UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIA E TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

PAULO VINICIUS PEREIRA PINHEIRO

ENHANCING SECURITY OF PRACTICAL QUANTUM KEY DISTRIBUTION: TWO-LAYER QKD AND BACKFLASH EMISSION FROM SILICON AVALANCHE PHOTODIODES

FORTALEZA

2016

PAULO VINICIUS PEREIRA PINHEIRO

ENHANCING SECURITY OF PRACTICAL QUANTUM KEY DISTRIBUTION: TWO-LAYER QKD AND BACKFLASH EMISSION FROM SILICON AVALANCHE PHOTODIODES

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2016

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

P721e Pinheiro, Paulo Vinicius Pereira.
Enhancing security of practical quantum key distribution: two-layer QKD and backflash emission from silicon avalanche photodiodes. / Paulo Vinicius Pereira Pinheiro. – 2016.
94 f. : il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2016.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. Emissão reversa. 2. Fotodiodos de avalanche. 3. Distribuição quântica de chaves. I. Título.

CDD 621.38

PAULO VINICIUS PEREIRA PINHEIRO

ENHANCING SECURITY OF PRACTICAL QUANTUM KEY DISTRIBUTION: TWO-LAYER QKD AND BACKFLASH EMISSION FROM SILICON AVALANCHE PHOTODIODES

Thesis presented to the Graduate Program of Teleinformatics Engineering at Federal University of Ceará in fulfilment of the thesis requirement for the degree of Doctor of Philosophy in Teleinformatics Engineering.

Aproved in: 28 / 07 / 2016 .

COMITTEE

_____

Prof. Dr. Rubens Viana Ramos (Supervisor)
Federal University of Ceará (UFC)

_____

Prof. Dra. Hilma Helena Macedo de Vasconcelos
Federal University of Ceará (UFC)

_____

Prof. Dr. João Batista Rosa Silva
Federal University of Ceará (UFC)

_____

Prof. Dr. Carlos Henrique Monken
Federal University of Minas Gerais (UFMG)

_____

Prof. Dr. Guilherme Penello Temporão
Pontifical Catholic University of Rio de Janeiro (PUC-RJ)

ACKNOWLEDGEMENTS

"To the almighty creator of all things in sky and on earth."

Several people are responsible for this work.

The first acknowledgement goes to those unnamed here. My sincere thank you

To all my lab colleagues and friends.

To everyone in Ceará Federal University department that directly or indirectly contributed to this work.

To my foreign friends and my Russian supervisor Vadim Makarov.

To my foreign friends.

To my friend and local supervisor Rubens Viana Ramos.

To the sweetest human being on this planet, my wife and friend Emanuela Nobre.

To my daughter Gloria Pinheiro.

To my family, dad, sis, mom, mother, father and sisters-in-law.

To my deceased brother George Pinheiro, that departed too soon to new and unexplored adventures.

RESUMO

O desenvolvimento de novas tecnologias quânticas para comunicação em redes ópticas permitirá, dentre outros, a realização de protocolos invioláveis para a troca segura de informação. O primeiro e mais desenvolvido destes protocolos é a distribuição quântica de chaves. Embora na teoria esta apresente segurança perfeita, a implementação em redes ópticas pode produzir falhas de segurança devido ao comportamento não ideal dos dispositivos ópticos e optoeletrônicos utilizados. Nesta direção, a presente tese traz duas contribuições para a melhoria da segurança de sistemas de distribuição quântica de chaves. No primeiro caso, os protocolos de distribuição quântica de chaves que operam com deslocamento diferencial de fase em quadratura e com detecção homódina são redesenhados para funcionar utilizando estados coerente e térmico da luz, junto com diversidade de polarização. No segundo caso, a caracterização da luz emitida por fotodiodos de avalanche durante uma detecção e o impacto desta emissão na segurança no protocolo BB84 são realizadas.

Palavras-chave: Protocolo de QKD de duas camadas, detectores de fótons, Ataque de espionagem por emissão reversa de fótons.

ABSTRACT

The development of new quantum communication technologies for optical networks will enable inviolable protocols to exchange secure information. The first and more ro-bust among them is the quantum key distribution (QKD). Although in theory the security is proven unconditionally safe, the implementation in optical networks can still produce flaws due the non-ideal behavior of the optical and optoelectronic devices. In this direc-tion, this thesis presents two contributions to improve security of QKD systems. The first is the redesign of two QKD protocols to use two quantum states of light, the coherent and thermal state, with a polarization randomness. The protocols are the differential quadra-ture phase shift QKD and QKD using homodyne detection. The second contribution is the experimental characterization of the light emitted by avalanche photodiodes during a detection and its implication in the security of the BB84 QKD protocol.

Keywords: quantum key distribution, two-layer QKD, photodetectors, breakdown emission, backflash attack.

LIST OF FIGURES

Figure 1.1 - Enigma rotor-machine used in world war II by the Nazi German army. 14
Figure 1.2 - Encryption and decryption scheme. Extracted from [1] 15
Figure 1.3 - Public key cryptography scheme. Extracted from [1] 16
Figure 1.4 - BB84 protocol explanation scheme. Picture redesigned from public documents in ID Quantique website (www.idquantique.com) 18
Figure 1.5 - Stages of quantum information processing development. Extracted from Vadim's Makarov public slides (http://www.vad1.com/lab) 20

Figure 2.1 - One-way QKD protocol scheme. The arrow in the quantum channel. area indicates the flow on the quantum information 23
Figure 2.2 - Ping-pong protocol sketch. The original paper [2] considered opposite roles between the users 23
Figure 2.3 - Two-way QKD protocol scheme 24
Figure 2.4 - Two-layer QKD scheme extracted and redesigned from [3] 24

Figure 3.1 - Optical setup for implementation of the multi-service quantum network, the first two-layer QKD. PBS_n - polarizing beam splitters, D_n - single photon detectors, $R(\theta)$ - polarization rotator and ϕ_B - Bob's phase modulator..... 34
Figure 3.2 - Representation scheme of the one-way QKD protocol. BS_n - beam splitters and D_n - single photon detectors 37
Figure 3.3 - Scheme for two-layer one-way QKD. $R_n(\theta)$ are polarization rotator - D_n are single-photon detectors - C circulator and F filters 40
Figure 3.4 - Polarization scheme of Bob's incoming and outcoming pulses. ρ_α - coherent state and ρ_t - thermal state 41
Figure 3.5 - Proposed optical scheme for CT-DQPS-QKD.PBS - polarization beam splitter; R -polarization rotator; ϕ_B - Bob's phase modulator; C -optical circulator; F - optical filters with central frequency at 1550 nm; BS - beam splitter and D_{ij}, D_T, D_B^1 and D_B^2 - single-photon detectors. 43
Figure 3.6 - R_{sec}[bit/s](logarithmic scale) versus L for DQPS-QKD and two-layer DQPS-QKD..... 47
Figure 3.7 - Balanced homodyne detection scheme. $\hat{a}$ and $\hat{b}$ are BS inputs and $\hat{c}$ and $\hat{d}$ outputs connected to regular positive-intrinsic-negative diode(PIN) D_0 and D_1 48
Figure 3.8 - Scheme for two-layer QKD using homodyne detection 50

Figure 3.9 - Theoretical probability distribution of the quadrature amplitude for total phase shifts of 0°, 90°, 180° and 270° when the signal is in a coherent state. Red line indicates wrong choice of basis and green line, distinguishable lines used for coding 52

Figure 4.1 - Detailed description of a PMT's. Circular types follow the same structure 55
Figure 4.2 - Photocathode band models. (a) Metal-alkali type and (b) III-V compound semiconductor type 57
Figure 4.3 - Photocathodes classification types by emission process. Extracted from [4] 57
Figure 4.4 - Types of photocathode regarding the photogeneration 58
Figure 4.5 - Typical spectral response characteristics of the photocathodes 59
Figure 4.6 - PMT series H7422 with external cooler 60
Figure 4.7 - Cathode radiant sensitivity on the right and the gain on the left for the H7422 series. Bold lines indicate the module used in this work 60
Figure 4.8 - Setups for the investigation of backflash emission by PMT's 61
Figure 4.9 - Histograms of backflash emission by different experiments with PMT's and APD's in four different scenarios 62

Figure 5.1 - Encapsulated Silicon avalanche photodetector model..... 65
Figure 5.2 - Photocurrent generation within the standard semiconductor structure. Top layer: conduction layer and bottom layer: valence layer 67
Figure 5.3 - Photosensitivity expressed in therms of spectral range for several models of silicon avalanche photodetectors 68
figure 5.4 - SPCM module from Excelitas, model SPCM-AQRH with an encapsulated Si-APD attached 68
Figure 5.5 - SPCM module from Excelitas, model SPCM-AQRH with an encapsulated Si-APD attached 69
Figure 5.6 - Basic passive quenching circuits: (a) configuration swith current-mode output and (b) equivalent circuit of the current-mode output configuration. The avalanche signal is sensed by the comparator that produces a standard signal for the pulse counting and timing. Extracted from [5] 70

Figure 5.7 - (a) Principle of active quenching: current-voltage I-V characteristic curve of SPAD and switch load line (dashed lines) of the AQC controlled voltage source. The Q arrow denotes the quenching transition and the R arrow the reset transition. (b) Output pulses from AQC designed for minimum dead time that operates with a standard SPAD, biased 0.9 V above breakdown voltage, displayed on a fast resolution oscilloscope at 5 ns/*div*. Extracted from [5] 70
Figure 5.8 - Simplified diagrams of the basic AQC configurations with (a) opposite quenching and sensing terminals of the SPAD and (b) coincident quenching and sensing terminals. Voltage waveforms for both diagrams represent the circuit nodes marked with the same letter. Extracted from [5] 71
Figure 5.9 - Circuit diagram of the simplified reverse-engineered of PerkinElmer SPCM-AQR module. Nowadays, the PerkinElmer company was bought by Excelitas and adopted definitely the new name. Extracted from [6]. 72
Figure 5.10 - Setups for measurement of breakdown emission from Si-APD units. (a) Face-to-face fibered setup and (b) setup for distinct wavelength analysis 73
Figure 5.11 - Units count-rates verified during a i nterval of 5000 s 74
Figure 5.12 - Histograms of pair counts for setup in Figure 5.10a (a) with no delay line and (b) with 40 ns delay line. The peak difference in (b) is due to the darkcount of the units, which was at the time 352 *counts*/s for the DUT unit and 474 *counts*/s for the SPCM 75
Figure 5.13 - Monochromator design Model SP-555 from SpectraPro-750i series manufactured by Acton research corporation 77
Figure 5.14 - (a) Spectral backflash emission in green subtracted the darkcount and in black the efficiencies of the sensor and gratting combined. (b) the final spectrum 78
Figure 5.15 - Setup for measurement of the loss due to the back propagating light. 80
Figure 5.16 - Receiver model designed by INO working on 785 nm. Crystal structure within the model and light paths based on polarization state 80
Figure 5.17 - Experimental setup designed to measure the time correlation between backflash and reflected photons 82
Figure 5.18 - Histogram of timing resolution of clicks in Bob's DUT unit for two scenarios: with DUT On and Off 82
Figure 5.19 - Experimental setup to calculate time correlations between clicks on the DUT's and SPCM units 83

