0 \;\leq\; S(\rho) \;\leq\; \log\,N$.

Chapter 2

Quantum optics with continuous variables

Whereas the previous chapter was quite generic, we will focus now on *continuous variables* (CV), that are crucial for the CVQKD protocols we will use later on. As light is an electromagnetic field, it can be described by its amplitude and phase. On the other hand, when we enter the quantum world, the description through field operators is more appropriate, leading to the phase-space representation, which is the most commonly used in this kind of applications. We will also introduce the actual quantum states of light used for CVQKD: *Gaussian states*.

The second part of the chapter is dedicated to the measurement process of such states: the *homodyne detection*. The homodyne detection is an interferometric measurement, it is therefore based on the beam splitter, which is studied here from both a classical and a quantum point of view. Important details on the theory and practice of the homodyne detection are also given at the end of the chapter.

2.1 Quantum states of light for CV communication

A *continuous variable system* [14] is a quantum system living in a infinite-dimensional Hilbert space described by observables with continuous eigenspectra. The most common and representative system of this type is composed by N bosonic modes corresponding to N quantum harmonic oscillators, e.g. N quantized radiation modes of the electromagnetic (e.m.) field.

The N bosonic modes live in the Hilbert space $\mathcal{H}^{\otimes N}$ to which correspond N couples of bosonic field operators $\{\hat{a}_i, \hat{a}_i^\dagger\}_{i=1}^N$, called *annihilation and creation operators*. These operators satisfy the commutation relations

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \Omega_{ij} \tag{2.1}$$

resumed in the so called *symplectic form* $\mathbf{\Omega} := \bigoplus_{k=1}^{N} \boldsymbol{\omega}$

$$\mathbf{\Omega} = \begin{pmatrix} \boldsymbol{\omega} & & \\ & \ddots & \\ & & \boldsymbol{\omega} \end{pmatrix} \quad \boldsymbol{\omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{2.2}$$

2.1.1 Single-mode quantum optics

The quantum states defining the e.m. field are the **Fock states** or **number states** $|n\rangle_{k\lambda}$ representing the number of photons in the mode with wave number k and polarisation λ (we introduce them now and we will get into more details in section 1.4.2). Since we work in single mode optics we will leave the indices k and λ, but we have to remember that the system is composed of N independent harmonic oscillators, so we have N different number operators, each of them acting on a particular oscillator. So $|n\rangle$ is eigenvector of the **number operator** $\hat{\boldsymbol{n}} = \hat{a}^\dagger \hat{a}$ with eigenvalue n, exactly the number of photons occupying the mode.

Since the Hamiltonian of a harmonic oscillator is $\hat{H} = \hbar\omega(\hat{n} + 1/2)$, the number operator is an eigenstate of the Hamiltonian, with eigenvalue the energy of the system:

$$\hat{H}|n\rangle = \hbar\omega(n + 1/2)|n\rangle. \tag{2.3}$$

The action of the annihilation and creation operators on $|n\rangle$ is

$$\hat{a}|0\rangle = 0; \quad \hat{a}|n\rangle = \sqrt{n}|n-1\rangle \ (n \geq 1) \tag{2.4a}$$
$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{2.4b}$$
$$\langle\hat{n}\rangle = n \tag{2.4c}$$
$$\Delta\hat{n} = 0 \tag{2.4d}$$

from which the meaning of the word annihilation (creation) is clearer, since with the operator $\hat{a}$ ($\hat{a}^\dagger$) we can jump from one mode to the one below (above), by annihilating (creating) a photon. The ground state of the harmonic oscillator is $|0\rangle$ with the energy of the ground state $E_0 = \hbar\omega/2$.

2.1.2 Phase-space representation of the e.m. field

The electromagnetic field can be represented as a wave propagating in time and space or as a harmonic oscillator in a certain mode. Another interesting (and crucial for this work) representation is the **phase-space representation**.

To introduce it, we can make a Cartesian decomposition of the $\{\hat{a}_i, \hat{a}_i^\dagger\}$, i.e. $\hat{a} \equiv (\hat{Q} + \imath\hat{P})$ and $\hat{a}^\dagger \equiv (\hat{Q} - \imath\hat{P})$, where $\hat{Q}$ and $\hat{P}$ are dimensionless canonical

observables, called the **quadrature field operators**

$$\hat{Q} \equiv \frac{1}{2}(\hat{a}^\dagger + \hat{a}) \tag{2.5a}$$

$$\hat{P} \equiv \frac{\imath}{2}(\hat{a}^\dagger - \hat{a}). \tag{2.5b}$$

It is interesting to use these operators because they have continuous eigenspectra

$$\hat{Q}|q\rangle = q|q\rangle \quad \hat{P}|p\rangle = p|p\rangle \tag{2.6}$$

where the eigenstates $|q\rangle$ and $|p\rangle$ are connected by the Fourier transform:

$$|q\rangle = \frac{1}{\sqrt{2\pi}} \int dp\, e^{-\imath qp/2}|p\rangle \ , \tag{2.7a}$$

$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int dp\, e^{\imath qp/2}|q\rangle. \tag{2.7b}$$

Let us now assume that we deal with just one harmonic oscillator (for simplicity of notation). The two variables $\boldsymbol{x} = (q, p)$ span a real symplectic space called **phase-space**. The corresponding couple of operators is $\hat{\boldsymbol{x}} = (\hat{Q}, \hat{P})$.

2.1.3 Gaussian states

We already saw that all the information about a quantum system is enclosed in its quantum state, which is represented by the density matrix $\hat{\rho}$. We want now to use another description for quantum states, a description in terms of a quasi-probability distribution defined over the phase-space.

First we must define the **Weyl operator**

$$D(\boldsymbol{\xi}) := e^{\imath \hat{\boldsymbol{x}}^T \boldsymbol{\Omega} \boldsymbol{\xi}} \tag{2.8}$$

with $\boldsymbol{\xi}$ living in the phase-space. It can be proven that an arbitrary $\hat{\rho}$ is equivalent to a **Wigner characteristic function**

$$\chi(\boldsymbol{\xi}) = Tr\left[\hat{\rho} D(\boldsymbol{\xi})\right]. \tag{2.9}$$

Applying a Fourier transform we find that the same $\hat{\rho}$ is equivalent to the **Wigner function**

$$W(\boldsymbol{x}) = \int_{\mathbb{R}^2} \frac{d^2\boldsymbol{\xi}}{(2\pi)^2} e^{-\imath \hat{\boldsymbol{x}}^T \boldsymbol{\Omega} \boldsymbol{\xi}} \chi(\boldsymbol{\xi}). \tag{2.10}$$

The Wigner function is a quasi-probability distribution, normalized but non-positive (it can assume negative values). In the last equation the continuous vari-

ables $\boldsymbol{x}$ are exactly the eigenvalues of the quadrature operators. So a quantum state $\hat{\rho}$ is equivalent to a Wigner function $W(q,p)$. The quantities χ and W form the *Wigner characterization* of a quantum state.

Important quantities that are also relevant for the Wigner characterization are the statistical moments of the state, especially the first and the second ones. The first moment is the **displacement vector** or **mean value**

$$\langle \boldsymbol{x} \rangle = Tr(\hat{\boldsymbol{x}}\hat{\rho}). \tag{2.11}$$

The second moment is the **covariance matrix V,** whose elements are

$$V_{ij} = \frac{1}{2}\left\langle \{\Delta\hat{x}_i \Delta\hat{x}_j\} \right\rangle, \tag{2.12}$$

where $\Delta\hat{x}_i = \hat{x}_i - \langle \hat{x}_i \rangle$ and $\{,\}$ is the anti-commutator. The diagonal elements provide the variances of the quadrature operators

$$V_{ii} = V(\hat{x}_i) = \left\langle \hat{x}_i^2 \right\rangle - \langle \hat{x}_i \rangle^2 .$$

One can derive [15] the uncertainty principle in the form

$$\boldsymbol{V} \; + \; \imath\boldsymbol{\Omega} \; \geq \; 0 \tag{2.13}$$

or the more intuitive form for the diagonal elements

$$V(\hat{Q})V(\hat{P}) \; \geq \; N_0^2, \tag{2.14}$$

where N_0 is the **shot noise**. Shot noise is often used as unit of measure, saying that we are working in *Shot Noise Units (SNU)*.

Definition 2.1. A **Gaussian state** is a bosonic state whose Wigner representation is Gaussian

$$\chi(\boldsymbol{\xi}) = \; exp\left[\frac{1}{2}\boldsymbol{\xi}^T\left(\boldsymbol{\Omega}\boldsymbol{V}\boldsymbol{\Omega}^T\right)\boldsymbol{\xi} \; - \; \imath(\boldsymbol{\Omega}\langle \boldsymbol{x} \rangle)^T\boldsymbol{\xi}\right] \; , \tag{2.15a}$$

$$W(\boldsymbol{x}) = \; \frac{exp\left[-\frac{1}{2}(\boldsymbol{x}-\langle \boldsymbol{x} \rangle)^T\boldsymbol{V}^{-1}(\boldsymbol{x}-\langle \boldsymbol{x} \rangle)\right]}{(2\pi)\sqrt{det\boldsymbol{V}}} \tag{2.15b}$$

In general if the first two moments can completely describe the state, we can write $\hat{\rho} = \hat{\rho}(\langle \boldsymbol{x} \rangle, \boldsymbol{V})$, which is a valid expression for a Gaussian state.

Not less important are *Gaussian operations*. A quantum operation is Gaussian if

it transforms Gaussian states into Gaussian states. A Gaussian unitary is generated by Hamiltonians $\hat{H}$ that are second-order polynomials in the field operators.

2.1.4 Examples of quantum states of light

In this section we will talk about the most common quantum states of light, useful for quantum communication. Together with the meaning and the form of these states, we will also have a look at their main features.

The first is the vacuum state, also seen as the ground state of the harmonic oscillator. Then, even if we have already seen the Fock states, we will enter more into detail, especially regarding their statistical properties. Then chaotic light will be considered and at the end, after introducing the displacement and the squeezing operator, we will consider the coherent state and the squeezed coherent state.

2.1.4.1 Vacuum state

The vacuum state is the ground state of the harmonic oscillator. This is probably the most important Gaussian state, since it is the basis for the homodyne detection that we will consider in section 1.5. We can define it as we did in equation 2.4a using the annihilation operator

$$\hat{a}|0\rangle \;=\; 0$$

and the energy of this state is

$$\langle 0|\hat{H}|0\rangle = \; \hbar\omega/2.$$

We can also define it via the displacement vector and the covariance matrix. The vacuum state has

$$(\langle \boldsymbol{x} \rangle, \boldsymbol{V}) = (0, I), \tag{2.16}$$

i.e. the mean value is 0 and the covariance matrix is the identity. We can deduce that the variances of both the field quadratures are equal to $1/4$

$$V(\hat{Q}) \;=\; V(\hat{P}) \;=\; \frac{1}{4} \tag{2.17}$$

and the state is centered in the origin of the phase-space.

2.1.4.2 Fock states

The vacuum state is a particular case of Fock state. A Fock state represents the number of photons of one mode of the e.m. field. It can be obtained from the vacuum state by applying the creation operator n times:

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle \tag{2.18}$$

with energy $E_n = \hbar\omega(n + 1/2)$. The mean value and the variance on n are

$$\langle n \rangle \; = \; n, \qquad (\Delta n)^2 \; = \; 0. \tag{2.19}$$

From the statistical moments we can derive the Gaussian description and information about its phase-space representation. As an extension of the vacuum state we find different interesting properties. First

$$\langle Q \rangle \; = \; \langle P \rangle \; = \; 0 \tag{2.20}$$

so the displacement vector is null and the state is centered in the origin of the phase-space. Then, for the second moment:

$$V(\hat{Q}) \; = \; V(\hat{P}) \; = \; \frac{1}{2}(n \; + \; \frac{1}{2}) \tag{2.21}$$

so the state is centered in the origin of the phase-space and its radius is $r = \sqrt{n \; + \; \frac{1}{2}}$ since

$$(\hat{Q}^2 \; + \; \hat{P}^2)|n\rangle \; = \; (n \; + \; \frac{1}{2})|n\rangle \; = \; r^2|n\rangle. \tag{2.22}$$

Since the phase and the number of photons (or the amplitude) of the field are conjugate observables, corresponding to the Heisenberg inequality $\Delta n \, \Delta\Phi \geq 1/2$ and for Fock states $(\Delta n)^2 \; = \; 0$, then the phase of the mode is completely unknown.

2.1.4.3 Thermal states

Another example of Gaussian state is the *thermal state*. By definition a thermal state maximizes the Von Neumann entropy. In the number-state representation a thermal state is given by

$$\hat{\rho}^t(\bar{n}) \; = \; \sum_{n=0}^{+\infty} \frac{\bar{n}^n}{(\bar{n} \; + \; 1)^{n+1}} |n\rangle \langle n|. \tag{2.23}$$

Its Wigner representation is given by a zero mean value and a diagonal covariance matrix such that

$$(x, \, V) \; = \; (0, \, (2\bar{n} + 1)I) \tag{2.24}$$

2.1.4.4 Coherent states

We now introduce a Gaussian unitary called **displacement operator** $D(\alpha)$:

$$D(\alpha) \; := \; exp(\alpha\hat{a}^\dagger \; - \alpha^\star\hat{a}), \tag{2.25}$$

where $\alpha = q + ip$ is the *complex amplitude*. It can be seen as the complex form of the Weyl operator.

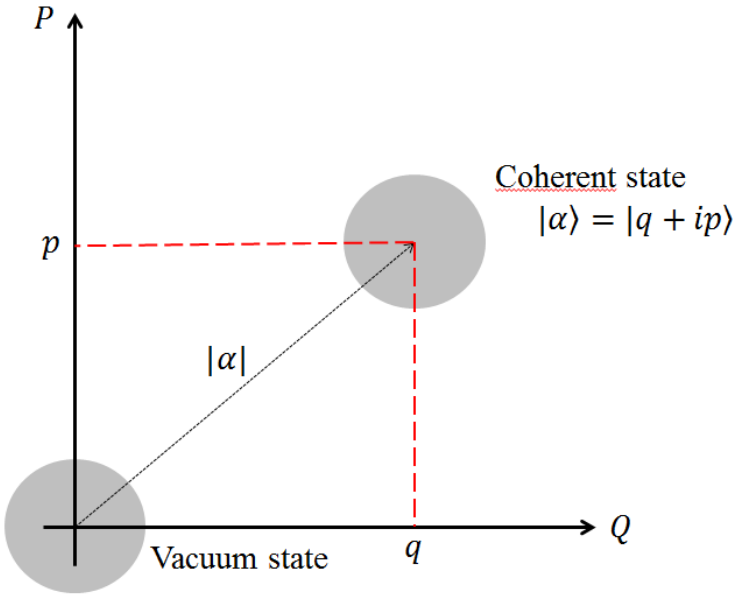


Figure 2.1: The vacuum state and the coherent state in phase-space

We can now derive the **coherent state** $|\alpha\rangle$ (figure 2.1) in two ways: from the displacement operator or from the fact that a coherent state is eigenvector of the annihilation operator $\hat{a}$.

First, when we apply $D(\alpha)$ to the vacuum state we obtain the coherent state, whose formal expression is

$$|\alpha\rangle \;=\; e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{2.26}$$

This corresponds to a translation in the phase-space: the vacuum state will be now centered at the coordinates indicated by the complex amplitude $(q/2, p/2)$.

But the coherent state is also eigenstate of the annihilation operator with eigenvalue α:

$$\hat{a}|\alpha\rangle \;=\; \alpha|\alpha\rangle. \tag{2.27}$$

Since $\hat{a}$ is not hermitian we are not sure that the base of $\{|\alpha\rangle\}$ is complete and orthonormal. As a matter of fact this set of eigenvectors is *over-complete*, meaning that there are more states than the dimension of the Hilbert space (see below for a more precise statement). The basis $\{|\alpha\rangle\}$ is not orthogonal, since if we consider another coherent state $|\beta\rangle$ we have

$$\langle\alpha|\beta\rangle \;=\; e^{-|\alpha-\beta|^2/2} \;\neq\; \delta_{\alpha\beta}$$

and it is over-complete since the set $\{|\alpha\rangle\}$ is a non-countable ensemble while the base $\{|i\rangle_{\hat{a}}\}$ is countable. In addition to that, considering the completeness relation,

we have for $|\alpha\rangle$

$$\int d^2\alpha |\alpha\rangle\langle\alpha| = 2\pi > 1.$$

It is also interesting to see some statistical properties, such as:

$$\langle n\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = |\alpha|^2, \tag{2.28a}$$
$$\langle n^2\rangle = |\alpha|^4 + |\alpha|^2, \tag{2.28b}$$
$$\langle (\Delta n)^2\rangle = |\alpha|^2 = \langle n\rangle, \tag{2.28c}$$
$$\langle Q\rangle = |\alpha| cos\Theta, \tag{2.28d}$$
$$\langle P\rangle = |\alpha| sin\Theta, \tag{2.28e}$$
$$(\Delta Q)^2 = (\Delta P)^2 = \frac{1}{4}. \tag{2.28f}$$

2.1.4.5 Squeezed states

One of the most important paradigms of quantum mechanics is the Heisenberg principle, telling us that if we have two incompatible observables we cannot reduce under a certain threshold the product of the errors on the measurement of the two of them. As a consequence, in the Wigner representation the vacuum state is not a point in the phase space, but a Gaussian distribution with variances corresponding to the vacuum noise. This is used as an advantage in quantum cryptography (see next chapter), and it is also important if we want to access the two observables for other purposes. But if we are interested in just one of the two we can actually reduce the variance of one of the two paying the price of increasing the other one. A state like this its called **coherent squeezed state** (figure 2.2).

To obtain this state we first have to introduce the **squeezing operator**

$$S(\xi) = exp(\frac{1}{2}\xi^\star\hat{a}^2 - \frac{1}{2}\xi\hat{a}^{\dagger^2}), \tag{2.29}$$

where $\xi = s\,e^{\imath\theta}$ is the *complex squeezing parameter*, with s being a *squeezing factor* and θ being a *squeezing direction*. From this expression we see that, since we are using the squares of the field operators, the physical process involved to the creation of a squeezed state is non-linear (ex. parametric fluorescence).

Let us apply $S(\xi)$ to the simplest Gaussian state we know: the vacuum. We obtain the **squeezed vacuum**

$$|\xi\rangle = S(\xi)|0\rangle = \sqrt{sech(s)}\sum_{n=0}^{\infty}\frac{\sqrt{(2n)!}}{n!}\left[-\frac{1}{2}e^{\imath\theta}\,th(s)\right]|2n\rangle. \tag{2.30}$$

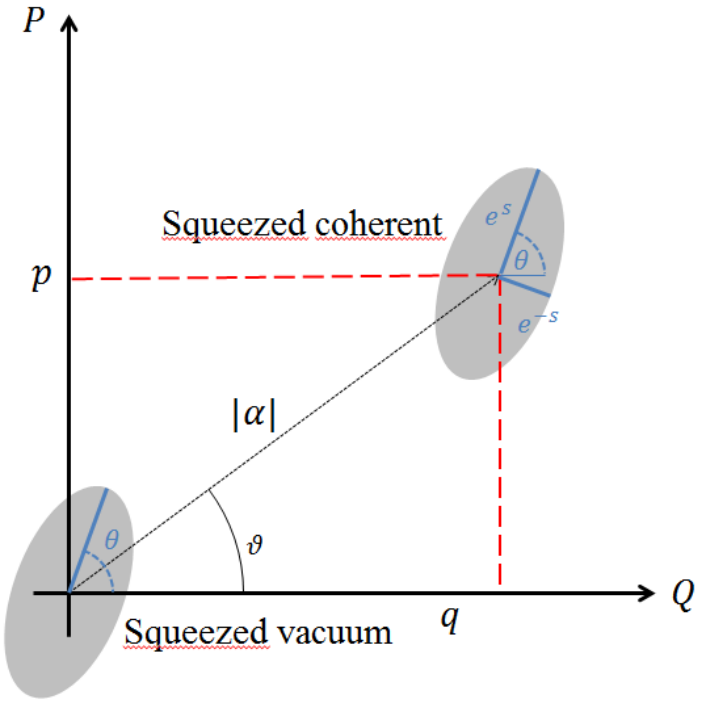


Figure 2.2: Squeezed vacuum and squeezed coherent states in phase-space.

Since

$$S^\dagger \hat{a} S = \hat{a}\, cosh(s) - \hat{a}^\dagger e^{\imath\theta} sinh(s), \quad S^\dagger \hat{a}^\dagger S = \hat{a}^\dagger\, cosh(s) - \hat{a} e^{-\imath\theta}\, sinh(s)$$

we derive

$$\langle n \rangle = \langle \xi | \hat{a}^\dagger \hat{a} | \xi \rangle = \langle 0 | S^\dagger \hat{a}^\dagger S S^\dagger \hat{a} S | 0 \rangle = sinh^2(s) \tag{2.31a}$$

$$\left\langle n^2 \right\rangle = 3 \langle n \rangle^2 - 2 \langle n \rangle \tag{2.31b}$$

$$\left\langle (\Delta n)^2 \right\rangle = 2 \langle n \rangle (\langle n \rangle + 1) \tag{2.31c}$$

which means that the squeezing increases the expectation value of n in the vacuum state. We also find

$$(\Delta Q)^2 = \frac{1}{4}\left(e^{2s} sin^2 \frac{\theta}{2} + e^{-2s} cos^2 \frac{\theta}{2} \right), \tag{2.32a}$$

$$(\Delta P)^2 = \frac{1}{4}\left(e^{2s} cos^2 \frac{\theta}{2} + e^{-2s} sin^2 \frac{\theta}{2} \right). \tag{2.32b}$$

So in the phase-space the circle is now distorted into an ellipse. The semi-minor axis along θ direction is $\frac{1}{2}e^{-s}$ and the semi-major one is $\frac{1}{2}e^{s}$.

We can squeeze in principle every state, but another interesting application is

for a displaced state. We obtain such a state by displacing the squeezed vacuum

$$|\alpha, \xi\rangle \;=\; D(\alpha)S(\xi)|0\rangle. \tag{2.33}$$

Since D and S do not commute, the application of the displacement before the squeezing generates a different state. It can be demonstrated that

$$\langle n\rangle = |\alpha|^2 + sinh^2(s), \tag{2.34a}$$

$$\left\langle (\Delta n)^2 \right\rangle = |\alpha|^2 \left[e^{2s} sin^2(\Theta - \frac{\theta}{2}) + e^{-2s} cos^2(\Theta - \frac{\theta}{2}) \right] + 2sinh^2(s)\left(sinh^2(s) + 1\right), \tag{2.34b}$$

$$\langle Q\rangle = |\alpha| cos\Theta, \tag{2.34c}$$

$$\langle P\rangle = |\alpha| sin\Theta, \tag{2.34d}$$

$$(\Delta Q)^2 = \frac{1}{4}\left(e^{2s} sin^2\frac{\theta}{2} + e^{-2s} cos^2\frac{\theta}{2} \right), \tag{2.34e}$$

$$(\Delta P)^2 = \frac{1}{4}\left(e^{2s} cos^2\frac{\theta}{2} + e^{-2s} sin^2\frac{\theta}{2} \right) \tag{2.34f}$$

2.2 The homodyne detection

Usual optical detection techniques is based on the properties of the incident light intensity or photon flux. Another important feature of a light beam, since light is a wave, is its phase. Homodyne detection [16] measures the quadrature operators expectation values of the incident electromagnetic field with respect to a measurement phase angle, i.e. it is an interferometric measurement. The phase reference information is contained in another light beam, called *local oscillator* (or LO). The measured beam is the *signal*, which in our case has a very low power, inducing a photocurrent comparable with the quantum noise of the detection. This technique is important because it can measure the non classical properties of light that are phase dependent. Let us first analyze the structure of the measurement scheme to move on afterwards into the meaning and the physical details of the process.

2.2.1 The beam splitter

2.2.1.1 Classical beam splitter

The essential part of a homodyne detection is the beam splitter (BS), an optical device into which two e.m. fields can be mixed. Each wave can be transmitted or reflected, so that the two outputs of the BS will depend on its transmission and reflection coefficients. A schematic is shown in figure 2.3.

The two (classical) input fields are E_1 and E_2 and the outputs are $E_3 = r_{13}E_1 + t_{23}E_2$ and $E_4 = r_{24}E_2 + t_{14}E_1$, where r_i, t_j are the *complex coefficients of reflection and transmission*. Therefore the matrix representation of the BS operation is:

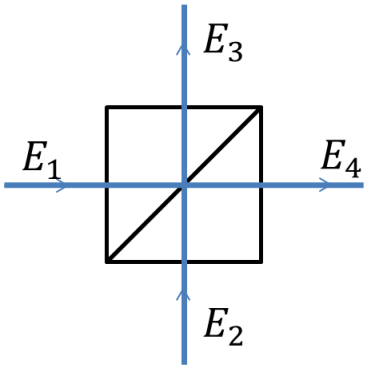


Figure 2.3: The beam splitter schematic.

$$\begin{bmatrix} E_3 \\ E_4 \end{bmatrix} = \begin{bmatrix} r_{13} & t_{23} \\ t_{14} & r_{24} \end{bmatrix} \begin{bmatrix} E_1 \\ E_2 \end{bmatrix}. \tag{2.35}$$

The output intensities are then obtained as a function of the input ones :

$$\begin{aligned} |E_3|^2 &= = |r_{13}|^2 |E_1|^2 + r_{13}^\star t_{23}\, E_1^\star E_2 + r_{13} t_{23}^\star\, E_1 E_2^\star + |t_{23}|^2 |E_2|^2 \\ |E_4|^2 &= = |t_{14}|^2 |E_1|^2 + t_{14}^\star r_{24}\, E_1^\star E_2 + t_{14} r_{24}^\star\, E_1 E_2^\star + |r_{24}|^2 |E_2|^2. \end{aligned} \tag{2.36}$$

We will be interested in lossless beamsplitters, for which one has:

$$|E_1|^2 + |E_2|^2 = |E_3|^2 + |E_4|^2$$

for any value of the input fields, from which we get

$$|r_{13}|^2 + |t_{14}|^2 = |t_{23}|^2 + |r_{24}|^2 = 1, \quad r_{13}^\star t_{23} + t_{14}^\star r_{24} = r_{13} t_{23}^\star + t_{14} r_{24}^\star = 0 \tag{2.37}$$

One has thus $|r_{13} t_{23}|^2 = |t_{14} r_{24}|^2$, or $|r_{13}|^2(1 - |r_{24}|^2) = |r_{24}|^2(1 - |r_{13}|^2)$, and thus

$$|r_{13}| = |r_{24}| = |r|, \quad |t_{14}| = |t_{23}| = |t|, \quad |t|^2 + |r|^2 = 1$$

There are various ways to choose the phases of the coefficients to fulfill equation 2.37, because each individual field can be dephased arbitrarily, depending on its own phase origin (or propagation distance). A usual choice is to take all coefficients real, with a minus sign on a reflection coefficient, corresponding to the π phase shift in the classical calculation of the Fresnel coefficients:

$$t_{14} = t_{23} = t, \quad r_{13} = -r_{24} = r.$$

Another more symmetric choice, that we will adopt later on, is to take t and r real,

but to add i on the reflection coefficients:

$$t_{14} = t_{23} = t, \quad r_{13} = r_{24} = ir.$$

2.2.1.2 Quantum beam splitter

We can describe the quantum field intensities as number operators $\hat{n} = \hat{a}^\dagger \hat{a}$. In the beam-splitter description we can therefore replace the classical amplitudes of the field by the field operators, as in figure 2.4.

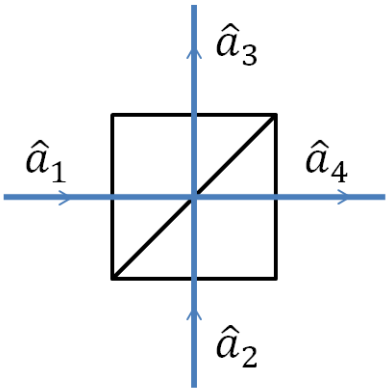


Figure 2.4: Quantum beam splitter schematic.

For a lossless BS, the above calculation applies and one has (with real r and t)

$$\begin{aligned} \hat{a}_3 &= ir\hat{a}_1 + t\hat{a}_2 \\ \hat{a}_4 &= t\hat{a}_1 + ir\hat{a}_2. \end{aligned} \tag{2.38}$$

So the output number operators are

$$\begin{aligned} \hat{n}_3 &= \hat{a}_3^\dagger \hat{a}_3 = r^2\, \hat{a}_1^\dagger \hat{a}_1 - irt\, \hat{a}_1^\dagger \hat{a}_2 + itr\, \hat{a}_2^\dagger \hat{a}_1 + t^2\, \hat{a}_2^\dagger \hat{a}_2 \\ \hat{n}_4 &= \hat{a}_4^\dagger \hat{a}_4 = t^2\, \hat{a}_1^\dagger \hat{a}_1 + itr\, \hat{a}_1^\dagger \hat{a}_2 - irt\, \hat{a}_2^\dagger \hat{a}_1 + r^2\, \hat{a}_2^\dagger \hat{a}_2\,. \end{aligned} \tag{2.39}$$

with $\hat{n}_1 + \hat{n}_2 = \hat{n}_3 + \hat{n}_4$ as expected.

Since we are in the quantum regime we may consider using a single photon input corresponding to the input state

$$|1\rangle_1 |0\rangle_2 = \hat{a}_1^\dagger |0\rangle_1 |0\rangle_2 = |10\rangle_{12}.$$

Seen from the output modes point of view we get:

$$|10\rangle_{12} = (ir\hat{a}_3^\dagger + t\hat{a}_4^\dagger)|00\rangle_{34} = ir|10\rangle_{34} + t|01\rangle_{34} \tag{2.40}$$

where the output state is *entangled* with respect to the output modes. Physically, if the photon is detected in one output port, the other one is projected in the vacuum state: this illustrates a feature of the quantum BS that has no classical equivalent.

2.2.1.3 A simple illustration: two-photon interference

As another simple illustration ot the quantum properties of a BS, let us consider the situation where two photons are present at the input. In the present single-mode calculation, two photons in the same mode are by construction indistinguishable. A more elaborate (multimode) picture can be used, by introducing e.g. single photon wave packets, but for simplicity it will not be considered here.

Considering first 2 photons in input 1, the input and output states are

$$\frac{1}{\sqrt{2}}(\hat{a}_1^\dagger)^2|00\rangle_{12} \rightarrow \frac{1}{\sqrt{2}}(ir\hat{a}_3^\dagger + t\hat{a}_4^\dagger)^2|00\rangle_{34} = \ -r^2|20\rangle_{34} \ + \ t^2|02\rangle_{34} \ + \ \sqrt{2}\, irt|11\rangle_{34} \tag{2.41}$$

giving the probabilities

$$P(2_3, 0_4) = |r|^4, \quad P(0_3, 2_4) = |t|^4, \quad P(1_3, 1_4) = 2|r|^2|t|^2,$$

which are the same probabilities one would have obtained by considering that the two photons are independently transmitted or reflected by the BS.

Intuitively we can (correctly) guess that if the two photons enter input 2 the results are similar: we just need to exchange the roles of t and r with respect to the output channels. In the case where $|r|^2 = |t|^2 = 1/2$ one gets $P(2_3, 0_4) = P(0_3, 2_4) = 1/4$ and $P(1_3, 1_4) = 1/2$, and **not** all probabilities equal to 1/3, as a wrong reasoning about the indistinguishability of photons might have suggested.

More interesting is the case in which each input channel has a photon, so the input state is $|11\rangle_{12}$, and the output one is

$$(ir\hat{a}_3^\dagger + t\hat{a}_4^\dagger)(t\hat{a}_3^\dagger + ir\hat{a}_4^\dagger)|00\rangle_{34} = \ \sqrt{2}\, irt(|20\rangle_{34} \ + \ |02\rangle_{34}) \ + \ (t^2 - r^2)|11\rangle_{34} \tag{2.42}$$

giving the probabilities (we remind that r and t are real numbers)

$$P(2_3, 0_4) = P(0_3, 2_4) = 2\, r^2t^2, \quad P(1_3, 1_4) = (r^2 - t^2)^2$$

or in the general case

$$P(2_3, 0_4) = 2\, |r|^2|t|^2, \quad P(0_3, 2_4) = 2\, |r|^2|t|^2, \quad P(1_3, 1_4) = (|r|^2 - |t|^2)^2$$

which sum up to 1.

The interesting situation here is a balanced BS, meaning that $|t| = |r| = 1/\sqrt{2}$,

where one has

$$P(2_3, 0_4) = P(0_3, 2_4) = 1/2, \quad P(1_3, 1_4) = 0 \tag{2.43}$$

i.e. the two photons always come out together. This effect is called "photon coalescence", and was first demonstrated by Hong, Ou and Mandel [17]. It can be attributed to a destructive interference of the situation where both photons are transmitted (amplitude t^2) and both photons are reflected (amplitude $(ir)^2 = -r^2$).

It requires the two photons to be in the same mode, that makes them indistinguishable, but apart from that they can be emitted by (synchronized) independent sources. The "HOM effect" has major applications in quantum computing with photonic qubits, so the ability to emit many indistinguishable photons with high efficiency is currently a major experimental issue.

2.2.2 Optical scheme of the homodyne detection

The basic principle of the homodyne detection is to mix the signal and the local oscillator on a beam splitter as shown in figure 2.5. The two outputs are collected by two photodetectors and the quantity of interest is the difference of the two photocurrents, which is proportional to the amplitude of the two interfering fields and related to their phase difference, as it will be shown in this section.

The significant configuration is that of a *balanced homodyne detection* in which the beam splitter is said to be 50:50, corresponding to $|r| = |t| = 1/\sqrt{2}$, and the photodetectors are identical. In this situation the classical component of the LO intensity is equally split in the two arms, so the difference between the photocurrents can erase the LO current mean value and classical fluctuations. So ideally the remaining signal is just related to the quantum properties of the fields. Imperfections and appropriate corrections will be discussed at the end of the section.

In this work we use homodyne detection in the time domain: the signal and the local oscillator are two pulses of the same duration arriving on the beam splitter at exactly the same time. The electrical signal of the detection is treated by the electronics circuit, and we perform real time acquisition, allowing us to transfer data for each pulse. The electronics circuit also amplifies the very small differential current and cuts off the noise at low frequencies; the details of the electronics acquisition system will be presented in chapter 6. Generally speaking, this measurement scheme is highly demanding from the implementation point of view: the balancing of the two arms of the detection (beam splitter ratio and photodiodes characteristics) must very precise and the amplifier noise must be very small.

2.2.3 Theoretical details

We said that the homodyne detection output is proportional to the amplitudes of both the signal and the local oscillator and depends on their phase difference. In this paragraph we will show these properties, considering first a classical approach and then a quantum modeling. The detection is supposed to be balanced (the balancing process will be explained in section 2.2.4).

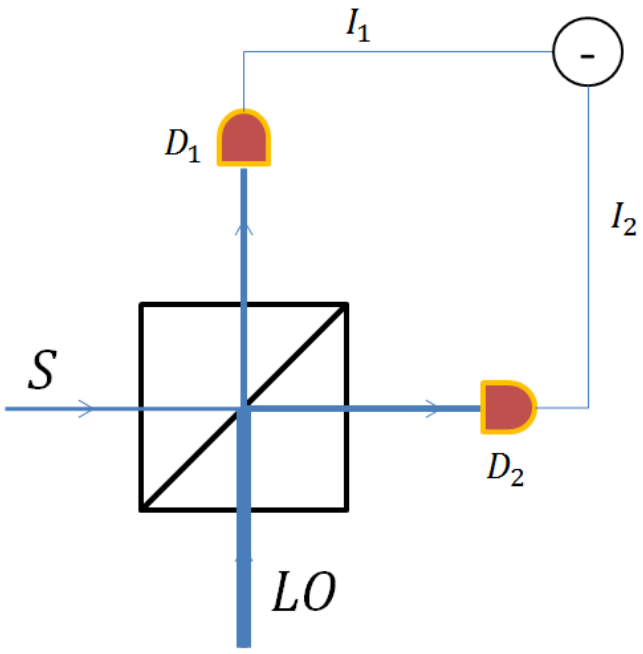


Figure 2.5: Optical scheme of the homodyne detection.

Classical fields The case in which only the local oscillator is injected in the detection is quite trivial: it is perfectly divided in two, the measured amplitudes are equal, and the subtraction gives 0.

Let us now consider two pulses (local oscillator and signal) arriving at exactly the same time on the beam splitter, so that (for the purpose of this explanation) we can consider the interaction to be time independent. The local oscillator is an electromagnetic field such as

$$E_{LO} = |E_{LO}|e^{\imath\phi} \tag{2.44}$$

with amplitude $|E_{LO}|$ and phase ϕ. The signal can be written as a complex number as well, this time explicitly by its real and imaginary parts

$$E_S = (q + \imath p) = (q_\phi + \imath p_\phi)e^{\imath\phi} \tag{2.45}$$

where the last equality is the decomposition of quadratures along the local oscillator phase. The two outputs of the beam splitter, because of the π phase difference between reflected and transmitted beams, are

$$E_{1,2} = \frac{1}{\sqrt{2}}(q_\phi + \imath p_\phi \pm |E_{LO}|)e^{\imath\phi}. \tag{2.46}$$

The photocurrents will be proportional to the squared modulus of the amplitudes:

$$\begin{aligned} I_{1,2} = \frac{1}{2}\left[(q_\phi \pm |E_{LO}|)^2 + p_\phi^2\right] &= \frac{1}{2}\left[|E_{LO}|^2 \pm 2q_\phi E_{LO} + q_\phi^2 + p_\phi^2\right] = \\ = \frac{I_{LO}}{2} &\pm \sqrt{I_{LO}} q_\phi + \frac{I_S}{2} \end{aligned} \tag{2.47}$$

Since the signal is low power and the LO is a classical strong field, we can say that $|q_\phi|, |p_\phi| \ll |E_{OL}|$, so I_S is negligible with respect to the other two terms. Now the output of the detection is the difference of the two amplitudes, i.e.

$$\delta I = I_1 - I_2 = 2\sqrt{I_{LO}} q_\phi. \tag{2.48}$$

Quantum fields As has been previously done for the beam splitter, the classical field amplitudes are replaced by the operators $\hat{a}$ and $a^\dagger$. Assuming that the LO field is in a coherent state of amplitude $|E_{LO}|$, a straightforward calculation gives

$$\begin{aligned} \delta\hat{I} = \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2 &= |E_{LO}|(e^{-\imath\phi}\hat{a}_s + e^{\imath\phi}\hat{a}_s^\dagger) \\ &= 2\sqrt{I_{LO}}\, \hat{Q}_\phi \end{aligned} \tag{2.49}$$

where $\hat{Q}_\phi$ is the quadrature operator selected by the LO, and corresponding to the classical q_ϕ above. So we can say that

- the output of the detection is proportional to the field quadrature operator $\hat{Q}_\phi$ of the signal;
- $\hat{Q}_\phi$ contains the phase relation with the local oscillator, which can be adjusted experimentally;
- the output is proportional to $\sqrt{I_{LO}} = |E_{OL}|$ that gives a huge amplification to the signal quadrature measurement.

The geometrical representation of figure 2.6 shows how the local oscillator phase gives a preferred projection direction for the measurement of the state. It follows that with a proper choice of the phase ϕ we can access the exact values of the two quadratures of the state, i.e. measure either $\hat{Q} = \hat{Q}_{\phi=0}$ or $\hat{P} = \hat{Q}_{\phi=\pi/2}$.

Using this phase-related projection process we can perform a tomography of the quantum state and retrieve its Wigner function by measuring over multiple phases ($0 \leq \phi < 2\pi$), scanning the whole phase-space. Then the Wigner function can be recovered from a suitable set of projections by using e.g. the Radon transform or a maximum likelihood numerical calculation (quantum tomography).

2.2.4 Homodyne detection balancing

In practice, $|r|^2$ and $|t|^2$ are not exactly 1/2, or the photodiodes may have different characteristics (rise time, quantum efficiency), so the detection is not exactly bal-

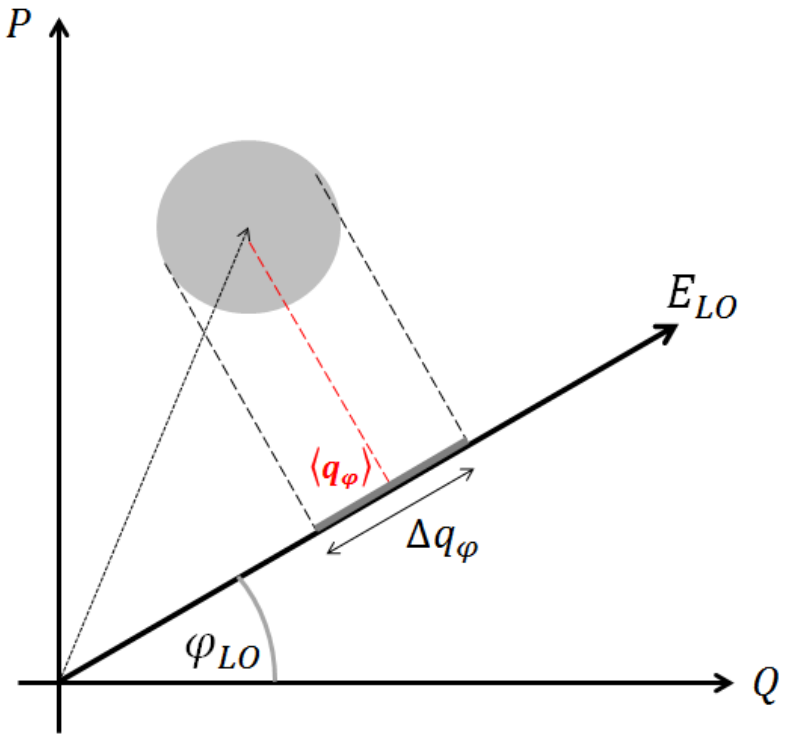


Figure 2.6: The homodyne detection measurement in phase-space.

anced. An order of magnitude of the required precision can be obtained from the following calculation. Let us assume that

$$|t|^2 = \frac{1}{2} + \varepsilon, \qquad |r|^2 = \frac{1}{2} - \varepsilon \tag{2.50}$$

with $\varepsilon \ll 1/2$. We analyze this classically, since the results are identical to the quantum case, which is however less intuitive for a short explanation. The two intensities after the BS, following the figure 2.5, are

$$\begin{aligned} I_1 &= |tE_{LO} + r(q_\phi + \imath p_\phi)|^2 \simeq (\frac{1}{2} + \varepsilon)\, I_{LO} + \sqrt{1-4\varepsilon^2}\, E_{LO}\, q_\phi \\ I_2 &= |rE_{LO} - t(q_\phi + \imath p_\phi)|^2 \simeq (\frac{1}{2} - \varepsilon)\, I_{LO} - \sqrt{1-4\varepsilon^2}\, E_{LO}\, q_\phi, \end{aligned} \tag{2.51}$$

where the signal intensity has been neglected as previously. Assuming that $4\varepsilon^2 \ll 1$, one can also neglect ε^2, so that

$$\delta I \;=\; 2\varepsilon I_{LO} + \; 2\sqrt{I_{LO}}\, q_\phi \tag{2.52}$$

In our time-domain experiment, the quantities of interest are the quantum fluctuations (or the shot-to-shot variations) of q_ϕ. If I_{LO} has no classical fluctuations

from shot to shot, the term $2\varepsilon I_{LO}$ will just contribute to a d.c. offset, and will not create a problem, unless it is too large and saturates the amplifier. If on the other hand I_{LO} has classical fluctuations (often called relative intensity noise, or RIN), then the homodyne signal will be strongly perturbed.

To be on the safe side, one usually considers that if I_{LO} is expressed as a number of photons in the LO pulse, then the variance of q_ϕ is on order of one photon, corresponding to the vacuum noise. Taking therefore $\langle q_\phi^2 \rangle \sim 1$, equation 2.52 gives the tolerance threshold for the unbalancing ε:

$$\varepsilon \ll \frac{1}{\sqrt{I_{LO}}} \tag{2.53}$$

It follows that for a typical local oscillator pulse of 10^8 photons, the balancing must be better than 10^{-4}. In practice other issues like the shape of the light pulse and the different characteristics of the two photodiodes (rise time, quantum efficiency) must also be taken into account, as will be discussed in the experimental chapters.

Chapter 3

Key Distribution and Quantum Continuous Variables

In chapter 1 and chapter 2 we discussed some basic features of information theory, quantum mechanics and quantum optics, focusing on Gaussian states and on the homodyne detection, the fundamental detection tool for optical quantum continuous variables. In the present chapter 3 we will use this knowledge to enter the field of cryptography, and introduce Quantum Key Distribution (QKD) within our Continuous Variable perspective.

In a first section we will see how the first cryptography protocols were born and developed, leading to the idea of *information-theoretical security*, that coincides with the scientific study of cryptography. In the novel approach provided by the *Vernam cypher* or *one-time pad*, discussed in section 3.1.2, the problem is transferred from the cryptographic protocol to the distribution of the encrypting and decrypting key.

The second section will focus on the Key Distribution problem, and show how quantum mechanics gives us very interesting tools for that purpose, giving rise to Quantum Key Distribution. We will see how QKD can be carried out using different quantum optical systems, and how implementations can be regrouped in two major categories: the Discrete Variable one (DV) that uses single isolated quanta as carriers of information, and the Continuous Variable one (CV) that transfers data using coherent detection schemes.

The last section presents the CVQKD protocol to be implemented on a silicon chip [18]. We will describe the main relevant quantities, and the security boundaries into which it is possible to extract a completely secure cryptographic key.

3.1 From classical to quantum cryptography

Cryptography is the study of secure communication strategies and protocols. The typical cryptography scenario sees two parties communicating, A and B (or *Alice* and *Bob*). Alice wants to send a message, called *plain-text*, to Bob. To do so she uses a code to encrypt the message obtaining the *cipher-text* that she sends to Bob. Bob knows the *key* (the procedure) to decode the encrypted message and retrieves the plain text. The communication can be eavesdropped by *Eve* (E) the eavesdropper,

(a) The Scytale description system

(b) The Caesar's cipher disc

Figure 3.1: Examples of ancient cryptographic systems.

who can read the cipher-text, but cannot translate it into the plain-text without knowing the key. We will see the limitations of various cryptographic protocols, and how the security level can be increased to finally get to the "ultimate" protocol, the *one-time pad*.

3.1.1 First cryptographic protocols

The first cryptographic system about which we have historical knowledge is the Greek *Scytale*, cited by Archilocus in VII century BC and explained by Plutarch in his *Parallel lives* at the end of I century AD. It is a *transposition cipher*, i.e. the plain-text is retrieved from the cipher-text by a re-arrangement of the order of the letters: a strip of leather or paper containing a string of characters is enrolled around a rod of precise diameter. The order of the letters along the strip is different from the letters read along the rod as in figure 3.1a. It was used both as a cryptographic system and as an authentication method since only the true sender/receiver would have the right rod diameter to write/read the message.

Another famous example is *Caesar's cipher*. Caesar's cipher is a *substitution cipher*, meaning that the letters in the cipher-text are different from the letters of the plain-text. The encryption/decryption procedure is as follows: after numbering the alphabet letters from $A \to 0$ to $Z \to 25$, to each letter of the plain-text the same number n is added. Caesar used $n = 3$ so that the word *ROMA* becomes *URPD*. To easily encrypt and decrypt a disc (as in figure 3.1b) can be used, but it also makes the code very easy to break.

More generally, substitution ciphers can be broken by *frequency analysis* (in all language certain letters appear more frequently than others), first described by the Arab mathematician Al-Kindi (about 800 AD). Frequency analysis broke every code until 1465 AD when Leone Battista Alberti, the *father of western cryptology*, invented the *poly-alphabetic ciphers*. A poly-alphabetic cipher is a substitution cipher in which any letter can go in any other letter without following a particular order and the assignments can change during the encrypting process. The most famous example is the Vigenère cipher, invented by Giovan Battista Bellaso in 1553 but attributed to Blaise de Vigenère. In this protocol a short keyword is used with the help of the *Tabula Recta* (figure 3.2). The tabula contains in its 26 lines all

PLAIN-TEXT	*I*	*L*	*O*	*V*	*E*	*S*	*U*	*N*	*N*	*Y*	*D*	*A*	*Y*	*S*
KEY	R	O	M	E	R	O	M	E	R	O	M	E	R	O
	17	14	12	4	17	14	12	4	17	14	12	4	17	14
CYPHER-TEXT	**Z**	**Z**	**A**	**Z**	**V**	**G**	**G**	**R**	**E**	**M**	**P**	**E**	**P**	**G**

Table 3.1: Vigenère code: example.

possible Caesar's ciphers. For each letter to encrypt one letter of the key is used to choose one line of the tabula (or equally we perform the sum mod26). The key is repeated in loop until the end of the message. Table 3.1 gives an example, encoding "I LOVE SUNNY DAYS" with the keyword "ROME".

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3.2: The *Tabula Recta* used for the Vigenère cipher.

The last example we discuss here is the *Enigma* machine, a poly-alphabetic code mechanism invented in Germany during WWII. It is a complex machine composed of 3 rotors and a plug-board. Each of the 3 rotors or wheels, containing the 26 letters of the alphabet, works as a Caesar's cypher. But they have different turnover point (a turnover point, when reached, makes the wheel on the right move by one step), and so they create a hyper-complex poly-alphabetic code when they are put together. The plug-board has a plug for each of the letters and allows to additionally switch couples of letters up to 13 pairs, even though usually only 10 couples were exchanged. Overall the number of possible combinations is more than 1.6×10^{22}.

Let us try now to analyze the security of these codes. The Scytale and Caesar's cipher are clearly easy to break. The Vigenère code and the Enigma machine are both poly-alphabetic codes. If in the middle XIX century Babbage and Kasiski found a way to break the Vigenère one, for Enigma the solution was really difficult to find, but finally the code was broken using the first computer machine *Colossus*.

So, finally, they have all been broken. But where is the weak spot? Analyzing all these protocols looking for a point in common, we find that each one of them, from the simplest to the most sophisticated, bases its security on the eavesdropper's lack of knowledge about the cryptographic code and/or on the lack of computational resources that she must employ to analyze every possible key. So, as a matter of fact, a code like these is *in principle* breakable by a powerful computer.

3.1.2 The one-time pad and the problem of the key

So is there a protocol that *in principle* cannot be broken, even though the procedure is known and the eavesdropper has the best possible computer, classical or quantum? This kind of protocols are said to be **information-theoretically secure**.

A protocol like this exists and it is called *one-time pad (OTP)* or *Vernam cipher*, invented in 1882 by Frank Miller and put under a patent in 1919 by Gilbert. S. Vernam (U.S. Patent 1,310,719). The OTP is a Vigenère code with additional features on the encryption key.

The message can be divided in blocks of n letters (typically $n = 5$) or the spaces between words can be erased, so that the length of the words cannot give information about the message. Then we address the main weakness of the Vigenère code, the fact that the key is repeated in loop. The repetition inserts correlations that are used to break the code. The only way to avoid the recurrence is to build a key that is as long as the message itself. Another feature is related to how the key is chosen. We previously chose "ROME", but it would be good for a 4 letters message. Again, to avoid repetitions, recurrences and correlations we must choose a key which is completely random and as long as the message.

At this point it is clear that the failure of a cryptographic system is related to the correlations it has in itself. If a second message must be sent we cannot use the previously used key, even though it is a random one: each key must be created for a single transmission. This is the reason why the protocol is called one-time pad.

Finally we look at the encryption and decryption process. The two processes use exactly the same key: while the cipher-text is built via the sum modulo 26, performed letter by letter, the plain-text is retrieved by performing the difference modulo 26. It follows that both Alice and Bob must possess the same secret key.

The OTP has been proven information-theoretically secure by Shannon in 1949 [19]. Later on, after Shannon introduced the concept of bit and the publication of the ASCII code, the binary alphabet replaced the Latin one and the sum modulo 26 has been replaced by the XOR gate (truth table in table 3.2). The specific characteristic of using bits and XOR is that performing twice the XOR corresponds to the Identity gate. So the operation needed to decrypt the message is still a XOR

sum.

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Table 3.2: *XOR* truth table.

After Shannon's demonstration the OTP has been called the *perfect cipher*. Still this protocol brings out a problem: Alice and Bob must have the same secret key to perform a completely safe communication. The problem has completely changed its nature: how do Alice and Bob obtain the same key?

The Key Distribution problem, that aims to deliver the same secret key to Alice and Bob, can be solved in 3 ways. The first approach consists in entrusting the keys to a *courier*. This scenario is in principle very similar to entrusting a message to your best knight who would ride to the destination.

3.1.2.1 Public key cryptography: RSA protocol

A second method is using *asymmetric cryptography* or *public key cryptography*. In public key cryptography two different keys are generated: a public one and a private one. It is the receiver (Bob) who creates the two keys. The public key can be used by any sender to encrypt the message. The encryption process is such that the decryption is possible only with the private key, known exclusively by Bob. The security of such protocols relies on mathematical operations or functions that are easy to perform knowing the public key but very complicated otherwise. In addition to key distribution asymmetric cryptography can also be used for authentication. The most famous and commonly used public key protocol is the RSA [20] proposed by Rivest, Shamir and Adleman in 1978, which provides both authentication and key distribution within a so-called Public Key Infrastructure (PKI).

The RSA protocol is efficient and largely used (the e-mail address/password system is based on it), but it breaks the unconditional security given by OTP: a safe key distribution depends on the fact that the eavesdropper does not have a powerful enough calculator *yet*. We look for a key distribution system built on something that cannot fail: the most reliable statements are the laws of physics. Since classical computation cannot lead beyond hard solving problems, we can use quantum mechanics to overcome this limit.

3.2 QKD with Continuous Variable

3.2.1 Quantum mechanics to solve the KD problem

The failure of classical systems lies in the fact that classical information can be copied without constraints: an eavesdropper can obtain a perfect copy of the cipher-

text and freely work on it without being noticed. This is the critical aspect that quantum mechanics can solve.

Let us suppose that the information is encoded into a quantum system. To extract this information from a quantum state a measurement is needed. But in section 1.2.2 we saw that any interaction with the state will produce a dramatic change in the state itself. In the same section it is explained how it is impossible to efficiently clone a quantum state. Moreover for non-commuting observables a measurement on one of them distorts inevitably also the other. This is why quantum states are better than classical ones for key distribution. It is important to highlight that from now on, talking about information and about what happens during the communication between Alice and Bob, everything will be related to the key exchange and extraction, not to the true message (that will be encrypted and decrypted with the extracted key afterwards using the already mentioned OTP).

We will now describe the first two proposed QKD protocols. Even though they do not use continuous variables, they are of extreme importance because they have started the whole field of QKD [21, 22].

3.2.2 The first (DV) protocols

In 1984 Bennett and Brassard developed the first QKD protocol, the BB84 [23] (denoting the authors and the year of invention). It is a discrete variable protocol that uses single quantum states as carriers of information (such as photons). The protocol uses two binary alphabets, the computational one ($|0\rangle, |1\rangle$) and the diagonal one ($|+\rangle = \frac{1}{2}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{2}(|0\rangle - |1\rangle)$). The letters of the two alphabets are eigenstates of the two Pauli matrices σ_z and σ_x (equation 1.40). Recalling the Bloch sphere representation in figure 1.2, we see that the two alphabets lie on two orthogonal bases, as the fact that they are eigenstates of two different Pauli matrices could have already suggested. Following that, talking about an alphabet or a basis will be equivalent (for example, computational basis, diagonal alphabet).

The protocol works as follows:

1. Alice generates a string of random bits.

2. Each bit can be encoded into one of the two bases, following the rule

$$0 \quad \rightarrow \quad |0\rangle,\ |+\rangle = |0\rangle_x \tag{3.1a}$$
$$1 \quad \rightarrow \quad |1\rangle,\ |-\rangle = |1\rangle_x \tag{3.1b}$$

   The encoding basis is randomly chosen for each bit.

3. Alice has now a string of qubits to send to Bob.

4. For each arriving qubit Bob randomly chooses a basis (σ_z or σ_x) onto which project (measure) the qubit. Neglecting for now both eavesdropping (presence of Eve) and noise, he faces 2 scenarios: half of the times he chooses the same alphabet used to create the qubit and the measurement will produce a good

result; the other half of the times he picks the wrong basis, which is orthogonal to the good one: the outputs "0" and "1" have the same probability so the measurement will produce half of these times (25% of the total) the good result and the other half (25% of the total) the wrong one. This is the last quantum communication step.

5. Now classical communication begins. First Alice and Bob exchange only the list of the basis they used to encode (Alice) and measure (Bob), deleting all the bits related to a different basis choice. This happens even though Bob's outcome is correct (he could not know anyway at this stage). They obtained the so-called *raw key*.

6. Now we take into account possible errors due to a noisy channel and/or to Eve. Alice and Bob perform two classical algorithms via a public channel: *Information reconciliation* and *Privacy Amplification*.

7. Information reconciliation reduces to zero the possible errors occurred during communication (see also section 1.3.1.3). After a pre-estimation (performed before the protocol) of the error rate R, the string of bits is divided in sub-strings of length l , such that the probability of having more than one error in the sub-string tends to zero: $lR \ll 1$. They perform a parity check on the subset discarding the last bit. If they get the same parity they keep the string, otherwise they search for the wrong bit by dividing into two the subset and by performing the parity check on the 2 halves, proceeding with the discard process until they find the error.

8. Privacy amplification is used to decrease the mutual information between them and a possible Eve, i.e. reduce the information Eve has about the final key. Let us show one example. After reconciliation Alice and Bob have same string of bits, but a part of them is also known by Eve. It can be demonstrated that this string is incomplete and/or has errors. So Alice chooses random couples of bits (for example, 121st and 36th) and she communicates to Bob only the position of them, not their values, and they replace the bits with their XOR value, finally obtaining the *secret key*.

It can be demonstrated that the knowledge Eve has about the key can be arbitrarily reduced, no matter the eavesdropping strategy she adopts. Note that she can use two different strategies:

- *Intercept-resend attack*: she directly measures single qubits on a random basis, recreating the qubit in accordance with the alphabet she used.

- *Translucent attack*: she produces ancillary qubits that interact with the qubits sent by Alice and later on she measures the ancillae.

While the intercept-resend strategy is more easy to perform, translucent attacks are more effective. We can divide them into three categories:

- *Individual attack*: Eve interacts with single pulses and stores the ancillae in a quantum memory. Then after the sifting in reverse reconciliation and before the key distillation she performs the measurement.
- *Collective attack*: Eve interacts individually with each pulse but the measurement is performed after the distillation stage, applying a collective measurement on her ancillae.
- *Coherent attack*: Eve interacts with blocks of pulses collectively and applies a joint measurement on them after listening to the distillation process.

The second important QKD protocol has been designed by Ekert in 1991 [24] and is called *E91*. Without entering into details, this protocol is particularly interesting because it uses entangled states generated by a source that may be external to Alice and Bob. For a single point-to-point link it provides the same functionality as BB84, and also opens the way to *quantum repeaters*, based on entanglement distillation and quantum teleportation.

3.2.3 Advantages of CV

The two protocols quoted above, besides being historically important, are also very efficient. We could discuss about their imperfections and how an eavesdropper could take advantage of them, but they do in fact work well, so why changing to continuous variables? We will not discuss whether continuous variables are better than discrete variables or vice-versa: they express two different physical approaches and depending on the application and on the practical implementation one or the other may be preferred.

Let us rather present the features of the two perspectives to clarify the choice of CV for our purposes. DV and CV approaches correspond to different degrees of freedom of the quantum state into which the information will be encoded, represented and measured. These theoretical and practical issues, resumed in table 3.3, are the reason why CVQKD protocols are different from DVQKD ones.

Light nature	Discrete variables	Continuous variables
Basic state	Fock state	Gaussian state
Physical quantities	Number, coherence	Field quadratures
Theoretical description	Density matrix	Wigner function
Measurement System	Counting: **APD, TES...**	Interference: **Homodyne detection**

Table 3.3: Comparison between DV and CV.

The quantum state of a photon is a Fock state and we represent it with a density matrix ρ. Using degrees of freedom as polarization, momentum, frequency, arrival time we can encode information in them. The way photons are measured is to count them (usually after selecting the ones with a particular set of properties). The quantities of interest are therefore the *photon number* and their coherence.

In the CV approach the simplest state is a Gaussian state, represented by its Wigner function. The main properties of a wave are amplitude, phase and frequency. If we fix the frequency, only amplitude and phase are relevant, and in the phase-space they can be translated into the field quadratures Q and P. The measurement is performed by demodulating the state, i.e. through homodyne detection.

The measurement setup is the main reason why we wanted to implement a CVQKD protocol instead of a DV one. In fact single photon counting requires particular detection instrumentation, such as APD (Avalanche Photo-Detectors), VLPC (Visible Light Photon Counters), TES (Transistor Edge Sensor), SNSPD (Superconducting Nanowire Single Photon Detectors), i.e. single photon counters. These devices need to be cooled, some of them at cryogenic temperatures, to suppress the dark counts that would hinder single photon detection.

Since the main purpose of this work is to implement the protocol using a very small device, DV detection techniques do not fit well with this requirement. On the contrary, as we will see in the next chapter, CV protocols can be easily implemented on-chip, in particular thanks to the homodyne detection, which necessitates only a balanced BS and two fast photodiodes, and not single photon counters.

3.3 The GG02 protocol

3.3.1 Information theory for Gaussian states

Another step is needed to be able to address quantum information using continuous variables: the passage to the continuous regime.

In the CV case, the alphabet is not a discrete ensemble but real numbers taken from a continuous domain. The passage to this domain is made by properly substituting sums with integrals over sections $\delta a, \delta b$ of the real axis. We define the **differential entropy** of the communication A as

$$S(A) \;=\; \int da\, p(A=a)\, \log_2\, p(A=a) \tag{3.2}$$

For a Gaussian distribution of variance $\langle A^2 \rangle$, the differential entropy is

$$S_{gauss}(A) \;=\; \frac{1}{2} \log_2(2\pi e \left\langle A^2 \right\rangle) \tag{3.3}$$

In a higher dimension (d) vector space we can generalize this expression for a random Gaussian vector of covariance matrix V

$$S_d(A) \;=\; \frac{1}{2} \log_2 \left((2\pi e)^d |V|\right) \tag{3.4}$$

The mutual information for continuous variables has the same properties of Shannon entropy defined in section 1.1.2.1, so:

$$I_{AB} \;=\; S(A) - S(A|B) = S(B) - S(B|A) = \;S(A) \;+\; S(B) \;-\; S(A,B) \tag{3.5}$$

Continuous channels are usually additive ones, where the noise is statistically independent from the signal A and it is added to the signal itself. The output of the channel will be

$$B \;=\; A \;+N \tag{3.6}$$

and using the independence between signal and noise

$$S(A,B) \;=\; S(A,N) \;=\; S(A) \;+\; S(N) \tag{3.7}$$

So the mutual information between A and B is

$$I_{AB} \;=\; S(B) - S(N) \tag{3.8}$$

Remembering equation 3.3, for Gaussian states this equation becomes

$$I_{AB} \;=\; \frac{1}{2}\log_2\frac{\langle B^2\rangle}{\langle N^2\rangle} \;=\; \frac{1}{2}\log_2\left(1+\frac{\langle A^2\rangle}{\langle N^2\rangle}\right), \tag{3.9}$$

where

$$\Gamma \;=\; \frac{\langle A^2\rangle}{\langle N^2\rangle} \tag{3.10}$$

is the **signal-to-noise ratio (SNR)** of the communication. Equation 3.9 is an upper bound: the equality holds only for statistically Gaussian states.

3.3.2 The protocol: reverse reconciliation

The GG02 protocol [18] can be implemented using coherent states or squeezed states (as a generalization of the first case). It can also be extended to EPR states. Depending on the experimental apparatus one of the three sources can be used and the validity of the security proofs does not change. In this work coherent states are used.

The protocol is divided into two main parts: the quantum communication, in which Alice and Bob exchange bits of information encoded in quantum states, and the classical communication, formed by classical algorithms performed through classical authenticated channels. In more detail the GG02 protocol follows these steps:

1. Alice generates $2N$ random values, following a Gaussian distribution $(0, V_A)$ of mean value $d = 0$ and variance $V = V_A$, where the variance is normalized by the shot noise N_0. Equivalently we can say that she generates N-times the 2 Gaussian random variables q_A, p_A.

2. Alice builds the coherent quantum state $|q_A + \imath p_A\rangle$ (see section 2.1.4.4) and sends it to Bob.

3. Bob measures one of the two quadratures by means of a homodyne detection. The choice of the measured quadrature is performed randomly for each received state. Bob has now a string of N Gaussian distributed values. This ends the quantum communication.

4. Using an authenticated classical channel Bob communicates to Alice his quadrature choices for the measurements. This is called *sifting*, and after it Alice and Bob share correlated but noisy data, that may be partially known by Eve.

5. Alice and Bob compare a randomly chosen part of their data using a classical authenticated channel, and evaluate the added noise in the transmission.

6. Alice and Bob correct the errors in the non-disclosed part of their data using error correcting codes. The basis for the correction is Bob's data, not Alice's data, and the error syndromes are sent by Bob to Alice. For this reason this step is called *reverse reconciliation*, because the data in the reconciliation process flows in the reverse direction with respect to the quantum transmission. This is said to be a **reverse reconciliation** protocol.

7. Alice and Bob have two sets of errorless correlated data, and an evaluation of the channel noise. If this noise is small enough, they can extract a fully secret key through privacy amplification algorithms. The size if the key decreases if the noise increases, and it goes to zero if the noise is too large.

3.3.2.1 Heterodyne detection

The protocol can be slightly modified when the homodyne detection is replaced by the *heterodyne detection*. We briefly introduce it for completeness but we will not enter into details, since the heterodyne detection has not been used in this work.

The heterodyne detection is a double homodyne detection in which the two measurement sets are shifted by a $\pi/2$ phase factor. In other words the two local oscillators have phases ϕ and $\phi + \pi/2$ respectively, while the signal is split in two and measured at the same time in the two homodyne sets.

This allows the simultaneous measurement of the signal over both Q and P. On the other hand when the signal is divided in two, the SNR ratio decreases, leading to a noisier double set of data.

3.3.3 Excess noise and key extraction through noisy channels

After transmission and sifting Alice and Bob have correlated data i.e. they share some information. This is translated, using equation 3.9, into saying that their mutual information I_{AB} is positive. For a Gaussian modulation and reception the

mutual information can be written as (see section 3.3.1):

$$I_{AB} = \frac{1}{2}\log_2(1+\Gamma_B) \tag{3.11}$$

where Γ is the SNR of the communication. Since Eve, using some eavesdropping strategy, can have access to some information as well, she will have some non-zero mutual information shared with Alice (Bob), saying I_{AE} (I_{BE}). For reverse reconciliation I_{BE} matters, and the condition for a successful key extraction is

$$\Delta I = I_{AB} - I_{BE} > 0 \tag{3.12}$$

also called *secret information rate* or *raw key rate*. It means that, at the end of the quantum communication, if the information that Eve has about Bob data is less than the information Alice has about it, then a key can be extracted.

3.3.3.1 Real decimal to binary transformation

The sets of data at Alice's and Bob's (namely $(q_i, p_i)_A$ and $(x_i)_B$ where $x = q$ or p) are not bits, but real numbers. At the end of the communication these numbers must be translated into binary digits. To do so the phase space is divided in squared regions of same area (creating a grid), so that each region corresponds a probability, given by the particular distribution of the generated numbers. To each part of the grid a string of bits that has the same probability appearance is assigned.

The size of the grid squares must be optimized in order to extract as information as close as possible to I_{AB}. If the grid is too tight, most of the corresponding bits will be wrong due to shot noise. If the grid is too loose, the number of extracted bits may be smaller that I_{AB}. Optimizing the grid is thus connected with the error correcting code, and is part of the reconciliation process.

In practice, this binarization and reconciliation process does not have a perfect efficiency, and Alice and Bob do not recover the full value of I_{AB}, but a fraction βI_{AB} with $\beta < 1$. As a consequence the secret key rate is reduced to

$$\Delta I_{eff} = \beta I_{AB} - I_{BE}. \tag{3.13}$$

As said before, finding error correcting codes with a value of β as large as possible is a major issue for obtaining a significant value of ΔI_{eff}. Codes with $\beta \sim 0.95$ have been implemented, allowing secret key distribution for distances up to 80 km.

3.3.3.2 Description of the transmission channel

In order to evaluate the secret ket rate from the mutual information, we must get into more details about what happens during the quantum communication. As previously said only the case of coherent states is taken into account (no squeezing),

and Alice sends Gaussian-modulated data to Bob. We will also consider only the reverse reconciliation protocol described in the previous section.

In principle Eve can implement any kind of Gaussian or non-Gaussian attack, but for simplicity we will consider only here the case of *individual Gaussian attacks*. This corresponds to the first security proof derived for GG02 in 2002, and can be treated with very simple algebraic formulas. Since then, security proofs have been extended to much more general situations (collective and coherent attacks), as will be briefly considered in the last section of this chapter.

We consider therefore a Gaussian channel, and assume also that the two quadratures are treated in the same way, since it can be shown that this leads to optimum key rates for Alice and Bob and to optimum eavesdropping strategies for Eve. Alice sends a modulated coherent state, and the variance VN_0 of her output beam includes a contribution $V_A N_0$ due to her Gaussian modulation, and a contribution N_0 due to the vacuum noise of the coherent state, so $V = V_A + 1$. Defining Q_A as the modulated part of Alice's beam, at Bob's site we have for each quadrature

$$Q_B = g(Q_A + Q_N) \qquad P_B = g(P_A + P_N) \tag{3.14}$$

where $g^2 = G$ is the total gain of the communication between Alice and Bob. $Q_N(P_N)$ is the additive noise (Gaussian distributed) of the quantum state sent by Alice and arriving at Bob's. One can thus define the following quantities:

$$\left\langle Q_A^2 \right\rangle = (V - 1)N_0 = V_A N_0 \tag{3.15a}$$
$$\left\langle Q_B^2 \right\rangle = G(V + \chi)N_0 = G(1 + V_A + \chi)N_0 = V_B N_0 \tag{3.15b}$$
$$\langle Q_A Q_B \rangle = g \left\langle Q_A^2 \right\rangle \tag{3.15c}$$

where χ is is called *equivalent added noise* by the communication channel. The same equations can be found for the quadrature P. From now we will normalize all variances to the shot noise variance N_0, which amounts to taking $N_0 = 1$.

The added noise χ can arise from many factors, including the eavesdropping of Eve, and it is useful to separate the different contributions to this noise, to be able to act and correct them individually. So let us split G as $G = T\eta$, where T is the transmission of the channel, and η the quantum efficiency of Bob's detector. Correspondingly, χ can be split in two parts, one containing the noise added to the channel, one containing the noise due to the detection:

$$\chi_{ch} = \frac{1-T}{T} + \varepsilon, \qquad \chi_{hom} = \frac{1-\eta}{\eta} + \frac{v_{el}}{\eta} \tag{3.16}$$

where ε is the excess channel noise (referred to the input), and v_{el} is the electrical noise of the detection system. The first term $(1-T)/T$ in χ_{ch} corresponds to the effective noise due to the losses $(1-T)$ in the channel, which reduce the signal to noise ratio. In a quantum picture, it is attributed to vacuum noise entering the

channel as soon as some light is lost. The second term ε is the *excess noise* and it represents the additional noise that cannot be attributed to pure losses. It may obviously be due to eavesdropping, but also to practical imperfections like phase noise, errors in the preparation of the state, etc. A similar interpretation applies to χ_{hom}. We note that T and η appear at the denominators because the noises are always *referred to the input*, as it is usual in signal processing.

The total noise will be the sum of the channel noise and the detection noise scaled by the transmission:

$$\chi \;=\; \chi_{ch} \;+\; \frac{\chi_{hom}}{T} \;=\; \frac{1-G}{G} \;+\; \frac{v_{el}}{G} \;+\; \varepsilon \;=\; \frac{1-G}{G} \;+\; \xi \tag{3.17}$$

where we used again the relation $G = T\eta$. As before the first term $(1-G)/G$ corresponds to the total losses in the channel, and the second term is the total excess noise $\xi = \varepsilon + v_{el}/G$. Given these definitions, the variance at Bob's is

$$V_B = \; G(V \;+\; \chi) = \; G(1 \;+\; V_A \;+\; \chi) = 1 + \eta T(V_A + \xi) \tag{3.18}$$

Given these definitions and relations, we now have to find a way to bound Eve's knowledge about Bob's data, based on an estimation of the channel properties T and ξ by Alice and Bob.

3.3.3.3 Bounding Eve's knowledge of Bob's data

Bob performs the measurement on one quadrature Q_B, that must be estimated by Alice and Eve to retrieve the key. We will denote the best estimators as respectively αQ_A and εQ_E, corresponding to the errors $Q_{B|A} = Q_B - \alpha Q_A$ and $Q_{B|E} = Q_B - \gamma Q_E$, where α and γ are optimized so that

$$V_{Q_{B|A}} \equiv min_\alpha \left\{ \left\langle Q^2_{B|A} \right\rangle \right\}, \quad V_{Q_{B|E}} \equiv min_\gamma \left\{ \left\langle Q^2_{B|E} \right\rangle \right\} \tag{3.19}$$

The same relations hold for the P's, and one can evaluate easily the commutator between $Q_{B|A}$ and $P_{B|E}$:

$$[Q_{B|A}, P_{B|E}] \;=\; [Q_B, P_B] \;=\; 2\,\imath N_0 \tag{3.20}$$

providing a Heisenberg inequality between the corresponding variances:

$$V_{Q_{B|A}} V_{P_{B|E}} \;\geq\; N_0^2 \tag{3.21}$$

Since the channel is assumed to behave in the same way for both quadratures, one has $V_{Q_{B|A}} = V_{P_{B|A}} = V_{B|A}$ and $V_{Q_{B|E}} = V_{P_{B|E}} = V_{B|E}$ and thus

$$V_{B|A}V_{B|E} \geq N_0^2 \tag{3.22}$$

This inequality implies a fundamental bound on Eve's conditional variance $V_{B|E}$, given Alice's conditional variance $V_{B|A}$, which can be evaluated by Alice and Bob by measuring the channel transmission and noise. The evaluation of the key rate relies therefore on establishing proper bounds on these conditional variances.

Here we will simply recall the main results, which have been established by Frédéric Grosshans in his PhD thesis, and constitute the basis of the GG02 protocol. Taking again $N_0 = 1$, one gets tor Alice

$$V_{B|A} \geq V_{B|A,min} = G(\chi + \frac{1}{V}) \tag{3.23}$$

and for Eve the conditional variance is limited by the inequality 3.22. A (non trivial) reasoning shows that the relevant Alice's variance to be used is $V_{B|A,min}$, so one gets

$$V_{B|E} \geq V_{B|E,min} = \frac{1}{G(\chi + \frac{1}{V})} \tag{3.24}$$

On the other hand the value of $V_{B|A}$ for a coherent state protocol is larger that $V_{B|A,min}$, and is given by

$$V_{B|A,coh} = G(\chi + 1) \tag{3.25}$$

We will see below that a secret key can be obtained if $V_{B|A,coh} < V_{B|E,min}$, i.e. if there is less noise on Alice's side than on Eve's. From the equations above this requires that

$$G^2(\chi + 1)(\chi + \frac{1}{V}) < 1 \tag{3.26}$$

giving an upper bound for the added noise χ that the communication can suffer.

3.3.3.4 Secret information rate

The equation above gives a condition for a non-zero secret key rate, but we need also the actual value of this rate, given the current hypothesis of Gaussian-modulated coherent states by Alice, individual Gaussian attacks by Bob, and reverse reconciliation [25]. For this purpose one needs to evaluate the mutual information between Alice and Bob on the one hand, and between Eve and Bob on the other hand. They are given by the following expressions [25]:

$$I_{BA} = I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} \tag{3.27}$$

where $V_B = \eta T(V + \chi)$, and

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E}} \tag{3.28}$$

where Eve's conditional variance is bounded by $V_{B|E,min}$ calculated above.

Finally the secret key rate is then given by

$$\Delta I_{individual} = I_{AB} - I_{BE} = \frac{1}{2}\log_2 \frac{V_{B|E,min}}{V_{B|A}} = -\frac{1}{2}\log_2(G^2(\chi+1)(\chi+\frac{1}{V})). \tag{3.29}$$

where all quantities V, G, χ are known or evaluated by Alice and Bob, by probing the properties of the transmission channel.

3.3.3.5 Practical issues

In practice, a few caveats should be noticed.

First, as said before, the data reconciliation has a finite efficiency β, reducing the secret key rate to $\Delta I = \beta I_{AB} - I_{BE}$.

Second, it is legitimate to consider that Eve can implement very powerful attacks on the channel itself (by exploiting T and ε). However, it can be considered more "paranoid" to consider that she can do the same on Bob's detectors (by exploiting η and v_{el}), because this detector is supposed to be in a secure site. This leads to the "realistic" hypothesis of excluding the possibility, which can be translated in changing $V_{B|E,min}$ into the (larger) value:

$$V_{B|E,real} = \eta\left[\frac{1}{T(\frac{1}{V}+\chi_{ch})} + \chi_{hom}\right] \tag{3.30}$$

which will be used to evaluate the secret key rate in the next chapters.

Another important issue is that a convenient method to evaluate the channel is to consider the correlation between the data sent by Alice (denoted as Q_A), and the signal received by Bob (denoted as Q_B). One defines therefore

$$\rho^2 = \frac{\langle Q_A Q_B\rangle^2}{\langle Q_A^2\rangle\langle Q_B^2\rangle} \tag{3.31}$$

Defining $V_N = \chi + 1$ as the variance of Bob's noise, one has $V_B = G(V_A + V_N)$. Then using equations 3.15 one can derive an expression of correlations depending only on the variances V_A and V_N:

$$\rho^2 = \frac{GV_A^2}{V_A G(V_A+V_N)} = \frac{V_A}{V_A + V_N} \tag{3.32}$$

which will be useful later on.

3.3.3.6 Collective and coherent attacks

When a collective attack is performed against CVQKD systems, Gaussian attacks are proven to be optimal [26, 27]. However the information shared between Eve and Bob is no longer upper-bounded by the mutual information, but by the *Holevo quantity* [28]

$$\chi_{BE} = S(\rho_{BE}) - \int dx_B p(x_B) S(\rho_E^{x_B}) \tag{3.33}$$

where $p(x_B)$ is the probability distribution of Bob's measurement outcomes, $\rho_E^{x_B}$ is Eve's state conditional on Bob's outcome and S is the von Neumann entropy.

For a Gaussian state the von Neumann entropy can be expressed by

$$S(\rho) = \Sigma_i G\left(\frac{\lambda_i - 1}{2}\right) \tag{3.34}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and the λ_i are the eigenvalues of the covariance matrix which characterizes ρ.

Therefore under collective attacks the (Holevo) raw key rate is

$$\Delta I_{collective} = \Delta I_{Holevo} = \beta I_{AB} - \chi_{BE} \tag{3.35}$$

If one goes to coherent attacks, which are the most powerful in Eve's hands, the study is more complicated. It has been proved [28] that for DV protocols under the assumption of symmetry of the reconciliation and channel probing protocols, coherent attacks are not more efficient than the collective ones.

For a consistent approach, it is also required to consider that the data samples used by Alice and Bob are not arbitrarily large, but have a finite size. Recent works by Anthony Leverrier [29, 30] have established that the key rate ΔI_{Holevo} above remains essentially valid for large enough data samples, with "finite size" correction that can be precisely evaluated. Such studies are outside of the scope of the present thesis.

Chapter 4

Introduction to Silicon Photonics

The technology of devices and systems typically evolves in two directions: performance upgrade and size reduction. The miniaturization process of optical systems has began several years ago and has led to high-performance fibered devices for both passive and active optical components. Optical shutters, beam splitters, phase and amplitude modulators, polarizers, have been built exploiting advances in manufacturing and have been used for demonstrating both classical and quantum effects. Similarly to the path followed by electronic devices, the next step is to pursue chip-scale integration, which will eventually lead to complete integration of both optical and electronic components of a system onto the same chip.

There is a currently a great variety of integration platforms for *photonic chips*, presenting specific advantages and disadvantages in the obtained features. There is therefore no unique technology suitable for the integration of any optical system, and the choice of the platform critically depends on the desired setup and performance requirements in each implementation. Among the existing platforms, silicon photonics presents several appealing characteristics, including in particular its compatibility with silicon-based CMOS wafer fabrication facilities that offer the potential for cost-effective chip production with high yield and reproducibility.

In the field of quantum communications, photonic integration efforts until today have mostly focused on component development based on integration on silicon, III-V compound semiconductors, nonlinear optical dielectric materials or glass [31–35]. From a system perspective, and in particular for QKD, a recent experiment has successfully demonstrated the operation of a GHz clocked discrete-variable QKD system using an indium phosphide (InP) transmitter chip and a silicon oxynitride (SiO_xN_y) receiver chip, to implement BB84 [23], Coherent One Way (COW) [36] and Differential Phase Shift (DPS) [37] protocols (not treated in this work) [38]. In this implementation, the single-photon detection was performed outside the chip.

The continuous-variable approach that we are pursuing in this work allows for extended integration, including the detection module, opening up the perspective of simple, compact and low-cost devices. As we will see, silicon photonics supplies in principle all the optical, passive and active, devices that are necessary for the realization of the GG02 CVQKD protocol that we have previously described, at telecommunication wavelengths ($\lambda = 1550nm$).

In the first part of this chapter we describe the main physical effects that take place in silicon based devices and in the second part we explain how they are used to realize the desired optical components.

4.1 Main physical effects

In the GG02 protocol the information is encoded into quantum states of light by applying amplitude and phase modulation. Silicon photonics features relatively low electro-optics effects at telecom wavelength, leading in general to poor opto-electronic performances; several effects have therefore been studied to obtain the amount of modulation required for applications.

The physical quantity of interest in this section is the complex refractive index $\tilde{n}$, defined as:

$$\tilde{n} \;=\; n + i\alpha, \tag{4.1}$$

where n is the refractive index and α is the absorption coefficient.

When an electric field is applied to a material, its refractive index can change in both the real and the imaginary part. If the change is in the real part, the effect is called *electro-refraction* (and corresponds to a change in the index of refraction), while if the imaginary part is modified it is called *electro-absorption* (and corresponds to a change in the dissipative properties of the material).

We also define the complex dielectric function (or permittivity) $\tilde{\varepsilon}$ as:

$$\tilde{\varepsilon} \;=\; \varepsilon' + i\varepsilon'', \tag{4.2}$$

where $\varepsilon' = n^2 - \alpha^2$ and $\varepsilon'' = 2n\alpha$.

Below we briefly present the physical phenomena that can lead to a change of the refractive index and so to an induced optical effect.

4.1.1 Pockels and Kerr effects

The so-called *Pockels effect*, of linear electro-optic effect, corresponds to a change in the refractive index of the material that is linearly proportional to the applied electric field. It is absent in centrosymmetric crystals like bulk silicon; however, under strong physical stress the symmetry breaks, allowing for the appearance of the Pockels effect in silicon as well.

If the change of the refractive index is quadratic in the electric field, then the associated electro-optic effect is called *Kerr effect*. This is present in all materials but is in general much weaker than the Pockels effect.

Even though these effects are suitable for modulation, the materials where they are typically present, such as lithium niobate, cannot be integrated with CMOS technology.

4.1.2 Franz-Keldysh effect (FKE) and Quantum-confined Stark effect (QCSE)

In semiconductors an electron can be promoted from the valence band to the conduction band by absorbing a photon with energy corresponding to the band gap $\hbar\omega = E_g$ (see figure 4.1(a)). If a strong uniform electric field is applied, the band structure is distorted and the electrons and holes wave functions can extend inside the gap region, decreasing the effective energy gap (figure 4.1(b)). This effect is called *photo-assisted tunneling*, or Franz-Keldysh effect (FKE).

The FKE can be used to modify both the real and the imaginary part of $\tilde{n}$: the absorption change $\Delta\alpha$ is bigger when the incident light has an energy close to E_g. If the difference between $\hbar\omega$ and E_g increases, then Δn is more important.

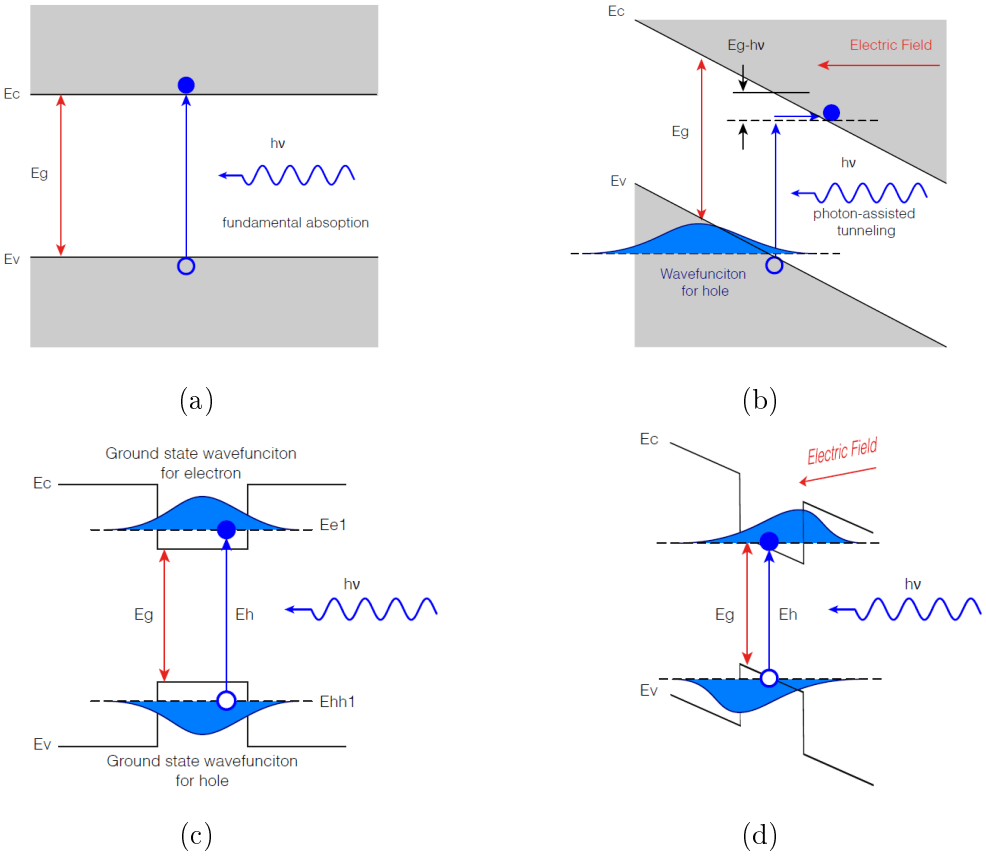


Figure 4.1: (a) Semiconductor band-gap structure at equilibrium and (b) FKE; (c) Quantum well band-gap structure and (d) QCSE [1].

We find a similar effect, called Quantum-confined Stark effect (QCSE), when the electric field is applied to a quantum well, which is a small band-gap structure 'sandwiched' between two bigger band-gap ones (figure 4.1(c)). Since E_g is small the wave functions of the holes and the electrons, both symmetrically distributed along the well, couple together forming an exciton. The band structure distortion due to an electric field induces the wave functions to collapse on the edges of the well, diminishing the energy needed for a photon absorption/emission (figure 4.1(d)). This energy is reduced also by the exciton energy that helps the transition.