LIST OF TABLES

Table 3.1 - Bit assignment for homodyne detection 52

Table 4.1 - Statistical results for backflash experiments with PMT and APD units..... 63

Table 5.1 - Emission probability for the setup in Figure 5.10b. The calculation of the spectral filter probabilities, the photodetection efficiency used was 0.55 limited to a spectral range of $510 - 860$ nm 70

Table 5.2 - Extinction ratio of loss setup 81

Table 5.3 - Cross-click rate and extinction ratio of the attack 84

CONTENTS

1	**INTRODUCTION**	14
1.1	**A short story of cryptography**	14
1.2	**Quantum key distribution**	17
1.3	**Breakdown emission in photodetectors**	18
1.4	**Challenges in practical quantum key distribution**	19
1.5	**Contributions and summary**	20
2	**TWO-LAYER QKD**	22
2.1	**Introduction**	22
2.2	**Two-way QKD**	22
2.3	**Two-layer QKD**	25
2.3.1	***Security analysis***	28
2.3.2	***Distinguishability of quantum states of light using a single-photon detector and a spectrum analyser***	30
2.4	**Conclusion**	32
3	**OPTIMAL SCHEMES FOR TWO-LAYER QKD**	33
3.1	**Introduction**	33
3.2	**First two-layer QKD**	33
3.2.1	***Setup and protocol***	34
3.2.2	***Security analysis***	35
3.3	**Two-layer one-way QKD**	37
3.3.1	***One-way QKD***	37
3.3.2	***Setup and protocol***	40
3.4	**Two-layer coherent termal QKD**	42
3.4.1	***Setup and protocol***	43
3.4.2	***Security analysis***	44
3.5	**Two-layer QKD using homodyne detection**	47
3.5.1	***Homodyne detection***	48
3.5.2	***Setup and protocol***	50
3.5.3	***Security analysis***	52
3.6	**Conclusion**	53
4	**PHOTOMULTIPLIER TUBES**	54

4.1 **Introduction** 54
4.2 **Photoelectron emission in PMTs** 55
4.2.1 ***Radiant sensitivity*** 59
4.3 **Backflash emission** 59
4.3.1 ***Device under test (DUT)*** 59
4.3.2 ***Time analysis*** 60
4.4 **Conclusion** 63
5 **SILICON AVALANCHE PHOTODETECTOR** 64
5.1 **Introduction** 64
5.2 **Si-avalanche photodetector** 66
5.2.1 ***Avalanche active quenching regime*** 69
5.3 **Breakdown emission analysis** 72
5.3.1 ***Time analysis*** 74
5.3.2 ***Spectral analysis*** 76
5.4 **Eavesdropping experiments** 79
5.4.1 ***Loss analysis*** 79
5.4.2 ***Backflash photons time resolution*** 81
5.4.3 ***Eavesdropping attack*** 83
5.4.4 ***Theory*** 84
5.5 **Conclusion** 85
6 **CONCLUSION** 86
6.1 **Conclusions** 86
6.1.1 ***Two-layer QKD*** 86
6.1.2 ***Breakdown measurements and quantum cryptography*** 86
6.2 **Further investigation** 87
6.2.1 ***Two-layer QKD*** 87
6.2.2 ***Breakdown measurements and quantum cryptography*** 87
BIBLIOGRAPHY 88

1 INTRODUCTION

1.1 A short story of cryptography

Historically the problem of secure communication has disturbed many scientists in several research fields, not only engineers and physicists. A growing demand for the ability to secretly communicate has engaged much effort and a considerable amount of resources. It is immeasurable the importance of secrecy for high-level decisions in several sectors, like government, army and finances. To achieve that goal, cryptography is essential. It is well known that RSA, or classical cryptography, has been fairly dominant since 1977 [7,8]. Its reliability had been exhaustively verified and it is being used in all layers of society communication, from ordinary cell phones who access the phone bank or social media to military and governmental decisions.

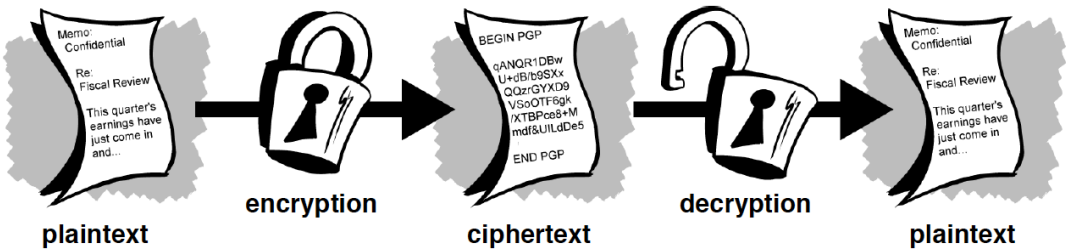
Cryptography is one of the oldest fields of technical study we can find records of, going back at least 4,000 years. It is considered as the art of using codes and ciphers to protect secrets after some mathematical operations. After the 20th century and the development of the industrial era, the pen and paper method could be replaced for something more automatized method [9], like the *enigma rotor machine* used in the second world war to communicate throughout the German battlefield [10].

Figure 1.1: Enigma rotor-machine used in world war II by the Nazi German army.

Data that can be read and understood without any special measures is called *plain text* or *cleartext*. The method of disguising plaintext is called *encryption*. Encrypting plain text results in an unreadable sequence of characters called *ciphertext*. You use encryption to ensure that information is hidden from anyone for whom it is not intended,

even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called *decryption*. The scheme in fig.1.2 shows the entire process.

Figure 1.2: Encryption and decryption scheme. Extracted from [1].



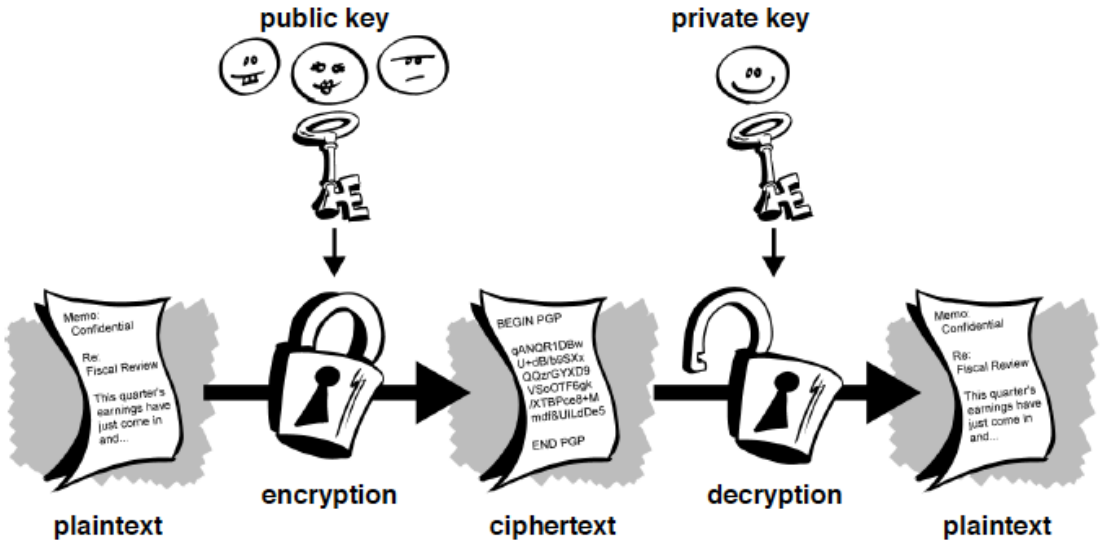
A *cryptographic algorithm*, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key - a word, number, or phrase - to encrypt the plaintext. The same plaintext encrypts to different ciphertexts with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Cryptography can be strong or weak, depending on some parameters. *Cryptographic strength* is measured in the time and resources it would require to recover the plaintext. The result of strong cryptography is a ciphertext that is very difficult to decipher without possession of the appropriate decoding key. How difficult? Given all of today's computing power and available time - even a billion computers doing a billion checks per second - it is not possible to decipher the result of strong cryptography in a reasonable time .

In conventional cryptography, also called symmetric-key, one common and unique key is used for encryption and decryption. It means that both parts of the communication have to posses the key to exchange messages. But there is a drawback, the key distribution. To solve this issue, the public key cryptography or asymmetric-key was proposed. It is a technique that uses a pair of correlated keys and one of them becomes public, which eliminates the need for a key transmission. For encryption, one of the keys, the *public key* is announced publicly for anyone who desires to send a message to this user. And the other key, called *the private key*, which only the user who created them posses, is used for decryption. It is computationally unfeasible to deduce the private key from the public key, given the fact that those keys are generated based on mathematical functions and prime numbers. So anyone who has a public key can encrypt information, but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information, as shown in fig.1.3.

The primary benefit of asymmetric key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples

Figure 1.3: Public key cryptography scheme. Extracted from [1].



of public-key cryptosystems are Elgamal (named after its inventor, Taher Elgamal [11]), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman 1977 [7,8]), Diffie-Hellman [12], and DSA, the Digital Signature Algorithm (invented by David Kravitz, a former NSA employee). Because conventional cryptography was once the only available means for relaying secret information, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks.

Albeit symmetric-key systems are simpler and faster, their main drawback is that the two parties must somehow exchange the key in a secure way. In order to communicate with one another confidentially, the sender and receiver must have exchanged a key using a secure channel before actually starting to communicate. Therefore spontaneous communication between individuals who have never met seems virtually impossible. If everyone wants to communicate with everyone else spontaneously at any time in a network of n subscribers, each subscriber must have previously exchanged a key with each of the other $n-1$ subscribers. A total of $n(n-1)/2$ keys must therefore be exchanged [13].

The most well-known symmetric encryption procedure is the DES-algorithm[14]. The DES- algorithm was developed by IBM in collaboration with the National Security Agency (NSA), and it was published as a standard in 1975. Despite the fact that the procedure is relatively old, no effective attack on it has yet been detected. The most effective way of attacking consists of testing (almost) all possible keys until the right one is found (brute-force-attack). Due to the relatively short key length of effectively 56 bits (64 bits, which, however include 8 parity bits), numerous encrypted messages using DES have been broken. Therefore, the procedure can now be considered only conditionally secure. Symmetric alternatives to the DES procedure include the IDEA and Triple DES algorithms, which are modified versions of the original DES.

Currently there is a large amount of research in this area: for example Murphy and Robshaw presented a paper at Crypto 2002 [15], which could dramatically improve cryptanalysis: the burden for a 128-bit key was estimated at about 2100 steps by describing AES as a special case of an algorithm called BES (Big Encryption System), which has an especially "round" structure. Even with that structure, the current status of the symmetric-key cryptography is consistent, but not unbreakable.

It is quite noteworthy that of all the cryptosystems developed in those 4,000 years of effort, most of them are still based on math. As soon as a powerful and operational device shows up, the entire communication security is threatened. It is an inevitability that cryptographers dread facing the arrival of powerful quantum computers, which breaks the security of the most reliable cartographic systems. Although these devices are thought to be a decade or more away, researchers are already in preparation.