FKE and QCSE are efficient in direct band-gap semiconductors, such as InAs or GaAs, while they typically cannot be used for fast modulation in germanium and silicon that are indirect band-gap materials.

4.1.3 Plasma dispersion effect

The *plasma dispersion effect*, or *free carrier dispersion effect*, consists in a variation of $\tilde{n}$ depending on the variation of the carrier concentration. It affects both the real and the imaginary part, according to the Drude-Lorentz equations [1, 39]:

$$\Delta n = \frac{-\lambda_0^2 e^2}{8\pi^2 c^2 \varepsilon_0 n}\left(\frac{\Delta N_e}{m_e^\star} + \frac{\Delta N_h}{m_h^\star}\right) \tag{4.3a}$$

$$\Delta \alpha = \frac{\lambda_0^2 e^3}{4\pi^2 c^3 \varepsilon_0 n}\left(\frac{\Delta N_e}{\mu_e m_e^{\star 2}} + \frac{\Delta N_h}{\mu_h m_h^{\star 2}}\right), \tag{4.3b}$$

where N denotes the carrier density, $m^\star$ the effective mass and μ the mobility of free electrons and holes.

The plasma dispersion effect is the physical phenomenon used in silicon modulators, since it is very effective also for indirect band-gap semiconductors and hence allows for modulation at high speed (on the GHz range).

We obtain plasma dispersion by means of *carrier depletion*, where the number of the free carriers is decreased by applying a reverse bias voltage.

4.1.4 Thermo-optic effect

Finally, the *thermo-optic effect* relies on the fact that the refractive index changes with the temperature of the semiconductor. A higher temperature provides energy to free carriers in the valence band to transit to the conduction band. Since this depends on the energy gap and the particular band structure of the material, each material has its own thermo-optic coefficient: for silicon this is

$$\frac{dn}{dT} = 1.86 \times 10^{-4} K^{-1}. \tag{4.4}$$

This value gives a Δn that is two to three times larger than other effects, while absorption is not affected. However, the thermo-optic effect is not as fast as the plasma dispersion one and its use faces the challenge of precise temperature control.

4.2 Optical structures

The phenomena described in the previous section are used as a basis to build the passive and active optical devices that are going to be the building blocks of the photonic chips described in the following chapters.

4.2.1 Waveguides

In silicon photonics, the guiding of light is typically achieved using waveguides built using Silicon-On-Insulator (SOI) structures. This technology offers in general waveguides with a very high refractive index, allowing for an increased circuit compactness even for complex layouts involving many elements. In these structures, the confinement is guaranteed by the refractive index difference between the insulator (silicon dioxide SiO_2) and the crystalline silicon. The insulator layer is put on top of the silicon substrate and a crystalline silicon layer is posed on top of the insulator.

Different SOI geometries lead to different features and fabrication challenges of the waveguide. We can see five different types of SOI waveguides in figure 4.2.

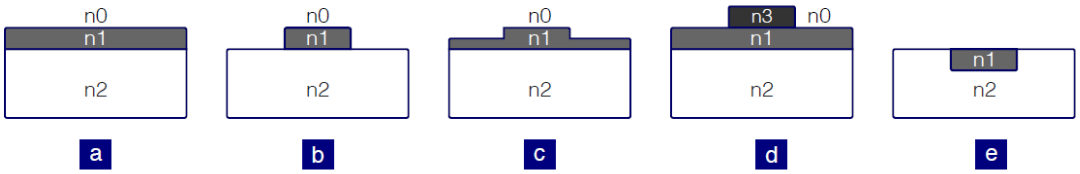


Figure 4.2: Different waveguide structures: (a) thin-film, (b) strip, (c) rib or ridge, (d) strip loaded and (e) buried strip waveguides [2]

An important feature of a waveguide is the filling factor Γ_{FF}, which is defined as the portion of the total optical flux $P(x, y)$ propagating along the z-direction confined and guided into a transversal region R, which usually corresponds to the core of the waveguide itself:

$$\Gamma_{FF} = \frac{\int_0^R P(x,y)dxdy}{\int_{-\infty}^{\infty} P(x,y)\,dxdy} \tag{4.5}$$

4.2.2 Phase shifters

The phase modulation required for our implementation is achieved by means of a phase shifter. As discussed previously, in silicon photonics this is achieved using the plasma dispersion or the thermo-optic effect, where the phase change is induced by applying a voltage to drive a change of free carrier concentration or by a temperature rise, respectively.

If Δn is the refractive index variation, the phase variation is

$$\Delta\phi = \frac{2\pi\Delta nL}{\lambda_0}, \tag{4.6}$$

where L is the device length and λ_0 is the wavelength of light in free space. From equation 4.6, we see that the phase change depends linearly on the device length.

To evaluate the performance of a phase modulator, an important figure of merit is the *modulation efficiency*, defined as $V_\pi L_\pi$, where V_π and L_π are the voltage and modulator length required for a π shift, respectively. These two quantities are not

independent: it is possible to calculate the characteristic length of the phase shifter from its V_π as

$$L_\pi = \frac{\lambda}{2\Delta n(V_\pi)} \tag{4.7}$$

The modulation efficiency is a characteristic of a given doping process (the role of doping will be discussed later in this chapter). In general, each material shows a different optimal product of V_π and L_π. One can also choose to optimize one quantity with respect to the other (e.g. it is possible to reduce the V_π voltage by increasing the length of the device).

A second important figure of merit is the insertion loss (IL), defined as the ratio of the input power entering the device and the maximal power obtained at the output:

$$IL\ (dB) = 10\log_{10}\left(\frac{I_{IN}}{I_0}\right) \tag{4.8}$$

4.2.3 Mach-Zehnder interferometer

Amplitude modulation is achieved by means of a Mach-Zehnder Interferometer (MZI). The two arms of the MZI contain two phase shifters as the ones previously described: the constructive/destructive interference at the output of the MZI obtained by changing the relative phase in the two arms leads to the variable modulation of the amplitude of the light pulse.

In an ideal symmetric MZI, balanced 50/50 beam splitters are used and two identical phase shifters are inserted in the two arms of the MZI. The phase difference at the output of the MZI is:

$$\Delta\phi = \frac{2\pi\Delta n_{eff}L}{\lambda_0}, \tag{4.9}$$

where Δn_{eff} is the induced refractive index difference between the two arms of the MZI. If no losses are taken into account, it follows that the output varies with Δn_{eff} as

$$I_{OUT} = I_0\cos^2\left(\frac{\pi}{\lambda}\Delta n_{eff}L\right) \tag{4.10}$$

For an asymmetric configuration, in which the phase shifters have different lengths, the output intensity becomes

$$I_{OUT} = I_0\cos^2\left[\frac{\pi}{\lambda}(\Delta n_{eff}L + n\Delta L)\right] \tag{4.11}$$

The modulation efficiency and the insertion loss are calculated similarly to the case of the phase shifter. An important additional feature of the amplitude modulator is the extinction ratio (ER), namely the ratio between the maximum and minimum intensity output:

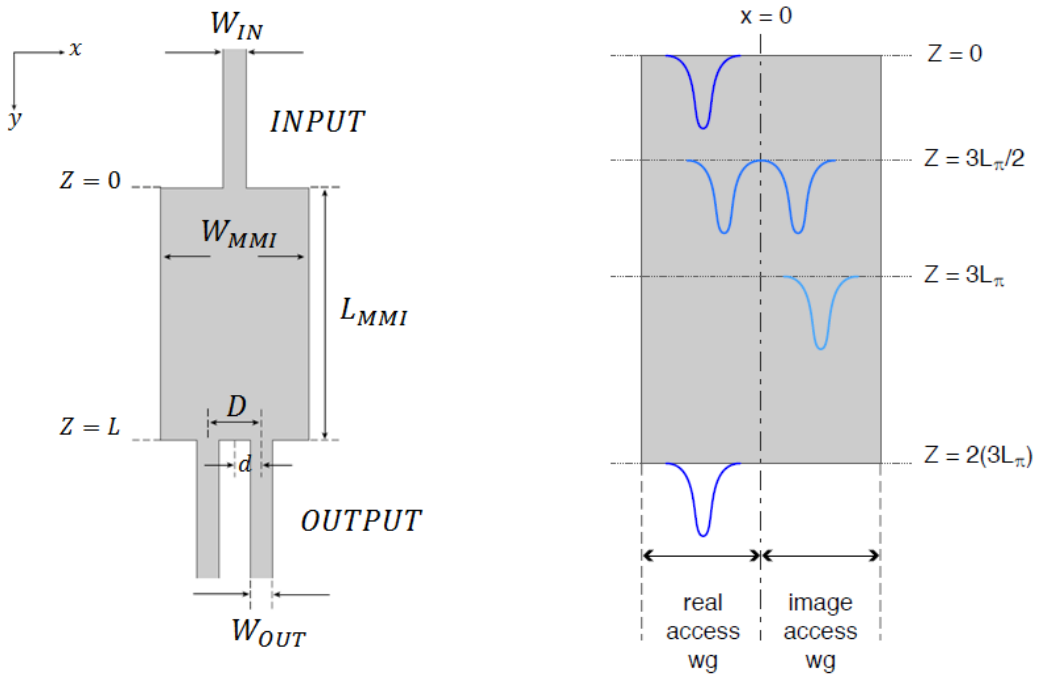
$$ER\ (dB) = \ 10\log_{10}\left(\frac{I_{max}}{I_{min}}\right) \tag{4.12}$$

4.2.4 Multimode interference (MMI) couplers

Coupling, splitting and combining of light pulses is carried out by multimode interference (MMI) couplers. An $N \times M$ MMI has N input and M output waveguides (see figure 4.3 for an 1×2 MMI). The structure connecting these waveguides is a larger waveguide, where multimode interference is used to obtain self imaging of the input modes onto the output modes. *Multimode Propagation Analysis* (MPA) is often used to properly design MMIs [40]. The evolution of the modes concerns only the xz (horizontal) plane, since the light is vertically confined by the thickness of the silicon layer. From the theory developed in [40] we find that the beat length between the 0-order and the first order modes is

$$L_\pi \approx \frac{4n_r W^2}{3\lambda_0}, \tag{4.13}$$

where n_r is the waveguide ridge refractive index and W is the width of the MMI.



(a) (b)

Figure 4.3: MMI: (a) main structure and (b) self-image reproduction scheme [2].

The propagation constant β_ν of the ν-order mode is spaced from the fundamental one β_0 by

$$\beta_0 - \beta_\nu = \frac{\nu(\nu+2)\pi}{3L_\pi} \tag{4.14}$$

A field entering the MMI in the position $(x, 0)$, where $x = 0$ corresponds to the center of the MMI, is denoted as $\Psi(x, 0)$. A self-image of $\Psi(x, 0)$, i.e. a reproduction of $\Psi(x, 0)$, is retrieved at a distance $L = p(3L_\pi)$ where p is integer (see figure 4.3(b)). If p is even, the image is direct and at the same horizontal position (x, L); if p is odd, the image is a mirrored one and it appears at $(-x, L)$.

Light can also be split by another device, the *star coupler-based beam splitter* shown in figure 4.4. The functioning of this device is based on simple diffraction: the large slab is designed to avoid reflections on the lateral edges before light is coupled into the two output waveguides.

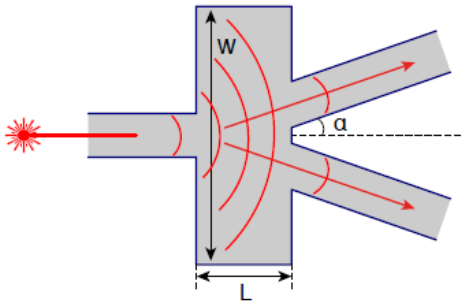


Figure 4.4: Star coupler-based beam splitter [2]

4.2.5 Grating couplers

The device used for injecting the light into the chip and for extracting it out of the chip is called *grating coupler*. A grating coupler is a sub-structured waveguide: the height of the waveguide rib changes with a period Λ (figure 4.5). When the light coming from an external fiber-coupled source enters a waveguide, it is not properly coupled due to mode mismatch between the waveguide and the fiber. The periodicity creates conditions for Bragg diffraction, allowing for the optimal coupling of the modes that satisfy the phase matching condition

$$\kappa_i \sin(\theta_i) + p\frac{2\pi}{\Lambda} = \frac{2\pi n_{eff}}{\lambda}, \tag{4.15}$$

where κ_i is the incident wave vector amplitude, θ_i its incidence angle, and p the diffraction order.

4.3 Electrical structures

Plasma dispersion based modulators are usually integrated in configurations based on *PN junctions* because the diode configuration allows for a bigger refractive index variation.

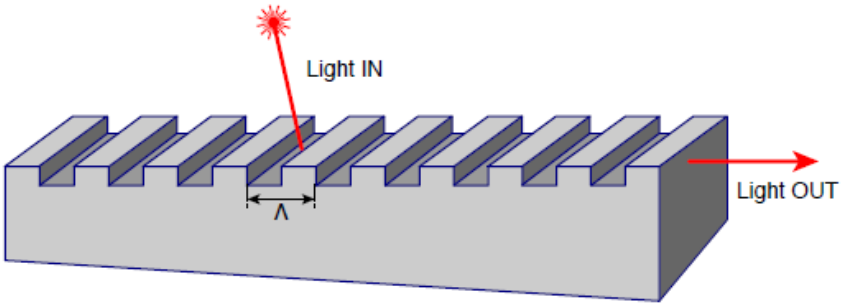


Figure 4.5: Grating coupler [2]

In such structures, silicon is doped with donor or acceptor atoms making the material respectively *n-doped* or *p-doped*. When two inversely doped materials are in contact (forming a *junction*) the excess of donor and acceptor concentrations initiates a diffusion process leading donors into the p region and acceptors in the n region. This happens close to the contact edge between the two differently doped materials, in a zone called *depletion region* (see figure 4.6). During the diffusion, the initially neutral materials start to be positively or negatively charged and an electric field arises, with a direction that is opposed to the diffusion of the carriers. In this way the diffusion process saturates and the system gets to equilibrium.

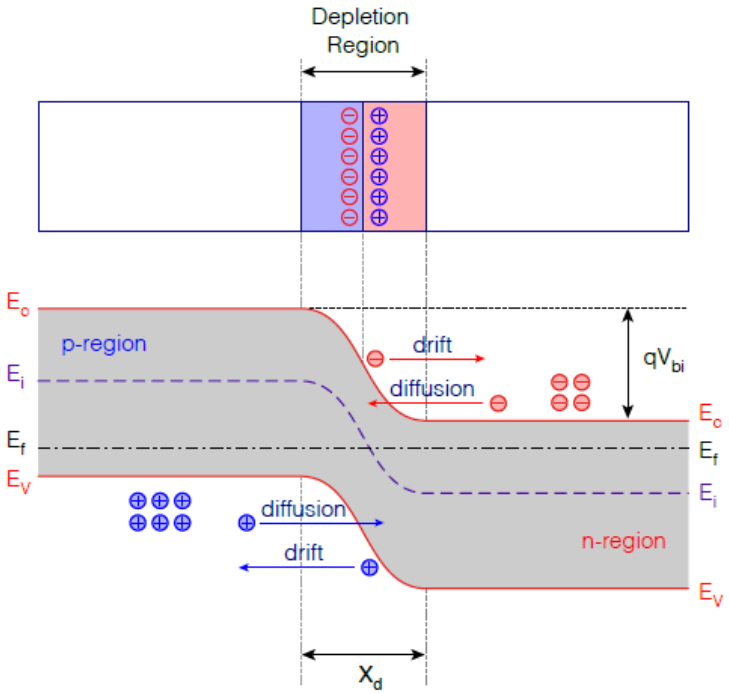


Figure 4.6: The PN junction [2]

The built-in potential (that generates the electric field) is

$$V = \frac{kT}{q} \ln(\frac{N_D N_A}{n_i^2}), \tag{4.16}$$

where k is the Boltzmann constant, T the temperature, q the electron charge, N_D the donor concentration, N_A the acceptor concentration and n_i is the electron-hole concentration for an undoped material.

In a reverse bias configuration, the applied bias voltage V_b creates an electric field such that the depletion region is larger, becoming

$$x_d = \sqrt{\frac{2\varepsilon}{q}\left(\frac{1}{N_D} + \frac{1}{N_A}\right) + (V + |V_b|)}, \tag{4.17}$$

where $\varepsilon = \varepsilon_r \varepsilon_0 = 1.03 \times 10^{-10} F/m$ is the electrical permittivity, which is the product of the relative permittivity ε_r of silicon with the vacuum permittivity ε_0.

The depletion region has a capacitance C_D:

$$C_D = \frac{\varepsilon A}{x_d}, \tag{4.18}$$

where A is the contact surface area. The diode also has a characteristic resistance, which, if we consider the diode's equivalent circuit, is connected in series. From this we can define a characteristic time response τ as the characteristic time of the equivalent RC circuit: $\tau = R_D C_D$.

Another important parameter is the drift time t_r, which is the transit time of a carrier through the depletion region when a bias is applied. It is calculated using the depletion region length and the carrier drift velocity v_d, as $t_r = x_d / v_d$.

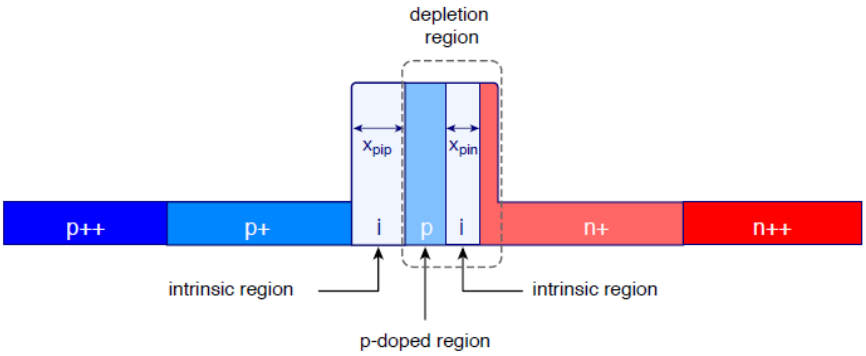


Figure 4.7: The PIPIN structure [2]

The above description corresponds to a standard PN junction. However, although such junctions achieve high Δn, this also comes with high $\Delta\alpha$, as we have seen previously in this chapter. To overcome this issue, more complex configura-

tions can be used, such as the so-called PIN or PIPIN junctions. The PIN junction is less absorptive because the active region is not doped (and hence it has fewer free carriers) but it also shows a lower Δn. PIPIN junctions have a p-doped active region, so for a given applied electric field they show higher Δn. The optimal choice of the diode structure depends on the system requirements in each implementation.

In our work, we have used PIPIN junctions, whose structure is shown in figure 4.7 and features a sequence of a p-doped layer, a non-doped one, another p-doped, a non-doped and finally an n-doped layer. A detailed description of the functioning of such structures falls outside of the scope of this thesis.

Part II

On-chip integration of the GG02 protocol

Chapter 5

Introduction to the experiments

In the second part of this manuscript we address our main objective, namely the implementation of an integrated version of the GG02 protocol on a silicon photonic chip. In this short introductory chapter we discuss qualitatively how the protocol must be implemented, highlighting the differences between standard and integrated optical setups. This will allow us to introduce the main quantities and parameters that must be taken into account for the realization of the experiment.

We will therefore start with an overview of the main features of the previously realized "bulk" setup, and then move to the "on-chip" version.

5.1 Standard implementation of CVQKD protocols

The standard optical "bulk" setup is shown in figure 5.1.

The protocol starts with the generation of the double pseudo-random Gaussian distribution for the quadratures q and p. In principle the Gaussian distributions have an infinite domain, spanning the axis from $-\infty$ to $+\infty$. In practice the beam sent by Alice is modulated in amplitude and phase, and the amplitude spans values between A_{min}, related to the extinction ratio of the amplitude modulator, and A_{max}, related to the available laser intensity. These values must be related to the variance V of the signal sent by Alice, with the requirement that $A^2_{min} \ll V \ll A^2_{max}$. It is therefore desirable that the dynamic range of the modulator, A^2_{max}/A^2_{min}, be as large as possible; for good telecom-grade Lithium Niobate modulators, a dynamic range of typically 30 dB is reachable. In practice, V may be only a few times smaller than A^2_{max}, and the large amplitude tails of the 2D distribution will be cut out. This does not stop the communication but generates errors, and should obviously be avoided.

Along with the pulses that carry the information, other calibration pulses are generated. These pulses are used to evaluate the parameters of the communication (like the excess noise and the shot noise) and to calibrate both the modulation process at Alice's and the relative phase between the two parties when Bob performs the measurement. Alice's modulators calibration can be ensured by tapping out and detecting part of the modulated beam, for continuous monitoring.

The communication consists in blocks of data: a string of N randomly chosen

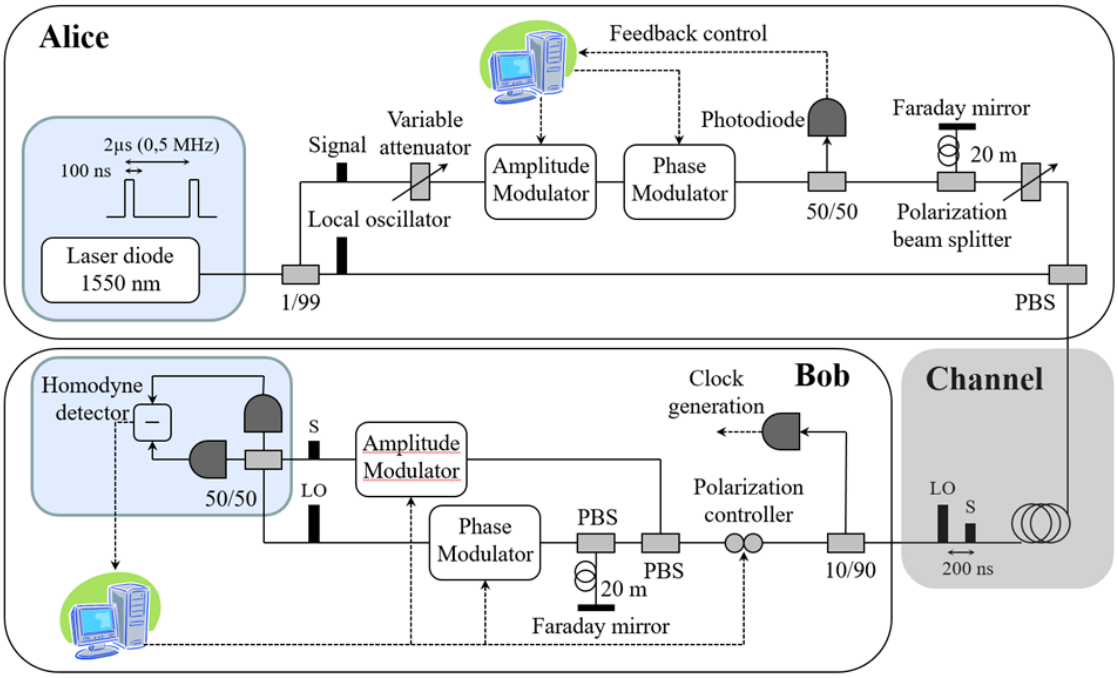


Figure 5.1: Overview of the optical setup in bulk configuration. The different parts of the setup are discussed in the text.

couples (q, p) (usually $N = 2^{13} = 8196$ or $N = 2^{12} = 4098$) is prepared and loaded into a buffer ready to be sent. Each string contains the states for both the key extraction (key symbols) and the system calibration (revealed symbols). This means that the states for the key have been prepared using the calibration data of the previous strings, resulting in a delay between the calibration and its actual use. This can lead to errors, especially in the evaluation of the shot noise N_0. Since N_0 is the unit of measurement of the variances and one of the key values for the excess noise estimation, an error in N_0 will propagate to all other measurements. To avoid this problem the shot noise is evaluated for each communication block, using the maximal attenuation given by an additional amplitude modulator at Bob's site. In addition, the typical drift time of the modulator parameters is longer ($\sim 1s$) than the communication of a few blocks ($\sim 10 - 100ms$), so the calibration is considered stable at least up to the moment at which the states are prepared and sent.

Even if the local oscillator is said to be *local*, in the current version of the protocol it is sent together with the modulated data for synchronization and coherence reasons. Therefore the local oscillator is generated by Alice, using the main part of the pulse also used for the (much weaker) signal beam. Such a system allows the two pulses (the local oscillator and the signal) to have the same spectral and time (duration) characteristics. The local oscillator and the signal are sent together in the same quantum channel, and to avoid interactions during the trip from Alice to Bob, the two pulses must be multiplexed. This is done in practice by using both a time delay (20 m optical delay line), and orthogonal polarizations (using a polarization beam splitter PBS). A demultiplexing process is required at Bob's, using first an automatic polarization controller, and then again a PBS and a delay

line in the inverse paths of the local oscillator and the signal, before the homodyne measurement can be made (see figure 5.1). We note that CVQKD can be implemented also with a locally generated local oscillator [41, 42]; this has several important advantages, but it is technologically very challenging, and it will not be considered further in the present work.

When receiving the pulses Bob must perform the measurement by projecting the signal on the Q or P axis. The projection is performed by the interference with the local oscillator at Bob's having a particular relative phase with respect to Alice's reference frame: it is $\phi_B - \phi_A = 0, \pi/2$ for the Q, P quadrature respectively. This requires a continuous control of the phase, performed by Bob using Alice's calibration pulses. This phase tracking is always required but in some cases, especially with a locally generated local oscillator, using heterodyne rather than homodyne detection may be a better choice.

For the measurement to be effective the two pulses must arrive at the same time on the beam splitter and the detection gate must be opened when the pulses are detected by the photodiodes. The synchronization process (clock generation) is realized by taking a part of the channel into a control photodiode that triggers the detection when it detects a pulse. Therefore, all together three signals are registered in practice (see figure 5.1): the feedback control used by Alice, the homodyne data and and the clock generation signal used by Bob.

5.2 Basic requirements for integrated CVQKD

5.2.1 Some conditions that need to be fulfilled

The performance of CVQKD devices, especially the modulators and photodetectors, must have specific features. Most of them (high dynamic range for modulators, high linearity and quantum efficiency for photodetectors) are easily fulfilled by standard telecom components, such as Lithium Niobate modulators, and InGaAs PIN photodiodes. It is not so clear however whether they can be fulfilled on a chip, where a pure electro-optic effect is not readily available, and where photodiodes (usually made with Ge on Si) are not always as good as their InGaAs counterparts.

Photodetectors must show a linear response to the light intensity over a large range, especially around the homodyne system working conditions. The detection electronics are designed to work with pulses carrying 10^6 to 10^9 photons, with a duration of 100 ns and a repetition period of 2 μs. The amplifier noise must be low because the electronic noise, v_{el}, depends on it. The working local oscillator power is chosen taking into account the linear response of the variance of the output, and should give at least a 10 dB dynamic range of linearity above v_{el} to allow modulation. For this reason, the local oscillator is usually chosen to be close to the maximum intensity giving a linear detection response.

The amplitude modulation apparatus must have a large dynamic range as said above, and the attenuation system must be as stable as possible. Drifts may be corrected by active stabilisation, but in general the optical properties of the devices must be at least stable over a few transmitted blocks.

5.2.2 Some design criteria

Given the many stringent requirements listed above, it should be clear that a direct transposition from the bulk to the integrated setup is not possible, and that many preliminary qualification steps are required.

For this reason, the on-chip optical setup will follow the same general idea of the bulk one, but some modifications and simplifications will be introduced, especially by removing pieces that are not necessary to perform a demonstration of the feasibility of the miniaturization of CVQKD. The basic optical layout is shown in figure 5.2, which is easily comparable to the setup in figure 5.1 shown before.

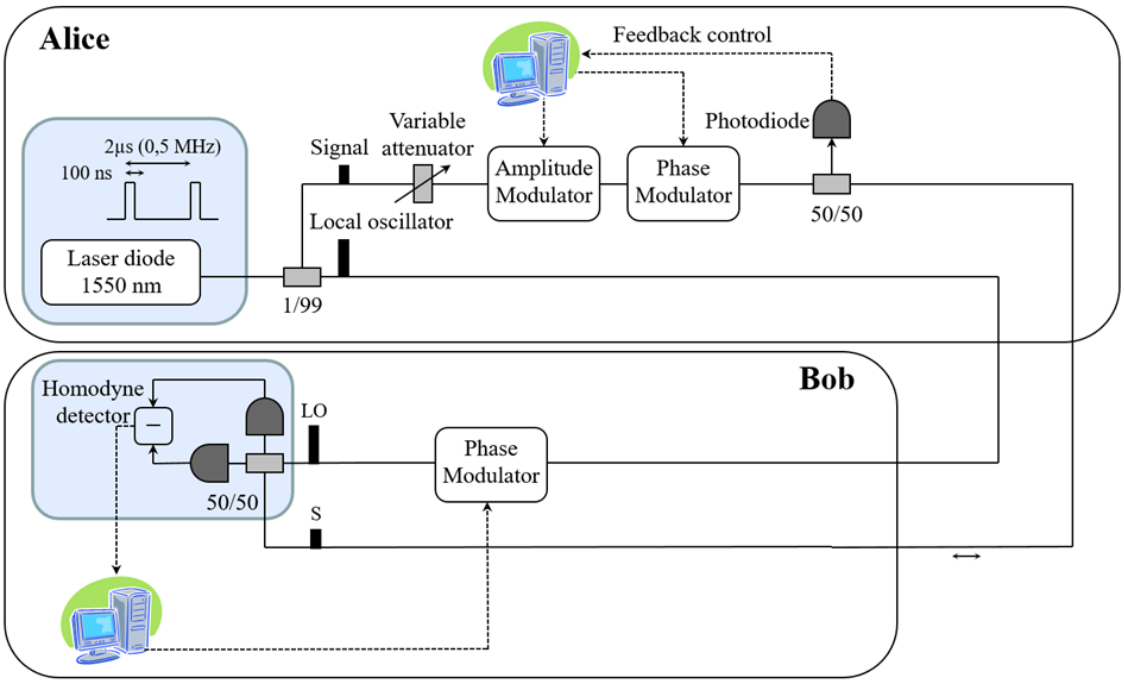


Figure 5.2: The optical setup in the on-chip configuration.

An obvious change in the setup is the removal of the devices for multiplexing and demultiplexing. In fact the multiplexing process is not required for the protocol to be demonstrated, so the transmission channel can be simplified as much as possible.

We will see in detail in the next two chapters what adaptations must be made to simplify even more the system and the protocol, in order to allow for a first demonstration of the capabilities of silicon photonics devices for CVQKD. This will require to take into account the broad diversity of the photonics devices, and their (sometimes unexpected) behaviour.

Chapter 6

All in one chip: a proof of principle for CVQKD

The problems arising from on-chip integration are not only related to the individual components, but also to system considerations, allowing them to work together. Like in bulk setups the suitable scheme for solving a problem is not unique, but whereas in a bulk setup a component can be replaced, removed or added, in a photonic circuit this modularity is not available. So, once an approach is chosen, the architecture is fixed and the chip must perform the designed task - or fail.

Since the integration of the GG02 protocol was not explored before this work, the first idea was to build an integrated proof-of-principle device implementing the protocol, based on a simplified scheme aiming at testing the feasibility of CVQKD using a silicon photonic chip. The first chip was designed as a direct transposition of the functioning bulk optical setup [43,44] presented in the previous chapter, for a proof of principle all-in-one chip communication using the GG02 CVQKD protocol.

In this chapter we will see how this chip is structured, from the individual components to the more complex and complete cryptographic system, exploring the capabilities and the limitations imposed by the adopted scheme. The proof of principle approach is based on the idea of avoiding an actual communication between the two parties to remove one or more degrees of freedom in the experimental realisation of the protocol, which will be accordingly modified. The communication will be performed within a single chip: Alice and Bob will be not only on the same photonic circuit, but also on the same continuous waveguide line, making them actually impossible to be separated.

In the first section the chip and its distinct parts are presented together with some important test measurements. These measurements allow us to predict and manipulate the modulator behavior and will give an idea of the structural constraints the systems is subjected to.

Then we describe the acquisition system: the on-chip implementation requires to strongly modify the electronics architecture, including the electrical scheme and physical implementation of the detection amplification. The electrical and optical approach also has to change accordingly, as discussed in sections 6.2 and 6.3.

After the test measurements we present the integrated CVQKD system, as well as the steps that must be done to achieve the communication. The most important characteristic of the system is that Bob's homodyne detection is the only phase-related measurement available on the chip, and it is not physically isolated from Alice's modulation setup. This leads to consequences we will discuss in section 6.5 and 6.6, when the homodyne detection calibration problem is faced. In fact, as we saw in section 2.2.4 the homodyne detection calibration is based on the assumption that only one classical field (the local oscillator) is injected in the detection's beam splitter. The impossibility to realise this condition, and the remedies used to overcome it, are exposed in these two sections.

6.1 Overview

The chip was designed by Nicholas Harris and Christophe Galland at the OpSIS company (University of Delaware), and manufactured in the foundry IME in Singapore. For this reason this chip is shortly addressed as the *OpSIS chip*.

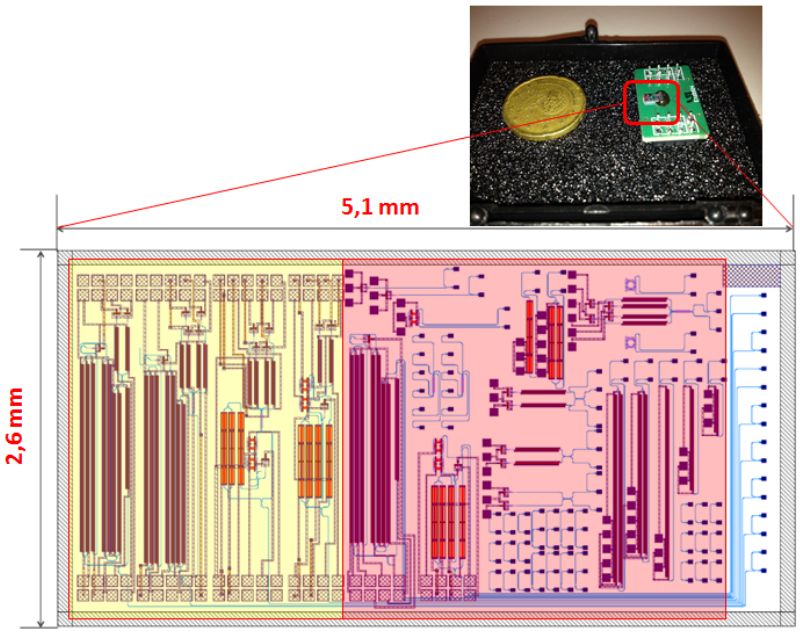


Figure 6.1: OpSIS chip: overview of the design.

The chip, shown in figure 6.1, is 5.1mm long and 2.6mm wide. Knowing that this was the first attempt to integrate a CVQKD system, the chip was designed to include different devices to be first independently tested and then put together in more complex systems in order to evaluate their overall interaction.

It can be ideally divided in two parts: the yellow highlighted part contains all the devices that can be used for light modulation and measurement; the red part contains four different complete systems for CVQKD, each one different from the other by the modulating devices (thermal or electrical) and the detection (homodyne or heterodyne). In this section we will look closely at the yellow part, in which the single devices are checked for independent tests.

The devices are divided into passive and active and they must be able to work at the (relatively slow) speed needed for CVQKD systems. Our system operates at 500 kHz; more specifically, Alice prepares and sends a a 100 ns pulse every 2 μs. The modulation for the state preparation must be faster than the repetition rate so that the device can settle to the desired configuration before the communication takes place.

6.1.1 Grating couplers

As we saw in Chapter 4, the grating couplers (GC), shown in figure 6.2, are the devices that allow the injection of light inside the photonic circuit. GCs must feature good coupling performance in terms of both low losses and high quality of the injected light.

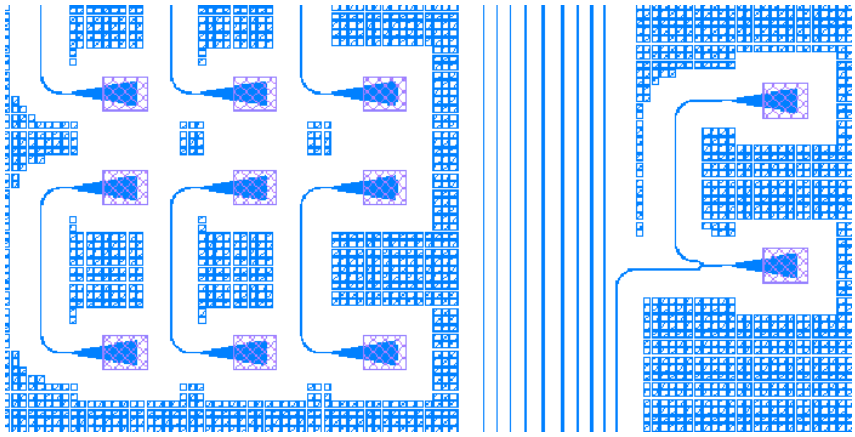


Figure 6.2: OpSIS chip: GC. On the left the coupling test structures with one input and one output. On the right the coupling structures for a CVQKD system: the light is split in two and a part is taken out to evaluate the coupling losses.

Usual coupling losses for an optimized coupling procedure are between $-3.5dB$ and $-5dB$. Furthermore, good coupling requires that the injected light possesses the appropriate mode features: the coupling procedure must optimize the transmission of light at the required frequency (telecom wavelength $\lambda = 1550nm$) and must filter out all the higher order modes, allowing only the TEM_{00} mode. The minimization of the losses (or the maximization of the transmission) corresponds to the optimization of the mode filtering as well. It must be kept in mind that the waveguides are designed to be single mode, so they work as mode filters when the light passes through them.

The polarisation filtering is naturally performed by the intrinsic structure of the GC (see section 4.2.5): the planar geometry allows only horizontally polarized light to be coupled in.

In figure 6.3 we show a spectral analysis of the transmitted light performed on the *in&out* test structures. The four curves are taken in different coupling configurations and they represent the losses due to the coupler-in and the coupler-out together. A single coupler provides losses equal to half the overall amount as they

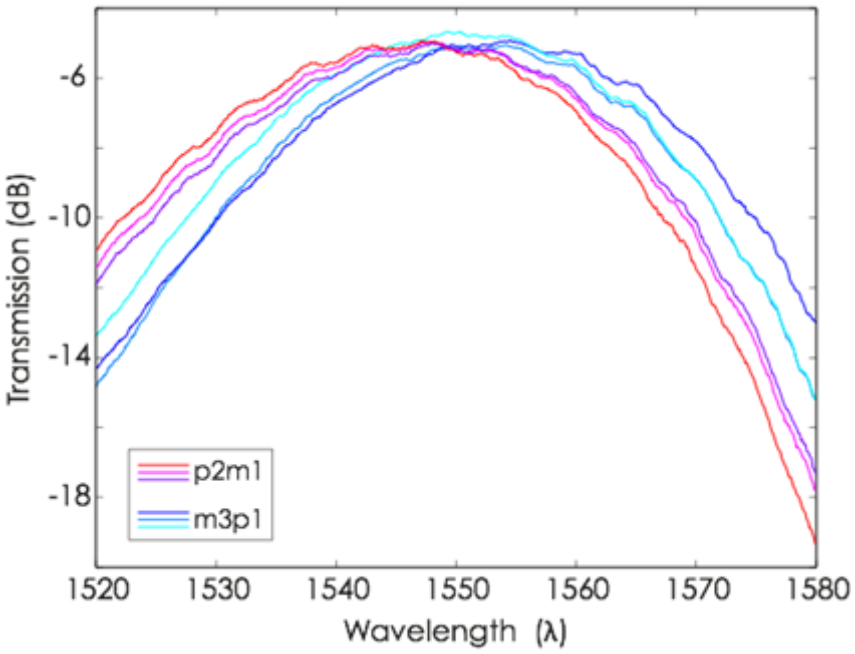


Figure 6.3: OpSIS chip: GC. IN/OUT transmission for different couplers on the same chip [3].

are supposed to be the same for both in and out coupling. This assumption is reasonable since the tests are performed with fiber arrays, whose structural configuration assures the symmetric distribution of losses. In the figure we see that a good configuration is easily achieved, providing a transmission of $-5dB$.

6.1.2 Beam splitters or MMI

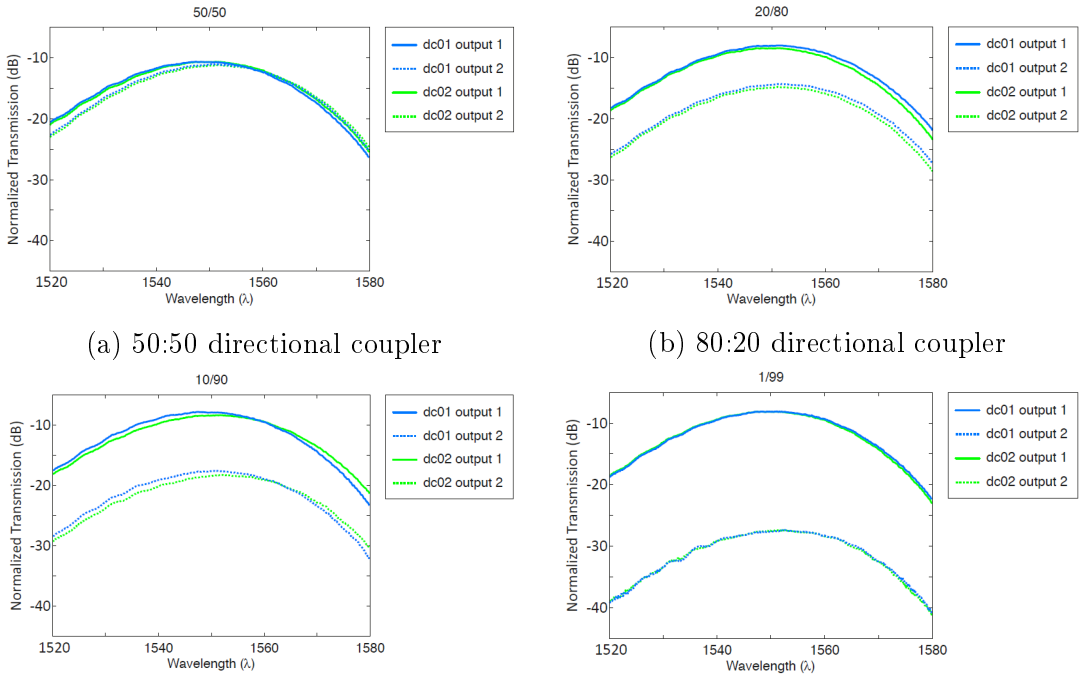
Light is split by means of MMIs (or directional couplers). Depending on the purpose of the splitter, MMIs with different splitting ratios have been inserted in the chip. To be more precise four types of BS can be found in the OpSIS chip: 50:50, 80:20, 90:10, 99:1.

The 50:50 BS are mainly used to measure the light coupled in the system (structure on the right of figure 6.2) and in Mach-Zehnder interferometers to split and recombine light. The other ratios are used for two main purposes. Since only one beam is used to feed the chip with light, it must be divided in two for local oscillator and signal use (see figure 5.2). This task typically requires 80:20 or 90:10 splitters. The 99:1 splitter serves to extract a small amount of light off the chip so that it can be measured for testing. This second purpose will be explained in more details in section 6.4.

Figure 2.4 shows the spectral analysis results for all types of MMIs.

6.1.3 Fast modulation devices

Fast modulation, in phase and in amplitude, is performed using PIPIN junctions and exploiting carrier depletion. As discussed in chapter 4 (section 4.2.2), the length



(a) 50:50 directional coupler

(b) 80:20 directional coupler

(c) 90:10 directional coupler

(d) 99:1 directional coupler

Figure 6.4: OpSIS chip: directional couplers spectral analysis of the transmission

of a PIPIN carrier depletion-based phase shifter affects linearly the induced phase shift for a given supplied current. Starting from this a device is engineered so that the phase shift and the losses (or the attenuation, depending on the point of view) can be achieved at the average supplied current, i.e. within the working conditions of the device, avoiding heating up the system and burning the device. For this purpose devices of different lengths have been inserted in the system, aiming to be used for the tasks of phase modulation, amplitude modulation, strong steady attenuation and low attenuation for fine transmission adjustment.

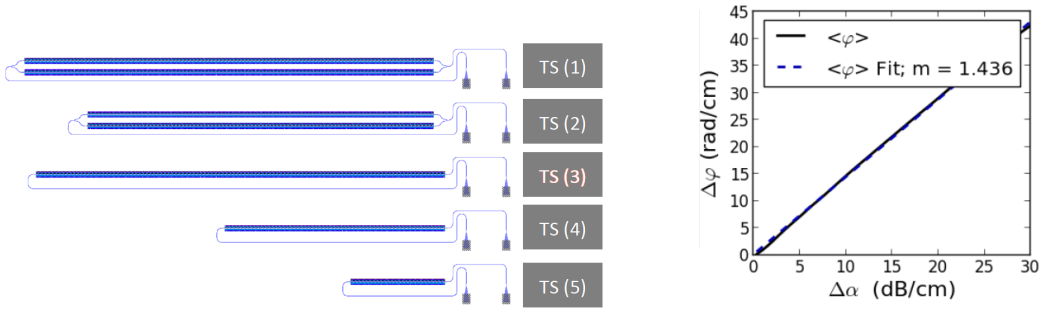
The basic PIPIN structure is the single phase shifter. In this chip, phase shifters can be found in 4 different lengths: 0.3mm, 0.7mm, 1.0mm (only in a Mach-Zehnder configuration) and 1.3mm (in both Mach-Zehnder and stand-alone configurations).

Phase modulation

The phase modulation is managed by using a single PIN junction that, by means of carrier depletion, changes the refractive index of the device. The light passing through a higher refractive index material slows down to a speed $v = c/n$, exiting the material with a different phase.

The phase shifters contained in the OpSIS chip provide a linear phase shift with respect to the induced absorption. In fact both ϕ and α have the same dependence on the refractive index n (linear) if the doping is constant. From the linear fit in figure 6.5a we can deduce that:

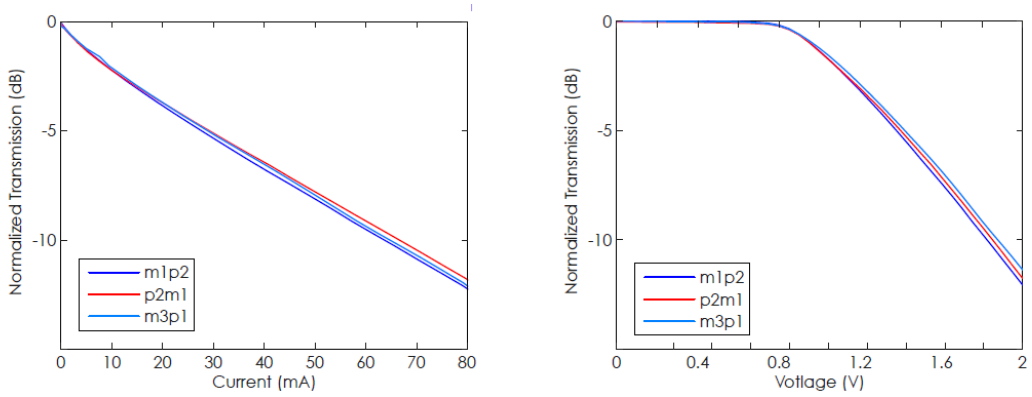
$$\frac{\Delta\phi}{\Delta\alpha} = 1.436\, rad/dB \tag{6.1}$$



(a)

Figure 6.5: OpSIS chip: **(a)** PIN test structures. From top: 1.3mm MZI, 1.0mm MZI, 1.3mm phase shifter, 0.7mm phase shifter, 0.3mm phase shifter. **(b)** Induced phase shift vs. induced losses

Since the PIN junctions in the chip are manufactured using the same doping concentration, the value in equation 6.1 holds for all the structures.



(a) (b)

Figure 6.6: OpSIS chip: 0.7mm phase shifter. Normalized transmission dependence on the (a) current and on the (b) voltage [3].

In figure 6.6 we show the transmission characteristics of the 0.7mm shifter. Each measurement has been taken on devices of two different chips to highlight the performance reproducibility of the structures.

However the use of the devices changes with their length: the 0.7mm phase shifter is normally used as a phase shifter, while the 0.3 mm device is used as a short attenuator, for which we must control the absorption induced phase shift.

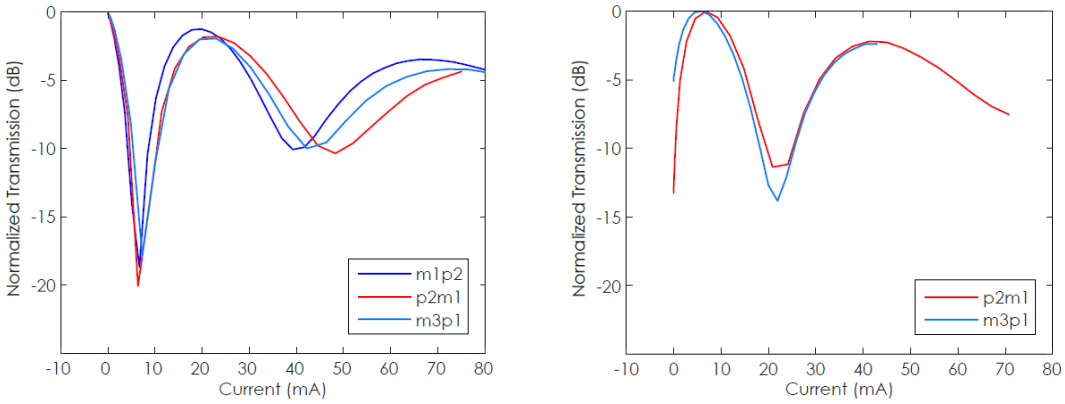
The insertion loss has been measured to be $3.6dB$ for the short shifter and $4.0dB$ for the 0.7mm one. The longest phase shifter was not tested since it is not present in the final complete systems available for communication.

Amplitude modulation and attenuation

When the single phase shifter is inserted in one arm of a MZI we obtain a device that operates on the amplitude of the light passing through it. The amplitude

modulation is achieved by means of the interference at the output of the MZI, obtained by driving the phase of the light passing through the interferometer's arms. This is obtained by inserting single phase modulators in each arm of the MZI. For PIN junction-based MZIs, the modulators are faster than the repetition rate of the system, and so they are used in the CVQKD context for the state creation process at Alice's. Additionally, they can be used as variable optical attenuators (VOA) since they can provide from $\sim 14dB$ to $\sim 18dB$ of attenuation, depending on the length of the structure.

However, we remark that using this device as a VOA is not optimal, since, as we can see in figure 6.7, the attenuation zone is narrow and the temperature drift could be faster than the duration of a data block. Similarly to the single phase shifters, the tests of figure 6.7 have been performed on devices of three different chips.



(a) (b)

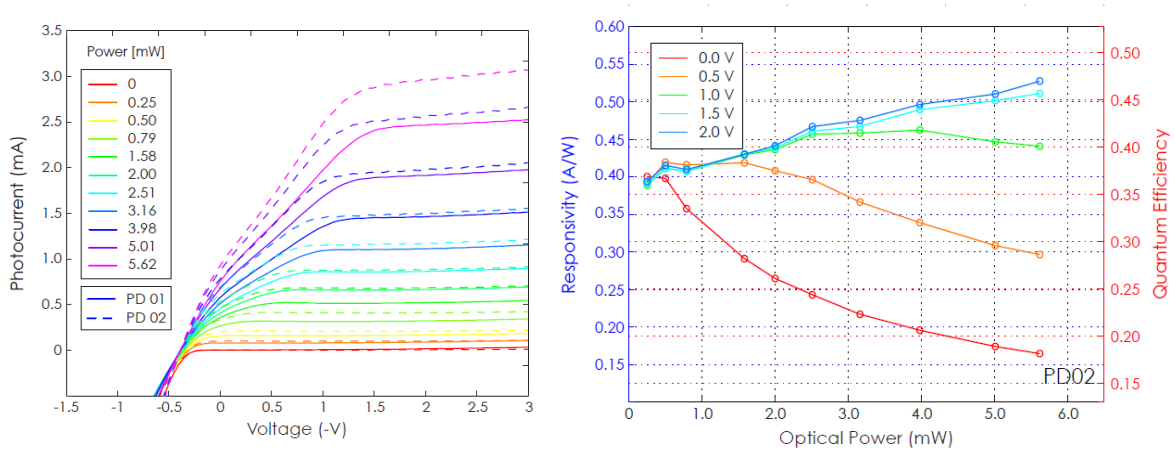
Figure 6.7: OpSIS chip: test (a) 1.3mm MZI and (b) 1.0mm MZI. Normalized transmission vs applied current.

An insertion loss of $\sim 6dB$ has been measured for the two types of attenuators.

6.1.4 Photodetectors

The detection is realized using Germanium photodiodes. It is well known that at telecom wavelength other materials are more efficient in terms of quantum efficiency than Ge (for example, InGaAs used in the bulk setup). However the integration of such materials on a silicon substrate is quite difficult and a technologically consistent solution is usually preferred.

We know that the photodetectors must be linear in terms of its response to the optical power. This linearity is usually translated into a flat behaviour in the IV curve. We see in figure 6.8a the IV characteristic of OpSIS chip's photodiodes. When the injected optical power increases the photodiode response is distorted: the usual "single-knee" structure is replaced by a "double-knee" behaviour after which the current continues to slowly rise for increasing reverse bias. If the current rises, the corresponding dynamic resistance $R_d = dV/dI$ is not zero. From the figure we can see that even if for a reverse bias higher than 1.5V the response is quite stable, the behaviour changes as the optical power increases. The four curves related to the



(a) IV characteristic (b) Responsivity and Quantum efficiency

Figure 6.8: OpSIS chip: Photodiodes. The straight and dashed lines represent the two different photodiodes on the same chip.

highest intensities show a non horizontal response added to the already mentioned double-knee structure. This characteristic could lead to a non linear behaviour for quite low optical powers. Since the linear response to the injected power is a fundamental requirement for the homodyne detection to work in a quantum regime, the non-zero dynamic resistance can prevent the realization of the protocol.

The other critical quantity for the protocol and in particular for the parameter estimation is the quantum efficiency of the photodiodes. This is plotted in figure 6.8b together with the responsivity and is calculated from it using the following equation

$$\eta_{PHD} = R\frac{hc}{e\lambda}, \tag{6.2}$$

where h is the Planck constant, c is the speed of light and e the fundamental electronic charge.

We see that the typical InGaAs resistivity $\sim 1A/W$ cannot be achieved with these photodiodes. However, a lower quantum efficiency $\eta_{PHD} \simeq 0.5$ should still be acceptable for the QKD protocol.

6.2 Acquisition and control systems

Although the implementation of the CVQKD protocol relies on optical signals, the communication with the photonic chip requires a complex control and data acquisition system. This is shown in figure 6.9 and can be divided into 3 main parts: the amplification of photodetector photocurrents and homodyne output, the two-way communication between the computer and the on-chip modulation system and finally the triggering of the experiment.

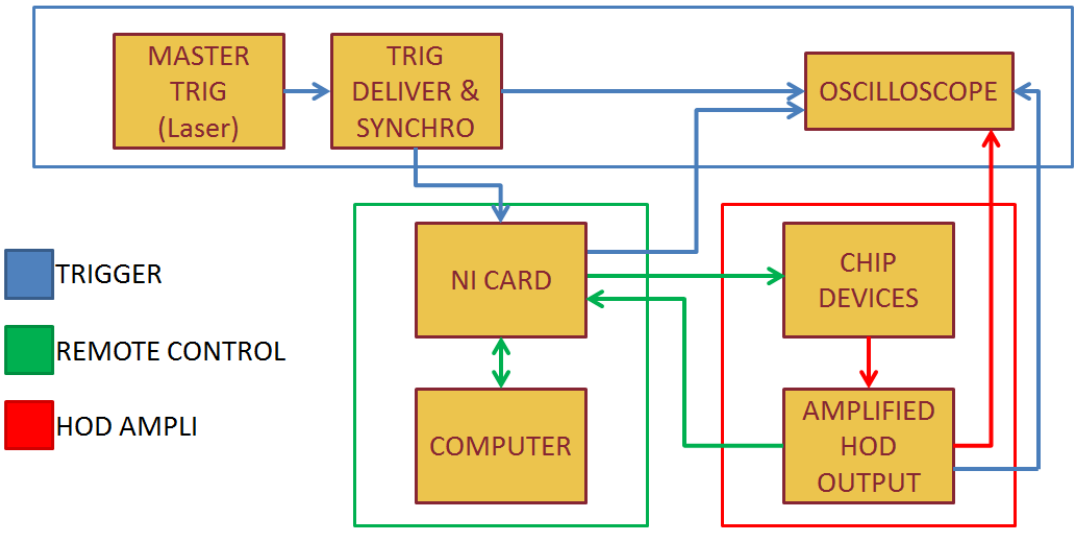
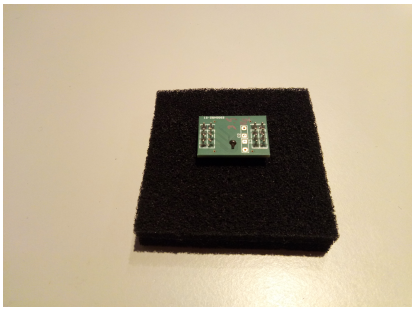


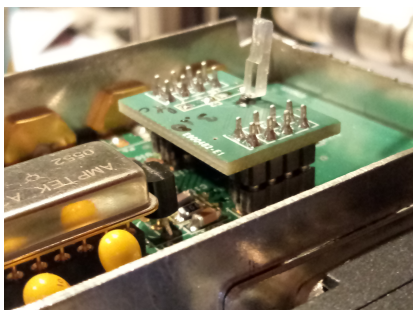
Figure 6.9: Schematic of the acquisition and control system. The various parts are highlighted by arrow of different colours.

6.2.1 Electrical support for the silicon chip

The chip we used in our experiments is small (overall surface $\simeq 1 - 10mm^2$, electrical pads are $80\mu m$ squares, separated by $20\mu m$) and testing it requires many changes is the experimental setup. A continuous direct interaction with the chip using standard probes and cables causes huge perturbations and shocks on the chip, leading to a poor quality of the measurement and to a high risk of breakup. The solution we adopted is to divide the electrical access in 3 steps.



(a) The chip and the first PCB support.



(b) The PCB support for the chip inserted in the detection circuit.

Figure 6.10: The multi-layer PCB support design.

1. The most delicate one is the direct connection on the pads of the circuit. This step is managed by gluing the chip on an ad-hoc PCB (Printed Circuit Board) and wire-bonding the chip's pads to bigger and more spaced electrical pads on the PCB. The thin wires are covered by a resin to protect them. This leads to different advantages (discussed in section 6.3.1), among which stability and security against breaking.

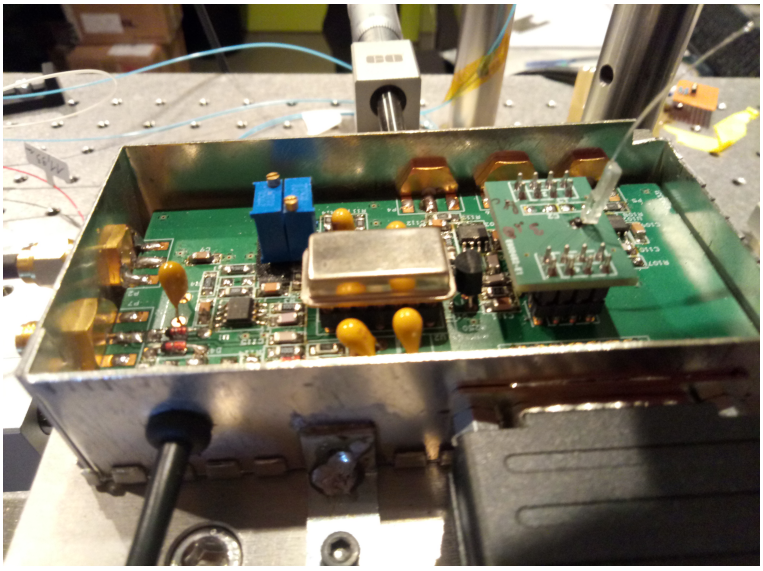


Figure 6.11: Acquisition system: multi-layer PCB structure with fiber-attached chip.

2. The second step is connecting the PCB to something bigger and more solid like standard mounting metal boxes. In a box like that a bigger PCB is placed, on which BNC and SMA connection are attached to connect the cables carrying the electrical signals. The internal structure of the PCB changes from chip to chip, so it will not be discussed here. What matters is how to electrically communicate with it. Each PCB has 16 pins (arranged in 4 rows of 4 pins each) as in figure 6.10a. They are used so that the PCB could be fixed on a suitably designed bigger support.

3. The third and last step is the connection of the PC box-PCB-chip system to the instrumentation (oscilloscope, pulse generators, remote control). To make this kind of lab operations more secure, the cables are connected on a separate "BNC box", which contains only male-BNC ports and communicates with the setup of step 2 via a flat 16-wire cable.

Steps 2 and 3 could be in principle performed at the same time: we are putting a PCB on top of another PCB (see figure 6.10b). There are two simple reasons explaining the separation of these two steps: the first is to prevent breaking, then the chip must also be fiber attached and this process would be really difficult to be performed on a big PCB of 10cm by 5cm. The second reason is even more practical: gluing the chip directly on the electrical circuit in the big box would mean that to change the chip we would have to change the whole box, i.e. to build a complete electrical support per chip. Separating the PCB-chip from the main electrical circuit allows us to easily and quickly change the chip for testing and measuring.

This electronic setup for the detection part of the protocol has been designed and built by André Villing, the electronics engineer at IOGS and it is shown in figure 6.11. Another box to drive the modulation chip has also been realized (shown in figure 6.12), but we will not enter into the details in this thesis since Alice's chip

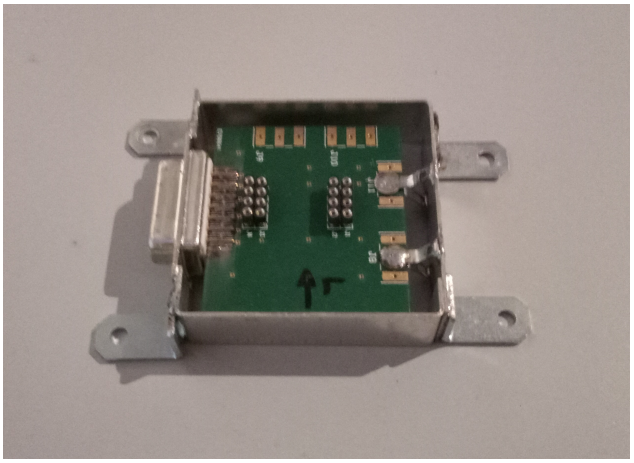
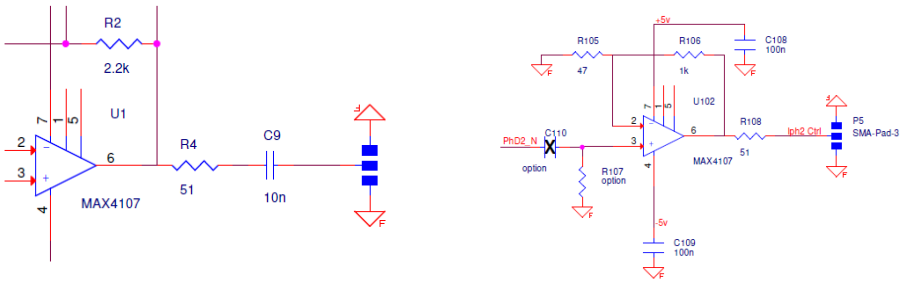


Figure 6.12: The box for Alice's chip.



(a) Second stage of amplification: the voltage amplifier.

(b) The amplification for single photocurrents.

Figure 6.13: Details of the electronic circuit.

has not been tested yet.

6.2.1.1 The amplification box for the homodyne detection

The homodyne detection output, as we saw in section 2.2, is a very small signal and hence to properly measure it, it must be amplified. For this purpose a 2-stage amplification electronic circuit has been built, following and improving an already existing model, previously used for the bulk version of the GG02 [4, 45–48].

The circuit is a double stage low noise amplifier based on the hybrid amplifier *A250* from Amptek. The photocurrent difference is automatically taken by putting the two photodiodes in series and extracting the current from the junction between them. The first amplification stage is a current amplifier and is the one actually using the hybrid *A250*. The current is then transformed into a voltage and a final voltage amplifier gives the output of the detection system.

The improvements brought to the system include updates on the amplification system and design adaptations for the chip-based detection.

The amplification system has not being significantly changed and any change has been in accordance with the adaptation of the overall archietcture. We note only that R_2 (see figure 6.13a for the circuit component references) has been doubled

to obtain twice the gain via the ratio $G_2 = \frac{R_2}{R_4} \simeq 40$.

The insertion of the chip-based homodyne detection implies a list of adjustments.

- The new photodiodes have quite different characteristics with respect to the classical InGaAs fibered bulk ones, and so the section before the A250 has been significantly modified by adding or modifying:
  - The photodiodes load resistors R_{13} and R_{14} (figure 6.14);
  - The two small amplification circuits used to see the output of a single photodetector before the homodyne detection difference is performed. Since the system is very sensitive to electrical noise, these two amplifiers have been first removed by short-circuiting R_{supp7} and R_{supp8}, and then reintroduced when needed to test if the photodiodes were working properly and to measure their bias voltage.
  - The filtering RC for the power supply of the circuit. This circuit drives both the A250 and the photodiodes supply voltage level and filtering.
- The entrance capacitor C_{14} in front of the A250. This capacitor is in charge of the frequency and the residual voltages filtering since for the A250 no voltage is allowed in the input, when the hybrid amplifier is in current mode.
- The insertion of two variable resistors for the photodiodes supply. The new photodiodes needed to be tested at work and to be set up precisely for the detection balancing. For this reason the first adjustment can modify the overall polarization level for the two photodiodes. As we saw in section 2.2, we consider the two photodiodes to be identical, but the rest of the circuit may be slightly asymmetric due to small differences in the components. The second variable resistor can correct this unbalance.

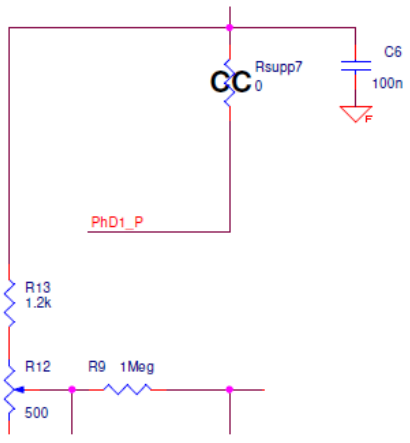


Figure 6.14: Electronics detail: photodiode's current extraction.

The amplification process can be considered real time, meaning that the time constant of the circuit response is shorter than the required acquisition time. The whole process obviously integrates a bit the signal. The typical output signal has the shape presented in figure B.9 and explained in more details in section B.0.3.

Figure 6.15: Electrical probes

6.3 Electrical and optical approach

6.3.1 From electrical probes to wire bonding

The photonic chips are composed by both passive and active elements. To drive the active components (modulators and photodetectors) we need to be electrically connected to the chip itself. When the circuit is designed, both electrical and optical approaching techniques must be taken into account, resulting in a specific design and positioning for grating couplers and electrical pads.

The first technique consisted in using the so-called *electrical probes* or *electrical fingers*, shown in figure 6.15. An electrical probe is a very commonly used device in standard silicon photonics: the probe's fingers are put in touch with the electrical pads by mechanically moving the probe itself. This mechanical stress on the chip induces vibrations and instabilities that are too intense for our quantum measurement setup. Moreover the length of the electrical connection, composed by the fingers and the cables standing between the photodiodes and the amplification system, brings a huge amount of noise.

For these reasons another approach has been chosen: the wire bonding, which consists in connecting two electrical pads via thin metal wires. In our case gold wires $10 - 20\mu m$ thick have been used, covered by a protective insulating resin, to avoid capacitive effects between wires and to protect them from breaking.

Putting this in the multi-layers PCB structure we described in the previous section allows us to reduce to the minimum the noise induced by the electrical connection between the photodiodes and the amplification.

Another solution would be a *OptoElectronic Integrated Circuit* (OEIC), which requires a completely different approach in terms of architecture and design.

6.3.2 Optical coupling

The last part of this section will give a quick overview of the two methods of coupling used in this work. The procedure of injecting the light in the chip is a fundamental matter. We saw in section 4.2.5 that the corresponding device on the silicon chips is the *grating coupler*. The optical delivery is made by means of fiber-based devices. Such a device will be called just *coupling device*.

The coupling procedure can be divided in 3 steps, aimed to put the coupler in the right position so that the quality and the intensity of the coupled light is optimal.

At first the relative angle between coupler and grating coupler is optimized: the coupler projection on the chip surface must be parallel to the wave guide exiting the grating coupler and the surfaces of coupler and grating coupler must be parallel.

Due to the small dimensions of the grating coupler and the high divergence of the light exiting a fiber, the delivering device must be placed at very short distances from the chip surface. Finally, when the device is at the right vertical distance from the chip, only an xy translation is required.

Single fiber

One common way to couple the light is using a single nude fiber. It is widely use in standard silicon photonics, for which the purity and the stability of the electromagnetic field mode are not always critical. In section 4.2.5 we also saw that the final edge of the device sending the light on the coupler must allow light to be incident with the proper angle. Moreover the whole setup is using PM (polarization maintaining) fibers: since a nude fiber coupling implies the usage of a SM fiber, a polarisation control must be taken into account, increasing the complexity of the whole control system and inserting more instabilities.

All these elements are amplified by the fact that the fiber vibrates. Even if it can be fixed on some ad hoc support, the final edge will always be free and exposed to the external stress.

Fiber array

A more stable coupling device is the *fiber array*. The advantage of the fiber array is its solidity. By means of a xyz translation stage, a yaw and pitch support, a standard double tilt support and a home-made roll support, we are able to address every movement needed for the coupling.

Even though the coupling is more stable with respect to the previous case, every source of vibration affects the coupling (from the AC to simply walking in the lab). This is a stability requirement due the sensitivity of the homodyne detection on a silicon chip: every small change in the coupled light beam modifies the properties of the detection itself.

One additional problem could arise from the combined effects of particular architecture of the chip and the wire bonding procedure: if the grating couplers are too close to the electrical pads of the circuit, the fiber array, which has dimensions comparable to the whole chip, could not have enough room to get to the grating

	HoD	HeD	PIN	Th+ring
1	X		X	
2		X	X	
3		X		X
4	X			X

Table 6.1: Available complete systems listed by homodyne (HoD) or heterodyne (HeD) detection and by PIN or thermal + ring resonators (Th+r) based modulation.

coupler: a non-optimal coupling can be performed with the array touching the bonding resin. This configuration is unstable and changes with time.

Another factor plays a role in the loss of coupling at longer time scale ($\sim$ 10 min): the heating and consequent dilatation of the chip due to the amplification circuit. This problem has not been studied: a new chip configuration has been used instead.

Fiber attaching

Fiber attaching suppresses all the problems regarding the stability: the fiber array is glued on the chip. The process requires specific instrumentation and besides stability it allows coupling configurations very close to the optimum. In figure 6.10b we can see the attached fiber array standing in place without the help of any support. The process has been performed in the LETI foundry with the help of PhD Olivier Castany.

6.4 A complete integrated CVQKD system

In this section we will show the CVQKD system that has been developed and discuss its main features.

The OpSIS chip gives the possibility to access 4 different complete integrated CVQKD systems, exploiting two types of detection concepts and two types of modulation devices, resumed in table 6.1. The detection can be a homodyne detection, already discussed in section 2.2, or a so-called heterodyne or double-homodyne detection that we will discuss further in sections 3.3.2.1 and 7.4.2. The modulation and the attenuation can be managed by the PIN junction-based devices or by the thermal ones.

Systems 3 and 4 have not been used because of the low speed of thermal modulation. Even if they have a greater extinction ratio, these modulators show a time response which is too close to the experimental 2 μs. This is the reason why they are more suitable for fixed (slow) attenuation. The same applies to the ring resonators (in fact in systems 3 and 4 ring resonators are used for fixed attenuation).

On the other hand before testing system 2 we started working with the new chip described in chapter 7. So finally only system 1 (figure 6.16) has been fully tested.

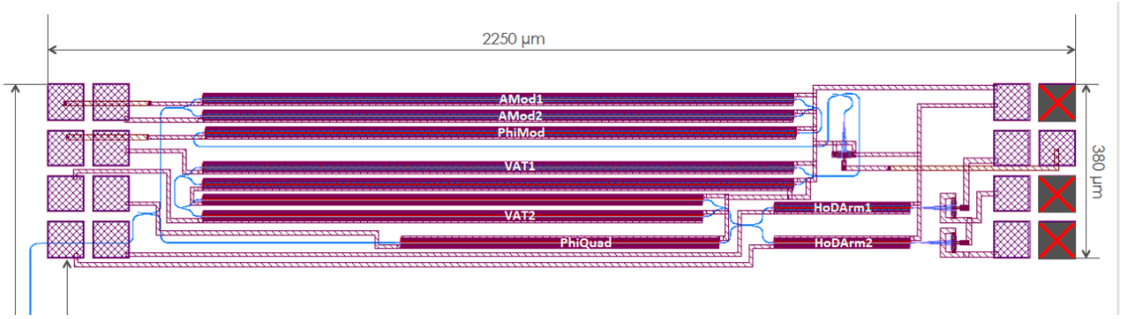


Figure 6.16: CVQKD system: detail.

6.4.1 Setup description

Let us get into the details of the on-chip electro-optical setup shown in figure 6.16.

The light is injected in the circuit through one single grating coupler, so a single light source is needed to feed both local oscillator and signal. It is then split in two by a 50:50 beam splitter: one way goes to another grating coupler whose light can be taken out and measured for coupling optimization; the other BS's output leads the light to the actual QKD system. The thin blue lines are waveguides, transporting light across the photonic circuit. A 80:20 BS is the first optical component of the cryptography setup. One output (with the higher transmission) represents the local oscillator, the other represents the signal.

The local oscillator arm (the lower part) consists in a single 0.7 mm long phase shifter (called *PhiQuad*), used by Bob to choose on which quadrature the projective measurement is performed.

The signal arm (the upper part of the figure) corresponds to Alice's side of the chip. It can be divided in two main parts: the modulation (phase and amplitude) and the attenuation.

Modulation at Alice's

The modulation is performed by a 1.3 mm long MZI and by a phase shifter of the same length. Both the arms of the MZI can be controlled; they are called *AMod1* and *AMod2* respectively. They are followed by the phase shifter, called *PhiMod*. After the modulation there is a control photodiode: a 99:1 BS takes almost all the light out of the optical setup to be measured in this photodiode to check if the amplitude modulation has been properly performed. The phase control is not possible since there is no direct access to the light pulse, but only on the photocurrent coming from the photodiode, so no interferometric measurement is possible at this stage. This means that the phase modulator must be calibrated using directly the final homodyne detection.

Attenuation at Alice's

The last procedure of Alice state preparation is the attenuation, performed by two MZI 1.3 mm and 1.0 mm long and called *VAT1* and *VAT2* respectively. The attenuation is necessary since the signal pulse must contain a small quantity of photons so that the total modulation amplitude is comparable to the variance of

the homodyne detection output. This amount of photons slightly varies depending on the detection properties and on the local oscillator intensity, but it is usually around a few tens of photons.

Detection at Bob's

The last part (right bottom side in figure 6.16) is the homodyne detection: the two waveguides containing the signal and the local oscillator are collected in a 2×2 50:50 BS. Each of the two output arms of the BS is equipped with two 0.3mm long PIN junction, used as fine attenuators to balance the imperfections of the BS from the local oscillator point of view (more will be explained in the next section 6.5). The modulators we are using at this stage are PIN phase modulators that, as we already know, act on both the phase and the amplitude of the light passing through them. However, since the devices are placed right in between the BS and the photodiodes, the phase variation does not affect the measurement.

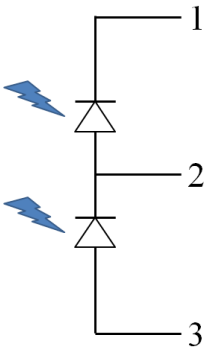


Figure 6.17: Electronic configuration of the photodiodes.

Then the light is measured by two photodiodes put in series. The photocurrent is directly taken and amplified by the amplification system described in section 6.2. It is important to notice that the electrical signal coming from the photodiodes is taken from three electrical nodes, not four (two for each photodiode) as it could be expected. In fact if the photodiodes electrical circuit is as in figure 6.17 and the output "2" is taken, the homodyne detection subtraction is automatically performed.

6.4.2 Insertion losses and extinction ratios

The components in the system induce passively and/or actively some losses. It is important to analyse this absorption to evaluate the capabilities of the system. Following the results resumed in figure 6.18 we can reconstruct the overall insertion losses (passive attenuation) and the maximum available active suppression.

The first BS, after the grating coupler, gives $-3dB$. The 80:20 BS attenuates $\sim 1dB$ on the local oscillator side and $\sim 7dB$ an the signal side, plus $1dB$ additional due to absorption.

On the local oscillator side there is the PhiQuad phase shifter, which has $IL = 4dB$. So the light that arrives on the detection's BS passing through the local

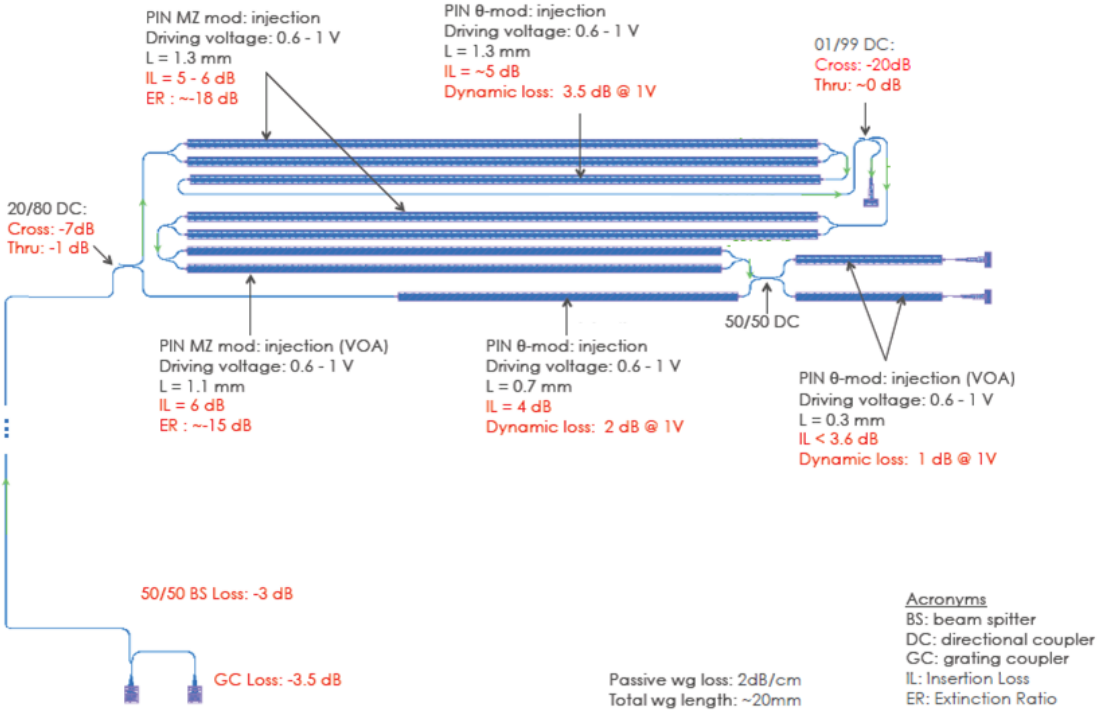


Figure 6.18: CVQKD system: losses scheme.

oscillator arm is passively attenuated by a total insertion loss of $IL_{lo} = -9dB$ with respect to the injected light.

The insertion losses on the signal side are due to two 1.3 mm long MZIs, one 1.0 mm MZI, one 1.3 mm phase shifter and a 99:1 BS. The two longer MZIs have a total $IL = 10 - 12dB$, the short one $6dB$, the phase shifter $5dB$ and the control photodiode's BS $20dB$ for the splitting ratio (99:1) plus $1dB$ for the absorption. The light arriving at the homodyne detection's BS through the signal arm is attenuated by $IL_s = 48 - 50dB$.

The overall passive attenuation leads to a systematic optical power difference of $\Delta IL = IL_s - IL_{lo} \simeq 40dB$ between the local oscillator and the signal.

For what concerns the active attenuation, on the local oscillator side there is only the phase shifter (PhiQuad), attenuating at most $2dB$ for a $\pi/2$ shift.

At Alice's 4 devices must be taken into account: AMod, PhiMod, VAT1 and VAT2. The longer MZI (AMod and VAT1) provide an extinction ratio of $ER \sim 18dB$ each and for VAT2 the extinction ratio is $15dB$. PhiMod, differently from PhiQuad, must modulate the phase up to $\Delta\phi = 2\pi$. This will provide a greater attenuation, up to $3.5dB$. So Alice has at its disposal a $51 - 54dB$ dynamic range.

6.5 Standard homodyne detection calibration

For CV systems, the interferometric detection is fundamental. In section 2.2.4 the procedure for the homodyne detection calibration is described: the detection is balanced when it is shot-noise limited. This condition is obtained by injecting the local oscillator in one of the detection inputs and by using the parameters at

disposal to make the two photocurrents equal. In this situation what is left is just the quantum noise. This can be verified by checking the linear relation that links the local oscillator optical power and the variance of the detection output.

In the current chip configuration the signal is always present in the detection, so the configuration for the detection calibration, i.e. the absence of the signal, must be attained via the attenuation of the signal. The amplification of the detection allows an optimized response and amplification without saturation for $\Delta t = 100$ ns long local oscillator pulses containing $\sim 10^8$ photons. This means that the signal must be attenuated by at least $80dB$ for the detection calibration process to be performed. From section 6.4.2 we know that if on the local oscillator side of the chip we want to obtain intensities of about $I \sim 10^8 ph/pulse \simeq 6.4\mu W$ (at telecom wavelength and 500kHz), the signal will be passively attenuated by $40dB$, having the possibility of a further dynamic attenuation up to more than $50dB$, for a possible maximum total attenuation (passive and active) greater than $\Delta A_{max} = 90dB$.

ΔA_{max} is achievable when the amplitude modulators and the attenuator are already calibrated, since all of them must be used to attain this maximum attenuation value. Of the three MZI used to manipulate the amplitude, only the one called AMod can be calibrated without the help of the detection, by using the control photodiode. For the VAT1 and VAT2 other alternative methods must be used. In fact, the straightforward approach could be to look directly at the two photocurrents and measure the point in which they decrease the most. Unfortunately the $40dB$ steady attenuation brings the ratio I_s/I_{OL} at a level so small that the sensibility of our instruments is not enough to detect changes down to the 4th significant digit.

We used two different methods for two different setups, both relying on the detection's electronic configuration: more specifically, one relies on the spectral analysis of the detection output (electrical noise measurements performed mainly by Paul Crozat at C2N), the other one exploits the advantages of the interferometric nature of the detection itself (modulation measurement performed at IOGS). In the next paragraph we briefly expose the first of the two procedures. The second one will be exposed in detail in section 6.6.

Spectral analysis for detection calibration

The electrical noise tests have been performed at the C2N laboratory. The system controlling the chip in the C2N lab is different from the one used at IOGS for the optical tests and the quantum communication since the remote control is absent, so the setting up of the detection must be manually performed. A continuous wave (CW) source is used instead of the pulsed one. Moreover the two detection's photocurrents are taken separately, filtered and then subtracted by means of a new amplification circuit detailed in figure 6.19, which is different from the compact PCB integrated one in that the amplification is external. The visual access to the detection's output and its variance are not available. In fact the continuous nature of the light makes it impossible to correlate the output to the pulse shape used as a reference in the pulsed regime.

However, if the light is modulated at the same frequency as the pulsed setup's repetition rate (RR=500kHz) a spectral analysis of the output will show the same

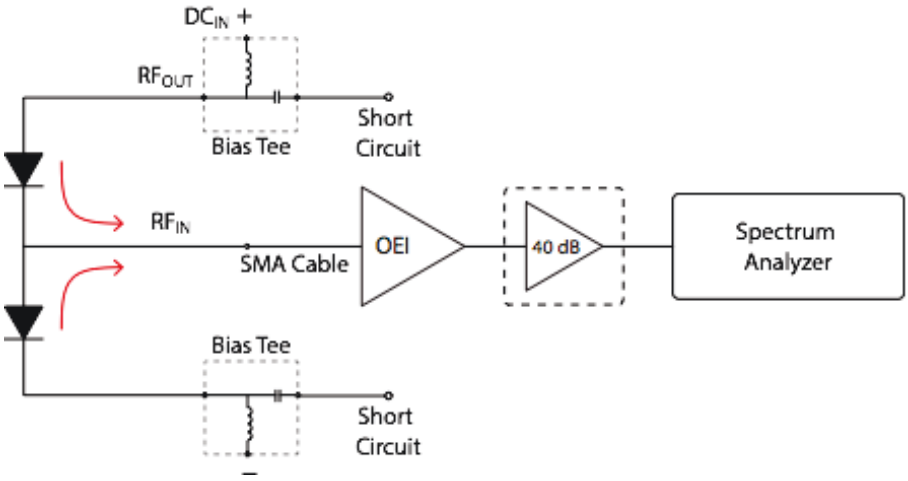


Figure 6.19: Electrical noise amplification circuit: scheme.

principal frequency peaks at frequencies $f = RR$ and its harmonics ($f_k = k \times 500kHz$, with k positive integer).

(a) Before attenuation and balancing. (b) After attenuation and balancing.

Figure 6.20: Spectral analysis: peak at 500kHz. From picture (a) to picture (b) we measure a $CMRR \simeq -52dB$.

The setup has access to the spectral analysis of the noise of the output signal. When the system is totally passive, the noise peak at $f = 500kHz$ stands at $2.5dBm$, over a background noise of $\simeq -70dBm$. By manually adjusting the modulators driving voltage, the peak can be reduced to the absolute value of $-52dBm$ over the same amount of white background noise. The CMRR is then $\simeq -54dBm$. Even though the noise peak is not completely suppressed, this method has been efficient enough to perform the noise measurements on the electrical chain of the system. We will not describe these measurements in more detail in this thesis.

6.6 A new method for the detection calibration

As discussed previously, the homodyne calibration procedure of the complete CVQKD system needs to exploit the modulators and attenuators of the signal, since the sig-

nal is always mixing with the local oscillator in the detection. Therefore, if the local oscillator pulse has an intensity of 10^8 photons, the signal must be actively attenuated by at least 40dB, that must be added to the passive 40dB insertion loss difference. But the condition for the modulator calibration is precisely to have an already balanced homodyne detection. A first basic approach to address this issue was to first maximize the attenuation with AMod exploiting the control photodiode placed after it, using this attenuation for a rough detection calibration in order to approximatively calibrate the VATs and then proceed iteratively alternating the calibration of the detection and of the VOAs until the shot noise limited regime is achieved. This method was not successful, but it made it possible to discover memory effects and crosstalk phenomena between the modulation devices in the system that must be taken into account for the calibration process.