Computer-security specialists are working and discussing quantum-resistant replacements for today's cryptographic systems everywhere - the protocols used to scramble and protect private information as it traverses the web and other digital networks. Although today's hackers can, and often do, steal private information by guessing passwords, impersonating authorized users or installing malicious software on computer networks, existing computers are unable to crack standard forms of encryption used to send sensitive data over the Internet.

But on the day that the first large quantum computer comes online, some widespread and crucial encryption methods will be rendered obsolete. Quantum computers exploit laws that govern subatomic particles, so they could easily defeat existing encryption methods. It is remarkable the advances in the quantum information processing field. Both quantum computation and quantum information are properly explored all over the world and it is already possible to see some prototypes. In therms of quantum communication, China, South-Korea, Japan and Switzerland have their own systems running 24/7 quantum protocols, with the premise of unbreakable security. Among the existing protocols, we enlight *quantum cryptography*, responsible to securely exchange cryptographic keys between authorized users. In the next section, the main subtopic of this field is briefly explained, *quantum key distribution*(QKD).

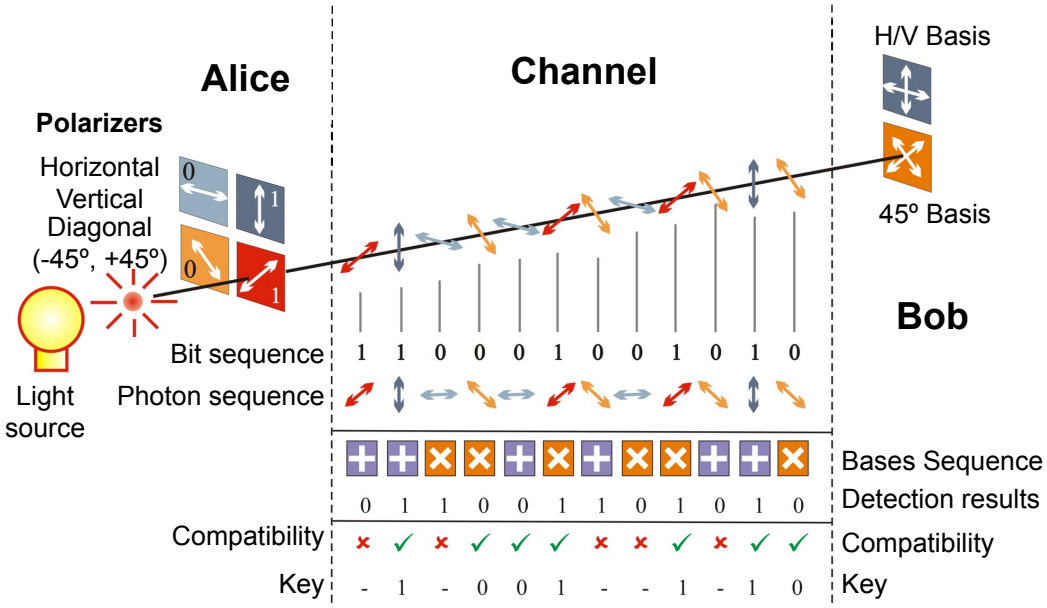
1.2 Quantum key distribution

Quantum cryptography exploits the fundamental laws of quantum mechanics to provide a secure way to exchange private information. Such an exchange requires a common random bit sequence, called a key, to be shared secretly between the sender and the receiver.

The basic idea behind quantum key distribution (QKD) has widely been understood as the property that any attempt to distinguish encoded quantum states causes a disturbance

in the signal. As a result, implementation of a QKD protocol involves an estimation of the experimental parameters influenced by the eavesdropper's intervention, which is achieved by randomly sampling the signal. If the estimation of many parameters with high precision is required, the portion of the signal that is sacrificed increases, thus decreasing the efficiency of the protocol.

Figure 1.4 - BB84 protocol explanation scheme. Picture redesigned from public documents in ID Quantique website (www.idquantique.com).



Here we explain the basis of a QKD protocol. In the mid-80s, Bennett and Brassard started the QKD era by releasing the first protocol, the BB84 [16]. The sender, Alice in most case scenarios, encodes a random bit sequence onto non-orthogonal quantum polarization states, say horizontal, vertical, diagonal and anti-diagonal, as in Figure 1.4. The receiver, Bob, randomly chooses a basis to measure the state. If the basis chosen by Bob and Alice agrees, the bit-value is correct. The agreement is made by public disclosure of basis choice. After a few steps of post-processing, the key is achieved.

The eavesdropper, usually called Eve, tries to intercept the information. Several attacks are well-established with their respective countermeasures. Nowadays, the systems are designed considering the QBER (quantum error rate) most of it linked to the eavesdropping. A few more words will be given about security in the next sections.

1.3 Breakdown emission in photodetectors

For a long time, avalanche photodiodes (APD) have been used for photodetection in a wide range of the emission spectrum. A few reasons are their high quantum efficiency and low dark count rate. These properties are particularly important for quantum cryptography [17–21], where the need for secure bits and a low signal/noise ratio is high.

To obtain a single photon counting behavior, the avalanche diode is operated in an all-or-nothing counting mode similar to the way Geiger detectors are used in nuclear physics for particle counting. In this so-called Geiger mode, the diode is reverse-biased above the breakdown voltage such that a single photoelectron can generate a self-sustaining discharge [22–24]. The discharge current is used as an indicator for the generation of a photoelectron and thus of an absorbed photon.

It has been known for a long time that avalanche of charge carriers in a few types of APDs is accompanied by photon emission. Here, we focus on Silicon APDs [25, 26]. First observations were reported by Newman [27]. Although this light emitted is not very strong, in several single photon counting applications, it may have serious impacts in terms of security [28]. In quantum cryptography, for example, such a light emission might enable an external observer to gain information about a photodetection event on the receiver side, opening a possible eavesdropping loophole to an otherwise secure communication channel. Another experimental situation in which this photoemission has to be considered are photon correlation measurements, as they are performed in single atom molecule spectroscopy.

It is therefore important to know the photoemission characteristics of this breakdown photoemission to avoid crosstalk with the light to be detected. In this work, we describe our investigation of the temporal and spectral distribution and our experimental results of an eavesdropping attack in Silicon APD based QKD systems.

1.4 Challenges in practical quantum key distribution

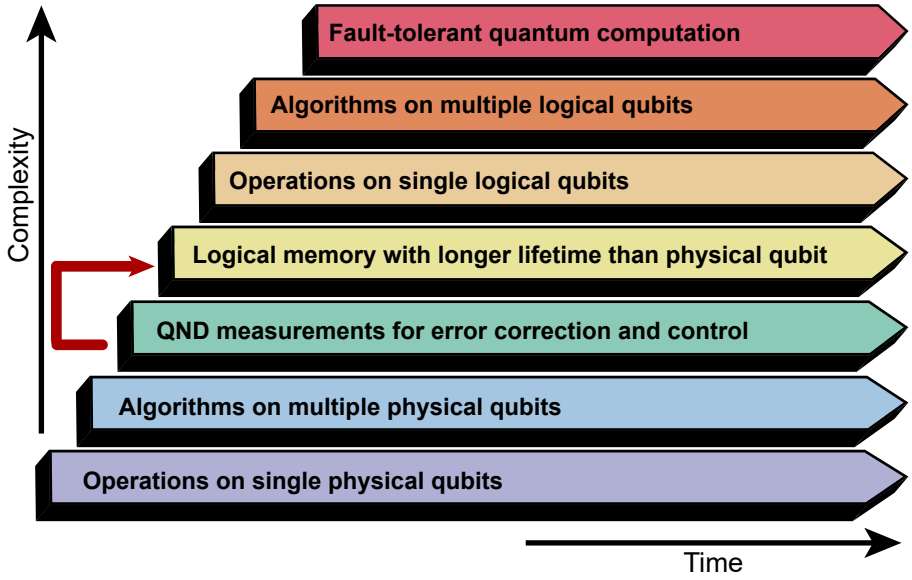
Quantum information processing systems follow a few steps before its consistent implementation and commercialization. Considering seven stages, each advancement requires mastery of the preceding stages, but also represents a continuing task that must be improved in parallel with the others.

The first two-stages are already well-established. Several experiments were conducted to perform local operations on single physical qubits to code and decode information. Also, a variety of algorithms are proposed to complement the single-qubit operations. A number of companies have released their commercial versions joining quantum and classical operations.

Superconducting qubits are the only-state implementation at the third stage, and they now aim at reaching the fourth stage (red arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

Based on Figure 1.5, it is quite clear that there is a long way ahead until we can see

Figure 1.5: Stages of quantum information processing development. Extracted from Makarov public slides (http://www.vad1.com/lab).



quantum computers widely used. Given the current technology development speed, next 5(five) decades are still needed for the full migration or a total unification of the classical and the quantum technology.

1.5 Contributions and summary

The contributions of this thesis are summarized in a number of journal and conference publications, categorized by chapter.

- **Chapter 1** - Introduction to this work with a useful concepts necessary for the understanding of the contents covered in the main body of the work.
- **Chapter 2** - Explains the Two-layer QKD framework proposed to enhance the security of a number of QKD protocols.
- **Chapter 3** - Proposal of optical setups using *Two-layer QKD*. Two publications released:

  * Two-layer One-way QKD (Oral) - presented in IV Workshop-school on Quantum Cryptography (WECIQ 2012), Fortaleza, Ce, Brazil.

  * Two-layer quantum Key distribution - Published in Quantum information processing magazine [3].

- **Chapter 4** - Experimental analysis of breakdown emission in PMTs (photomultiplier tubes).

- **Chapter 5** - Experimental verification of breakdown emission in Si-APDs and its importance in quantum cryptography scenario.

  * Measurements of light emission from silicon avalanche photodetectors (poster), presented at QCrypt 2015, Tokyo, Japan, September 28 - October 2, 2015.

  * Experimental verification of breakdown emission in Si-APD and it influence in quantum cryptography. To be published.

- **Chapter 6** - Final conclusions and future works.

2 TWO-LAYER QKD

Abstract

This chapter presents Two-Layer QKD, a framework designed to increase security of quantum key distribution protocols. Two-Layer is the combination of the two-way QKD, which is a well established protocol, with an additional security feature. The premise is to add an extra layer or security, turning almost all existing and consolidated protocols close to the unconditional security.

2.1 Introduction

In recent years, quantum key distribution has been extensively studied and improved. Several protocols were proposed: BB84 [16], Ekert-91 [29], B92 [30–32], SARG04 [33], continuous variable QKD [34], one-way QKD [35], decoy-state QKD [36], DPS- QKD [37–39] and MDI-QKD [40]. The security analysis of such protocols is not trivial. For example, a proof of security for DPS-QKD against any type of attack does not exist yet. Furthermore, it seems that all QKD protocols theoretically are secure; however, their experimental implementations are not. The reason is the real optical and optoelectronics devices do not behave exactly like their theoretical models in the security analysis of QKD protocols.