For this reason the system cannot be treated with a modular approach, taking the contribution of each device individually but must be viewed as a system in which every device always interacts with all the other ones. We will present now such a model, which has been theoretically proposed by Pierre Rouchon.

6.6.1 Phenomenological model for the OpSIS chip

The detection output depends on devices that modulate amplitude and phase at the same time. This double effect must be taken into account especially when all the devices are apparently in continuous interaction, even when they are not directly addressed.

A single k-th PIN junction is represented by the complex impedance Z_k

$$Z_k \;=\; e^{a_k + b_k v_k}, \tag{6.3}$$

where v_k is the tension driving the junction, a_k, b_k are complex parameters and $k = 1, 2, \phi, 0$ correspond to AMod1, AMod2, PhiMod and PhiQuad respectively. The two VOAs, VAT1 and VAT2, are considered as a unique impedance Z_v with fixed driving voltage v_v.

A coherent state $|\alpha\rangle$ of amplitude α is injected in the system. The action of the signal on the coherent state is the total impedance Z

$$Z \;=\; (Z_1 + Z_2) Z_\phi Z_v \;=\; (Z_1 + Z_2) Z_\phi, \tag{6.4}$$

where, since Z_v is constant we can fix it to be $Z_v = 1$ without loss of generality. The local oscillator pulse passes through PhiQuad, whose impedance is Z_0.

The output of the detection in this perfect modelling is

$$y \;=\; \frac{1}{2}|(Z_0 + iZ)\alpha|^2 - \frac{1}{2}|(iZ_0 + Z)\alpha|^2 = \frac{Z_0 Z^\star - Z_0^\star Z}{i}|\alpha|^2 = \; -2Im(Z_0 Z^\star)|\alpha|^2 \tag{6.5}$$

This model is still based on the assumption that the detection is balanced or that

we can somehow successfully suppress the signal. But even if it does not propose an alternative method to solve the detection calibration process, it gives the tools to evaluate the modulators response even if the detection is not perfectly calibrated. In fact, if the calibration parameter b_0 is left to be calculated from some fit, we do not need to care if its value is the one that perfectly balances the detection.

To be more precise, an equation can be extracted from the model when we take into account one amplitude modulator and the phase modulator (for example, AMod1 and PhiMod), while the other parameters and devices are considered to be fixed:

$$y = a + b\cos(c \cdot V_p + d)e^{r \cdot V_p} + f\cos(g \cdot V_a + c \cdot V_p + h)e^{r \cdot V_p}e^{k \cdot V_a} \tag{6.6}$$

This equation has 2 variables, V_p and V_a, i.e. the voltages applied to the two modulators, and 9 parameters $(a, b, c, d, f, g, h, k, r)$. Equation 6.6 is obtained by using the explicit form of the impedances, putting equation 6.3 in equation 6.5. The parameters must be calculated by fitting experimental data. To do so, the master equation 6.6 must be split into two sub-cases in which V_p or V_a are constant respectively. This leads to the two sub-equations depending only on V_a or V_p respectively.

The AMod voltage dependence is given by

$$y_a = A + B\cos(g \cdot V_a + C)e^{k \cdot V_a} \tag{6.7}$$

and the PhiMod voltage dependence by

$$y_p = a + b\cos(c \cdot V_p + d)e^{r \cdot V_p} + D\cos(E + c \cdot V_p + h)e^{r \cdot V_p} \tag{6.8}$$

6.6.1.1 Calibration measurements

Amplitude Modulator

The modulator calibration for the homodyne detection balancing consists in finding the voltage V_0 at which the attenuation provided by the modulator is maximal.

The chip design allows us to properly calibrate only the first MZI, since this is the only one connected to a single photodiode that could read the photocurrent. When the AMod1 driving voltage V_{mod} is applied, a photocurrent proportional to the modulator's transmission is detected. The plot of the detector's photocurrent against V_{mod} is shown in figure 6.21, from which the maximal attenuation driving voltage can be extracted: $V_0 = 3.91V$.

Variable Attenuators

The only way to evaluate the effect of the VOAs action is to extract information out of the homodyne detection, which is an interferometric measurement. The maximal attenuation corresponds to the minimal variation of the output when the phase changes. Let us now assume to use equation 6.7 for a given and fixed V_p

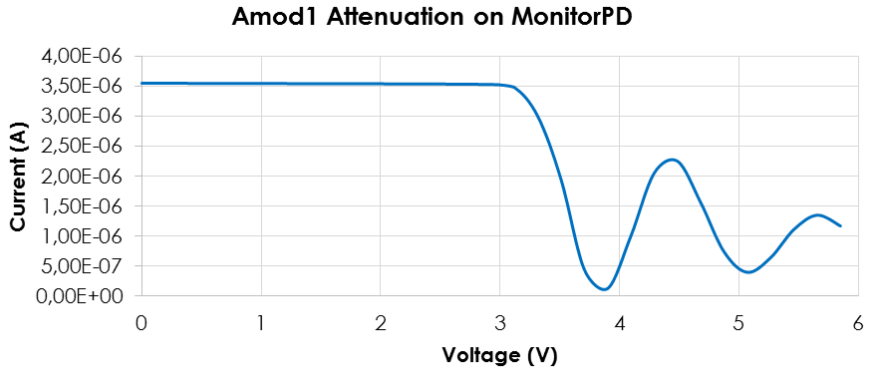


Figure 6.21: AMod1: photocurrent (proportional to the transmission) vs the applied voltage.

value, i.e. for fixed B and C parameters, namely B', C'. The output should follow the equation. If the same measurement is performed for different sets of the B, C parameters, different curves will appear, each one of them corresponding to a particular phase drift induced by PhiMod's action.

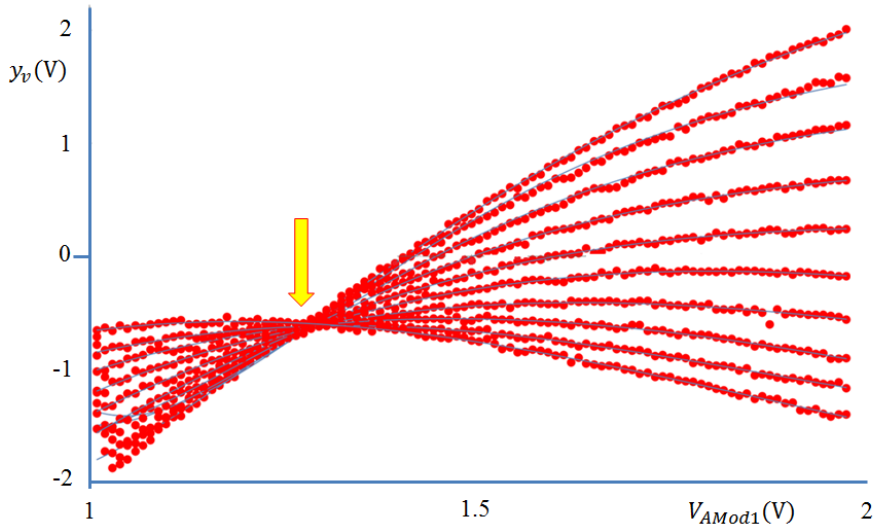


Figure 6.22: VAT1: output voltage vs applied voltage.

In figure 6.22 this situation is shown: different curves represent different phases. VAT1 attenuation is tested as a function of the applied voltage. Each point in the figure represents the average value of 100 acquisitions, in order to reduce the noise and find better data for the fit.

We notice that the fit of the function $y_v(V_{mod})$ perfectly matches with the experimental data, demonstrating both the suitability of the model and the accuracy of the experimental data.

There is a specific voltage (highlighted by the yellow and red arrow) for which the phase dependence is less relevant, i.e. the attenuation is maximal: this value

Device	V_0
1	1.29V
2	1.33V
3	1.96V

Table 6.2: Set of V_0 values for the signal attenuation

is V_0 for the VAT1. The exact value is extracted finding the interception of the different curve's fit.

To further confirm the quality of the model and the data, the same measurement has been performed setting AMod at its V_0 voltage and VAT1 has been tested again. In this scenario we expect to find a flatter curve with less vertical variation with respect to the previous case, because the signal is attenuated by $\sim 18dB$ by AMod. The result is shown in figure 6.23.

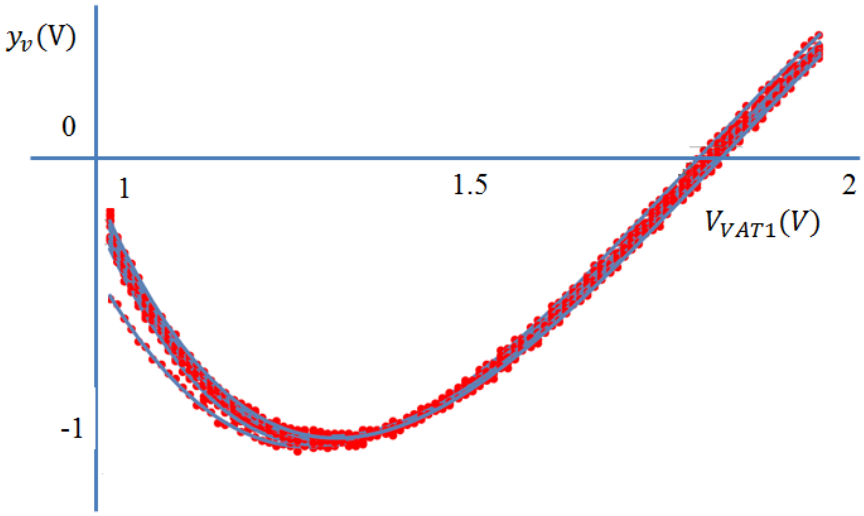


Figure 6.23: VAT1: output voltage vs applied voltage when AMod 1 is attenuating.

Using this method a set of V_0 values for the signal suppression can be found: it is listed in the table 6.2.

6.6.2 Shot Noise Limited slope

The next step is to use the set of the V_0 values we found for the three MZI (AMod, VAT1 and VAT2) for tracing the shot noise limited (SNL) slope of the homodyne detector. The result is shown in figure 6.24.

The figure does not show a proper linear behaviour. In fact the balancing of the detection does not seem to be achieved. Even if the linear fit seems to hold for low local oscillator's intensities, the detection is not SNL where it is needed to be, i.e. for $\sim 10^8$ ph/pulse.

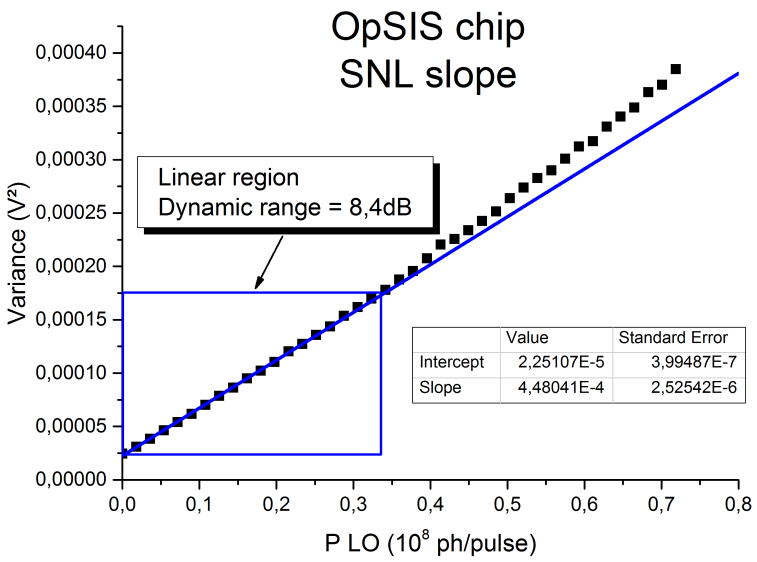


Figure 6.24: OpSIS chip: SNL.

The main cause of the loss of linearity is the appearance of non linear affects in the photodetectors: when a photodetector is hit by a too intense optical beam, the amount of carriers is not enough to properly convert light into current. The capacity to bear a higher number of incident photons can be slightly modified by reverse biasing the photodiode: a higher reverse bias increases the width of the depletion region, which is the active area in which the current is generated.

A study of the impact of the photodiode reverse bias voltage (the polarisation voltage) is shown in figure in figure 6.25. It is clear that the bias voltage does not affect the photodiodes linear response significantly: the non-linear behaviour is always present even for very low optical intensities. This forces the amplification system to operate in non optimal conditions, since the overall optical power must be lowered below the $\sim 10^8$ ph/pulse threshold.

6.7 Conclusion

The all-in-one design consists essentially in avoiding the actual communication between two separated parties so that critical issues (useless to the aim of demonstrating the integrability of the protocol) such as the multiplexing, the detection synchronisation and the phase drift tracking at Bob's, are not affecting the protocol implementation. But this leads to an even more important drawback: it is impossible to inject in the detection the local oscillator alone, because it always mixes with the signal. Thus the calibration of the detection and of the whole system is partially compromised.

It has been possible to develop a method (section 6.6.1) for the amplitude modulators calibration, to allow the complete suppression of the signal, but the evaluation of the parameters of the fit for 3 different devices takes more time than the intrinsic

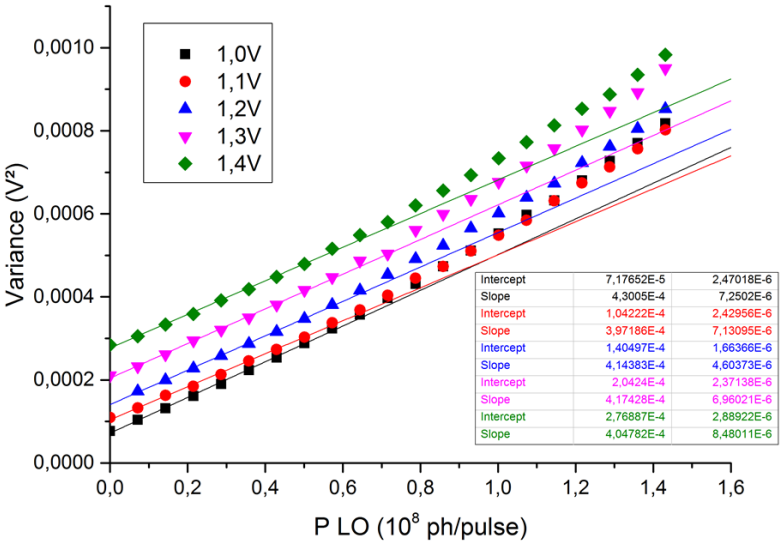


Figure 6.25: OpSIS chip: detectors. Study of the influence of photodiode bias voltage on the linearity.

drift of the characteristics of these particular modulators. Such a delay makes the method not experimentally feasible with the OpSIS chip.

Moreover this first integration attempt does not take into account the crossover between what silicon photonics can offer and what quantum cryptography needs. The first incompatibility concerns the standard techniques used in silicon photonics experiments and their consequences on the coupling stability needed for quantum noise measurements, which is much higher than the stability required by standard silicon photonics measurement. The chip has been initially designed to be electrically driven by electrical probes and connected to an external amplification, situation in which the coupling was impossible to achieve. The improvements brought to the setup (the built-in PCB-on-PCB amplification structure and the wire bonding) are the solution for a more stable coupling.

Finally the memory effects and the crosstalk between components makes this approach not suitable for QKD, even though it gave hints concerning how the integration of the GG02 should be done. The most important are:

- The separation of Alice and Bob.
- Since crosstalk is possible, it would be better to design a chip in which the structures are not too close to each other.
- Control outputs must be present after each device, to treat its effects independently from the others.

Chapter 7

Separation of Alice and Bob for real communication

In the previous chapter we studied a chip configuration without a real separation between Alice and Bob. The expected advantages of suppressing the communication channel were actually not present, because various unexpected cross-talk effects appeared in this particular chip architecture. In addition, we have observed inadequacies in the individual components, especially in the photodetectors, and we have found technical defects in the circuits.

Starting from the suggestions given in section 6.7 it may have been possible to design a better chip, but in the meantime another generation and configuration was already in the manufacturing process in the LETI foundry (Grenoble). In this new device the modulation and detection are physically separated, on two different chips. In this chapter we discuss this device, with details of the features of this approach and the results that we have obtained.

A new architecture and a new foundry imply that the behavior of the components is different, so in the first section the devices will be tested independently. The most important part of the experiment is, as discussed earlier, the homodyne detection, and hence its study will be the subject of the second section of this chapter.

The separation of modulation and detection changes the setup design: the channel is now present and external optical devices may be used. For testing purposes we may therefore use an external modulation, as the one studied previously for the bulk configuration of the protocol. After the detection is ready, the problem of the modulation can be addressed. This *divide et impera* course of action allows to separate and better understand the issues coming from the different devices.

Since the detection is now completely separated from the rest of the systems, we can properly solve the problem of the external modulation calibration. When Alice and Bob are ready, the actual communication starts, so the excess noise can be evaluated and a secret key extracted: this will be presented in the third section.

In the last section we describe ongoing work about calibrating the on-chip modulation and the realization of a heterodyne detection. The modulation chip is required for a true complete integration of the protocol, while the heterodyne detection will represent a significant improvement in the implementation of the system.

7.1 Overview and devices testing

The second chip was designed by Mélissa Ziebell [2] and manufactured in Grenoble in the LETI foundry. For this reason it will be called *LETI chip* or *second generation chip*. Even though this new generation brings several upgrades, it must not be considered as the final version.

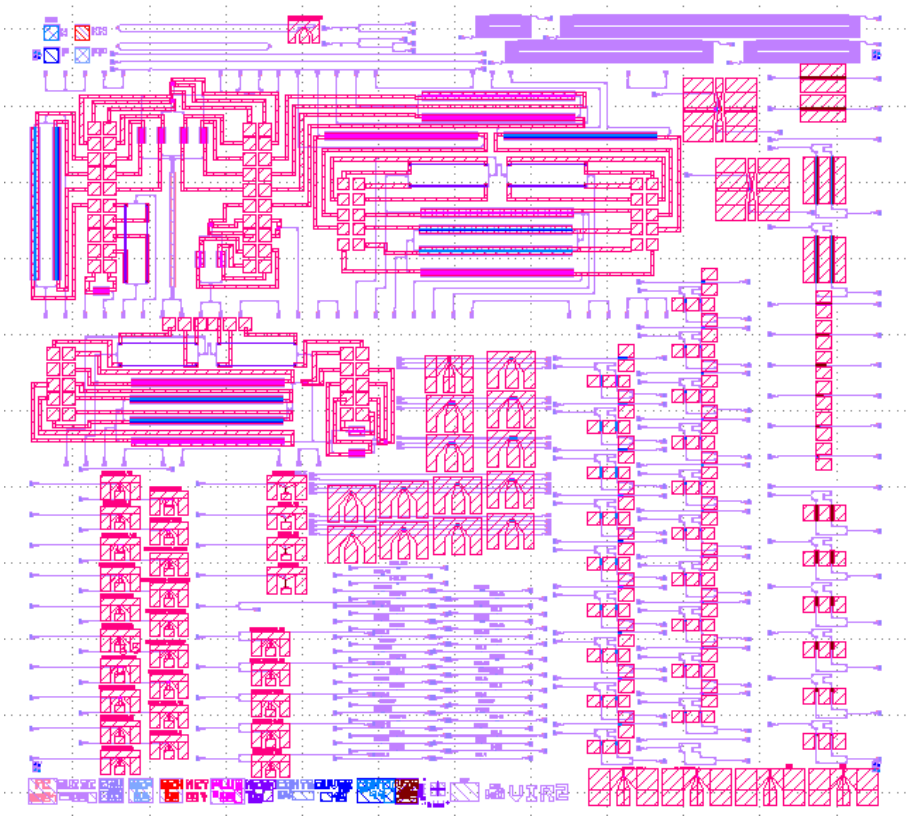


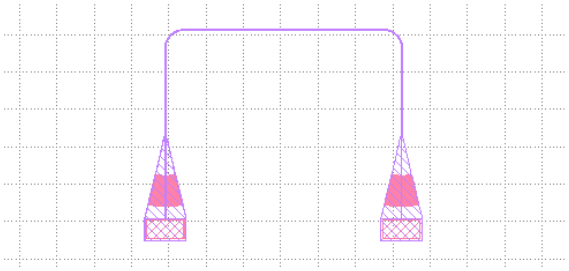
Figure 7.1: LETI chip: overview.

In figure 7.1 we can see the overall circuit schematic. As for the OpSIS chip, we can identify all the components needed for the implementation of the GG02 protocol. They have been independently tested in the *Centre de Nanosciences et de Nanotechnologies* (C2N).

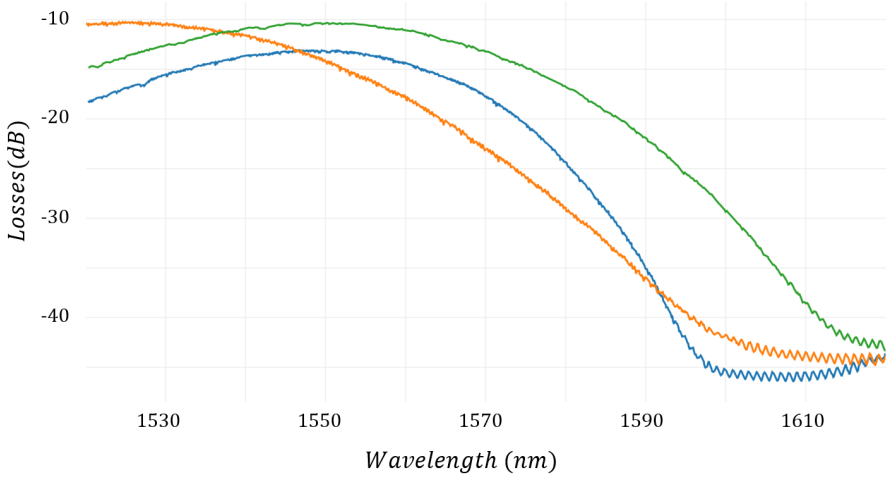
The devices are divided into passive and active and they must be able to work at relatively high speed ($\sim$ MHz). In fact as we saw, the system operates at 500 kHz, i.e. Alice prepares and sends a state every 2 μs. Before being sent, the state must be ready and stable, therefore the light modulation for the state preparation must be faster than the repetition rate. Moreover the protocol needs the state carrying the information to be a few photon pulse, so a steady and strong attenuation is needed. "Steady" still means that the speed should be comparable to the clock frequency so that the main level can be adjusted between two pulses.

7.1.1 Grating couplers

Coupling is tested using a simple IN/OUT structure (figure 7.2a) composed by a grating coupler for the light injection connected by a simple waveguide to another grating coupler for light extraction. A preliminary test coupling spectrum is shown in figure 7.2b for three different positions of the coupling setup, achieved by manual optimization.



(a) LETI chip: In/Out structure for coupling optimization



(b) LETI chip: coupling losses and λ shift. The IN/OUT transmission for (green) almost optimal coupling, (blue) non-optimal coupling distance and (orange) non-optimal coupling angle

Figure 7.2: LETI: coupling test

The optimized coupling is represented by the (green) curve centered at 1550nm, with an *in&out* transmission between -6dB and -10dB (3 to 5dB of attenuation for each coupler). The different curves correspond to a different coupling distance or angle θ. In fact θ controls the phase matching condition at the grating coupler, which optimizes the coupling of a particular wavelength following equation 4.15.

Usually coupling-in and coupling-out using a fiber array induce the same losses, so we can say that the single coupler losses are half the total IN/OUT losses. In the scenario pictured in figure 7.2b a single coupling operation gives 5dB of losses.

7.1.2 Beam splitters or MMI

In this chip we have 3 different types of Multi-Mode Interference couplers. We recall that a MMI coupler that has n inputs and m outputs is said to be $n \times m$. In this chip we find:

- balanced 2×2 for homodyne detection;
- balanced 2×4 for heterodyne detection (more details in 7.4.2);
- balanced 1×2 and 2×1 for light separation and recombination in the optical scheme for test intensity measurements and in MZI.

They have been designed to give performances very close to 50:50 behaviour, with an insertion loss $IL = 1$dB only. However, they are really sensitive to the quality of the light that passes through them, which must be single mode, TEM00, with propagation direction as close as possible to the axis of the MMI.

All these properties are usually satisfied, since the waveguide itself acts like a filter, even though the coupling leaves some spurious contribution: after 1 or 2 mm of waveguide the higher order modes have completely vanished and the light propagates in the same direction as the waveguide ones (no reflections on the edges). This condition optimizes the MMI behaviour. However in some devices, as we can see in the homodyne detection in figure 7.8, the portion of waveguide from the coupler to the MMI is really short: considering that the grating couplers are separated by $127\mu m$, the distance between grating couplers and MMI is about of the same order. This does not allow the light to be properly filtered, affecting the BS ratio since spurious modes will reduce the interference visibility in the MMI.

7.1.3 Fast modulation devices

In section 4.2.2 various kinds of phase shifters have been described. The fast devices used in this chip all rely on the same technology of current injection for carrier depletion, so they all go at the same speed (∼10GHz), which is more than enough for CVQKD purposes.

Phase modulator

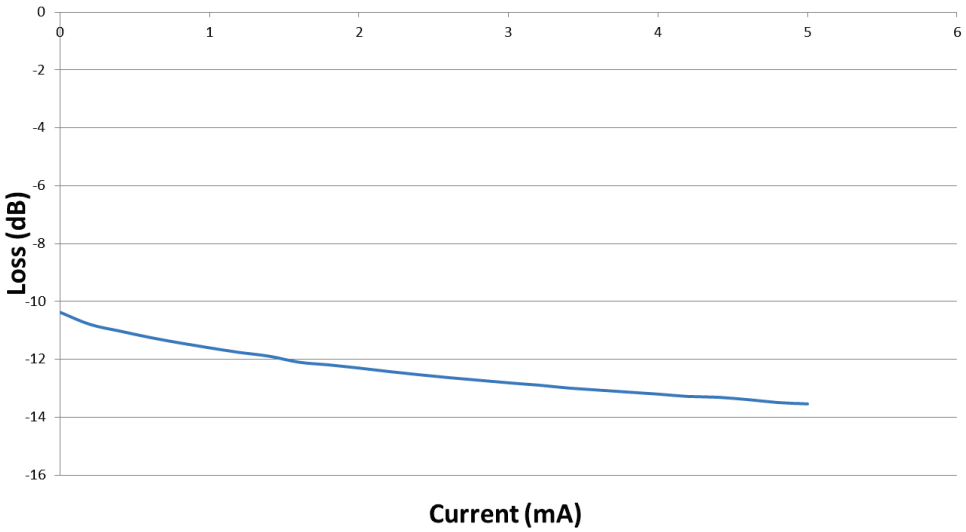


Figure 7.3: LETI chip: Phase shifter losses (in dB) vs injected current (in mA).

No measurement on the phase drift has been performed for this generation of chips: this implies that the relation between the applied current and the induced phase change will be evaluated directly on Alice's chip. We have however studied the loss as a function of the current: increasing the current leads to higher losses. The device has been engineered to have at least a 2π shift at 5mA, considered to be the maximum allowed current. We see from figure 7.3 that at 5mA the losses are increased by 3dB with respect to zero drive. This must be taken into account when Alice creates the state to send to Bob.

Amplitude modulator

The same device inserted in a Mach-Zehnder interferometer becomes an amplitude modulator.

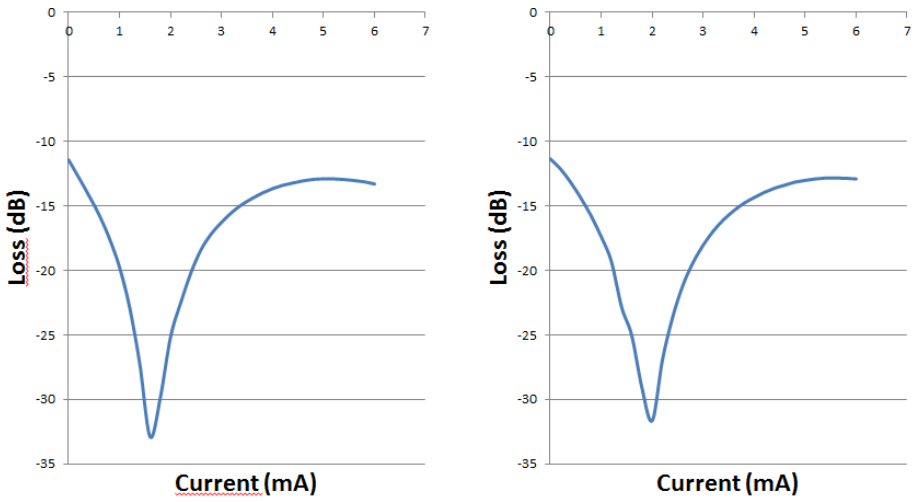


Figure 7.4: LETI chip: PIPIN MZI attenuation using arm 1(left) and arm 2 (right).

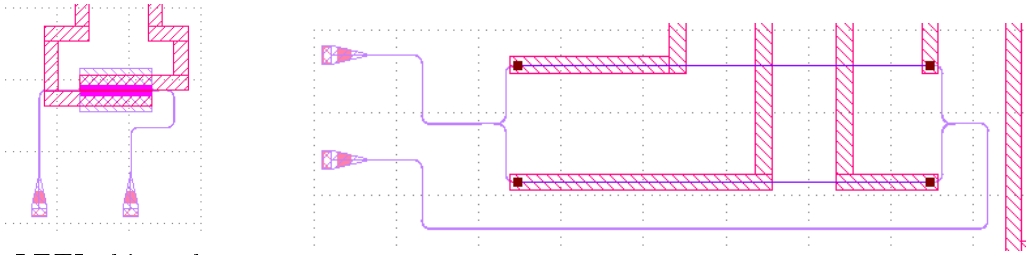
In figure 7.4 the attenuation (or amplitude modulation) is plotted against the applied current on just one arm of the interferometer. We can see that the response of the two arms is quite similar.

For the protocol to be efficient we need a dynamic amplitude range of at least 10dB. From the figure we can see that a 20dB dynamic range is achievable.

Variable Optical Attenuator (VOA)

This device (figure 7.5a) is made with the same technology as the phase shifter but it is used differently.

The balancing of the homodyne detection needs to be very precise, so the amount of light in each arm of the detection must be adjusted with the same precision. Since the beam splitter of the detection is supposed to be close to (but not exactly) a 50:50 performance, a fine adjustment of the intensity difference in the two arms is required. Moreover after the beam splitter the phase has no effect anymore since the interference has already taken place. All this makes the phase shifter-based attenuator the right device to be a VOA for balancing the detection.



(a) LETI chip: short VOA's test structure

(b) LETI chip: Thermal MZI's test structure

Figure 7.5: LETI: test structures for VOA.

7.1.4 Slow Attenuation

The slow and strong attenuation can be provided by *thermal Mach-Zehnder attenuators*. The concept is the same as the MZI amplitude modulators we just saw, i.e. two phase shifters are inserted in the two arms of the MZI to create destructive interference, but in this case the phase shifters are thermal (see figure 7.5b).

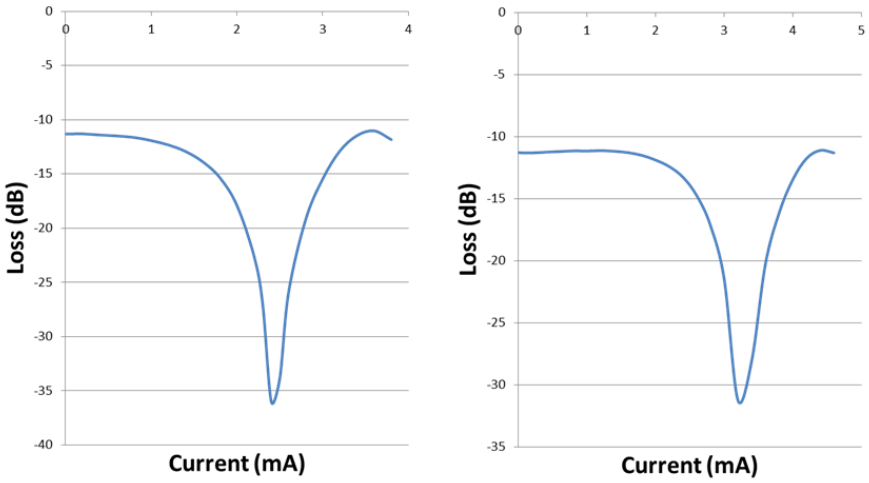


Figure 7.6: LETI chip: Thermal MZI attenuation using arm 1(left) and arm 2 (right).

The thermal phase control is more accurate and induces less losses, so that the amplitude of the light exiting the two arms and interfering in the second MZI's beam splitter is the same. This allows the visibility of the interference to be greater than the one that can be achieved with the electrically induced depletion shifter. Figure 7.6 shows how the attenuation reaches 25dB (sometimes 30dB, but it depends on the fabrication of the particular device in the chip's wafer). Such a device is used only as a VOA because the speed of the thermalization process of the device ($\sim$ 1MHz) is too slow for the state preparation process.

7.1.5 Photodetectors

As we will see in the following sections, the LETI photodiodes are better than the OpSIS ones, in view of their use for CVQKD. In particular the dark current is smaller and the non-linear effects arise in intensity regions far from the desired working conditions. Moreover, the dynamic resistance of the photodiode has a much better behaviour, as seen by looking at the I-V curve, which must be as flat as possible after the reverse bias knee.

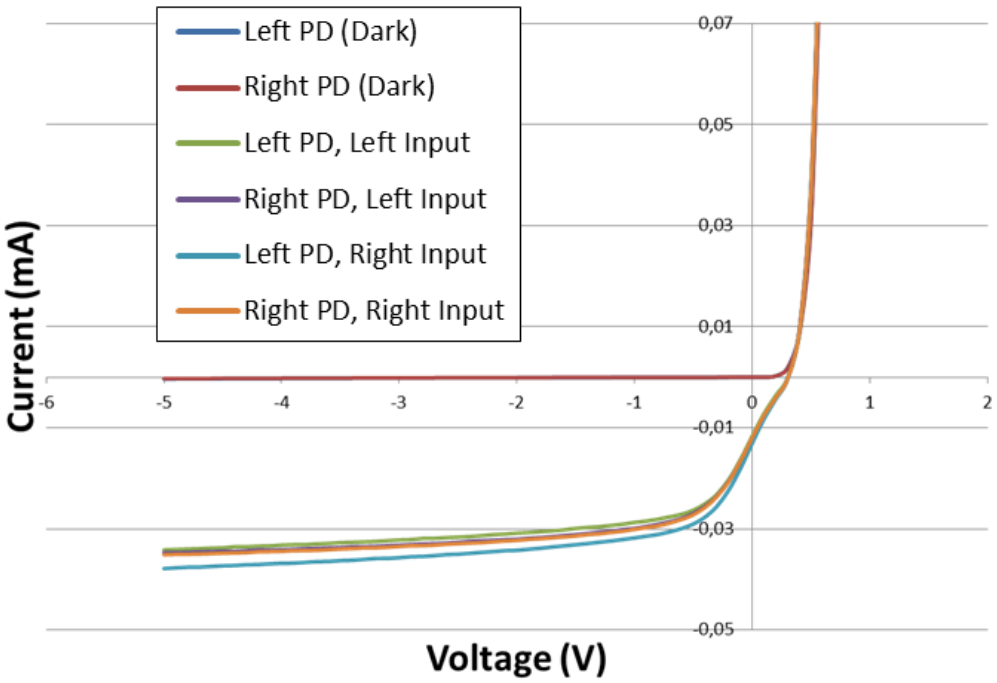


Figure 7.7: LETI chip: homodyne detection photodiode I-V curves depending on the input channel. The dark current I-V curve is plotted as well.

Figure 7.7 shows exactly this behaviour: for reverse voltages below 1.0V-1.5V the I-V characteristic becomes more and more flat.

Another important characteristic is the responsivity, measured as R=1 A/W. From the responsivity it is easy to calculate the *quantum efficiency* η_{PHD} from equation 6.2. In our case the quantum efficiency is $\eta_{PHD} = 0.8$.

These detectors can handle a high optical power because they are larger than standard ones: a bigger surface allows the atoms reacting to light to behave properly. In fact when the optical intensity is too high, non-linear effects (such as double electron generation) may occur and defects in the crystal may be created. While non linear effects disappear when the intensity decreases, the defects are permanent, and the performance of the photodetectors is irreversibly dteriorated. These two factors are the main cause of the loss of linearity we experienced in the other chip. The better quality of the new photodiodes will be highlighted in the following by a comparison between the SNL slopes taken with the two different chips.

7.2 Calibration of the homodyne detection

In chapter 6 we observed various problems when Alice and Bob are on the same chip, because the signal and the local oscillator are always mixing in the homodyne detection. As confirmed by the difficulties of balancing the detection in the OpSIS chip, a proper calibration of the receiver requires to inject only the local oscillator in it. From the OpSIS chip study it also appeared that integrated circuit elements behave differently from their bulk counterparts, and that different parts of the circuit may interact in a non-predictable and sometimes non-repeatable way, creating thereby uncontrollable cross-talk effects.

Therefore a physical separation of Alice (generation and modulation part) and Bob (detection part) appears to be required, for both the characterization and the operation of the system. In this section we will begin by the calibration of the balanced detection, the basic element of a successful realization of a CVQKD protocol.

7.2.1 Overview

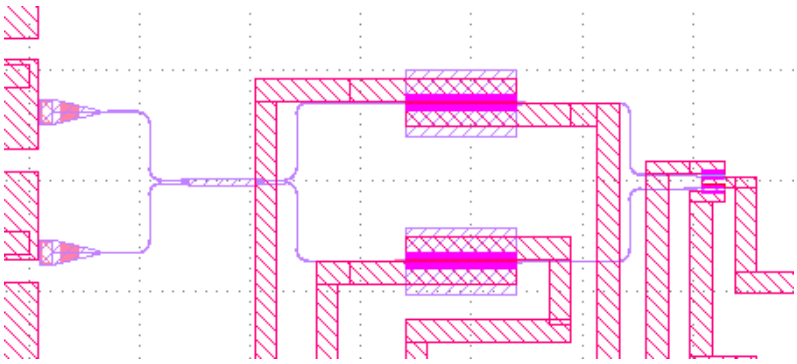


Figure 7.8: LETI chip: The homodyne detection

Figure 7.8 shows the homodyne detection photonic circuit implementation. On the left there are two grating couplers, one for the local oscillator and one for the signal. Light, through integrated waveguides, travels to the 50:50 beam splitter (or 2×2 MMI, see section 4.2.4). After the BS on each arm is inserted a VOA (paragraph 7.1.3) to compensate for the imperfections of the BS. Finally two photodiodes, which are electrically connected in series, transform the light intensity into current.

7.2.2 Balanced homodyne fetection for SNL behavior

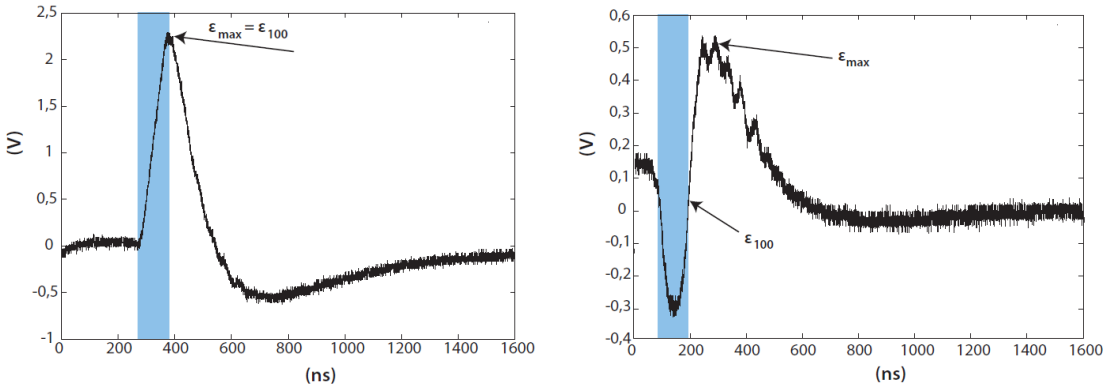
The general procedure to balance the detection is described in section II, and relies on injecting the local oscillator alone (no signal) in one input of the homodyne detection. Due to imperfections of the system (coupling, beam splitter ratio, different efficiencies of the photodetectors) the two photocurrents will not be equal, so the subtraction will not completely cancel the contributions of classical light.

The most obvious way to balance the detection is to attenuate the most intense BS output while directly measuring the two photocurrents. This operation

needs very high resolution, as discussed in section 2.2. The photocurrents could be measured using the single photodetectors amplifiers discussed in section 6.2. They transform the photocurrent in voltage that can be displayed and measured with the acquisition card or with an oscilloscope. The amplified signals are about 5mV pulses, with a noise in the tenths of μV, which may provide a coarse adjustment, but not the final one. Using external amplifiers is not really helpful either.

So the best method for balancing is using the homodyne detection output itself, as described by Simon Fossier in his work on the "bulk" CVQKD setup [4].

Figure 7.9: Unbalanced and balanced detection [4]



(a) Unbalanced detection

(b) Balanced detection

In figure 7.9 an output signal is shown, when the detection is (slightly) unbalanced or (accurately) balanced. The pulse duration is Δt_{pulse}=100 ns, highlighted in blue. Since a fully balanced detection should provide a signal with zero mean value, the recorded signal should be only noise. This is not the case however, due to very small response time differences between the two photodiodes: a classical part always remains in the differential photocurrent. This waveform is not what we want to measure (we are only interested in its shot-to-shot variations), but it is very useful to balance the detection.

In more detail, since the DC component of the photocurrent is cut at the entrance of the charge amplifier, one expects that after 100 ns the total electrical charge accumulated in the detection must be around zero, meaning that the subtraction has been properly performed. The interesting AC components show up later on, and the actual measurement can be performed in this region, i.e. between the pulse's end and the end of the response of the integrator, at a time t such that $\Delta t_{pulse} < t < \Delta t_{pulse} + 400ns$. As we will discuss in section 6.2, the acquisition is triggered at the top of the peak in this time interval, because the gain of the chain is maximum there. As a consequence cancelling the observed waveform at Δt_{pulse} gives a good criterion for balancing the detection.

Then the quantities of interest are the shot-to-shot variations of the pulse, measured as said above. They are due to shot noise in the absence of signal beam, and also to the (random) signal modulation in the presence of a signal beam. If the detection is too unbalanced the amplifier saturates, and the observed shot-to-

shot variance will be strongly reduced; this is clearly to be avoided, and the above criterion on the waveform is enough for achieving that

A finer criterion is given by considering that the LO itself may have classical fluctuations, usually called RIN (Relative Intensity Noise). The variance of this noise scales quadratically with the LO intensity, contrary to the shot-noise variance which scales linearly. At a given point the balancing may be good enough to avoid saturation, but still not able to suppress the RIN term which is quadratic with the local oscillator intensity and proportional to the fourth power of the unbalance ε. So by reducing further the unbalancing, the additional RIN term in the variance will decrease, until it is completely suppressed when $\varepsilon = 0$.

The balancing process is physically performed by driving the VOA of the more intense arm of the detection. Increasing the applied current (or equivalently voltage following the I-V characteristic of the device) increases the attenuation imposed by the VOA. The detection balancing is reached when the variance of the detection reaches its minimum (due to balancing, not to saturation !), which is the SNL.

The final proof to the proper balancing is the SNL slope. This figure also has the role to show where the non-linear phenomena start to appear, telling us what are the power limits of the detection. In figure 7.10 we show the SNL slope for the LETI homodyne detection, up to the maximum power of the laser diode, manually coupling the light in. From this figure we can also determine the value of the electrical noise v_{el}, as the intercept point of the line with the vertical axis.

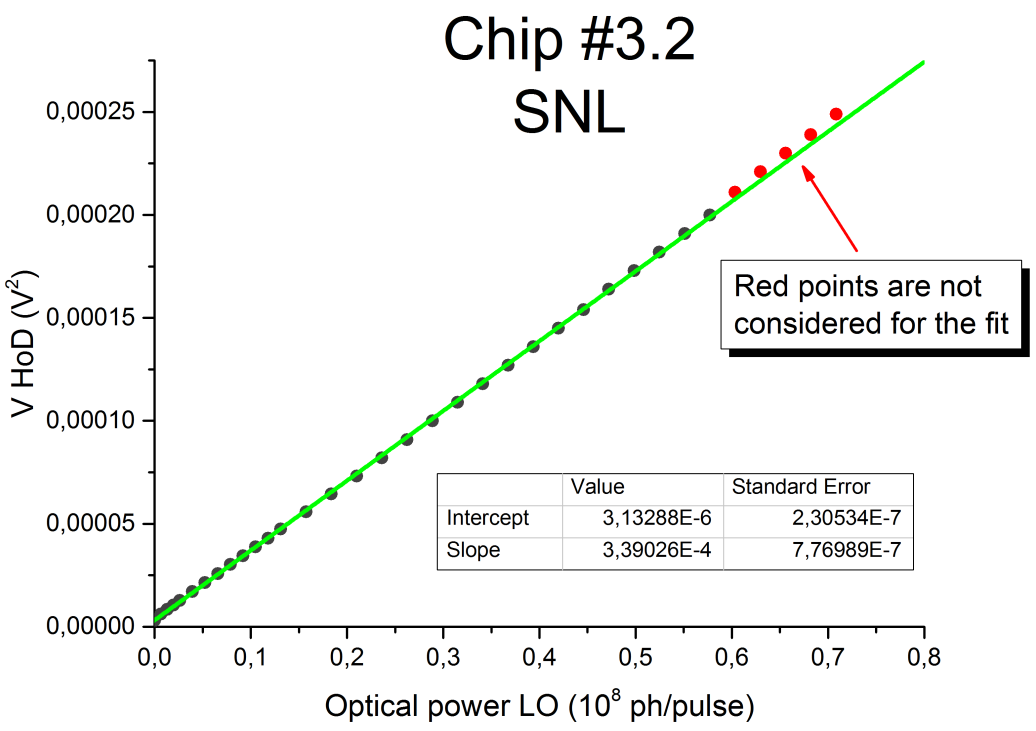


Figure 7.10: LETI chip: SNL slope

7.2.3 Detection stability

Once the detection is balanced many factors continue to evolve in the experiment, continuously changing the conditions of the detection, and therefore its balancing.

Before the very recent fiber attaching (by gluing the fiber on the chip), the coupling was subject to every source of vibration (even taking a step in the laboratory), which could be seen on the oscilloscope as a perturbation of the homodyne pulse.

Addressing this problem in a more general way is important as the stability of the coupling is a major issue for the detection and for proper operation of the overall system. The coupling may modify the quantity and the quality of the injected light, change the intensity of the light interacting in the BS, the visibility of the interference, and eventually the BS ratio (see section 7.1.2). The manual coupling configuration had another source of instability: the fiber array was always in direct contact with the resin of the wire bonding on the chip and the resulting stress between glue and array caused a slow but continuous relative shift, so the system decoupled until reaching an equilibrium. This equilibrium position, although it did not optimize the coupling, was the coupling condition for the measurement, because it ensured more stability. The fiber attaching erased this problem.

Another source of balance instability comes from the device that allows the balance, namely the VOA. The VOA (and indeed all of the setup) is not thermally stabilized in this chip design, so the temperature drift due to the application of a voltage and the flowing of a current introduces an additional term to the refractive index, slowly changing the VOA attenuation. Thermal stabilization would greatly improve the stability of the system, and could be an improvement for the next chip generation.

Since however the temperature drift is quite slow ($\sim$ 10 min) with respect to the characteristic time of the communication (corresponding to the communication of one block of data $\sim$ 10 ms), at this stage a manual adjustment allows the stability of the system during multiple runs of the experiment. This operation could be computer-controlled, but since it is not strictly necessary for the purpose of the current experiment, we also leave this task for later improvements.

7.3 Integrated detection for hybrid GG02

From now on let us assume that the detection is perfectly balanced: the SNL slope (figure 7.10) tells us we are in the quantum regime. The balancing of the detection is a necessary but not sufficient condition for the realisation of an integrated detection for CVQKD. The final test is to perform actual communication to estimate the excess noise and the key rate.

The protocol (see section 3.3 and section II) consists in 3 parts: the state creation at Alice's, the detection and the parameter estimation, and finally the key extraction. As first test we decided to use a known modulation setup: this allows the integrated homodyne detection to be fully and independently tested. Therefore we used the modulation scheme of the bulk setup, developed in refs. [4,46,47].

The setup (figure 7.11), composed by all polarization maintaining (PM) fibered devices, is as follows:

1. The laser diode, driven by current pulses, generates light pulses of duration Δt_{pulse}=100 ns at a repetition rate f=500 kHz (a pulse every 2 μs).
2. The laser beam is divided into two by a 90:10 (or 99:1) 1×2 fibered BS. The 90% BS output corresponds to the bright LO and the 10% to the signal.
3. The signal passes through the electro-optic modulators (amplitude and phase) and a VOA. This represents Alice's state generation stage.
4. The channel on the signal side (or *arm*) is represented by another VOA, which determines the transmission coefficient T.
5. Both signal and local oscillator are connected to an optical delay line (VOPD).
6. The outputs of the delay lines are directly the input fibers of the fiber array, which couples the light in Bob's chip.

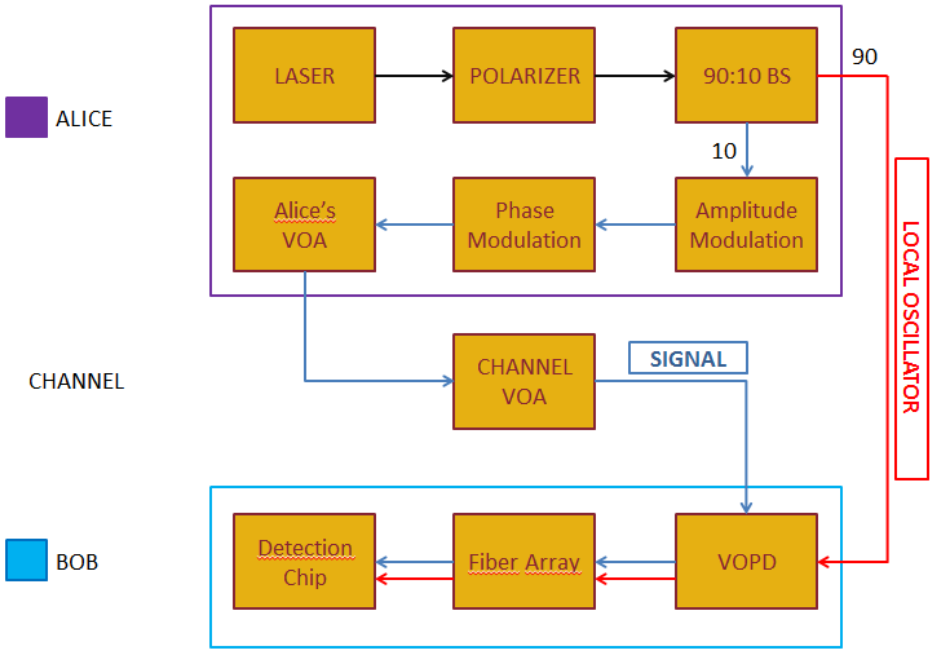


Figure 7.11: The optical configuration for the communication with the integrated LETI homodyne detection.

A system like this needs two more steps of pre-communication calibration.

- The homodyne detection is an interferometric measurement, so the two pulses arriving on the detection BS must have the same frequency, electromagnetic field mode, length and time arrival.
- The Lithium Niobate electro-optic modulators (from EOSPACE) need real-time calibration.

Interferometer balancing

The emitted laser pulses are strongly chirped due to the pulse driving, and travel through dispersive media different from air. When they arrive at the detection BS a difference in the arrival time induces an inhomogeneous phase difference distribution along the pulses length. When the two pulses interfere this heterogeneity causes the formation of oscillating patterns typical of this non-optimal phase and frequency distribution. To avoid this phenomenon the interferometer must be balanced within 2 mm [4]. A long fiber is inserted in the LO channel to equal the optical path length within a few centimeters, then an optical delay line is used for fine tuning.

Modulator calibration

The effect of the EOSPACE modulators on the detection output, when a linear voltage sweep is imposed on them, is sinusoidal. This has a different meaning if the modulator acts on the amplitude or on the phase of the signal, even though the final output of the homodyne (interferometric !) detection is always written as

$$V_{HoD} = A\sin(\pi V/V_\pi + V_{bias}) + V_{offset}. \tag{7.1}$$

For the amplitude modulation the interesting quantity is $A\sin(\pi V/V_\pi + V_{bias})$, so the modulation is sinusoidal for a linear input voltage.

For the phase modulation, the action is performed on the term $(\pi V/V_\pi + V_{bias})$. So, even though the final output is sinusoidal, the phase changes linearly with the applied voltage, while the amplitude has a sinusoidal response.

The values of V_π and V_{bias} must be carefully controlled and adjusted, and in the absence of an active computer-controlled feedback, the experiments must be performed faster than possible (thermally induced) drifts.

7.3.1 Parameter evaluation

When the detection and the interferometer are balanced and the modulation is calibrated, the system can be used for parameter estimation. Let us look at relevant quantities, starting from Alice and following the optical design in figure 7.11.

From a general point of view the communication is performed by creating, sending and receiving states such as $|q + ip\rangle$, where q and p are random Gaussian distributed variables, with null mean value and a certain variance V_i, which changes while the state travels from Alice to Bob through the channel. For the parameter estimation we need to keep record of both the list of values (generated and measured) and their variances.

Alice generates q_A and p_A with a variance V_A. These data are produced by Alice, so they are well known. Then the state passes through the channel, defined by a transmission coefficient $T = t^2$, where t is related to amplitude of the signal.

Upon reception Bob measures q_B and p_B. If the channel acts symmetrically on them, their variance is V_B. The quantities q_B, p_B, V_B are directly measured, so they should be known. Nonetheless, in Bob's measurement many things are taken into

account, which we can divide in two categories: the noises, measured as variances, and the imperfection and losses of the detection system, which are adimensional coefficients. The noise variables are three: the local oscillator shot noise N_0, the electrical noise v_{el} and the excess noise ξ. The first two can be measured, while the third one is the central parameter of the estimation process.

7.3.1.1 Evaluation of the detection efficiency η

Beside the noise, losses and imperfections in the detection are:

- the coupling losses $\eta_{coupling}$;
- the photodetector efficiency, considered the same for the both of them, η_{PHD};
- the BS asymmetry coefficient ε, which can be translated into the BS reflection and transmission coefficients $r = \sqrt{\frac{1}{2} - \varepsilon}$ and $t = \sqrt{\frac{1}{2} + \varepsilon}$;
- the losses due to the detection balancing procedure, i.e. the attenuation effect of the VOA, η_{VOA}, because part of the light is attenuated before the photodiode and it does not contribute to the subtraction;
- the insertion loss of the BS, related to its transmissivity η_{BS}.

The evaluation of the overall η for the detected signal field goes through the quantum study of the beam splitter, considering every loss in the system as the interaction with a vacuum state, as it is schematically shown in figure A.1. The explicit calculation is presented in Appendix A and we report here only the final formula for η, and the experimental values of the various losses and efficiency coefficients, for the parameter evaluation.

From a direct classical measurement it is possible to evaluate the combined effect of $\eta_{coupling}$, η_{BS} and η_{PHD}: in fact when classical light is injected in one of the beam splitter inputs and nothing in the other one, the direct photocurrent measurement at the photodiodes is proportional to the attenuation due to coupling, beam splitter insertion loss and photodiode inefficiency. From the data in table 7.1 we see that injecting the light in one input or the other does not change the overall losses. Moreover we notice that, supposing the photodiodes have the same performances, the BS acts symmetrically for both inputs assuring a good detection behaviour and a good coupling system. The assumption of identical photodiodes has already been discussed in section 6.2, so the results in table 7.1 show that the BS acts symmetrically with respect to its two input channels. It is then reasonable to assume a general symmetry of the system.

The total amount of photocurrent at the output must be equal to the light injected and then attenuated by the coupling losses, the BS insertion loss and the photodiodes quantum efficiency, i.e.

$$P_1 + P_2 = \eta_{coupling}\eta_{BS}\eta_{PHD}P_{IN} \tag{7.2}$$

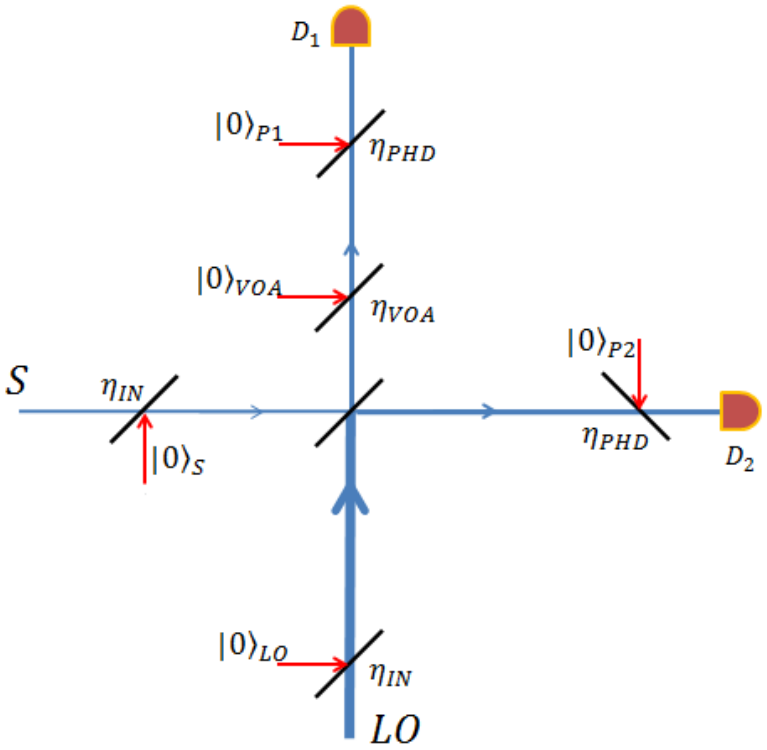


Figure 7.12: The scheme of a beam splitter with current losses in our system.

We know from section 7.1.5 that $\eta_{PHD} = 0.8$. Considering a BS insertion loss of 1dB, then $\eta_{BS} = 0.9$ and from the results in table 7.1 we can extract the coupling losses as $\eta_{coupling} = 0.0272$. The effective η is the variance of the part of the homodyne output corresponding to the interference between signal and local oscillator, normalized by all the contribution of the detection output (interferences between the vacuum states and the local oscillator). We can then deduce, following the results in Appendix A, that:

$$\eta = 0.017 \tag{7.3}$$

Input ch.	Input P	PHD1	PHD2	t/r
Top	$460\mu W$	$5.2\mu A$	$4.0\mu A$	56.6/43.4
Bottom	$460\mu W$	$4.0\mu A$	$5.2\mu A$	56.5/43.5

Table 7.1: Photocurrents measured injecting classical light alternatively into one of the two BS inputs and respective transmission-to-reflection ratio considering two identical photodiodes. Channels refer to the scheme of figure A.1.

7.3.2 Deviations from standard GG02

The GG02 protocol has been already discussed, theoretically in section 3.3 and from a more experimental point of view in section II. Nonetheless this particular on-chip/bulk hybrid implementation has its own constraints and procedures to be added in the protocol and to be taken into account when the parameters are evaluated. Besides the limitations due to the setup and the structure of the experiment, other restrictions have been removed to simplify the implementation of the protocol, without distorting the main protocol concept. In the following we present the reasons and consequences of these choices.

Alice's and Bob's remote control

As heritage of the all-in-one-chip solution exposed in the previous chapter, the experiment is still controlled by only one computer. This means that Alice and Bob are physically controlled by the same PC, and managed by the same software.

This allows us to not care about the synchronization of Bob's detection with the arriving pulses: in a separated communication this requires to use a small part of the received light (mostly the LO) as a trigger pulse for detection. Similarly, using a single PC implies that the classical communication channel does not exist. Again this is not critical as long as we are mostly interested in validating the optical part of the setup. The modifications induced by this choice to the theoretical protocol are listed below.

- Avoiding a classical data transfer, we are for the moment excluding the presence of actual eavesdropping.
- Correspondingly, the questions of synchronization or delay time are ignored (but we point out that they are not directly related to the QKD protocol itself).
- Alice's modulators calibration is performed using Bob's detection and Bob's phase tracking with respect to Alice's reference frame that is contained in Alice's modulators calibration itself. This consequence of using a single classical processing system simplifies the data analysis (meaning the control software). More importantly it also slightly affects the parameter estimation since we reduce two sources of error to one. In fact, if on Alice's side the calibration of the modulation would bring some noise, on Bob's side the phase tracking would have done the same.

As a last point, additional errors are associated with the use of two separated devices for phase control (Alice's modulation and Bob's tracking). On figure 2.6 it can be seen that Bob's phase tracking corresponds to measuring and cancelling the phase difference ϕ. One must however take appropriate measures to avoid phase ambiguity from a single projective measurement, since $\cos(\theta) = \cos(-\theta)$ for the x-axis projection and $\sin(\theta) = \sin(\pi - \theta)$ for the y-axis. This problem can be solved by using multiple test pulses in a "star" configuration, or by using a heterodyne detection, as discussed further in section 7.4.2.

In order to streamline the execution of the protocol in the current setup, Bob's phase choice for the measurement of the quadratures is actually performed by Alice's phase modulator. This task can be done without further loss of generality, by randomly adding a phase $\pi/2$ to Alice's, simulating Bob's choice. As said before, this is not changing the idea of the protocol, and reduces a bit more both the amount of noise of the measurement and the complexity of the control system.

Reduced number of input channels in the acquisition system

The current acquisition software manages only one flux of input data. We saw in section II that a complete protocol requires three inputs, one at Alice's and two at Bob's. For the moment only one input is available, and Alice and Bob are managed by the same PC, so the only input is used for the detection. On Bob's side the second input (triggering) is not necessary in the current configuration. The main role of Alice's input is to continuously check her own modulation for the state preparation. But Alice's modulation must also be calibrated, and this plays a central role in our study as we will see now.

The generation of the quantum states is based on a double Gaussian distribution of data for q and p, with a variance V_A . The value of V_A is used to evaluate V_N and consequently the excess noise ξ.

At Alice's we must differentiate two different kinds of variances. The first one is the variance of the random numbers produced by Alice's pseudo-random number generator, used to define the values of q and p. This variance is dimensionless and its scale corresponds to the one chosen for the random numbers; we call it $\bar{V}_A$.

The other variance is the measured one and it could be expressed in the natural units used for the measurements, that is in our case the square of a voltage $[V^2]$. However, consistently with the theory part, it is much more convenient to normalize it to shot-noise units (SNU), and this is the variance we call V_A. Since Alice has not access to a direct measurement of her states, she directly knows $\bar{V}_A$ but not V_A. Bob's measurement can be easily normalized to the SNL, and is directly related to V_A. It is therefore essential to calibrate the linear relation between them:

$$V_A = \alpha \bar{V}_A \tag{7.4}$$

where α is a dimensionless coefficient that relates one variance to the other.

7.3.3 Measuring α, ξ, and ρ

In light of the impossibility of a direct measurement of V_A, the evaluation of ξ requires the estimation of the α parameter. The relations we have seen in section 3.3.3 must be rewritten. The variances are expressed in SNU, but the values in the natural units could also be retrieved by changing the units of N_0.

The variance of Bob's measurements is now

$$V_B \;=\; G(\alpha \bar{V}_A \;+\; V_N) \tag{7.5}$$

or more explicitly

$$V_B \;=\; 1 + v_{el} + \eta T \left(\alpha \bar{V}_A \;+\; \xi\right), \tag{7.6}$$

where 1 corresponds to the shot noise level for the chosen intensity of the LO. In our setup the transmission of the channel is in principle $T = 1$, since the light exiting Alice's stage passes through a VOA which is (for now) not attenuating.

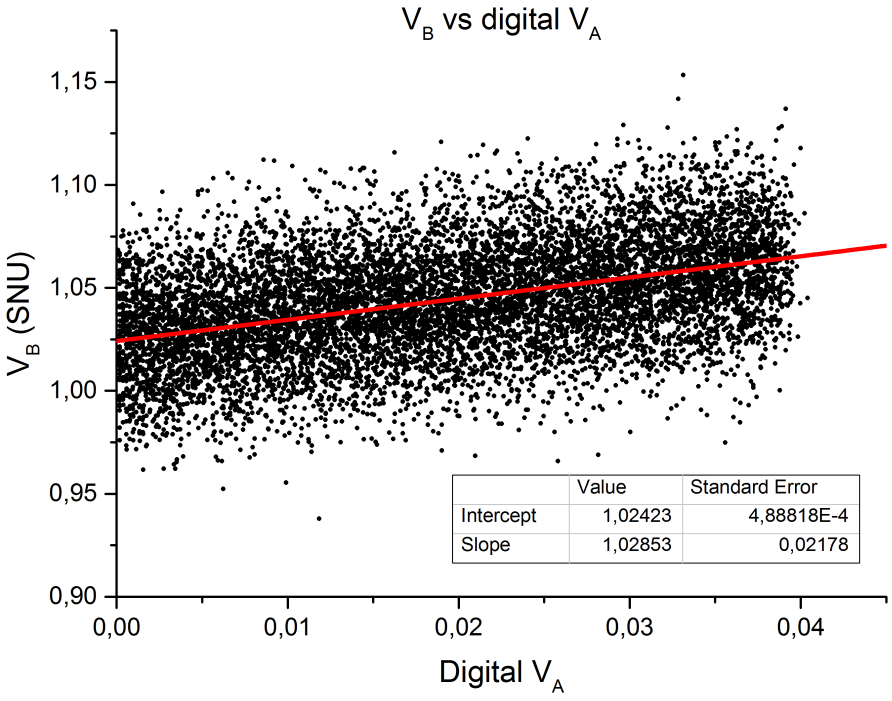


Figure 7.13: Normalized variance at Bob's versus the digital variance $\bar{V}_A$ generated by Alice.

We use the the linear fit $y = mx + k$ in figure 7.13 to find the value of α from the slope

$$m = \eta T \alpha \tag{7.7}$$

Since $T = 1$ by convention (no line loss), and η has been measured previously, we can retrieve the conversion factor $\alpha = 60.5$. This is an important parameter for relating Alice's and Bob's data: it allows to rescale Bob's data with the proper value of the generated variance at Alice's.

In this way figure 7.13 transforms to figure 7.14. The fit has been done by taking the average value every 90 points. The averaging procedure ensures that the noisy distribution of the points does not contain sub-structured behaviours, as we can see from the figure. Then the linear fit is taken again over the averaged and less noisy points to look for the intercept value.

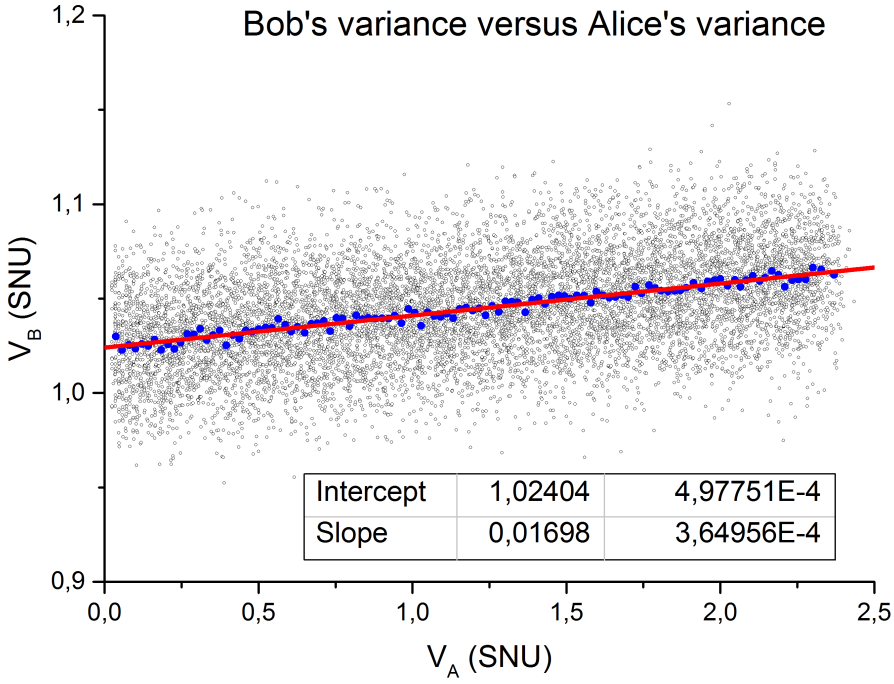


Figure 7.14: Normalized variance at Bob's versus Alice's generated variance in SNU.

As a first step we will determine the quantity

$$\Xi = \xi + \frac{v_{el}}{\eta T}, \tag{7.8}$$

which includes the transmission excess noise and the electronic noise together, and can be directly determined from the noise measurements. Evaluating ξ and v_{el} separately requires to do an independent measurement of v_{el}, which is not always possible during the communication; we will come back to this later.

From figure 7.14 the intercept point at $V_A = 0$ is $k \simeq 1.024 \pm 5\ 10^{-4}$, and one has from previous definitions (the shot noise level being normalized to 1):

$$k = 1 + v_{el} + \eta T \xi = 1 + \eta T \Xi \tag{7.9}$$

and consequently

$$\Xi = \frac{k-1}{\eta T} = 1.41 \pm 0.03 \tag{7.10}$$

During the experiment an independent measurement of v_{el} has also been performed, giving the result $v_{el}/\eta T = 1.41$. This tells that, within the precision of the measurements, all the excess noise Ξ may be attributed to the electronic noise, and $\xi = 0$. Given the non-negligible error bars, we will rather use a conservative estimate $\xi = 0.03$.

Another method of evaluation of the excess noise [4] is using the correlation ρ between Alice's and Bob's data, as defined in chapter 3, and related to the noise variances by

$$\rho^2 = \frac{V_A}{V_A + V_N} \tag{7.11}$$

Using equation 7.12, Ξ vs Alice's variance can be calculated to be:

$$\Xi = \frac{V_A}{\rho^2}\left(\frac{V_B - 1}{V_B} - \rho^2\right) \tag{7.12}$$

where it is again needed to rescale Alice's variance from the digital values to shot noise unis. The measured value of ρ as a function of V_A is plotted on figure 7.15.

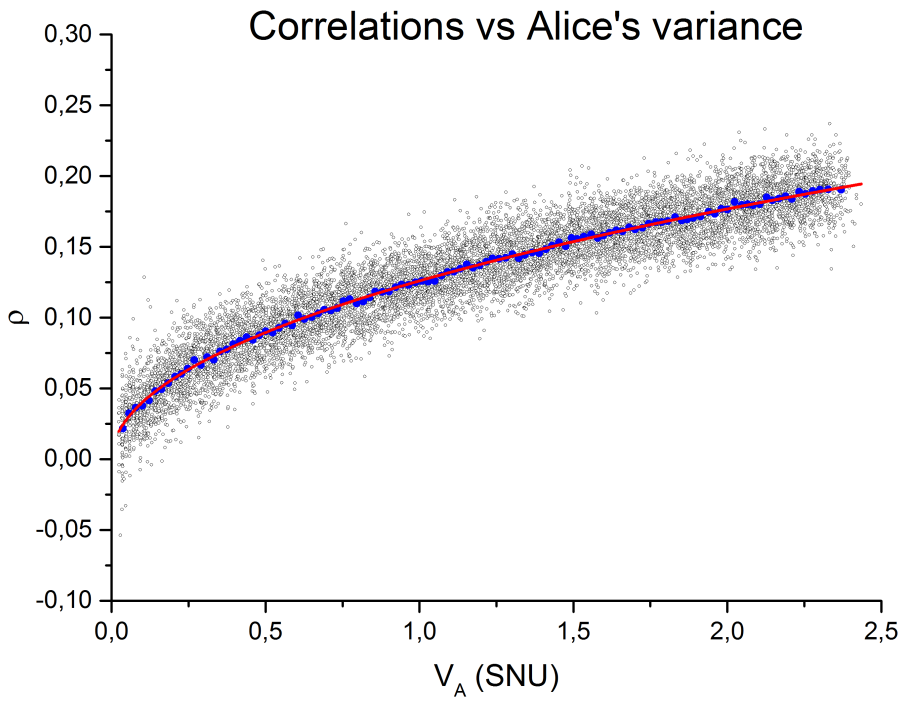


Figure 7.15: The correlations ρ versus Alice's generated variance in SNU.

On can then obtain Ξ as a function of V_A, plotted in figure 7.16

From a linear fit of this curve we are able to extract two pieces of information: the slope tells us whether the excess noise (or equivalently Ξ) depends on the variance generated by Alice, while the intercept value gives us the estimation of Ξ itself. Looking at the fit parameters we can say that the dependence on V_A is practically non-existent and that

$$\Xi = 1.49 \pm 0.03 \tag{7.13}$$

This leads to the alternative evaluation of the excess noise as

$$\xi = (1.49 \pm 0.03) - 1.41 = 0.08 \pm 0.03 \tag{7.14}$$

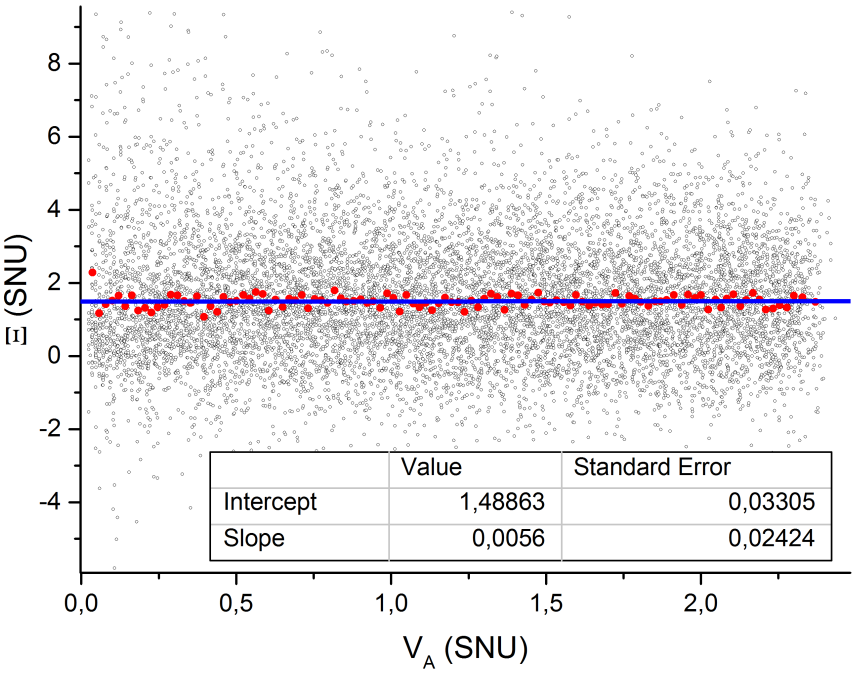


Figure 7.16: Ξ versus Alice's generated variance in SNU.

We have thus two different values of the excess noise ξ which are comparable within a few error nevertheless. The worst case scenario for both evaluations 7.12 and 7.14 gives us an estimated range of values for ξ:

$$0.03 \leq \xi \leq 0.12 \tag{7.15}$$

As it can be guessed this evaluation is not final: making it more precise would require larger blocks of data to improve the statistics, which in turn requires longer acquisition time, and therefore better stability of the experiment. In particular, thermal drifts of v_{el} have been observed, and have obviously strong unwanted effects, due to the subtraction needed to obtain ξ from Ξ.

7.3.4 Value of the secret key rate

At this point, having estimated all the parameters of the communication and the channel, we can extract the theoretical key rate of our version of the GG02 protocol.

We know that ξ represents the added noise to the communication. It can come from Eve's eavesdropping action and from the imperfections in the implementation. For secret key exchange, one always considers a worst case scenario where all the excess noise is attributed to Eve: this amounts to maximizing the information she can get in order to ensure security to Alice and Bob.

We also saw that collective attacks against CVQKD protocols are more general

than individual attacks, and general coherent attacks can be reduced to them as well. For this reason we calculate the key rate (in figures 7.17 and 7.18) under collective attacks supposing that the excess noise ξ is entirely due to Eve. Therefore we use Holevo's formula in realistic mode (more details are given in appendix C).

In both figures the key rate is expressed in terms of how many secret bits we can extract from a single utilisation of the channel, i.e. for each pulse we send. The choice of this unit has been made because it gives a better and more general idea of the quality and efficiency of the communication, since the bits/channel use is independent of the experimental setup speed. The key rate in the usual units (bits/s) is simply retrieved by multiplying the bits/channel use by the repetition rate of the setup, which is 0.5 10^6 pulses/s in our case.

The x-axis reproduces the losses in the channel. This choice, as for the bits/channel use, has been made to provide general information on the protocol implementation. In fact for fixed attenuation over the channel, the communication can be achieved over different distances, depending on the properties of the channel. A typical value is 0.2 dB/km for telecom optical fibers.

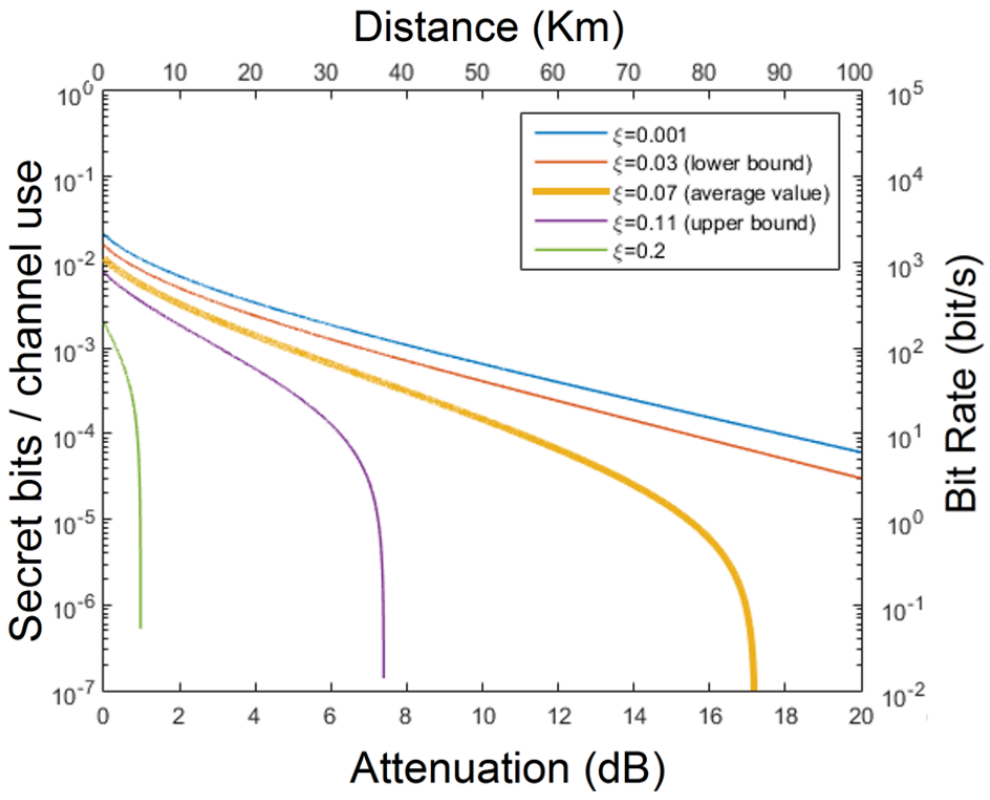


Figure 7.17: Key rate in terms of bit/pulse and bit/sec vs. the losses in the channel. The distance that the communication can reach is evaluated for standard fibers connection (0.2 dB/km). The different curves are taken for different ξ values, while η is fixed. $\beta = 0.95$ for general LDPC codes under collective attacks.

In figure 7.17, η is fixed to our experimental value and the evolution of the key rate is studied with respect to the excess noise, for a variance at Alice's $V_A = 2$.

We can see that for our current range of excess noise values ($\xi = 0.03$ to 0.12) we can extract a secret key for acceptable loss in the channel.

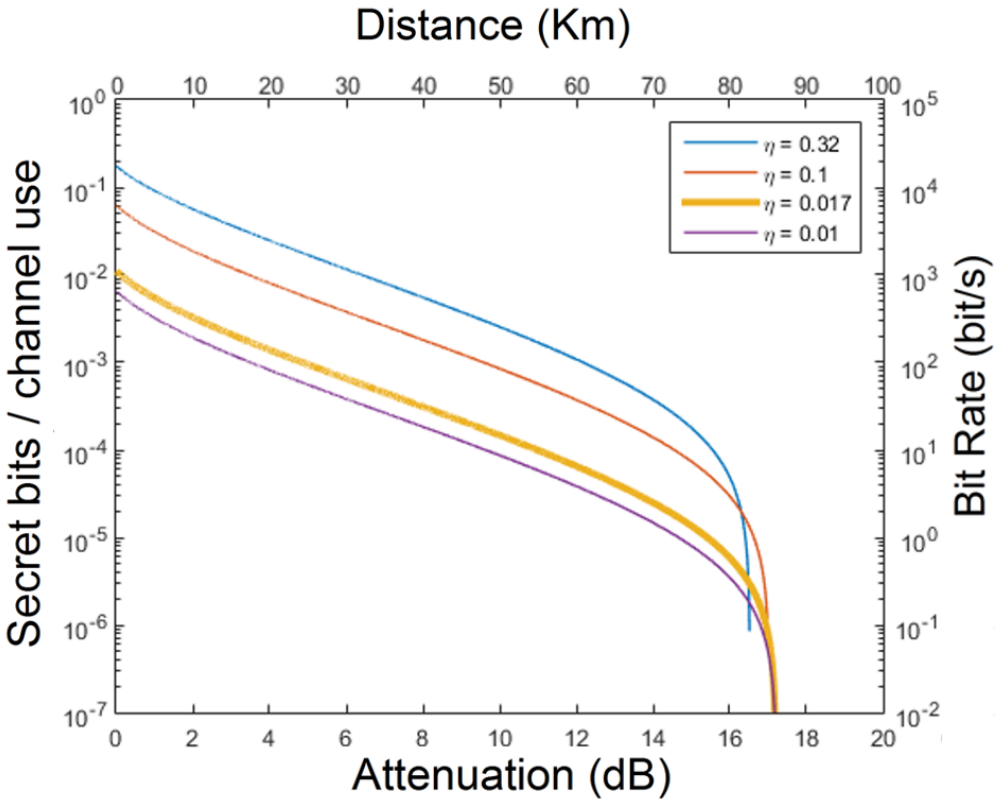


Figure 7.18: Key rate in terms of bit/pulse and bit/sec vs. the losses in the channel. The distance that the communication can reach is evaluated for standard fibers connection (0.2 dB/km). The different curves are taken for different η values, while ξ is fixed. $\beta = 0.95$ for general LDPC codes under collective attacks.

Figure 7.18 studies the behaviour of the key rate when ξ is fixed. The chosen value is $\xi = 0.07$, in the middle of the range we previously found (see equation 7.15). The value of η is changing from very low up to $\eta = 0.32$, corresponding to a better coupling condition (see Appendix A). We can see that for a fixed excess noise the variation of the detection efficiency does not affect the key rate too much.

In order to avoid misinterpretations about the roles of η and ξ, let us remind again that one of the main reasons for which the current ξ is too large is that η is too small. Since ξ is referred to the input, an improvement of one order of magnitude for η (10 times larger) would give an improvement of one order of magnitude for ξ (10 times smaller). This could be possible by decreasing the fiber coupling losses, which are, for technical reasons, ~ 12 dB larger than they should be.

7.3.5 Conclusion

The work carried out until now with the separated homodyne detection has shown that communication is possible, but we are still limited by technological barriers.

The main performance difference with the bulk setup arises from the value of η: in previous works (see [43, 44, 48]) long distance communication has been achieved with detection efficiency values more than 30 times greater ($\eta \simeq 0.6$) than the current value for the integrated configuration ($\eta = 0.017$). The missing 15dB mainly come from the coupling losses. In particular, two factors are playing a crucial role. First, the fiber array used for fiber attaching was designed for air coupling, with special reference to the OpSIS chip architecture: it follows that fiber attaching cannot be optimally performed. Moreover the wire bonding, in particular the protective resin poured on the wires, does not allow the fiber array to get to the optimal approaching distance, since the grating couplers are too close (in this architecture) to the electrical connection. In fact the second generation was designed before having realized the need of both wire bonding and fiber attaching.

Nonetheless the detection is linear over a large local oscillator power range, allowing the system to have ~ 20 dB of dynamic range in terms of output variance, as shown in the SNL slope in figure 7.10.

The measured excess noise, and consequently the extracted key rate, suffer from two critical conditions: the very low η value (as just said) and the imperfect modulator calibration. From the calibration of the modulators, especially the amplitude one (AM), we obtain the maximal attenuation condition, which has unwanted consequences on both the real-time measurement of N_0 and the correct centering of the Gaussian distributions (for q and p) in the phase space.

Without any doubt to increase the quality of the key rate more data are needed as well as a live control on the electronic noise.

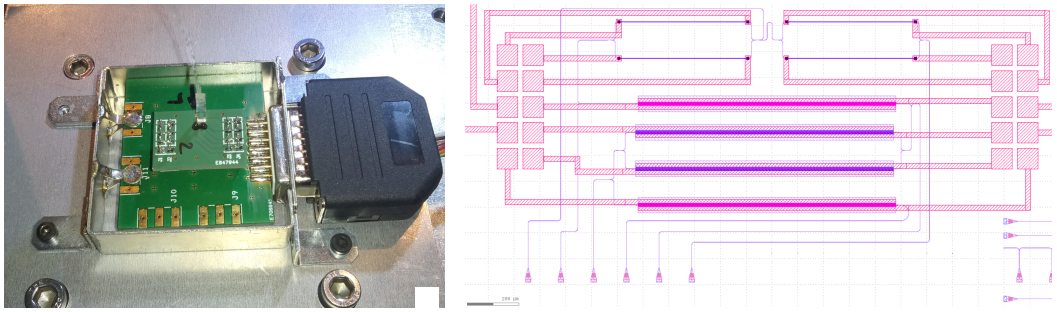
New measurements are already running to optimize the AM calibration so that the excess noise and the theoretical key rate could be improved. In parallel new devices for coupling are about to be manufactured, to increase the value of the detection efficiency.

7.4 Work in progress

7.4.1 Alice's modulation chip

To complete the study of the integrated QKD protocol, Alice must also be implemented on a chip. The chip, shown in figure 7.19a), has already been designed and it is fully packaged, electrically (wire bonded) and optically (fiber attached). As we saw in chapter 6 a complete homodyne detection calibration is needed first.

In figure 7.19b we can see the optical scheme of the Alice's chip. All the six grating couplers are used (we can number them from 1 to 6 going from left to right). The third coupler is the injection one. Light is then split into two by a 50:50 BS (every MMI coupler is 50:50 in this chip). The lower part corresponds to the local oscillator path, and it is injected from the fourth coupler. We can notice that in the local oscillator path there is a PIPIN phase modulator, which corresponds to Bob's $0/\pi$ phase shifter. The choice to put it in Alice's chip instead of in Bob's one, has been made to maximally simplify the detection circuit, so that the detection calibration is performed in the simplest conditions.



(a) The packaged modulation chip for Alice.

(b) The optical scheme of the chip

Figure 7.19: Alice's modulation chip.