Several improvements in the QKD protocols had been released in attempt to increase security. However, almost none of them is capable to achieve complete security. Recently, a new step toward secure QKD with real devices, named two-layer QKD [41].

The idea behind the framework is to use an extra layer running on top of the QKD layer in any protocol. The first layer is the QKD protocol while the second layer is a two-state protocol whose purpose is exclusively to protect the first layer. In this chapter, fundamental concepts about the two-layer QKD protocol are presented starting by an overview of two-way QKD.

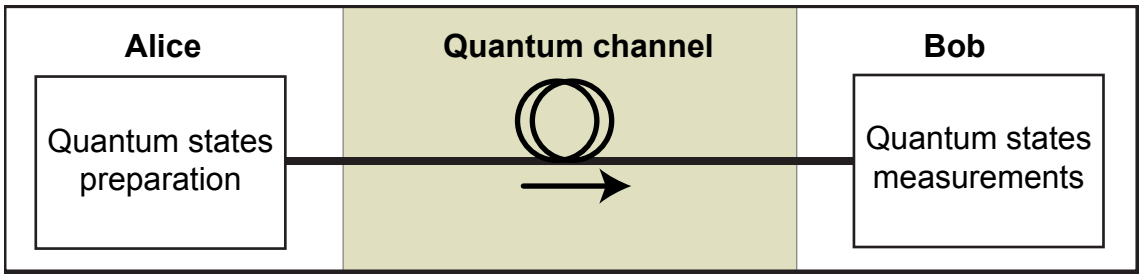
2.2 Two-way QKD

After the pioneering work of Bennett and Brassard published in 1984 [16], several alternatives for QKD protocols were proposed, mostly following the same classical premise: one member of communication is responsible for prepare and send the information bits for a second member, which role is measure and compare the received bits with the previous member [20, 29, 30, 37]. New types of protocols arose presenting different perspectives: using continuous variables Gaussian states [42], using homodyne detection [43], using time-bin coding [20], using phase coding [37, 38] and the new proposals, which also uses EPR pairs without detection device dependency, called *device-independent QKD* [40]. In

addition, for the majority of those protocols, versions with decoy states are also available to overcome security issues [36, 44, 45]

All protocols listed above follow the called *one-way* QKD model, i. e. the information between members of the communication travels in only one channel and follows only one direction [35]. As shown in Figure 2.1 the quantum states which are going to carry the information are prepared on Alice's side. After traveling through the quantum channel, the states ares measured on the Bob's side.

Figure 2.1: One-way QKD protocol scheme. The arrow in the quantum channel indicates the flow on the quantum information.



Alternatively, the *two-way* QKD protocol was proposed with a novel approach [46]. The paper considered the nickname "ping-pong" for the protocol, given that the information changed between the users perform a round-trip in the scheme. One of the main features is the ability to realize *deterministic communication*, what in the paper is called *instantaneous communication*; i. e. the information can be decoded during the transmission and an additional information exchange is unnecessary, avoiding lost of bits in post-processing steps. Despite the fact of compromising the security, the *two-way* uses two patch channels to communicate between the legitimate users. Figure 2.2 shows a sketch of the protocol with an overview in the next lines.

The initial proposal used EPR pairs. When two photons are maximally entangled in

Figure 2.2: Ping-pong protocol sketch. The original paper [2] considered opposite roles between the users.

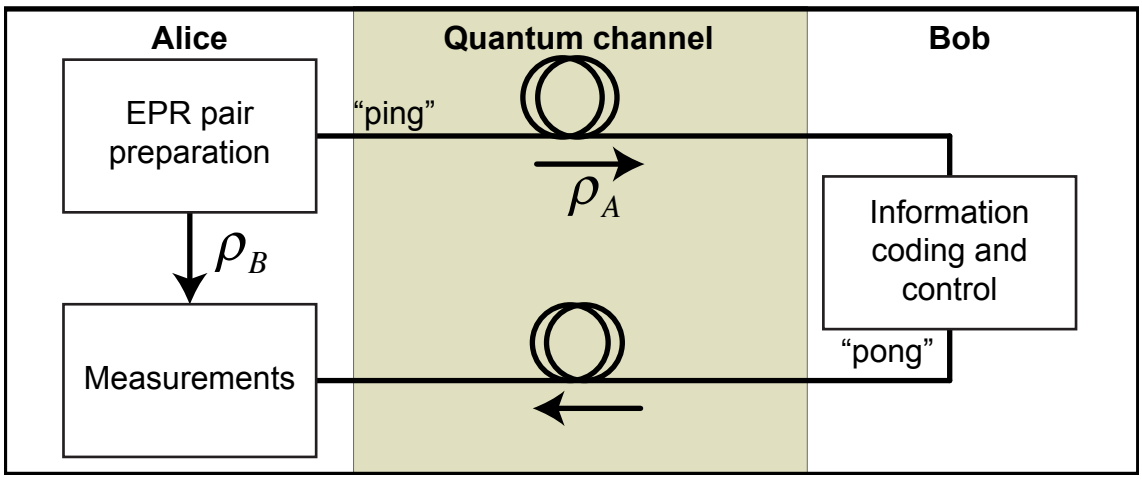
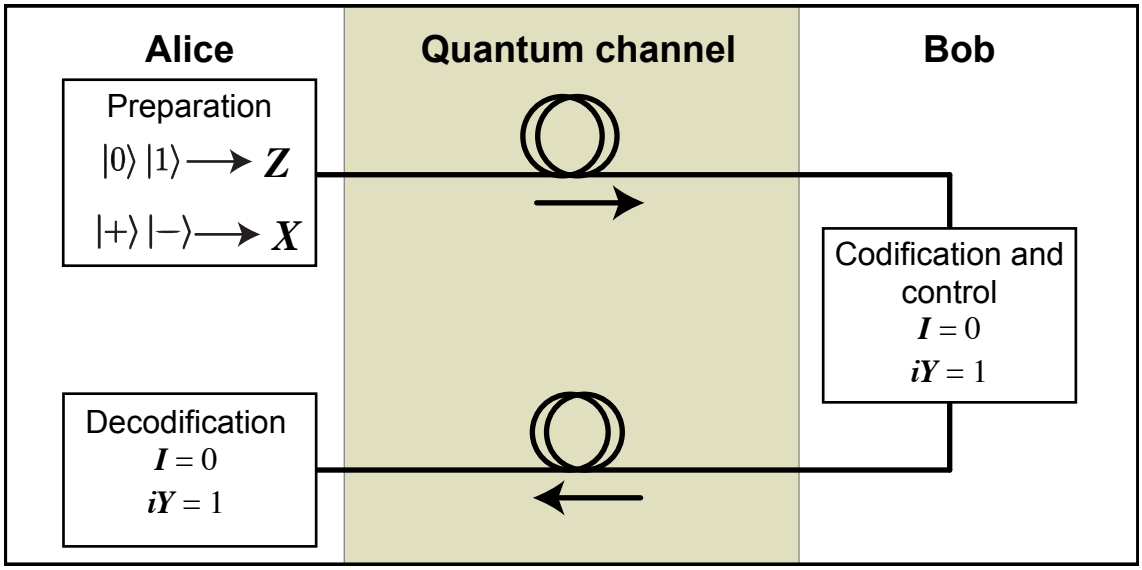


Figure 2.3: Two-way QKD protocol scheme.



their polarization degree of freedom, then each single photon is not polarized at all [46]. For instance, denote $|0\rangle$ and $|1\rangle$ as horizontal and vertical polarization states respectively, then the Bell states created are $|\Psi^{\pm}\rangle_{AB} = \left(1/\sqrt{2}\right)(|01\rangle \pm |10\rangle)$, maximally entangled states by nature in the two-particle Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. A measurement of the polarization of one photon, say A, leads to a complete random result. This is a reflected by the fact that the corresponding *reduced density matrices*, $\rho_A^{\pm} := Tr_B\{|\Psi^{\pm}\rangle\langle\Psi^{\pm}|\}$ are both equal to the complete mixture, $\rho_A^{\pm} = \frac{1}{2}\mathbb{1}_A$. Hence, no experiment performed in only one photon can distinguish between those states. However, since the states $|\Psi^{\pm}\rangle$ are mutually orthogonal, a measurement in *both* photons can perfectly distinguish the states from each other. In other words, one bit of information can be encoded in the states $|\Psi^{\pm}\rangle$, which is completely unavailable to anyone who has only access to one of the photons [2]. A simple verification can be achieved by considering the unitary operator

$$\hat{\sigma}_z^A \equiv (\hat{\sigma}_z \otimes \mathbb{1}) = (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes \mathbb{1}, \tag{2.1}$$

and applying to the states $|\Psi^{\pm}\rangle$. The bits flip and turn them into the opposite state. I.e.

$$\rho_A^{\pm}\left|\Psi^{\pm}\right\rangle = \left|\Psi^{\mp}\right\rangle. \tag{2.2}$$

The protocol is summarized as follows: Alice prepares a pair of photons entangled in Bell states $|\Psi^{\pm}\rangle = \left(1/\sqrt{2}\right)(|01\rangle \pm |10\rangle)$ and sends only one photon to Bob. Bob applies the local unitary operator in his photon and send it back to Alice. Performing Bell measurements on both photons, Alice is able to decode the message. In the original letter, Bob had also a *control mode* used to perform a local measurements and compare his results with Alice for possible eavesdropping attacks.

EPR pairs are useful in this case if someone who has access to only one single photon, can *encode* one bit of information, but cannot *decode* it, since no access to the other

photon is granted. Lately, the idea of the protocol using EPR pairs was abandoned due security issues [47, 48]. The approach using non-entangled states was then released [34] to mainly solve eavesdropping issues. The scheme of the *two-way* QKD protocol is shown in Figure 2.3. Alice prepares a qubit using one of the four states from two pairs of basis $\boldsymbol{Z}(|0\rangle$ and $|1\rangle)$ or $\boldsymbol{X}(|+\rangle$ and $|-\rangle)$ and sends to Bob. To re-code information, Bob has to decide whether apply or not the $\boldsymbol{i\hat{Y}}$ unitary operation in his qubit. Encoding is realized by following the transformations on the qubit states:

$$\begin{cases} \boldsymbol{i\hat{Y}}\left(|0\rangle, |1\rangle\right) = \left(-|1\rangle, |0\rangle\right) \\ \boldsymbol{i\hat{Y}}\left(|+\rangle, |-\rangle\right) = \left(|-\rangle, -|+\rangle\right). \end{cases} \tag{2.3}$$

The incoming states are completely unknown by Bob. Despite this he does not need to know them to perform the encoding. Alice, by its turn, can deterministically decode Bob's message by measuring the qubit in the same basis she prepared, without demanding extra classical information from public announcement [34]. The security of the protocol is considerably increased when no more information is publicly disclosed, like the basis or measurement results. Now, not only QKD keys can be exchanged, but the entire message without needs of extra steps of cryptography. Note that the control mode in Bob remains present to increase security.