GC number	1	2	3	4	5	6
Task	VOA1 out	PMod out	Light in	LO out	AMod out	Signal

Table 7.2: Alice's chip grating couplers purpose, numbered from left to right following figure 7.19b.

The other half of the light goes in the signal side of the chip. A PIPIN MZI first performs the amplitude modulation. Light is then phase modulated by a PIPIN shifter and the pulse can be measured from the light coming from grating coupler 2. The attenuation process is carried out by two thermal MZIs. It is important to highlight that after each device a BS takes part of the light out of the line so that it can be extracted via a grating coupler and properly measured. This allows us, in principle, to evaluate and test the in-line behaviour of each component separately, since we have access to the actual pulse at each stage and not to just a photocurrent, hence interferometric measurements are also possible. This means that Alice is able to perform autonomous calibration of her devices.

Table 7.2 shows what the grating couplers correspond to.

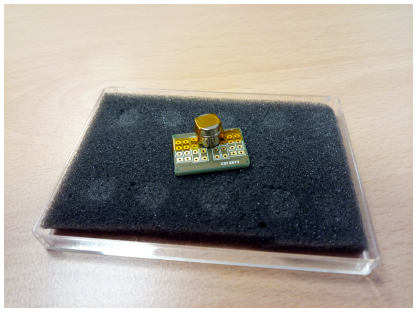
7.4.2 Bob 2.0: the Heterodyne detection

The next improvement will be the introduction of the *double homodyne detection* or *heterodyne detection*. The protocol shown in chapter 3 is based on the single homodyne detection: Bob randomly chooses to measure either Q or P. In principle, if both signal and local oscillator are split in two, they can be recombined in two different measurement sets and both Q *AND* P can be measured at the same time. In fact if one detection is shifted by $\pi/2$ with respect to the other, we obtain a point in the Bob's referenced phase-space, without needing a variable phase shifter to choose one quadrature. With a few calibration pulses it would be possible to evaluate the phase difference between Alice's and Bob's reference frames and consequently add the reverse rotation to Bob's data.

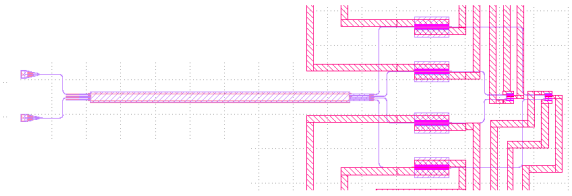
On the other hand, the noise affecting each measurement, in particular the SNR, will be greater than the one affecting a single measurement, since the amount of signal we measure is half, while the quantum noise is still the same.

From a technical point of view a double detection needs a double amplification system and a new PCB support to adapt the needs to a larger number of photodiodes and attenuators.

The chip is shown in figure 7.20, where we can see its picture and its optical scheme.



(a) The heterodyne detection (Bob 2.0), not packaged



(b) The heterodyne detection chip's optical scheme

Figure 7.20: Bob's heterodyne detection chip.

Part III

Conclusion

This work has been performed at the *Laboratoire Charles Fabry (LCF)*, in collaboration with the *Laboratoire d'Informatique de Paris 6 (LIP6)*, and the *Centre de Nanosciences et Nanotechnologies (C2N)*, whose different expertise have brought the cooperation at a very multidisciplinary and stimulating level.

The new frontier of integrating Continuous Variable systems for quantum cryptography on silicon photonics circuits has been addressed. The main objective of this work was to evaluate the feasibility of this process using standard silicon photonics at telecom wavelength, and eventually obtain on-chip real communication and key exchange. The project, from both an experimental and a theoretical point of view, evolved in time while evaluating the actual differences between the bulk and the integrated setup, and exploiting the advantages of the chip configuration to overcome the limitations due to the miniaturization.

From the work carried out during three years it arises that the technological challenge mostly relies in the architecture of the chip and in the quality of the photodiodes. The criticality of the photonic circuit design becomes evident when one realizes that standard techniques are not stable enough, producing sources of noise too big with respect to the quantum noise, which should be the main contribution to the total communication noise. Regarding the photodiodes, we can see in figure 7.21 that the ability to endure high optical intensities maintaining a linear response allowing a dynamic range greater than 10dB in terms of detection variance is not as straightforward as it is for standard bulk InGaAs fibered photodetectors. The Germanium based integrated photodiodes, which have a very small active surface and capacitance, need specific geometries to manifest such a linear response.

In particular the work on the all-in-one chip configuration demonstrates that the interaction of the two (local oscillator and signal) pulses does not allow the detection calibration, so one must be able to inject them independently inside the detection. In fact, since the detection balancing is a prerequisite for the modulators calibration, it must be performed at best and the modulators should not be used for detection balancing purposes as they are not calibrated. Even though one can find an iterative procedure for both detection and modulators calibration, this is too computationally heavy and quite long to be introduced in real time communication. However, the imperfections found in this configuration helped to conceive and design a better photonic circuit for the second generation.

The chip designed by Mélissa Ziebell (C2N) and manufactured in LETI (Grenoble) allowed us to separate Alice from Bob, and the state creation from the detection. Since a balanced detection is the starting point for communication, the work has proceeded towards a first testing stage with hybrid configuration, with only Bob's chip as the integrated part and the modulation left in "bulk".

The calibration can be easily performed by injecting only the local oscillator in the detection, allowing us to reach an output variance dynamic range of $\simeq 18dB$.

The latest results about the communication parameters (excess noise and key rate), which are getting increasingly better with our ongoing experiments, show that for very poor values of the detection efficiency η a key can be exchanged for a short range. We remark that η highly depends on the coupling losses into the chip, which are currently particularly high due to a purely technical problem, and can be

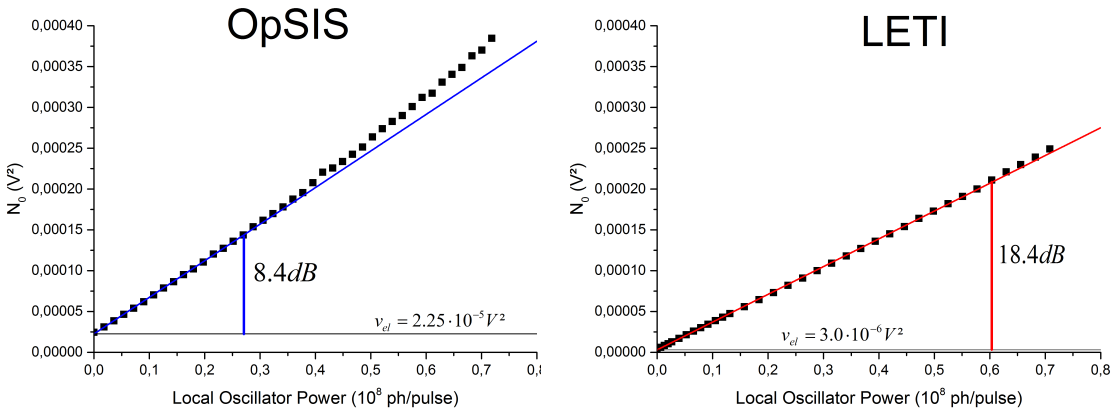


Figure 7.21: SNL comparison between the two chip designs: OpSIS (left) vs LETI (right).

in principle easily improved.

The use of the Alice's modulation chip that is now ready for testing will open the door to the complete integration of the protocol implementation. Even though the modulator calibration is now computer controlled, we expect that the new devices may feature different behaviors in terms of chirp. Moreover every active component induces both phase and amplitude modulation, a fact that must be carefully taken into account for the calibration process.

Another further improvement is to evolve the detection from a single homodyne detection (measuring one quadrature of the signal) to a heterodyne one. This will allow us to measure both quadratures at the same time, which will simplify the protocol implementation by removing Bob's modulator, whose calibration and utilisation naturally induce errors. Furthermore, this would additionally be in line with the most recent security proofs for CVQKD.

In conclusion, we have successfully demonstrated homodyne detection displaying quantum-limited behavior on a silicon photonics circuit and have additionally used it for obtaining correlations in a real CVQKD communication scenario compatible with positive secret key generation rate at moderate losses. With further anticipated improvements in our experiments, Alice's modulation chip ready to be tested for fully integrated CVQKD, and a heterodyne detection support in the pipeline for improving the quality of the protocol implementation, we may conclude that silicon photonics is a promising platform for cost-effective quantum cryptographic applications.

Part IV

Appendices

Appendix A

Quantum model of the detection and η evaluation

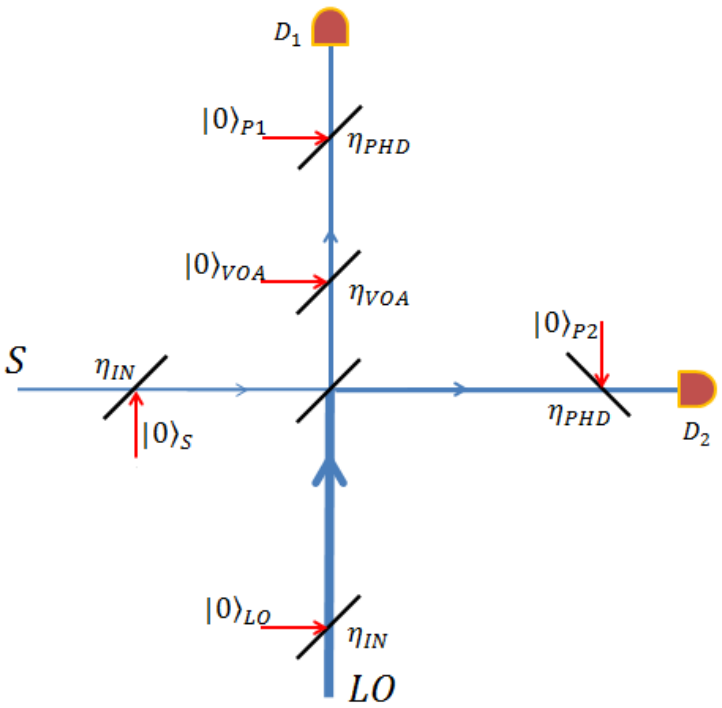


Figure A.1: Model of the detection

The model of the detection which has been used in this work is shown in figure A.1. For the evaluation of ξ and consequently of the key rate, the parameter η must be properly calculated using the quantum model for each source of losses and the quantum operators for the electromagnetic fields interacting in the detection. This quantum modeling of losses considers a loss $\star\eta$ as the interaction via BS with a vacuum source: the vacuum field is injected in the line externally with a weight $(1 - \star\eta)$.

Appendix A. Quantum model of the detection and η evaluation

The variables playing a role in the model are:

- t and r the transmission and reflection coefficients, with $t > r$;
- $\eta_{IN} = \eta_{BS}\eta_{coupling}$ the losses due to the coupling and to the intrinsic beam splitter's insertion loss. They are measured to be equal on both the local oscillator and the signal arm;
- η_{VOA} the suppression on one output arm of the BS for detection balancing;
- η_{PHD} the quantum efficiency of the two photodetectors, supposed to be identical;
- $\hat{a}_{LO}$ the local oscillator's field operator;
- $\hat{a}_s$ the signal's field operator;
- $\hat{a}_{0,LO}$ the vacuum's field operator injected in the local oscillator arm because of η_{IN};
- $\hat{a}_{0,s}$ the vacuum's field operator injected in the signal arm because of η_{IN};
- $\hat{a}_{0,VOA}$ the vacuum's field operator injected in the BS's output 1 because of η_{sup};
- $\hat{a}_{0,P1}$ the vacuum's field operator injected in the BS's output 1 because of η_{PHD} of photodiode 1;
- $\hat{a}_{0,P2}$ the vacuum's field operator injected in the BS's output 2 because of η_{PHD} of photodiode 2.

The field entering the BS from above is:

$$\sqrt{\eta_{IN}}\hat{a}_s + \sqrt{1-\eta_{IN}}\hat{a}_{0,s} \tag{A.1}$$

The field entering the BS from the left is

$$\sqrt{\eta_{IN}}\hat{a}_{LO} + \sqrt{1-\eta_{IN}}\hat{a}_{0,LO} \tag{A.2}$$

After the BS, on the output of photodiode 1, the field is the sum of the transmission of the left input and the reflection of the upper input:

$$\begin{aligned}\hat{a}_{1,BS} &= t(\sqrt{\eta_{IN}}\hat{a}_{LO} + \sqrt{1-\eta_{IN}}\hat{a}_{0,LO}) + r(\sqrt{\eta_{IN}}\hat{a}_s + \sqrt{1-\eta_{IN}}\hat{a}_{0,s}) = \\ &= \sqrt{\eta_{IN}}(t\hat{a}_{LO} + r\hat{a}_s) + \sqrt{1-\eta_{IN}}(t\hat{a}_{0,LO} + r\hat{a}_{0,s})\end{aligned} \tag{A.3}$$

After the BS the suppression is performed to balance the LO intensity on the two arms: the resulting field is

$$\hat{a}_{1,VOA} = \sqrt{\eta_{sup}}\hat{a}_{1,BS} + \sqrt{1-\eta_{sup}}\hat{a}_{0,sup} \tag{A.4}$$

Finally the not perfect quantum efficiency induces losses as well, introducing the vacuum field $\hat{a}_{0,P1}$:

$$\hat{a}_1 = \sqrt{1-\eta_{PHD}}\hat{a}_{0,P1} + \sqrt{\eta_{PHD}}\hat{a}_{1,VOA} \tag{A.5}$$

which we can also write explicitly as

$$\begin{aligned} a_1 \; =& \sqrt{1-\eta_{PHD}}\hat{a_{0,P1}} \; + \; \sqrt{\eta_{PHD}}\left\{\sqrt{1-\eta_{VOA}}\hat{a_{0,VOA}} \; + \; \sqrt{\eta_{VOA}}\,[\sqrt{\eta_{IN}}(t\hat{a}_{LO} + r\hat{a}_s) + \right. \\ & \left. + \; \sqrt{1-\eta_{IN}}(t\hat{a}_{0,LO} + r\hat{a}_{0,s})\right]\Big\} \end{aligned} \tag{A.6}$$

On the photodiode 2 arm, similarly we have after the BS the reflection of the left input and the transmission of the upper one, remembering to insert the π relative phase shift between them:

$$\begin{aligned} a_{2,BS} \; =& t(\sqrt{\eta_{IN}}\hat{a}_{LO} + \sqrt{1-\eta_{IN}}\hat{a}_{0,LO}) - r(\sqrt{\eta_{IN}}\hat{a}_s + \sqrt{1-\eta_{IN}}\hat{a}_{0,s}) = \\ =& \sqrt{\eta_{IN}}(t\hat{a}_{LO} - r\hat{a}_s) + \sqrt{1-\eta_{IN}}(t\hat{a}_{0,LO} - r\hat{a}_{0,s}) \end{aligned} \tag{A.7}$$

In this case the VOA doesn't work, so the beam arrives directly on the photodiode, and we can write explicitly:

$$\hat{a}_2 \; = \; \sqrt{1-\eta_{PHD}}\hat{a_{0,P2}} \; + \; \sqrt{\eta_{PHD}}\left[\sqrt{\eta_{IN}}(t\hat{a}_{LO} - r\hat{a}_s) \; + \; \sqrt{1-\eta_{IN}}(t\hat{a}_{0,LO} - r\hat{a}_{0,s})\right] \tag{A.8}$$

The photocurrents are obtained by calculating the number operator of the two fields $\hat{a}_1$ and $\hat{a}_2$, where the number operator of a field operator $\hat{a}$ is $n = \hat{a}^\dagger\hat{a}$ (see section 2.1.1).

In this calculation only the terms which are at least proportional to the local oscillator field operator (or to its hermitian) survive. In fact the amplitudes of the other fields (the signal and all the different vacuum ones) are so small that they cannot be detected if not by an interaction with the local oscillator, which is grater by many orders of magnitude.

Remembering the relations obtained in section 2.2 we find for the values of the two photocurrents. In the photodetector 1:

Appendix A. Quantum model of the detection and η evaluation

$$\begin{aligned} I_1 =&\eta_{PHD}\ \Big\{\eta_{VOA}\Big[\eta_{IN}(t^2 I_{LO}+r^2 I_s+rt\sqrt{I_{LO}}Q_s)+ \\ &+\sqrt{\eta_{IN}(1-\eta_{IN})}\sqrt{I_{LO}}(t^2 Q_{0,LO}+rtQ_{0,s})\Big]+\sqrt{\eta_{IN}\eta_{VOA}(1-\eta_{VOA})}\sqrt{I_{LO}}tQ_{0,VOA}\Big\}+ \\ &\sqrt{\eta_{PHD}(1-\eta_{PHD})\eta_{IN}\eta_{VOA}}\sqrt{I_{LO}}tQ_{0,P1} \end{aligned} \tag{A.9}$$

and in the photodetector 2:

$$\begin{aligned} I_2 =&\eta_{PHD}\ \Big[\eta_{IN}(r^2 I_{LO}+t^2 I_s-rt\sqrt{I_{LO}}Q_s)+\sqrt{\eta_{IN}(1-\eta_{IN})}\sqrt{I_{LO}}(r^2 Q_{0,LO}-rtQ_{0,s})\Big]+ \\ &+\sqrt{\eta_{PHD}(1-\eta_{PHD})\eta_{IN}}\sqrt{I_{LO}}rQ_{0,P2} \end{aligned} \tag{A.10}$$

The difference between the two photocurrents is the output of the detection. The local oscillator is canceled by the balancing condition $t^2\eta_{VOA}=r^2$ imposed by the VOA. The same relation cancels the contribution of the vacuum field coming from the local oscillator input. The final result is

$$\begin{aligned} \Delta I &= I_1 - I_2 = \\ &= \eta_{PHD}\,\eta_{IN}\,\sqrt{I_{LO}}\,(1+\eta_{VOA})\,rt\,Q_s\ + \\ &+\ \eta_{PHD}\,\sqrt{\eta_{IN}(1-\eta_{IN})}\,\sqrt{I_{LO}}\,(1+\eta_{VOA})\,rt\,Q_{0,s}\ + \\ &+\ \eta_{PHD}\,\sqrt{\eta_{IN}\eta_{VOA}(1-\eta_{VOA})}\,\sqrt{I_{LO}}\,t\,Q_{0,VOA}\ + \\ &+\ \sqrt{\eta_{IN}\eta_{PHD}(1-\eta_{PHD})}\,\sqrt{I_{LO}}\,(t\eta_{VOA}Q_{0,P1}\ -\ rQ_{0,P2}) \end{aligned} \tag{A.11}$$

The effective η that must be used in the calculation of the communication parameters is the variance of the photocurrent terms corresponding to the signal Q_s normalized with the sum of the variances of all the terms assumed to be Gaussian distributed and independent one from another.

It can be noticed that every term is proportional to $\sqrt{I_{LO}}$, so every variance will be proportional to I_{LO}. When the normalization is performed this proportionality is canceled, so it's more practical to directly write the variances neglecting the local oscillator intensity factor. The variances of these terms are simply their squares,

since they are supposed to be Gaussian. It follows that:

$$
\begin{aligned}
V_s &= \eta_{PHD}^2\, \eta_{IN}^2\, (1+\eta_{VOA})^2\, r^2 t^2 && \text{(A.12a)}\\
V_{0,s} &= \eta_{PHD}^2\, \eta_{IN}\, (1-\eta_{IN})\, (1+\eta_{VOA})^2\, r^2 t^2 && \text{(A.12b)}\\
V_{0,VOA} &= \eta_{PHD}^2\, \eta_{IN}\, \eta_{VOA}\, (1-\eta_{VOA})\, t^2 && \text{(A.12c)}\\
V_{0,P1} &= \eta_{IN}\, \eta_{PHD}\, (1-\eta_{PHD})\, t^2\, \eta_{VOA} && \text{(A.12d)}\\
V_{0,P2} &= \eta_{IN}\, \eta_{PHD}\, (1-\eta_{PHD})\, r^2 && \text{(A.12e)}\\
& && \text{(A.12f)}
\end{aligned}
$$

Since $t^2\, \eta_{VOA} = r^2$, we have that $V_{0,P1} = V_{0,P2} = V_{0,P}$.

Now we can use our experimental results evaluate this contributions. From the fiber attaching process we know that $r^2 = 0.434$, $t^2 = 0.566$ and the product $\eta_{coupling}\eta_{PHD}\eta_{BS} \simeq 0.0195$. From the ratio t^2/r^2 we estimate $\eta_{VOA} \simeq 0.767$. The photodiodes have responsivity $R = 1A/W$, so the quantum efficiency is $\eta_{PHD} \simeq 0.8$.

Finally the effective η is

$$\eta \;=\; \frac{V_s}{V_s \,+\, V_{0,s} \,+\, V_{0,VOA} \,+\, 2V_{0,P}} \;=\; 0.017 \qquad \text{(A.13)}$$

This very low value is mostly limited by the input coupling efficiency $\eta_{coupling} = 0.0272$, and for a more acceptable $\eta_{coupling} = 0.5$ one would get $\eta = 0.32$.

Appendix B

Acquisition card (PCI and USB)

As mentioned in the previous section, the chip is very sensitive to electrical noise. This is due to the interaction between all the components of the electrical chain. A crucial role is played by the remote control acquisition card.

The acquisition card plays on apparently different grounds: the noise added to the chain, the signal filtering, the bandwidth, the sampling frequency. Every aspect is connected to the other, so at the end the choice will be put upon the device that gives the best trade-off. The aim of the chapter is to expose the pros and cons of the two tested systems and explain the reasons that led us to the final choice.

Since the software has been originally developed for NI (National Instruments) drivers, two NI cards have been used for both dynamic and static control: a NI PCI6110 card and more recently a NI USB3636 card.

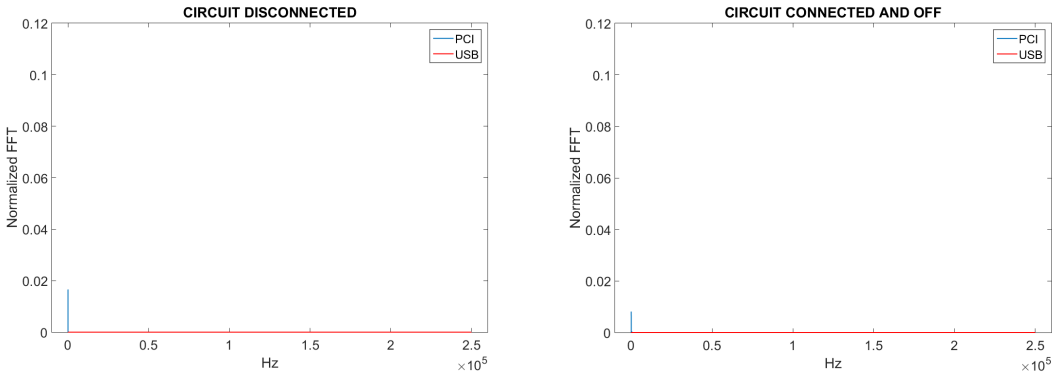
B.0.2.1 FT study of the noise

The inherited system was apparently well functioning with the new integrated chip, even if it was designed for a bulk and more noise resistant configuration. The FT studies had been performed in the past years giving no interesting results. The on-chip measurement showed the presence of periodical structures of unclear origin, giving the input for a more thorough Fourier analysis.

For the study to be complete one must separate the contribution of each elements in the electrical acquisition chain, that is composed by the block PC+acquisition card, the detection's electronics circuit, its power supply and the reaction to light injection. At each step, the presence of a different card has different impacts to the global noise.

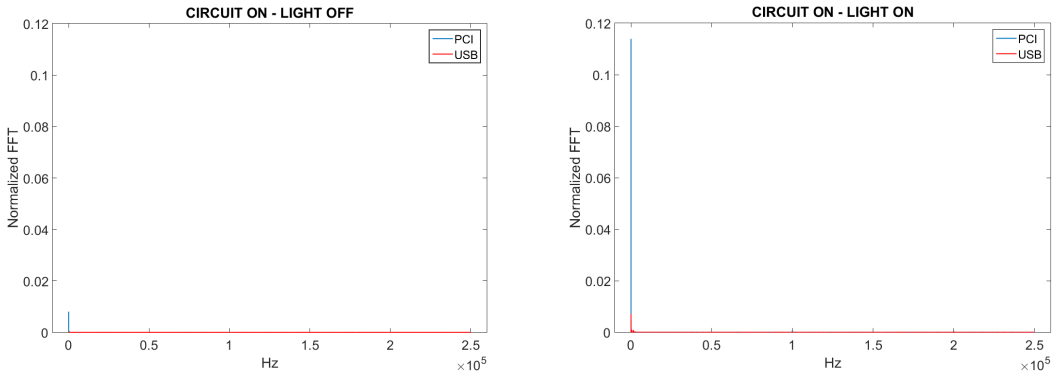
At first we can have a look at the comparison of the frequency distribution of the noise for the all the four situations in figure B.1, where all the pictures have the same scale. In this way is highlighted how the injection of the light induces a bigger noise. In every FT figure both the PCI's (blue) and the USB's (red) noises are plotted and superposed, to properly compare them. The contrast will be exposed addressing different frequency ranges.

Trigger and acquisition cards noise



(a) Card only

(b) Card + circuit (off)



(c) Card + circuit (on)

(d) Card + circuit (on) + light

Figure B.1: FFT: frequency range 0-250 kHz

The analysis of the noise of the acquisition cards is performed by simply connecting the trigger to the card and running the experiment. Even though we could use an internal clock to drive the acquisition, it is useful to analyze the noise employing the actual working configuration. At this stage the USB noise is more than an order of magnitude smaller than the PCI one. Even if the PCI is noisier, its contributions to the noise are very small ($\sim 0.5 \cdot 10^{-4} V$) but we can still glimpse some feature that will appear more intensively later. What we see is

- a frequency comb of exactly $\Delta f = 60 Hz$;
- a frequency comb of about $\Delta f = 997.4 Hz$ strongly decreasing after 10kHz;
- $f_0 = 50 Hz$ and some of its harmonics up to 500Hz

Connecting the amplification circuit (switched off)

Connecting a circuit brings noise even if it is switched off. In fact the electrical chain is modified, new passive and active elements play a role. The USB card does not suffer this passage, remaining at a very low noise level. The PCI card gains the little contributions ($\sim 5 \cdot 10^{-4} V$) of the power line hum ($f_0 = 50 Hz$) and its third harmonic ($3 f_0 = 150 Hz$).

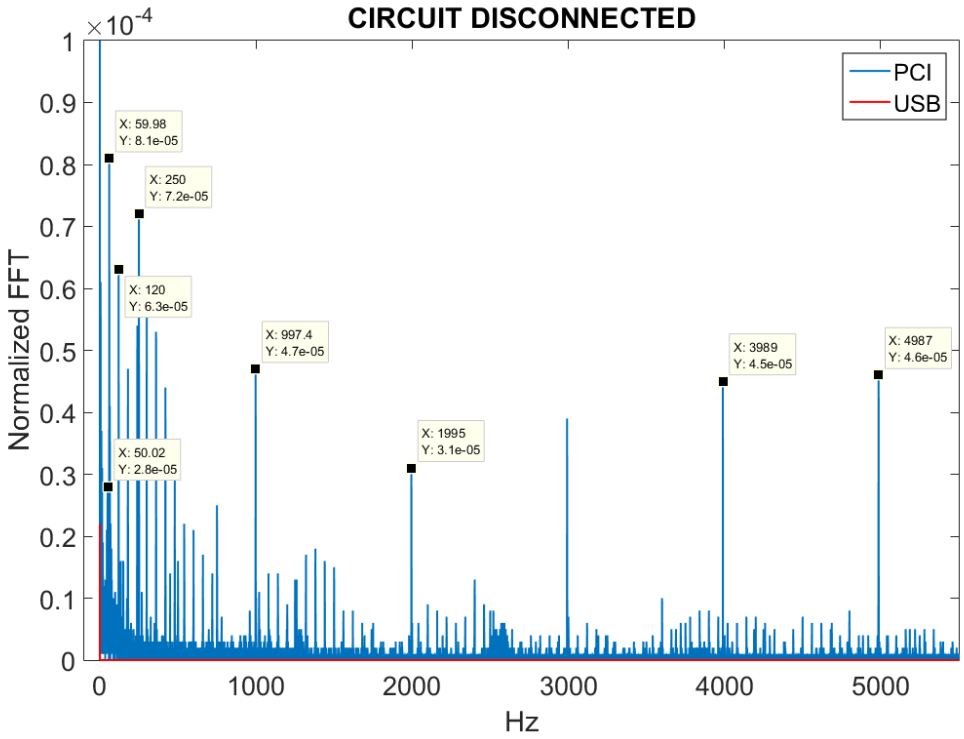


Figure B.2: Noise of the card

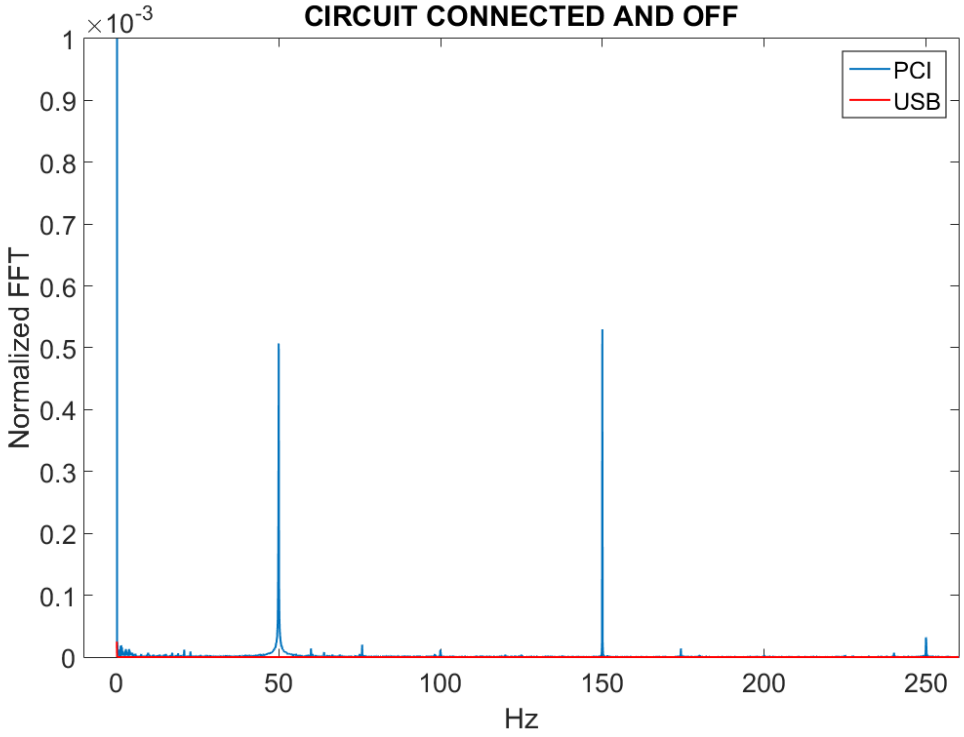


Figure B.3: Card + circuit (off)

Switching on the amplification circuit

When we turn on the power supply of the amplification system, the USB noise

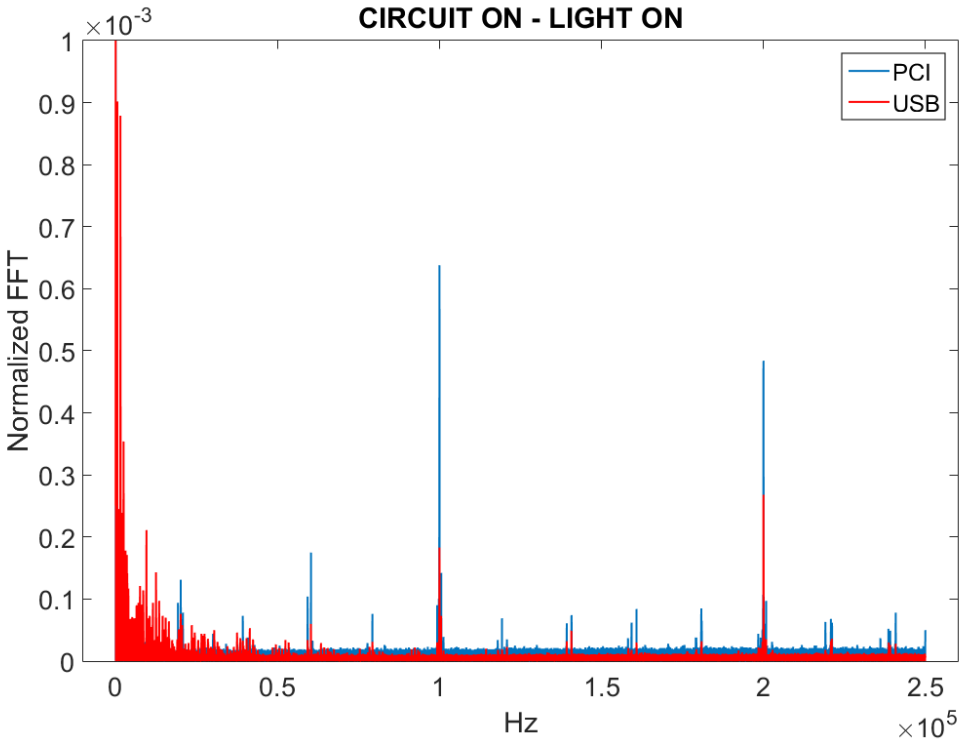


Figure B.4: FT noise analysis in working conditions (1): high frequencies

rises significantly, becoming comparable to the PCI one, but still smaller. A small contribution at the frequency $\simeq 7.5Hz$ appears: it corresponds to the length of a transferred block of data, i.e. is the characteristic time of the communication due to the buffer created by the software to manage the stream of data. The size of a block was $2^{16} = 65536$ at the moment of the measurement (it can be modified). Since the frequency of the communication is 500kHz, we find $f_{buffer}\frac{5\cdot10^5 Hz}{65536} = 7.63Hz$; This is still negligible. More details about the structure of the communication are given in section II.

Coupling the light in the system

Feeding the system at work with the local oscillator light increases the noise, especially regarding the USB card. Its noise at low frequency becomes now very important, rising by a order of magnitude. We can identify the following contributions:

- the bigger one at $f_1 = 62Hz$ ($\sim 1.4 \cdot 10^{-3}$) for both cards (figure B.8).
- f_{buffer} and its third harmonic have gained one order of magnitude and are now comparable to f_1 (figure B.7).
- the contribution of $f_0 = 50Hz$ and $3f_0$ have not changed, as expected, since they are due the main power supply line (figure B.7).
- Two strong PCI contributions at very high frequency $f_{high} = 100kHz$ and $2f_{high} = 200kHz$ (figure B.4), comparable with f_0.

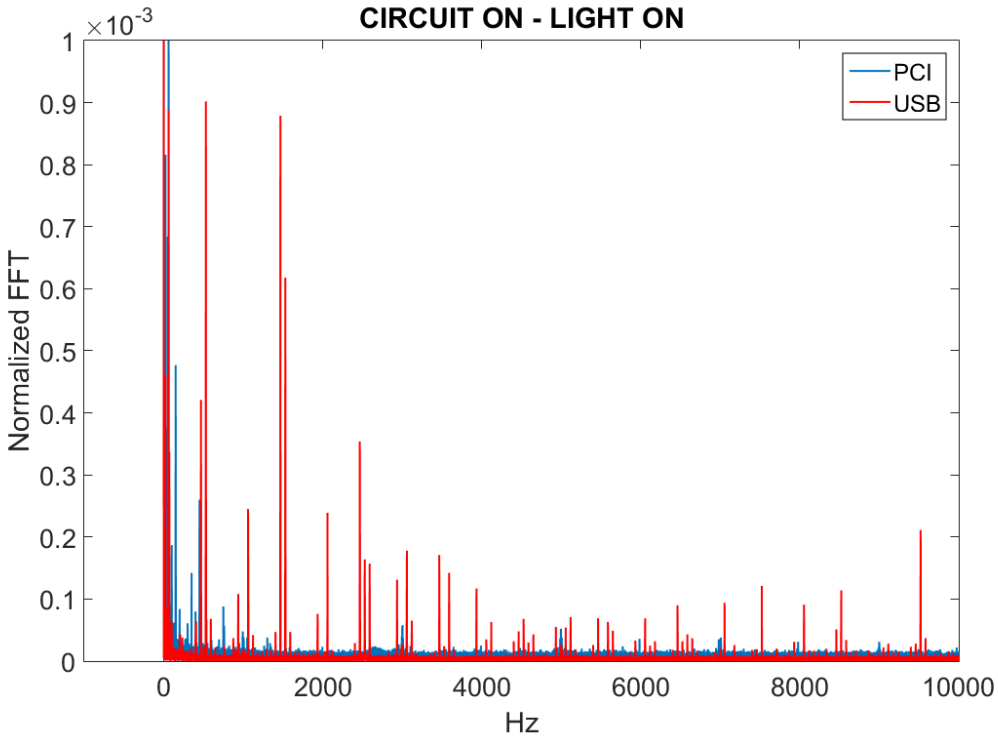


Figure B.5: The teeth at f_{C1} andf_{C2}

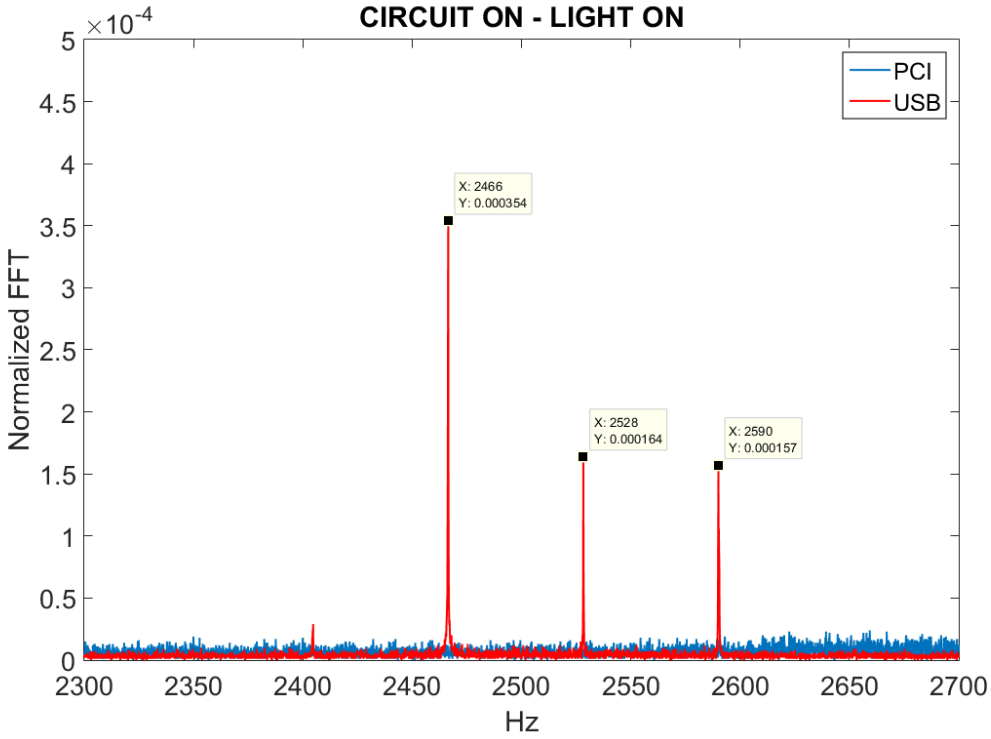


Figure B.6: Zoom in

- Two comb structures, one inside the other, in the USB noise for the middle range of frequencies (from $\sim 10^2 Hz$ to $\sim 10^4 Hz$) whose causes are not clear.

The two long comb have both $\Delta f = 1kHz$, but starting frequencies $f_{C1} = 530Hz + nkHz$ and $f_{C2} = 1000Hz + nkHz$ (see figure B.5) and they span the region $10^3Hz - 10^4Hz$. Each tooth has a substructure of side peaks at $\Delta f = \pm 62Hz$ from the central peak as shown in figure B.6.

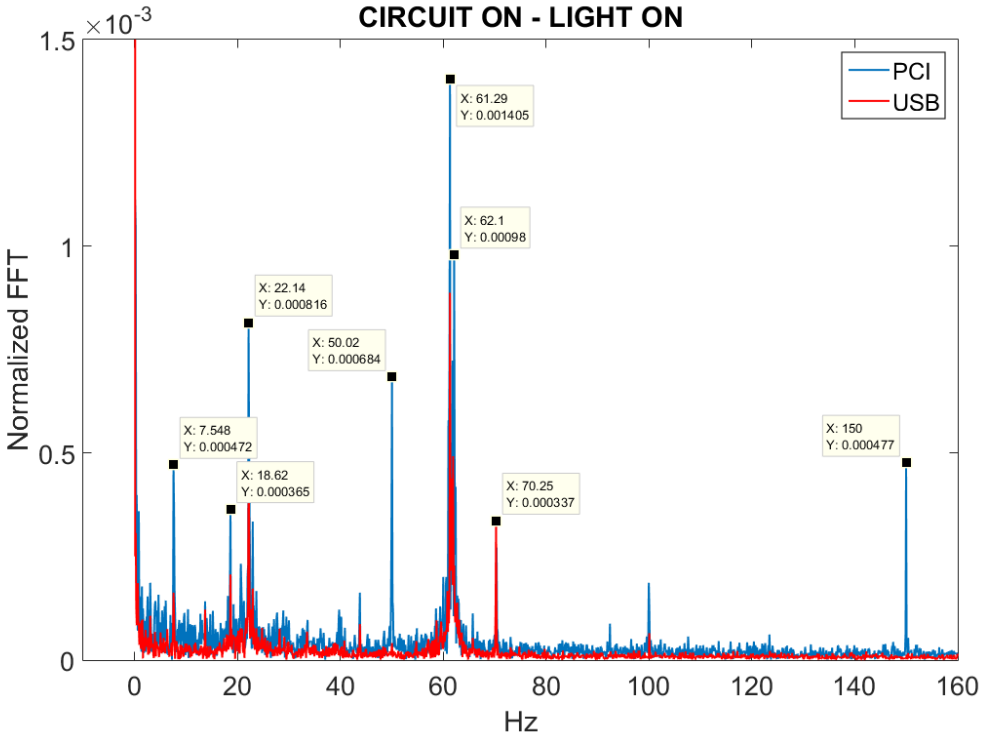


Figure B.7: FT noise analysis in working conditions (3): Noise of the card

B.0.2.2 Sampling and bandwidth

The FT study shows that the USB card is in general less noisy than the PCI one, except for what we see in the middle range of frequency in figures B.5 and B.6. Moreover the USB6363 has in principle the possibility to go twice faster than the PCI6110 in terms of sampling. On the other hand this maximum speed must be divided by the number of input channels.

Another main issue is the real time communication: the PCI card communicates at the same speed of the clock of the experiment, sending and acquiring information at each clock input. The USB is bound by the PC internal USB bus so, even if it can actually acquire at higher speed, the file are stocked in the card and then sent in the processing area. This problem can be partially overcome by reducing the size of the communication block (for the FT study it was $l_{block} = 2^{16} = 65536$ pulses).