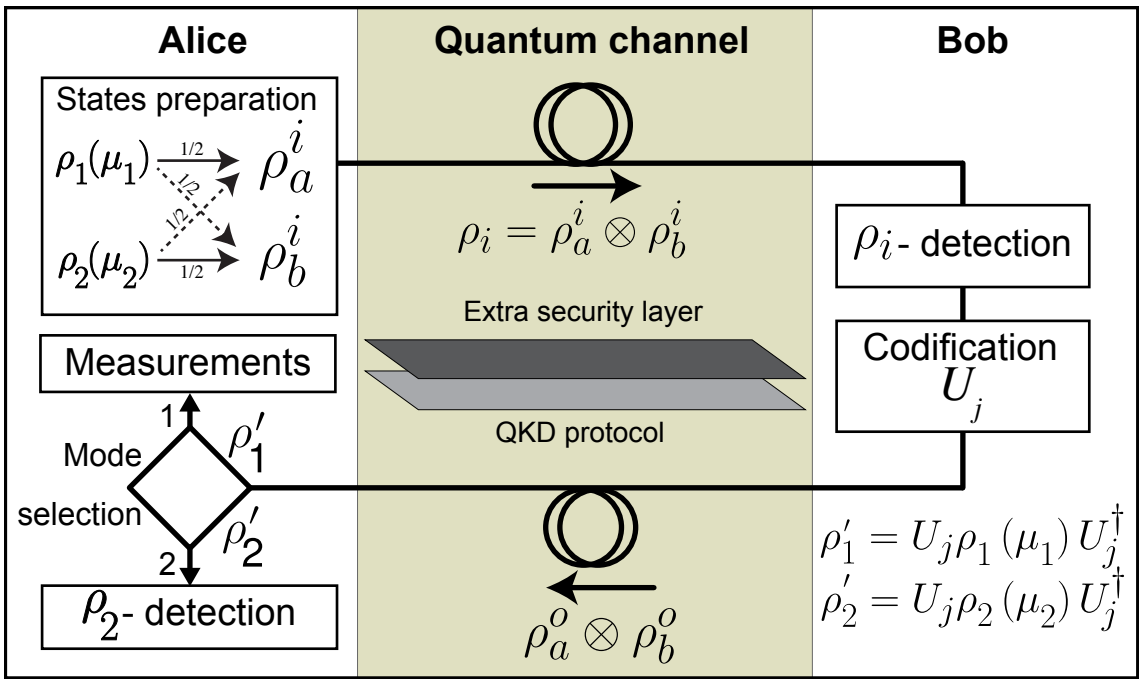
The redesigned protocol is then presented in the next section, created to increase efficiency and security, but keeping important features of the original protocol, like speed and reliability.

2.3 Two-layer QKD

Recently, Mendonça proposed a quantum multitask protocol[41]. A system able to integrate several quantum protocols, like quantum secret sharing (QSC), quantum secure direct communication (QSDC) and the most consolidated quantum key distribution (QKD). So far in the paper, the expression *two-layer QKD* was not employed. It is quite notable the origin of the name regarding the addition of an extra security resource to the framework. Here, we named this framework as *two-layer QKD*. Here we present a modification of the original *two-way* protocol with some security improvements. Numerous are the advantages to have in only one optical setup the ability to run such protocols, but it also arises security and reliability concerns. In this direction, coherent and thermal sources are used in a clever way to increase the level of security. We also explore the potential of this combination and, attached to *two-way* model, redesign some of the QKD protocols to add an extra layer of security.

Regarding QSC and QDSC, the Figure 2.3 is easily adapted into Figure 2.4 to run those protocols. As the focus of this work is devoted to QKD protocols; so for further details on how to use the scheme to run other protocols, please check [41]. Similarly to the conventional two-way, Alice is responsible to prepare and measure the qubits used in

Figure 2.4: Two-layer QKD scheme extracted and redesigned from [3].



the communication. Two light-sources are used and the produced light is sent into two optical modes, say time interval, spatial or polarization modes. Only one of the two light sources is used for QKD, so the task of the receiver is to discriminate between the states possessing only one sample per time. In order to distinguish with small error rate possible, the best strategy is to use unambiguous discriminator measurement scheme (section 2.3.2). However, as stated in [49], it is a common misconception that the unambiguous discrimination (UD) of *mixed states* is impossible. Indeed, it is impossible for all *orthogonal* mixed states ensemble, but there exist sets of *nonorthogonal* mixed states for which UD is possible. The critical feature of such sets is that their elements do not have identical support[1]. In fact, all that is required for a nonzero probability of error-free discrimination is that one of the density operators have a nonzero overlap with the intersection of the kernels[2] of the others. In other word, for those states who has a null kernel, the error-free discrimination fails [50, 51]. To enlight the previous statement, consider an ordinary vector $\vec{x}$ and the product $\rho_t \cdot \vec{x} = 0$. For the result to be valid, $\vec{x} = 0$. What means that the ρ_2 density matrix has a null kernel due its diagonal type matrix nature. On the other hand, given ρ_1 and ρ_2 as two different quantum states, the statistics of a large number of measurements of each state will certainly disagree, making the distinguishability possible.

So far, as the discrimination mechanisms is enlightened, the remain sequence of the protocol will be discussed. The scheme shown in Figure 2.4 represents a scheme suitable for any adaptation of a two-way QKD protocol. The light produced by both sources, $\rho_1(\mu_1)$ and $\rho_2(\mu_2)$, is directed to any of two optical modes $a(b)$ with probability of 1/2,

[1]The *support* of a mixed state is the space spanned by its eigenvectors with nonzero eigenvalues.
[2]The *kernel* is the space orthogonal to its support.

as show in Alice top part of Figure 2.4. Here, only the state ρ_1 is used in the QKD protocol. In the forward path of the quantum channel, the propagating state has the form of $\rho_i = \rho_a^i \otimes \rho_b^i = 1/2\left[\rho_1\left(\mu_1\right) \otimes \rho_2\left(\mu_2\right)\right]_{ab} + 1/2\left[\rho_2\left(\mu_2\right) \otimes \rho_1\left(\mu_1\right)\right]_{ab}$. The superscript i index indicates the Bob's input state. In Bob's setup, to ensure security, a previous measurement is performed before the coding. The type of measurement is adjusted by the eavesdropping attacks to avoid. But mainly ρ_i-detection consists in a scheme for detection of $\rho_i = \rho_{1(2)} \otimes \rho_{2(1)}$ to countermeasure trojan horse attacks, where an eavesdropper injects into the receiver a different quantum state than the signal and captures back after its output to check which unitary operation was performed on that state. The next section presents optical schemes with different arrangements for Bob's setup and his attacks prevention measures. Bob then modulates both states with the same information j and sends back to Alice the states $\rho_a^o \otimes \rho_b^o = U_j \rho_a^i U_j^\dagger \otimes U_j \rho_b^i U_j^\dagger$. Once the states are back in Alice, as she knows the modes corresponding to each state, she splits them into two different paths. The path 1, corresponding to $\rho_1^{'} = U_j \rho_1 \left(\mu_1^{'}\right) U_j^\dagger$ leads the states to the QKD measurement apparatus, where the key is generated. The path 2, $\rho_2^{'} = U_j \rho_2 \left(\mu_2^{'}\right) U_j^\dagger$, has the role of certifying the authenticity of $\rho_2^{'}$. In case of non-expected results in this stage, it is a clear signal of a possible eavesdropping attack.

Here, $\mu_1 \neq \mu_1^{'}$ and $\mu_2 \neq \mu_2^{'}$ due the loss in the quantum channel and the ρ_i-detection stage. However, this is not a problem, as it will be shown later Alice can infer the values of $\mu_{1(2)}^{'}$ by knowing the previous values and loss in the channels. The usage of a second quantum state of light in this framework has several advantages, whether some conditions can be followed:

1. Eve can not distinguish between ρ_1 and ρ_2
2. Alice can distinguish between large sets of samples of ρ_1 and ρ_2.
3. The state ρ_2 can not carry any useful information from Bob.

The items 1 and 2 can be satisfied if the conditions $\rho_1 \neq \rho_2$ and the non-orthogonality are followed. The item 3 is also satisfied if $U_j \rho_2 U_j^\dagger = \rho_2$. Another useful approach to check distinguishability is to make use of distance measurements. In general, a distance measure quantifies the extent to which two quantum states behave in the same way. While these distance measures are usually given by certain mathematical expressions, they often possess a simple operational meaning, i.e., they are related to the problem of distinguishing two systems. Two quantum states ρ_1 and ρ_2 can be distinguished by a measuring process and with a single measurement if the distance between them is D_{max}. On the other hand, if $D\left(\rho_1, \rho_2\right) = D_{min}$, the states are not distinguishable. Between D_{max} and D_{min}, the states can be distinguishable if there is a large set of samples of at least one of the states. The lower the value of distance is the number of samples are required. Considering the distance measure D and the Figure 2.4, the formalism of secure communication states that

some conditions must be satisfied, otherwise the security is not reached. The conditions are

$$D(\rho_1, \rho_2) = \epsilon, \quad D_{min} < \epsilon << D_{max} \tag{2.4}$$

$$D\left(U_j \rho_1 U_j^\dagger, U_j \rho_2 U_j^\dagger\right) = \epsilon, j = 0, 1 \tag{2.5}$$

$$D\left(\rho_2, U_j \rho_2 U_j^\dagger\right) = D(\rho_2, \rho_2) = D_{min}, j = 0, 1 \tag{2.6}$$

$$\rho_2 \vec{x} = \vec{0} \Rightarrow \vec{x} = \vec{0}. \tag{2.7}$$

Equation (2.4) states that it is possible to distinguish from two large sets of samples of ρ_1 and ρ_2. Since Eve is forced to make individual attacks (without previous knowledge about the mode of the states), she has to try to distinguish between ρ_1 and ρ_2 using only one sample of each state. In this case, the best strategy is to apply unambiguous discrimination; however, as stated in Equation (2.7), ρ_2 has null kernel, what makes the attack unsuccessful. Since the discrimination between ρ_1 and ρ_2 is not perfect, Eve will never be sure about the state she is attacking. This point is crucial for the security improvements of a QKD system protected by the two-state protocol. Equation (2.5) shows that, after Bob's codification, the distinguishability between the states does not change, i. e. $D(\rho_a^o, \rho_b^o) = D(\rho_a^i, \rho_b^i)$. Equation (2.6) states that any operation applied in ρ_2 by Bob will not change the distance or the state itself, as the useful information is carried by ρ_1.

Since Alice is always able to separate the modes correctly, the state ρ_2 will never be at output 1 and, hence, it will not cause errors in the QKD protocol. Simultaneously, the state ρ_1 will never be at output 2 and, hence, it will not cause errors in the ρ_2 detection scheme. The case where the states are exchanged or the ρ_2-detection are in disagree, an eavesdropping attack should be considered.

2.3.1 Security analysis

Since the proposal of the first quantum key distribution (QKD) protocol, named BB84 in tribute to its creators, many others protocols were developed successfully in order to improve the previous performance or security. And nowadays, security has attracted a crescent attention on development and enhancement. Basically for each QKD protocol stated, security is one of the main issues and usually demands a quite long time of investigation. The methodology mostly used is simple: based on previous attack's strategies, loopholes for these protocols are searched and, when found, proof-of-principle setups are designed and a theoretical security analysis is developed. We started this analysis by checking which are the strategies that can be adopted by an eavesdropper for the two-layer QKD. The purpose here is to make assumptions for a further, improved and experimental investigation.

Eve's goal is to determine which U_j was used by Bob without causing any error in Alice and Bob. Here the discussion is based on four kinds of attacks named I, II, III and IV. In the type I attack, Eve attacks the states in Bob's output. Considering a general strategy of attack, after Eve's action, the quantum states arriving at Alice's place are

$$\rho_3^j \otimes \rho_4^j = E\left(U_j \rho_a^i U_j^\dagger\right) \otimes E\left(U_j \rho_2 U_j^\dagger\right). \tag{2.8}$$

In (2.8) E is the operator that models Eve's attack. During Alice's mode separation (on average) half of the time ρ_3^j will be at output 1 and ρ_4^j at output 2 and vice-versa. Therefore, the quantum states at Alice's output 1 and 2 are

$$\left(\frac{1}{2}\rho_3^j + \frac{1}{2}\rho_4^j\right)_1 \otimes \left(\frac{1}{2}\rho_3^j + \frac{1}{2}\rho_4^j\right)_2. \tag{2.9}$$

In order to avoid errors in Alice, the following conditions on ρ_3^j and ρ_4^j must be satisfied

$$D\left(\frac{1}{2}\rho_3^j + \frac{1}{2}\rho_4^j, U_j \rho_1 U_j^\dagger\right) = D_{min}, \tag{2.10}$$

$$D\left(\frac{1}{2}\rho_3^j + \frac{1}{2}\rho_4^j, U_j \rho_2 U_j^\dagger\right) = D\left(\frac{1}{2}\rho_3^j + \frac{1}{2}\rho_4^j, \rho_2\right) = D_{min}. \tag{2.11}$$

In other words, the state in (2.9) must be indistinguishable of the state sent by Bob. If condition (2.10) is not true, there will be errors in the QKD protocol. If condition (2.11) is not obeyed errors in the two-state protocol should arrise. However, the conditions (2.10) and (2.11) cannot be simultaneously satisfied, they imply $D\left(U_j \rho_1 U_j^\dagger, U_j \rho_2 U_j^\dagger\right) = D_{min}$ that is not in accordance with (2.5). In this case there will be errors in both protocols.

In the type II attack, Eve tries to identify the state's mode before Bob's operations. I. e. Eve tries to distinguish between ρ_1 and ρ_2. Once ρ_1 was identified, attacks of the type I are applied exclusively on it. However, due to (2.4) Eve cannot realize that, taking each state individually, without errors or without a degree of uncertainty. As explained before, the best strategy to Eve would be to apply an unambiguous discrimination.

In the type III attack, Eve applies a Trojan horse attack. She stores in a quantum memory the states sent by Alice, prepares her own states, in general quantum states different from those used by Alice, and sends them to Bob. At Bob's output, Eve recovers the states and measure them aiming to obtain some information about the quantum operation realized by Bob. After that, according to the results of her measurements, Eve applies an unitary operation in both states sent by Alice and sends them back to Alice. In order to prevent this attack, as can be seen in Fig. 2.4, Bob uses a detector that informs if the states processed by him are compatible with the states sent by Alice. The crucial point here is the parameter μ whose value is known only by Alice. At the end of the quantum communication Alice publicly announces the values of μ used for ρ_1 and ρ_2, and Bob checks if his measurement results are in accordance with those. Since Eve does not know μ_1 and μ_2 she will have to guess which quantum states to use in order to realize

the attack without causing an alert signal in Bob. Since μ is a continuous variable, this task can be very challenging. Without changing the quantum state processed by Bob, the type III attack is not useful.

In type IV attack, Eve tries to control Alice's measurement setup by sending a different quantum state from ρ_1, say ρ_E. However, since Eve does not know in which mode ρ_1 is, sometimes the quantum state ρ_E will be at output 2, hence, being measured by the scheme able to identify ρ_2 causing errors and informing Eve's presence.

Summarizing, attacks type I, II and IV will always cause errors in Alice while type III will cause errors in Bob. Furthermore, Eve will not be sure about the bit values obtained in her attacks because she does not know between ρ_1 or ρ_2 (type I and II attacks) the state of the attack, she cannot change the quantum states sent to Bob (type III) and she cannot to control externally the bit value received by Alice (type IV).

2.3.2 Distinguishability of quantum states of light using a single-photon detector and a spectrum analyzer

The state of a quantum system is a mysterious object and had been subjected of too much attention since the earlier days of quantum theory. We know that it provides a way of calculating the observed statistical properties of any desired observable which is not, itself, observable. This means that we cannot determine by observation the state of any single physical system. If we have some prior information, however we may be able to use this to determine, at least to some extent, the state of a particular system. Consider, for example, a single photon that we know has been prepared with either horizontal or vertical polarization. A suitable oriented polarizing beam splitter can be used to transmit the photon if it is vertically polarized and reflect it if its polarization is horizontal. Determining the path of the photon by absorbing it with a suitable detector can certainly determine the state as one of horizontal or vertical polarization[52].

The distinguishability between quantum states of light is a challenging task. One attempt to overcome the issues is to check the electrical power of the signal produced by a threshold single photon detector (TSPD) using a spectrum analyser [53]. It was verified that for coherent and thermal states with low and equal mean photon number, they can be perfectly distinguished using a large number of samples. The reason is that there is fixed proportionality factor when the measurements are made in a fixed spectral band, which is $(P - P^2)$, where P is the probability of having a detection in the SPD. By checking Equations (2.15) and (2.16), we can also verify that for the states with the same mean photon number, $\mu_t = |\alpha|^2$ as they are different equations, the electrical power measured will be different, or $(P_c > P_t)$.

The initial proposal is to use coherent and thermal light states, as the first one is used in most real implementations and the second one has an important property which are going to be explained later. But here only the coherent state is used for QKD and the

thermal state used to increase security. Beforehand, a quick remind about the states used is given below. The coherent and thermal states are respectively represented by:

$$\rho_\alpha = |\alpha\rangle \langle\alpha| , \qquad |\alpha\rangle = \sum_{n=0}^{\infty} \exp\left(-\frac{|\alpha|^2}{2}\right) \frac{\alpha^n}{\sqrt{n!}} |n\rangle , \tag{2.12}$$

$$\rho_t = \sum_{n}^{\infty} \frac{\mu_t^n}{(1+\mu_t)^{1+n}} |n\rangle \langle n|. \tag{2.13}$$

Equations (2.12) and (2.13) are the representation in terms of density matrix of the coherent and thermal states respectively. Their overlap is given by

$$\langle\alpha| \rho_t |\alpha\rangle = \frac{\exp\left(-\frac{|\alpha|^2}{1+\mu_t}\right)}{(1+\mu_t)}. \tag{2.14}$$

Since they are not orthogonal for finite values of their mean photon numbers (μ_t and $|\alpha|^2$), the distinguishability can not be achieved [3]. Considering a particular case, if $\mu_t = |\alpha|^2$ then the lower the mean photon number is, smaller is the distinguishability. However, they can be distinguished considering they are not null and there is a large enough number of available samples of at least one of them. The task is relatively simple using a threshold single-photon detector (TSPD). Below, Equations. (2.15) and (2.16) state the distribution probability for the coherent and thermal states regardless the afterpulsing, respectively

$$P_c = 1 - \exp\left(-\eta|\alpha|^2\right)(1-p_d) , \tag{2.15}$$

$$P_t = 1 - \frac{1}{1+\eta\mu_t}(1-p_d) , \tag{2.16}$$

where η is the single-photon detector(SPD) efficiency and p_d is the darkcount probability.

Using a spectrum analyzer to measure, in a fixed frequency band, the electrical power of the signal produced by a threshold single-photon detector, a large sample of thermal states can be distinguished of a large sample of coherent states. The reason is because the electrical power in a fixed band is proportional to $(P - P^2)$ where P is the probability of an avalanche to be fired [53]. Since $|\alpha^2|$ and μ_t are chosen such that the probabilities in (2.15) and (2.16) are different (but still keeping the condition (2.4) satisfied), the electrical powers measured will also be different. Applying this strategy, Alice and Bob can check if the quantum states they are receiving are in fact those they were expecting to receive. Considering the two-layer QKD protocol here discussed, in general any other quantum state having the vacuum probability different from the vacuum probability of the thermal state can be distinguished from the thermal state if a sufficient larger number of samples are provided.

Considering the usage of the quantum light discriminator using a threshold single-photon detector and a spectrum analyzer in the two-layer QKD protocol, once Alice choose the value of μ_t, knowing the losses in the optical channel, she can infer the optical power she

will measure in a given frequency band. If she measures something different from expected, she aborts the key distribution. Hence, any Eve's attack that changes the electrical power measured by Alice will denounce her presence. That is the reason why type I, II and IV attacks cannot be used: they somehow modify the quantum states arriving at Alice's output 2 and the quantum state measured by a quantum light discriminator, composed by a single-photon detector and a spectrum analyzer.

A similar quantum light discriminator is also used by Bob. The goal is to avoid type III attack. For example, Eve could stop the coherent and thermal states sent by Alice, to keep them in a quantum memory and send two single-photons to Bob, say $|1\rangle |1\rangle$. After Bob's modulation, at Bob's output, Eve gets two photons with the same information. However, the usage of the states $|1\rangle |1\rangle$ instead of $\rho_\alpha \otimes \rho_t$ will result in an electrical power (measured by the spectral analyzer) different from that one expected by Bob.

2.4 Conclusion

Quantum key distribution is still a quite new research topic. Numerous are the protocols proposed, implemented and have their security analyzed. Regarding security of QKD protocols, there is a non-negligible number of eavesdropping attacks. So, every new proposal in this field is quite challenging.

Here, the *two-layer* framework used for QKD systems was discussed. We presented an alternative to the usual security methods. It promises to highly increase the security by using a second quantum state of light as a shield protection layer over the QKD protocol layer. Also, a brief security analysis was performed. The intention with this preliminary security section is to rise the community interest to improve the analysis, either theoretically and experimentally. We also want to avoid misleading between the two-way and two-layer terminology. The first one is a very known QKD protocol and the second is a modification that runs over the protocol.

3 OPTICAL SCHEMES FOR TWO-LAYER QKD

Abstract

Several protocols for QKD were proposed over the last decades. Using different approaches, like discrete variables, continuous variables [54, 55], polarization states, phase states, one-way QKD [20,35], two-way QKD [3,41,56], using decoy states [36] and even with device independent [40], most of them still suffer from security issues. Recently, a new proposal have attracted attention due its promise of increasing security and the adaptability to another protocols, the Two-layer QKD [3], explained in the previous chapter of this work. Here, we propose a number of optical setups using existing QKD protocols with the advantage of the two-layer QKD framework. The new protocols are: two-layer one-way QKD, two-layer CT-DQPS QKD and two-layer QKD using homodyne detection.