Last but not least is the bandwidth of the cards. Figure B.9 show that the USB card has a higher integration time, i.e. a shorter bandwidth. In this sense the PCI card acquires faster and "more in real time". In the picture the two pulses have been sampled using a clock slightly different from the pulse generation frequency. On the x-axis are the sample: in terms of time, since the pulses have a frequency

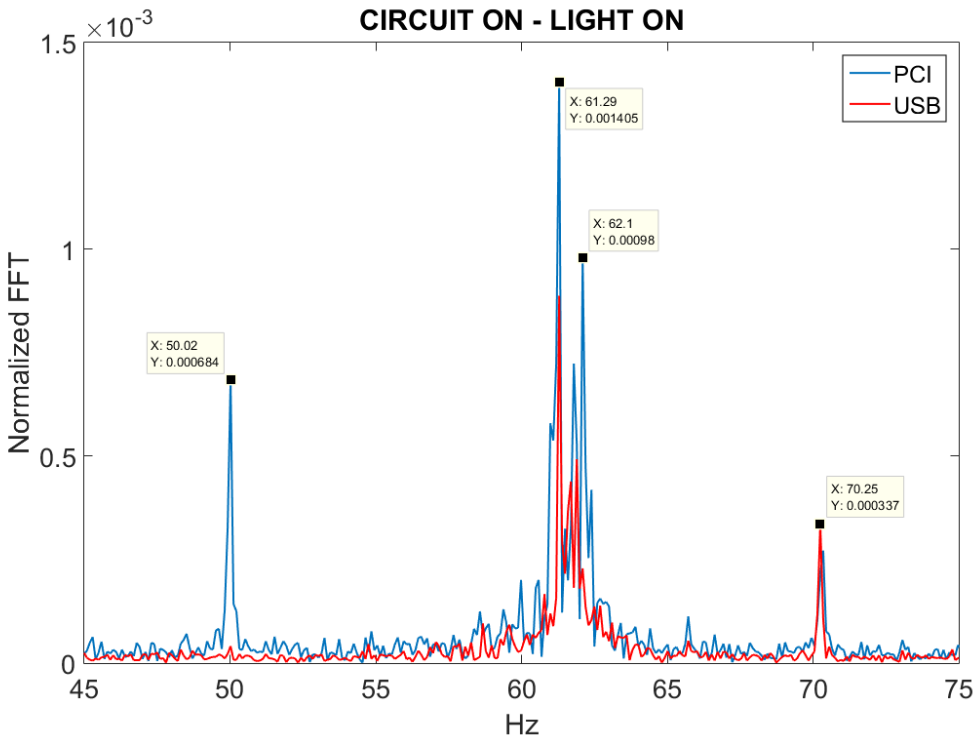


Figure B.8: FT noise analysis in working conditions (3): Card + circuit (off)

of 500kHz, the distance between them is $2\mu s$. Fortunately this difference in the bandwidth is not crucial, representing just another small contribution to the overall integration process, which is stronger in the homodyne's amplification electronics. Nonetheless this phenomenon manifests itself only *after* the detection process. In fact the display of the oscilloscope shows the same figure for both USB6363 and PCI6110, but when the signal enters the card it suffers a different action.

It is important to highlight that this change of shape is not without repercussions. The most important consequence is related to the acquisition time, i.e. the point of the pulse which is more suitable for the measurement. We discuss this right in the section below.

B.0.3 Triggering the system

The trigger system is shown in figure B.10. The trigger master is given by the laser electronic circuit, which generates an electrical TTL perfectly synchronized with the light pulses (the same TTL is used to modulate the current in the laser diode). A pulse generator can deliver and delay the same TTL to the remote control (via the NI card) to drive the I/O process. The same generator is used to deliver the trigger to the oscilloscope, which is now synchronous with the acquisition. The visual approach to the detection and trigger can be considered useless or redundant, but it is thanks to the comparison between measured data and the figures on the oscilloscope that the bandwidth features of the USB card has been discovered (section B.0.2.2).

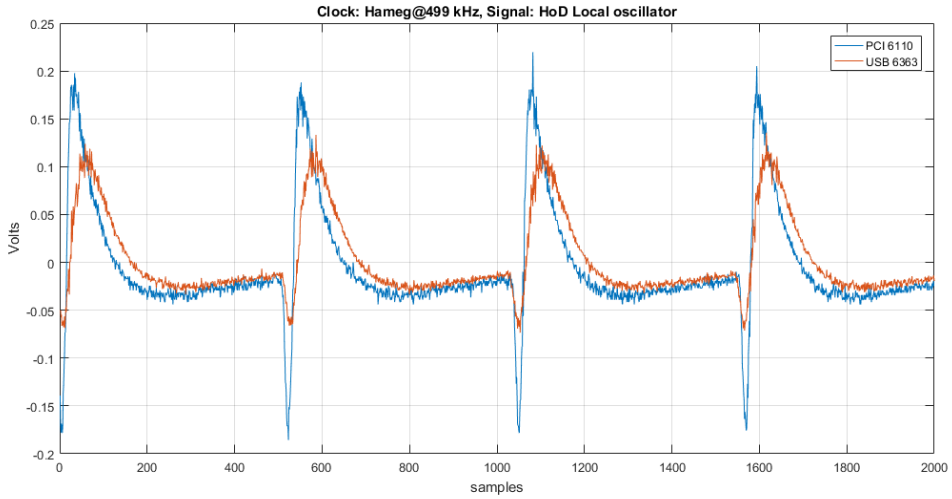


Figure B.9: Homodyne detection output seen by the two acquisition cards

The issue with the triggering is setting the right delay for the NI card, so that the whole process of acquiring the homodyne signal and generating the voltage to apply to the modulators can start at the proper time. To understand what "proper time" means a brief introduction about the analysis of the homodyne output must be done (more details are given in section 2.2).

The homodyne detection signal (see figure B.9) looks almost like an oscillation of one period, with a deep-peak (or peak-deep) structure in which the second half of it relaxes to zero in a time which is longer than half of the period itself. We can divide the figure in two parts.

The first part (deep) corresponds to the pulses arriving on the photodiodes and charging the detection electronics. The second part (peak) is the response of the electronics to the charge accumulation. It is in this second part that the acquisition must be done, more precisely on the extremal point maximum or minimum depending on the shape) of the second part. This is just a general visual approach. In fact the true aim is to maximize the gain of the electrical chain so that the ratio $\frac{N_0}{v_{el}}$ is as big as possible so that v_{el} becomes negligible. In this process, we must be careful about increasing the gain without any remora: in fact there is a critical point in which non linear effects start to appear. In figure B.11 it is shown how changing the delay of the trigger changes the total as well. What we actually see is a variation of the slope in the relation between the input optical power I_{LO} and the variance of the output, when only the local oscillator is injected in the detection. This relation will be used often during this work and it will be called **SNL slope**, since it tells where the detection is shot noise limited. From the linear fits we can extract the slope coefficients m and the intercepts values q. The best curve is the one that maximizes the ratio

$$\frac{m}{q} \propto \frac{N_0}{vel} \tag{B.1}$$

or minimizes its reciprocal, without entering a non-linear regime. We can see

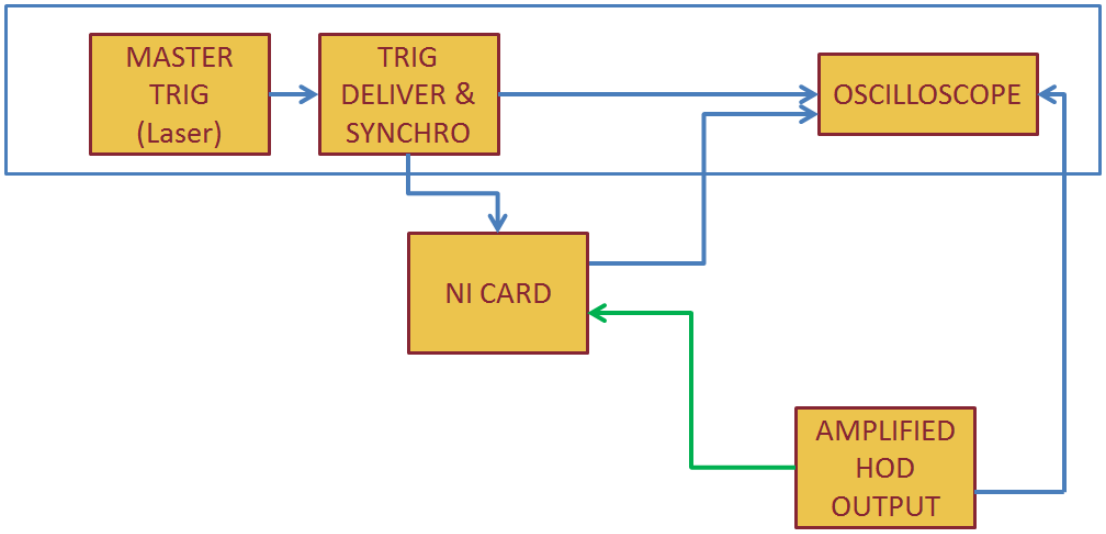
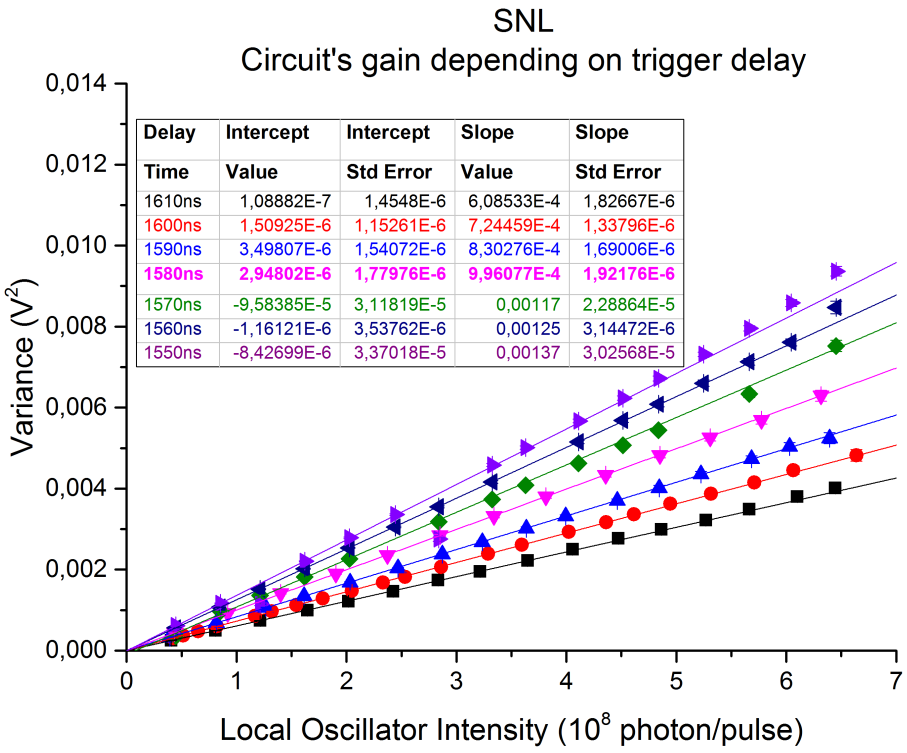


Figure B.10: The triggering system. The delays are checked visually on the oscilloscope and measured with the control system



Delay	Intercept	Intercept	Slope	Slope
Time	Value	Std Error	Value	Std Error
1610ns	1,08882E-7	1,4548E-6	6,08533E-4	1,82667E-6
1600ns	1,50925E-6	1,15261E-6	7,24459E-4	1,33796E-6
1590ns	3,49807E-6	1,54072E-6	8,30276E-4	1,69006E-6
1580ns	2,94802E-6	1,77976E-6	9,96077E-4	1,92176E-6
1570ns	-9,58385E-5	3,11819E-5	0,00117	2,28864E-5
1560ns	-1,16121E-6	3,53762E-6	0,00125	3,14472E-6
1550ns	-8,42699E-6	3,37018E-5	0,00137	3,02568E-5

Figure B.11: Bulk setup with the PCI card: the SNL slope (proportional to the gain) changes with the delay

from B.1, in which $\frac{q}{m}$ is calculated for each trigger delay time, that sometimes the linear fit gives absurd results. This is due first to the appearance of a non-linear behaviour when the local oscillator pluses are brighter, then to the fact that *vel* is not measured but calculated from the fit itself. We can overcome this problem following another approach.

Delay time (ns)	$\frac{q}{m}$ ratio
1610	1.810^{-4}
1600	2.110^{-3}
1590	4.210^{-3}
1580	2.910^{-3}
1570	$q < 0$
1560	$q < 0$
1550	$q < 0$

Table B.1: $\frac{q}{m}$ ratio vs. the trigger delay

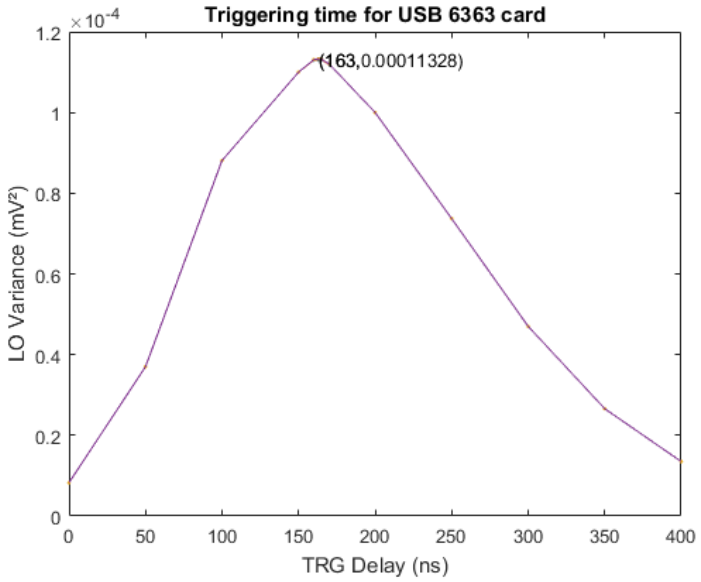


Figure B.12: LETI chip with USB card: the variance changes with the delay

A more accurate method consists in defining the triggering delay time as the delay time that maximizes the variance of the local oscillator. Starting from this we can proceed in two step: *vel* is measured, since it is the electrical noise of the chain without light, so it must be independent from the local oscillator power. Then, fixing the local oscillator optical power (i.e. fixing a point on the x-axis) we measure the variance at that point for different delays. We did this test with the LETI chip (studied in chapter 7) using the USB card and we obtained the results in figure B.12.

The fact that the delay found in the first case is completely different than the one in the second case may be explained by the fact that in the first case not only the chip was different, but also the pulse generators (which have different internal default delays) and also the acquisition cards.

Appendix C

Holevo's key rate

In a reverse reconciliation scheme under collective attacks using continuous variable QKD protocols, the raw key rate is expressed through the Holevo's formula:

$$K_{collRR} = I_{AB} - \chi_{BE} \tag{C.1}$$

where I_{AB} is the mutual information between Alice and Bob and χ_{BE} is the Holevo quantity [5, 28]

$$\chi_{BE} = S(\rho_{BE}) - \int dx_B p(x_B) S(\rho_E^{x_B}) \tag{C.2}$$

where $p(x_B)$ is the probability distribution of Bob's measurement outcomes, $\rho_E^{x_B}$ is Eve's state conditional on Bob's outcome and S is the von Neumann entropy.

Eq. C.1 does not represent the actual key rate. In fact, since the reconciliation process is not optimal, the ideal value of I_{AB} overestimates the actual amount of information shared by Alice and Bob. The final key rate can be expressed using a β factor (positive and not greater than 1) multiplying I_{AB}:

$$K_{collRR} = \beta I_{AB} - \chi_{BE} \tag{C.3}$$

Following the results obtained by Lodewyck [5] we can state that for our implementation

$$\beta > 0.95 \tag{C.4}$$

It's appropriate to reintroduce equations 3.16

$$\chi_{ch} = \frac{1-T}{T} + \varepsilon, \qquad \chi_{hom} = \frac{1-\eta}{\eta} + \frac{v_{el}}{\eta} \tag{C.5}$$

which define the noise induced by the channel and the detection, as well as equation 3.17

$$\chi = \chi_{ch} + \frac{\chi_{hom}}{T} = \frac{1-G}{G} + \frac{v_{el}}{G} + \varepsilon = \frac{1-G}{G} + \xi \tag{C.6}$$

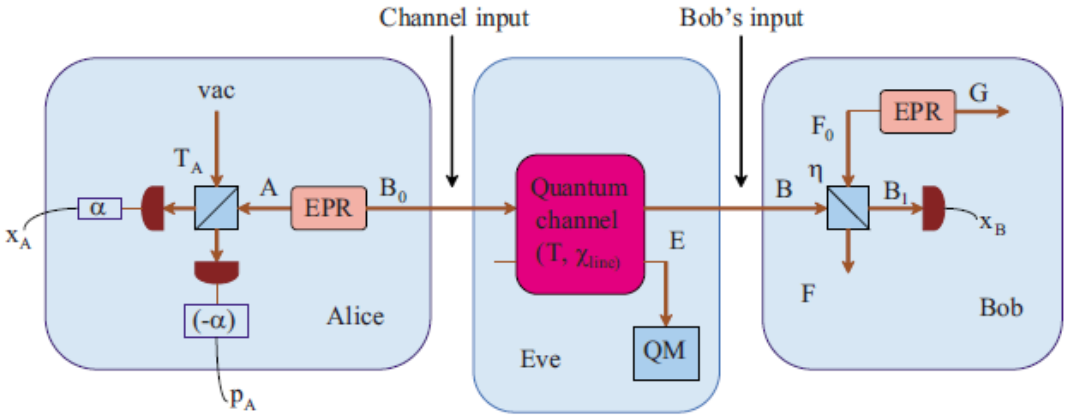


Figure C.1: The GG02 protocol with an EPR source, with Alice, Bob and Eve [5]

which gives the total noise due to both channel and homodyne detection. Remembering that $V = V - A + 1$, the mutual (Shannon) information between Alice and Bob is

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{C+\chi}{1+\chi}\right). \tag{C.7}$$

The Holevo quantity is more difficult to calculate. The von Neuman entropy for an n-mode Gaussian state ρ is

$$S(\rho) = \Sigma_i G\left(\frac{\lambda_i - 1}{2}\right) \tag{C.8}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and the λ_i are the eigenvalues of the covariance matrix which characterizes ρ.

Since Eve's system purifies the system of Alice and Bob, we can say that

$$S(\rho_E) = S(\rho_{AB}) \tag{C.9}$$

We can treat the integral in eq. C.2 as follows, using an expedient. It has been demonstrated by Grosshans itself [18] that the GG02 protocol in the *prepare and measure* scheme is equivalent to the same protocol in exploiting an EPR source. The difference between the two schemes lies in the difficutly of the implementation and on the complexity of the theory behind them. It results that the EPR scheme is more difficult to implement, while it is easier to explore theoretically. Let's picture now the GG02 in an EPR scheme, as shown in figure C.1: after Bob's projective measurement with outcome x_B, the system AEFG is pure, so that $S(\rho_E^{x_B}) = S(\rho_{AFG}^{x_B})$, where $S(\rho_{AFG}^{x_B})$ is now independent from x_B is the protocol uses Gaussian modulation. Knowing that we can finally write

$$\chi_{BE} = S(\rho_{AB}) - S(\rho_{AFG}^{x_B}) \tag{C.10}$$

The entropy $S(\rho_{AB})$ is calculated from the covariance matrix

$$\Gamma_{AB} = \begin{bmatrix} V\mathbb{1} & \sqrt{T(V^2-1)}\cdot\sigma_z \\ \sqrt{T(V^2-1)}\cdot\sigma_z & T(V+\chi_{ch})\mathbb{1} \end{bmatrix} \tag{C.11}$$

whose symplectic eigenvalues are

$$\lambda_{1,2} = \sqrt{\frac{A \pm \sqrt{A^2 - 4B}}{2}} \tag{C.12}$$

with

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{ch})^2 \tag{C.13a}$$
$$B = T^2(V\chi_{ch}+1)^2 \tag{C.13b}$$

Similarly the symplectic eigenvalues of $S(\rho_{AFG}^{x_B})$ are calculated:

$$\lambda_{3,4} = \sqrt{\frac{C \pm \sqrt{C^2 - 4D}}{2}} \tag{C.14}$$

where

$$C = \frac{V\sqrt{B} + T(V+\chi_{ch}) + A\chi_{hom}}{T(V+\chi)} \tag{C.15a}$$
$$D = \sqrt{B}\frac{V+\sqrt{B}\chi_{hom}}{T(V+\chi)} \tag{C.15b}$$

The last eigenvalue is $\lambda_5 = 1$, so $G\left(\frac{\lambda_5 - 1}{2}\right) = 0$. Finally we write

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) + G\left(\frac{\lambda_3 - 1}{2}\right) + G\left(\frac{\lambda_4 - 1}{2}\right) \tag{C.16}$$

Appendix D

The control software

The experiment is remotely controlled by a software that takes care of the driving voltages of the modulators, acquires the homodyne detection signal and analyzes the data for live evaluation and post processing.

The software can be run in two separated modes: the *calibration* mode, which is used as test configuration, and the *run* mode, used for live and continuous communication.

The calibration mode offers more options as a complete testing environment. During pre-communication stages, one can choose to measure the electronic noise v_{el}, the instrinsic detection noise (local oscillator and electronic noise itself) N_0+v_{el}, so that the shot noise can be precisely retrieved.

In the run mode it's not possible to measure these quantities, which must be entered as fixed parameters of the communication after being measured using the calibration mode.

On the other hand in both communication and run mode all other options can be chosen independently. Before listing them, the structure of the communication must be described.

The computer and the optical/electronic part of the setup communicate using two buffers, one for the input and one for the output, running at the same time during the execution of the software. It must be highlighted that "input" and "output" from the buffer's (so the computer's and Alice's) point of view are inverted when Bob's point of view is taken into account: Bob's output corresponds to the buffer's input.

The data flow is performed in "blocks" of data. Each block, generated by Alice, is formed by a series of pulses (or symbols). The total number of the pulses in each block is the size of the block itself.

The pulses in each block can be used for four different purposes (see figure D.1):

- N_0 evaluation symbols
- key extraction (secret symbols)
- parameters estimation (revealed symbols)

- modulators calibration symbols

The percentage in which the four types are present in the block is chosen before the communication starts.

The N_0 **evaluation symbols** are used for the live evaluation of the shot noise. In fact this parameter is not perfectly fixed, since it depends on the optical power fluctuations. A live measurement allows the monitoring of this important parameter. To measure the shot noise the signal must be attenuated, so from Alice's point of view these pulses have amplitude $A = 0$, while the phase is chosen randomly between 0 and π, to average an eventual phase imperfection in the phase evaluation. In the phase space this points are represented as the origin of the phase space itself.

The **secret symbols** are the states used for the actual key extraction i.e. the *raw key*. From the raw key, by means of error correction and privacy amplification codes, the actual key is extracted. These states are Gaussian distributed. The generation is made by Alice's pseudo-random number generator, using a variance $\bar{V_A}$ around the origin of the phase space.

The **parameters estimation** is performed using the so-called **revealed symbols**, meaning the symbols that Alice and Bob publicly communicate to estimate the channel properties and the communication feature. These states, Gaussian distributed, have the same structure of the secret symbols. The parameters η, ξ, α, T can be estimated using these symbols.

Finally, the last part of the block is dedicated to the **calibration of the modulators**, which will be used in the following block. The calibration aims to evaluate a few but fundamental properties of the amplitude and phase modulators. The bulk amplitude modulators have a sinusoidal response if the driving voltage is linearly increased. The phase modulator's response is sinusoidal too. By means of a sinusoidal fit one can calculate V_π and V_{bias} for both the modulators, where V_π is the voltage that give a π shift at the output of the modulator, while V_{bias} follows the intrinsic drift of the modulators and, in the case of the phase modulator, it follows the phase drift of the channel as well.

The blocks of data are put in the output buffer, waiting to be executed. Before the communication starts a few block must be created and put in pre-buffer. The pre-buffer is mainly used for calibration purposes. This means that the calibration data (V_π and V_{bias}) calculated in the first pre-buffer block are successively used in the first communication block, meaning that there is a delay between the modulators calibration and its actual utilization. During this time of few block (typically 8 to 16 block = 16 to 32 ms at 0.5 MHz) the modulators are considered to be stable. On the other hand this delay is a source of error that, even if very little, is still present.

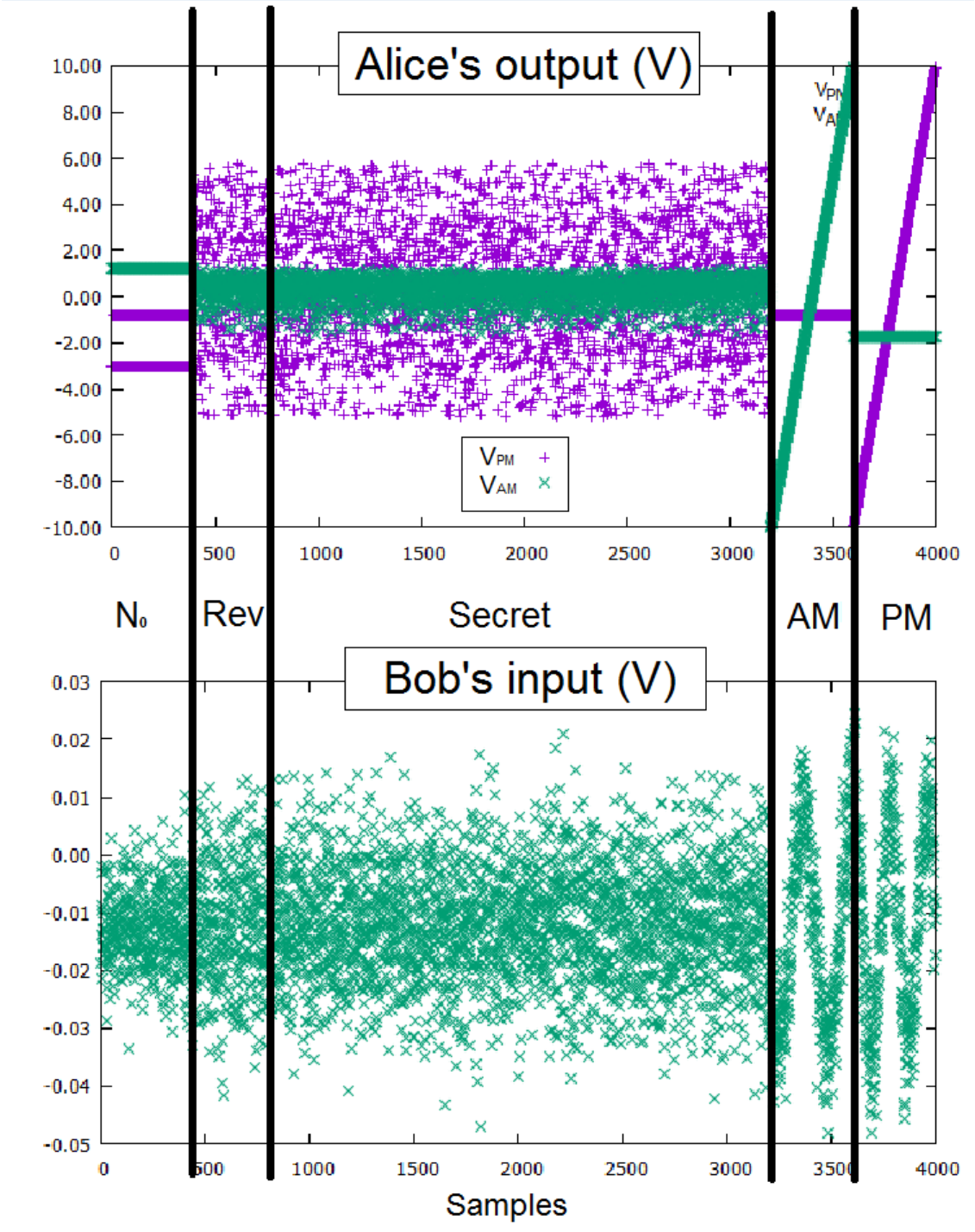


Figure D.1: The structure of a block of data. Above the voltage generated by Alice for the two modulators, below the corresponding homodyne output measured by Bob

Bibliography

[1] M. Fukuda. *Optical semiconductor devices.* NY Wiley, 1998.

[2] M. Ziebell. *Transceiver optique en silicium pour les réseaux d acces.* Ph.D. thesis, Université Paris 11, 2013. HAL: https://tel.archives-ouvertes.fr/tel-00873582/document.

[3] M. Ziebell. *Integrated QKD Comparison Testing*, 2014.

[4] S. Fossier. *Implementation and Evaluation of Quantum Key Distribution Devices at Telecom Wavelength.* Ph.D. thesis, Université Paris-Sud - Paris XI, 2009. HAL: https://tel.archives-ouvertes.fr/file/index/docid/429450/filename/these.pdf.

[5] J. Lodewyck et al. *Quantum key distribution over 25 mk with an all-fiber continuous-variable system.* Phys. Rev. A., **76** 042305, 2007.

[6] C. E. Shannon. *A mathematical theory of communication.* The BEll System Technical Journal, **27** 379–423, 1948.

[7] M. Planck. *On the Theory of the Energy Distribution Law of the Normal Spectrum.* Annalen der Physik, **2**(237), 1901.

[8] A. B. E. Podolsk and N. Rosen. *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev., **47** 777, 1935.

[9] J. S. Bell. *On the Einstein-Poldolsky-Rosen paradox.* Physics, **1**(3) 195–290, 1964.

[10] A. Aspect. *Viewpoint: Closing the Door on Einstein and Bohr's Quantum Debate.* Physics, **8** 123, 2015.

[11] W. K. Heisenberg. *Uber den anschauclichen Inhalt der quantentheoretischen Kinematik und Mechanik.* Phys, **43** 172–198, 1927.

[12] J. J. Sakurai. *Meccanica quantistica moderna.* Zanichelli, 1990.

[13] W. K. Wootters and W. H. Zurek. *A Single Quantum Cannot be Cloned.* Nature, **299** 802–803, 1982.

[14] C. Weedbrook et al. *Gaussian quantum information.* Rev. Mod. Phys., **84** 621, 2011.

[15] R. Simon et al. *Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms.* Phys. Rev. A, **49**(3) 1567, 1994.

[16] H. P. Yuen and V. W. S. Chan. *Noise in homodyne and heterodyne detection.* Opt. Lett., **8**(8) 419–421, 1983.

[17] C. K. Hong, Z. Y. Ou and L. Mandel. *Measurement of subpicosecond time intervals between two photons by interference.* Phys. Rev. Lett., **59**(18) 2044–2046, 1987.

[18] F. Grosshans and P. Grangier. *Continuous Variable Quantum Cryptography Using Coherent States.* Phys. Rev. Lett., **88**(5) 057902, 2002.

[19] C. E. Shannon. *Communication Theory of Secrecy Systems.* Bell System Technical Journal, **28**(4) 656–715, 1949.

[20] R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, **21**(2) 294–299, 1978.

[21] G. Benenti, G. Casati and G. Strini. *Principles of Quantum Computation and Information.* World Scientific, 2004.

[22] M. Nielsen and I. Chuang. *Quantum Computing and Quantum Information.* Cambridge University Press, 2000.

[23] *Quantum cryptography Public key distribution and coin tossing*, volume 175, 1984.

[24] A. E. Ekert. *Quantum cryptography based on Bells theorem.* Phys. Rev. Lett., **67** 661, 1991.

[25] F. Grosshans and N. J. Cerf. *Continuous-variable quantum cryptography is secure against non-Gaussian attacks.* Phys. Rev. Lett., **92** 047905, 2004.

[26] R. Garcia-Patron and N. J. Cerf. *Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution.* Phys. Rev. Lett., **97** 190502, 2006.

[27] M. Navascues et al. *Optimality of Gaussian Attacks in Continuous Variable Quantum Cryptography.* Phys. Rev. Lett., **97** 190503, 2006.

[28] R. Renner. *Security of Quantum Key Distribution.* Ph.D. thesis, ETH Zurich, 2005. Https://arxiv.org/abs/quant-ph/0512258.

[29] A. Leverrier. *Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States.* Phys. Rev. Lett., **114** 070501, 2015.

[30] A. Leverrier. *Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction.* Phys. Rev. Lett., **118** 200501, 2017.

[31] A. Politi et al. *Silica-on-silicon waveguide quantum circuits.* Science, **320**, 2008.

[32] L. Sansoni et al. *Integrated photonic quantum gates for polarization qubits.* Nature Comm., **2**(566), 2011.

[33] P. Serrafi et al. *Continuous-wave quasi-phase-matched waveguide correlated photon pair source on a III V chip.* Appl. Phys. Lett., **103** 251115, 2013.

[34] F. Kaiser et al. *Polarization entangled photon-pair source based on quantum nonlinear photonics and interferometry.* Opt. Comm., **327** 7–16, 2014.

[35] A. Orieux and E. Diamanti. *Recent advances on integrated quantum communications.* Journal of Optics, **18** 083002, 2016.

[36] D. Stucki et al. *Fast and simple one-way quantum key distribution.* Appl. Phys. Lett, **87** 194108, 2005.

[37] *Photonics Asia 2002 32-39 International Society for Optics and Photonics*, 2002.

[38] P. Sibson et al. *Chip-based quantum key distribution.* Nature Communication, **8**(13984), 2017.

[39] N. W. Ashcroft and N. Mermin. *Solid State Physics.* Cengage Learning, 1976.

[40] L. B. Soldano and E. C. M. Pennings. *Optical Multi-Mode Interference Devices Based on Self-Imaging: Principles and Applications.* J. Lightw. Technol., **13** 4, 1995.

[41] B. Qi et al. *Generating the Local Oscillator Locally in Continuous-Variable Quantum Key Distribution Based on Coherent Detection.* Phys. Rev. X, **5** 041009, 2015.

[42] D. B. S. Soh et al. *Self-Referenced Continuous-Variable Quantum Key Distribution Protocol.* Phys. Rev. X, **5** 041010, 2015.

[43] P. Jouguet et al. *Long-distance continuous-variable quantum key distribution with a Gaussian modulation.* Phys. Rev. A, **84** 062317, 2011.

[44] P. Jouguet et al. *Experimental demonstration of long-distance continuous-variable quantum key distribution.* Nature Photonics, **63** 378–381, 2013.

[45] F. Grosshans. *Communication et cryptographie quantiques avec des variables continues.* Ph.D. thesis, Université Paris-Sud - Paris XI, 2002. HAL: tel-00002343v2.

[46] J. Wenger. *Dispositifs impulsionnels pour la communication quantique à variables continues.* Ph.D. thesis, Université Paris 11, 2004. HAL: tel-00006926.

[47] J. Lodewyck. *Communication et cryptographie quantiques avec des variables continues.* Ph.D. thesis, Université Paris-Sud - Paris XI, 2002. HAL: tel-00130680v2.

[48] P. Jouguet. *Security and performance of continuous-variable quantum key distribution systems.* Ph.D. thesis, Université Paris-Sud - Paris XI, 2013. HAL: tel-01174739.

Part V

Abstract

Résumé de la thèse.

L'objectif de cette thèse est de mettre en œuvre des protocoles de *distribution de clé quantique à variable continue* (CVQKD, de l'anglais Continuous Variable Quantum Key Distribution) basés sur des circuits optiques intégrés, réalisés à partir de composants photoniques sur silicium. Un dispositif intégré consomme moins d'énergie et d'espace et est par conséquent plus efficace et potentiellement moins coûteux. L'avantage des dispositifs photoniques sur silicium est qu'ils fonctionnent correctement à température ambiante et qu'ils sont capables de satisfaire toutes les exigences requises pour les protocoles CVQKD, qui sont précisées dans la thèse. Nous voulons donc démontrer que cette technologie peut être choisie comme base pour l'intégration de protocoles CVQKD.

Le travail est divisé en deux parties: dans la première nous présentons des outils théoriques et expérimentaux utiles pour ce travail, allant d'une introduction à la cryptographie quantique, aux principes de base de la photonique sur silicium. La deuxième partie est centrée sur les expériences que nous avons réalisées, y compris les procédures et les résultats. Le contenu des chapitres est le suivant:

Chapitre 1 Le premier chapitre présente en trois sections les concepts de base de la mécanique quantique et de l'information quantique. La cryptographie quantique repose sur le concept d'*information*, dont nous rappelons la définition dans le cadre de théorie de Shannon. Certaines quantités fondamentales de cette théorie sont discutées, en particulier l'*entropie de Shannon* et ses applications. La deuxième partie résume les notions essentielles de la mécanique quantique, en partant d'une brève introduction historique, et en insistant sur la définition, l'évolution et la mesure d'un état quantique. Nous discutons aussi les notions de superposition quantique et d'intrication, ainsi que les inégalités de Heisenberg, la nature perturbative d'une mesure, et le théorème de non-clonage, qui est particulièrement important en cryptographie quantique. Dans une dernière étape nous rapprochons ces deux théories, dans le cadre du nouveau domaine de l'information quantique. La nouvelle unité d'information, le *qubit*, est définie, ainsi que d'autres opérations importantes, combinant l'approche quantique et la notion d'information

Chapitre 2 En communication quantique, on doit utiliser un système physique qui peut être transmis d'un interlocuteur (Alice) à l'autre (Bob). Un photon ou un ensemble de photons sont bien adaptés à ce but, et ce deuxième chapitre rappelle des notions utiles d'optique quantique. Les propriétés quantiques de la lumière utilisés dans ce travail sont appelées variables continues, en se référant à la nature du système de mesure qui n'utilise pas de compteurs de photons, mais une détection interférométrique, appelée aussi détection "cohérente". On présente donc les états que nous utiliserons, les états Gaussiens, et le système de mesure interférométrique, la détection homodyne.

Chapitre 3 Les principes généraux de la cryptographie quantique et de la distribution quantique de clés secrètes sont présentés dans le chapitre 3. L'objectif de principe est d'atteindre ce qu'en anglais on appelle *information theoretical security* (*sécurité du point de vue de la théorie de l'information*) c'est-à-dire une situation où la sécurité est mathématiquement assurée par le protocole cryptographique utilisé. Un exemple de tel protocole est le *one-time pad*, ou code de Vernam, nécessite une clé aléatoire différente pour chaque communication entre Alice et Bob. Le problème est alors transféré à la protection de l'échange de clé, et la cryptographie quantique garantit cette protection, en se basant sur les lois de la physique.

Il existe deux méthodes principales pour mettre en oeuvre la distribution quantique de clé, en utilisant soit des variables discrètes soit des variables continues. La configuration de mesure spécifique à chaque méthode influence également la structure du protocole et l'analyse des données. Ce travail de thèse est réalisé en utilisant les variables continues, déjà introduites dans le chapitre précédent, et le protocole est décrit plus en détail dans ce chapitre.

Chapitre 4 La première partie se termine par le quatrième chapitre, qui présente une introduction élémentaire à la photonique sur silicium. Le chapitre est divisé en trois sections principales, qui décrivent successivement les phénomènes physiques utilisés dans la photonique du silicium, puis les structures optiques et électriques nécessaires à l'intégration optique, et finalement la détection par des photodiodes en Germanium. Quelques précisions sont données sur les structures (PIN ou PIPIN) utilisées.

Chapitre 5 La deuxième partie, décrivant le travail original réalisé, commence par un chapitre introductif sur la mise en œuvre expérimentale du protocole cryptographique, en se référant à sa mise en oeuvre par des composants télécom usuels, sans intégration. Les propriétés optiques et électriques des circuits ainsi que le traitement du signal sont présentés, et on en déduit une liste d'exigences pour la mise en œuvre sur puce. En se basant sur ces critères les chapitre 6 et 7 présentent deux approches différentes utilisés pour réaliser un protocole CVQKD avec des circuits photoniques sur silicium.

Chapitre 6 La première approche consiste à construire une puce pour réaliser une preuve de principe simple, dans laquelle Alice et Bob conservent leurs fonctionnalités propres, mais sont placés sur le même support physique.

La première section de ce chapitre présente les résultats des tests effectués sur les composants optiques intégrés que nous avons déjà énumérés au chapitre 4. Une présentation plus approfondie du système d'acquisition et d'amplification occupe une partie importante de ce chapitre, en relation avec le chapitre 7.

La coexistence d'Alice et de Bob vise à faciliter la mise en œuvre, car le canal de communication et les distorsions qu'il induit sont absents. Mais il devient

alors impossible de complètement séparer Alice et Bob, et la présence permanente du signal d'Alice dans la détection homodyne au cours du processus d'étalonnage compromet l'exécution du protocole lui-même. Cependant la détection homodyne a été caractérisée et les résultats sont montrés à la fin du chapitre. Cette étape du travail a permis de mettre en évidence des différences importantes entre le système usuel et le système intégré.

Chapitre 7 Les difficultés rencontrées dans le chapitre précédent nous conduisent à utiliser une autre architecture pour une deuxième génération de puces, conçue pour fonctionner avec deux parties séparés physiquement pour Alice et Bob. Il s'avère d'abord nécessaire de refaire certains tests sur les composants, car la nouvelle puce a été fabriqué par une nouvelle fonderie (LETI), et a des propriétés différentes de celles du "chip" précédent. Puisque la configuration de mesure de Bob peut maintenant être utilisé indépendamment de la modulation d'Alice, la calibration de la détection homodyne a été effectué facilement et correctement. Il est alors possible de tester le protocole complet permettant l'extraction de la clé. Le système qui a été testé est une configuration hybride avec détection intégré et modulation en bulk. Le choix a été fait pour permettre une analyse complète et indépendante de la détection sur puce, de sorte que les effets et problèmes particuliers dus à la puce de modulation puissent être identifiés successivement lorsque la puce sera utilisée.

La nouvelle conception et la fabrication nous ont donc permis de surmonter certaines des contraintes apparues avec la génération précédente, et d'augmenter l'efficacité de la communication. Ceci a permis une vraie extraction de clé, avec cependant des taux et des distances relativement faibles. Un aperçu du travail à venir est effectué dans la dernière section. Il comprend deux étapes: le remplacement de la modulation externe par une modulation intégrée, et l'utilisation éventuelle d'une détection hétérodyne.

Conclusion Ce travail montre que la photonique sur silicium est une technologie très prometteuse pour l'intégration des systèmes CVQKD sur des "chips" optiques. En dépit des problèmes techniques rencontrés, il a été démontré que l'extraction d'une clé est réllement possible. De plus, l'expérience acquise en travaillant sur des configurations de test permettra de concevoir des dispositifs et des architectures plus adaptés et performants, dans la perspective d'un dispositif plus stable et plus simple à utiliser.

Title: Experimental study of the integration of continuous-variable quantum key distribution into a silicon photonics device.

Key words: quantum optics, integrated silicon photonics, quantum key distribution, continuous variables.

During recent years there have been significant developments in quantum cryptography, bringing quantum key distribution (QKD) devices on the market. This can be done by using either discrete variables (DV) and photon counting, or continuous variables (CV) and coherent detection. Current technological evolutions are now aiming at developing smaller, cheaper and more user-friendly devices.

This work focuses on the implementation of CV-QKD using silicon photonics techniques, which provide a high degree of integration. This is exploited to build an on-chip realization of a cryptographic protocol, using Gaussian modulation of coherent states. Two different approaches have been used, first by physically implementing the sender (Alice) and the receiver (Bob) on the same chip for validation purposes, and then by having them onto two separate chips. The measured communication parameters give the possibility to extract a secret key.

Titre: Étude expérimentale de l'intégration d'un système de distribution quantique de clé à variables continues sur un circuit optique en silicium.

Mots clés: optique quantique, photonique intégrée sur silicium, distribution quantique de clé, variables continues.

Les évolutions récentes de la cryptographie quantique ont permis de proposer sur le marché des appareils de distribution quantique de clé secrète (QKD). Ceci est obtenu en utilisant soit des variables discrètes et des compteurs de photons (DV), soit des variables continues et des systèmes de détection cohérente (CV). Les avancées technologiques s'orientent maintenant vers la réalisation de dispositifs plus petits, moins chers, et plus commodes à utiliser.

L'objectif de cette thèse est de mettre en oeuvre un protocole CV-QKD sur un circuit optique intégré en silicium, en utilisant une modulation Gaussienne d'états cohérents. Deux approches sont utilisées: dans la première l'émetteur Alice et le récepteur Bob sont sur le même circuit photonique (chip) pour une validation de principe, et dans la deuxième ils sont séparés. Les valeurs mesurées des paramètres de la communication permettent d'échanger une clé secrète.