3.1 Introduction

Security of the QKD protocols still demands a high effort and massive resources from the scientific community. For instance, as the quantum technology is still in the beginnings, most of the protocols still do not have a full security analysis. I.e. a complete proof of security against all attacks. It is notable that even with all theoreticians attempting to prove the unconditional security of the QKD protocols, the experimental implementations are far from the equations. The reason is, among other issues, the real optical and optoelectronics devices do not follow perfectly their theoretical models stated in the security analysis of QKD protocols. In this thesis, we propose a new step toward secure QKD with real devices, a framework named two-layer QKD. The major contribution of the proposal is to add an extra layer of security that, using randomness states adjustments, fundamentally increases the security to a top level. By using the framework, it is possible to redesign some of the most promising QKD protocols to use the advantages of an extra-layer of security.

This chapter proposes three new QKD protocols using of the two-layer QKD framework, two-layer one-way QKD, two-layer CT-DQPS QKD and two-layer QKD using homodyne detection. The protocols are explained respectively.

3.2 First two-layer QKD

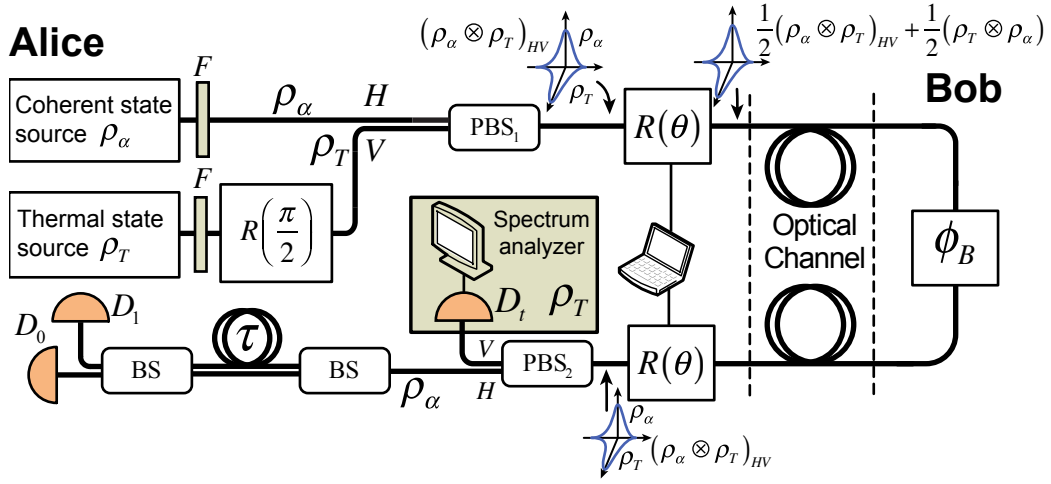
The idea of two-layer QKD is not being proposed in this work. It was released a few year ago [41]. The initial proposal is to use it as a setup for quantum multi-service network, where several quantum communication protocols could run using the same apparatus. It is highly advantageous if the same optical setup can be used for running different quantum protocols, as resources are always limited. The optical scheme revisited here can be used

for quantum key distribution (QKD), quantum secure direct communication (QSDC) and quantum secret sharing (QSS). Additionally, it is per se resistant to some eavedropping strategies, as the attack based on single-photon detector blinding.

3.2.1 Setup and protocol

The proposed optical scheme is shown in Figure 3.1. The use of thermal states protectS the coherent states emitted by Alice and phase modulated by Bob. Basically, Alice produces optical pulses with coherent states at the horizontal mode and thermal states at the vertical mode, both of them having the same (low) mean photon number to avoid PNS attacks. Note that is not necessary any synchronism or coherence between the sources except for time. Both states have to enter the setup at the same time. Following the sources, filters keep the spectral range limited to ensure security. After the thermal state source, a $\pi/2$ rotator ensures the vertical mode to the state. Alice then, randomly, sets her polarization rotator $R(\theta)$ in 0 or $\pi/2$. Thus, for each optical pulse at Alice's output, the quantum state entering the optical channel is $1/2(\rho_\alpha \otimes \rho_t)HV + 1/2(\rho_t \otimes \rho_\alpha)HV$. Bob, by its turn, has a polarization insensitive phase modulator [57]. Bob's phase modulation does not change the thermal state but it adds the phase ϕ_B to the coherent state. Leaving Bob's place, the optical pulses are sent back to Alice.

Figure 3.1: Optical setup for implementation of the multi-service quantum network, the first two-layer QKD. PBS$_n$ - polarizing beam splitters, D$_n$ - single photon detectors, $R(\theta)$ - polarization rotator and ϕ_B - Bob's phase modulator.



For each pulse returning to Alice's setup, she applies the same polarization rotation she had applied when the pulse was leaving her place. Thus, before PBS_2, all pulses will have the coherent state at H-mode and thermal state at V-mode. These modes are separated by PBS_2 and the thermal state at the V-mode is monitored by a single-photon detector plugged to a spectrum analyzer, which role is to measure the electrical power in a fixed spectral band. On the other hand, the coherent state at H-mode is sent to a

fiber interferometer whose time difference between upper and lower arms, τ, is equal to the time separation between two consecutive pulses.

The codification part in Alice, after the PBS_2 following the horizontal path, is the implementation of the differential phase shift QKD (DPS-QKD) [19, 37, 38, 58, 59]. The protocol can be readily implemented if Bob and Alice play the opposite roles as happens in traditional DPS-QKD. Thus, Bob modulates randomly each pulse that arrives at his place applying the phases 0 or $\pi/2$. Alice, by its turn, has the interferometer placed at the coherent state output. The protocol rules are the same as in the original work. In experimental implementation, it is quite noticeable the need of polarization control to keep the states in the correct polarization all the time. So, for future implementations, polarization controllers have to be added to the system.

One important aspect of releasing new QKD protocols or modification of existing ones is the security analysis. Here we attempt to give a preliminary analysis, which may be used to most common attack strategies.

3.2.2 Security analysis

The security of the proposed optical setup can be explained as follows. Alice has two secrets: the mean photon number and the polarization rotation angles applied. During the communication, only one mean photon number value is used. As explained before, the coherent and thermal states with the same mean photon number can be distinguished if one has a large number of samples. With the setup shown in Figure 3.1, only Alice can have a large amount of samples (pulses) because she is the only one able to separate with 100% of certainty the coherent and thermal states. Thus, Alice knows exactly the electrical power value she has to measure at the thermal state output. If she measures a different value, two possible reasons are: or the thermal state changed to another type of quantum state or the mean photon number was altered.

In order to gain some information, the eavesdropper can attack the coherent state after Bob's phase modulation. However, Eve does not know which polarization mode to attack, so, she has to attack both modes. In the intercept-resend attack, having only one pulse to make correctly the distinguishability, sometimes the eavesdropper will be confused and, during the state reconstruction, with some probability (depending on the method used to determine in which mode is the coherent state), she may change ρ_α and ρ_t positions. In this case, Alice will receive some coherent states at the thermal state output and some thermal states at the coherent state output. The attack is detected because the electrical power value measured at thermal state output will be different from the expected value. Moreover, the thermal state at coherent state output will increase the error rate of the quantum communication protocol.

Considering the photon number splitting (PNS) attack, Eve will have to count the photon number of both modes. If each mode has at least two photons, a single-photon

from each mode can be captured and the rest of the photons are sent to Alice through a loss-less fibre. If at least one of the modes has only one or zero photons, the optical pulse is absorbed and a vacuum state is sent to Alice. As can be seen, in this attack Eve's action does not cause the appearance of coherent states at the thermal output, but it changes the photon number distribution of the pulses arriving at the single-photon detector at thermal output and, hence, the electrical power value measured at thermal state output once more will be different from the expected value. To see this clearly, let $p^{\alpha}_{0(1)}$ and $p^{t}_{0(1)}$ be, respectively, the probabilities of the coherent and thermal states sent by Alice having zero (one) photon. Thus, the quantum state of the light arriving at Alice's place in the V-mode is, approximately, $(1-q)\left|0\right\rangle\left\langle 0\right| + q\left|1\right\rangle\left\langle 1\right|$, where $q = [1-p^{\alpha}_{0}-p^{\alpha}_{1}]\dot{[}1-p^{t}_{0}-p^{t}_{1}]$. As can be noted, for simplification, the situations where the pulses sent by Alice have more than two photons were not considered since the mean photon number used is much lower than 1. Thus, the probability of detection caused by that state is $1-(1-q\eta)(1-p_d)$. In order to do not disturb the electrical power value measured by Alice, the condition $1-(1-q\eta)(1-p_d) = 1-(1-p_d)/(1+\eta\mu_t)$ must be obeyed. However, for $\mu_t < 10$ this condition is never satisfied for any value of η, hence the PNS attack will cause an error in Alice.

Considering the beam splitter attack, it can be realized without disturbing Alice's measurement if the beam splitter used has reflectivity equal to the channel loss and Eve provides a loss-less channel between her and Bob's setup. However, since Eve cannot attack all pulses, the amount of information obtained by Eve is limited. As happens in the PNS attack, she has to obtain at least one photon from each mode.

At last, the optical setup shown in Figure 3.1 is naturally resistant to attacks in which the single-photon detectors are externally controlled [21, 60–63]. If Eve tries to control Alice's single-photon detectors, the strong light used will change the electrical power measured at the thermal state output, announcing the attack.

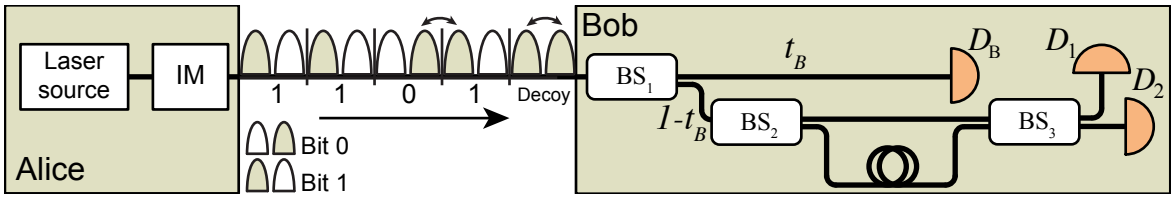
For all attacks discussed the main concern is only with the probability of Eve to cause an alert signal in Alice by changing the electrical power value measured. However, even when this is not the case, She still has a hard problem to solve: which mode (H or V) contains the useful information. So, she has to measure both modes and try to find out where is the useful information. For example, if the information is coded in the difference of phase between two consecutive coherent states (as it will be discussed latter), and Eve has success in her attack getting four photons from the two consecutive pulses, namely $p_{1\alpha}$, p_{1t}, $p_{2\alpha}$ and p_{2t}, she has to measure the phase difference between $p_{2\alpha}-p_{1\alpha}$, $p_{2\alpha}-p_{1\alpha}$,$p_{2\alpha}-p_{1t}$, $p_{2t}-p_{1\alpha}$ and $p_{2t}-p_{1t}$. Thus, even if Eve can measure the phase difference without destroying the individuals phase information, she has four phase difference values and she has to guess which of them represents the correct information, limiting the information leakage.

3.3 Two-layer one-way QKD

3.3.1 One-way QKD

The idea behind the one-way QKD is to obtain the secret key bits from the simplest possible setup without introducing loss and/or controllable optical elements in the system [20, 35]. In this direction, the arrival time of the pulses is the solution adopted. The security is guaranteed by the occasional measurement of the quantum coherence between two consecutive non-empty pulses. A simplified scheme is shown in Figure 3.2.

Figure 3.2: Representation scheme of the one-way QKD protocol. BS_n - beam splitters and D_n - single photon detectors.



The protocol is explained as follows: Alice prepares a sequence of weak coherent and vacuum pulses, separated by a parameter τ by using a CW-laser with an external intensity modulator. She encodes bits using time slots with two pulses each one, as shown in Figure 3.2. If in a time slot, only the first pulse has the mean photon number of μ, then it represents a logical 0 bit. On the other hand, whether only the first pulse is a vacuum pulse, the logical bit 1 is then represented [11]. The mathematical expressions for each logical bit are in equations bellow:

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}\,|0_k\rangle_{2k}\,, \tag{3.1}$$

$$|1_k\rangle = |0_k\rangle_{2k-1}\,|\sqrt{\mu}\rangle_{2k}\,, \tag{3.2}$$

$$|D_k\rangle = |\sqrt{\mu}\rangle_{2k-1}\,|\sqrt{\mu}\rangle_{2k}\,. \tag{3.3}$$

For security reasons, Alice also sends decoy sequences in order to reveal the presence of an eavesdropper. The decoy time slot is formed by both pulses of coherent states. Due to the coherence of the laser, there is a well-defined phase between any two non-empty pulses: each one from the decoy sequence and outside the slot time for the bit sequence 1-0 [35]. So as Alice produces equally spaced pulses, the coherence between two consecutive pulses is checked by a single interferometer at Bob's apparatus (see Figure 3.2).

The pulses propagate to Bob on a quantum channel characterized by a transmission t, and are split at a non-balanced beam-splitter with transmission coefficient $t_B \leq 1$. The path corresponding to the D_B single photon detected is called *data line* since it is used to establish the raw key by measuring the time arrival of the photons. The counting rate of the protocol is given by the expression

$$R = 1 - exp\,(i\mu t t_B \eta) \approx \mu t t_B \eta, \tag{3.4}$$

with μ as the mean photon number and η being the quantum efficient of the photon counter. The pulses transmitted through the security line (also called *monitoring line*) are only used to check the reliability of the transmission. In this path, a single interferometer is responsible to verify the coherence between two consecutive arrival pulses. Indeed, when both pulses in j and $j+1$ window time are non-empty, then only D_1 can fire at time $j+1$. Coherence can be quantified by Alice and Bob through the visibility of the interference

$$V = \frac{p(D_1) - p(D_2)}{p(D_1) + p(D_2)}, \tag{3.5}$$

where $p(D_j)$ is the probability that detector D_j fired at a time where only D_1 should have fired. On the other hand, every click in detector D_2 is attributed to a break in the coherence caused by an external agent, an eavesdropper.

Let's summarize the protocol [35]:

1. Alice sends a large number of times "bit 0" with probability $(1-f)/2$, "bit 1" with probability $(1-f)/2$ and the decoy sequence with probability f.

2. At the end of the exchange, Bob reveals for which bits he obtained detections in the dataline and when detector D_{2M} has fired.

3. Alice tells Bob which bits he has to remove from his raw key, since they are due to detections of decoy sequences (sifting).

4. Analyzing the detections in D_{2M}, Alice estimates the break of coherence through the visibilities V_{1-0} and V_d associated, respectively, with 1-0 bit sequences and decoy sequences, computing Eve's information at the end.

5. Finally, Alice and Bob run error correction and privacy amplification routines and to find a secret key.

The performance of a QKD protocol is quantified by the achievable secret key rate R_{sk}. To compute this quantity, several parameters have to be introduced. The fraction of bits kept after sifting (sifted key rate) is $R_s(\mu) = [R + 2p_d(1-R)]p_s$, with $R = \mu t t_B \eta$ the counting rate due to photons defined above, p_d the probability of a dark count, and $p_s = 1 - f$ here. The amount of errors in the sifted key is called the quantum bit error rate (QBER, Q) . Moreover, this key is not secret: Eve knows a fraction I_{Eve} of it. Some classical post-processing (error correction and privacy amplification procedures) allow us to extract a key that is error-less and secret, while removing a fraction $h(Q) + I_{Eve}$, where h is binary entropy. Then,

$$R_{sk} = R_S(\mu)\left[1 - h(Q) - I_{Eve}\right]. \tag{3.6}$$

After the explanation of the raw key for a general protocol, a comparison with the BB84 protocol implemented using interferometric bases X and Y have to be done to infer the raw key for an asymmetric use of bases such that $p_s = 1 - f(BB84_{XY})$. First of all, it is required that all visibilities are equal: $V_X = V_Y$ in $BB84_{XY}$ and $V_{1-0} = V_d$ in one-way scheme - otherwise, Alice and Bob abort the protocol. Under this assumption, the QBER of $BB84_{XY}$ is $Q(\mu) = R[(1-V)/2] + (1-R)p_d p_s/R_s \equiv Q_{opt} + Q_{det}$; while for one-way is $Q(\mu) = Q_{det}$, independent of V.

In order to estimate I_{Eve}, we restrict the class of Eve's attacks [20], waiting for a full security analysis. Because of losses and the existence of multiphoton pulses, Eve can get a good fraction of information. This fraction is either $r = \mu(1-t)$ or $r = \mu/2t$, according to whether PNS attacks do not or do introduce errors [18]. Then Eve performs the intercept-resend attack on a fraction p_{IR} of the remaining pulses. In $BB84_{XY}$, she introduces the error $(1-r)p_{IR\frac{1}{4}} = (1-V)/2$ and gains the information $I = (1-r)p_{IR\frac{1}{2}} = 1-V$. On the present protocol, the IR will be performed in the time basis, so $I = (1-r)p_{IR}$. However, since we use only one decoy sequence, if Eve detects a photon in two successive pulses she knows what sequence to prepare; the introduced error is then $1 - V = I\xi$ with $\xi = 2e^{-\mu t}/(1+e^{-\mu t})$ the probability that Eve detects something in one pulse and nothing in the other. Plugging $Q(\mu)$ and $I_{Eve} = r + I$ into Equation (3.6) , we have R_{sk} as an explicit function of μ; Alice and Bob must choose μ in order to maximize it. Based on a numerical optimazion realized in [35], the present protocol is more robust than $BB84_{XY}$ against the decrease of visibility.

Regarding to the security analysis, the explanation is not quite simple; so, a larger and detailed review for the analysis is found in [35]. The first attack strategy analyzed is the PNS. This attack per se causes errors since a measurement of the number of photons in both consecutive pulses break the coherence between them. Another possibility is the adoption of an unbalanced cascade of beam splitters. The errors occur when Alice and Bob calculate the visibility, since the amplitude values of the extracted photon pulses is quite different from the others.

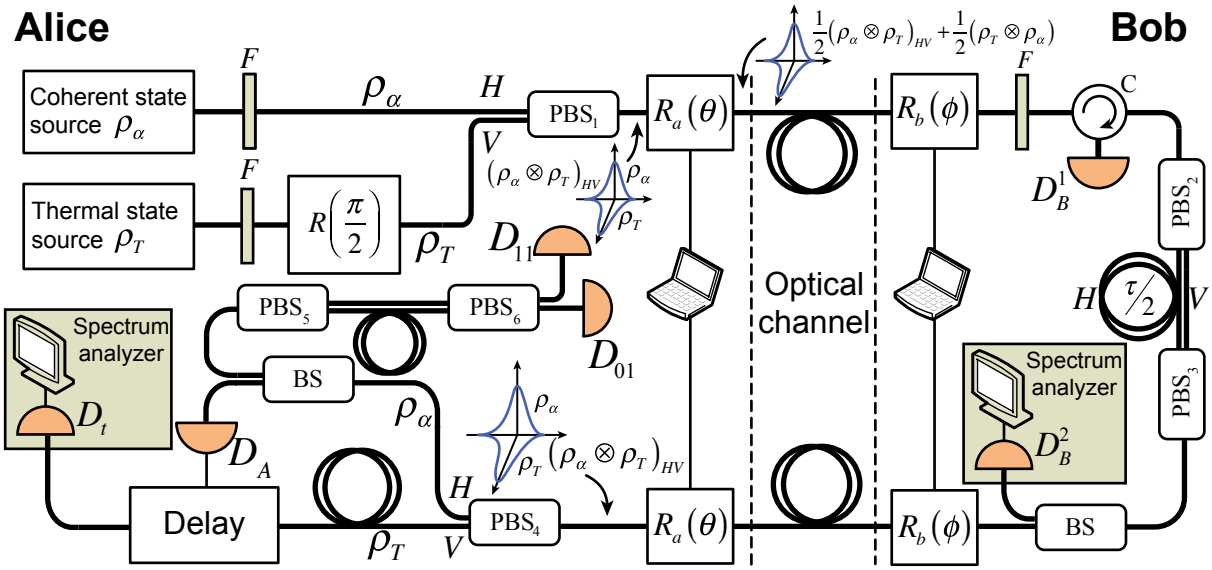
The only attack that an eavesdropper is able to succeed is the traditional beam splitter attack. Instead of using a sort of beam splitters, she uses only one to remove a fraction of $1 - t_f$ of the photons sent by Alice; what left, t_f, is sent to Bob through a lossless channel. Thus, $\mu(1-t_f)$ photons per pulse sent by Alice are detected by the intruder. So, every time a detection is counted, the eavesdropper will have all information about the bit chosen by Alice. If the pulse contains more than one photon, then Bob will have detection just as if the eavesdropper is not present. To solve that trick, Alice must use μ as low as possible to diminish the intruder chances.

3.3.2 Setup and protocol

Two-layer one-way QKD protocol is shown in Figure 3.3. Initially, Alice produces a set of quantum states ρ_α and ρ_t, representing, respectively, the coherent and thermal states. The filters F placed at the output of each laser keeps the light from both sources inside the same spectral range, avoiding side-channels attacks by an eavesdropper. Those attacks consist in the search for photons in different frequencies aiming to identify which source generated those photons. Before reaching PBS_1, the thermal state is rotated by $\pi/2$, changing its polarization state from horizontal (H) to vertical (V). Now the coherent state is in H polarization and the thermal state is in V polarization. After the PBS_1, both modes are joined and follow to the first polarization rotator $R_a(\theta)$, which is able to rotate by 0 or $\pi/2$, randomly exchanging their polarization mode. The state at Alice's output is then represented by Equation (3.7) and the top part of the Figure 3.4.

$$\rho_{out} = \frac{1}{2}\left(\rho_\alpha \otimes \rho_t + \rho_t \otimes \rho_\alpha\right)_{HV}. \tag{3.7}$$

Figure 3.3: Scheme for two-layer one-way QKD. $R_n(\theta)$ are polarization rotator - D_n are single-photon detectors - C circulator and F filters.

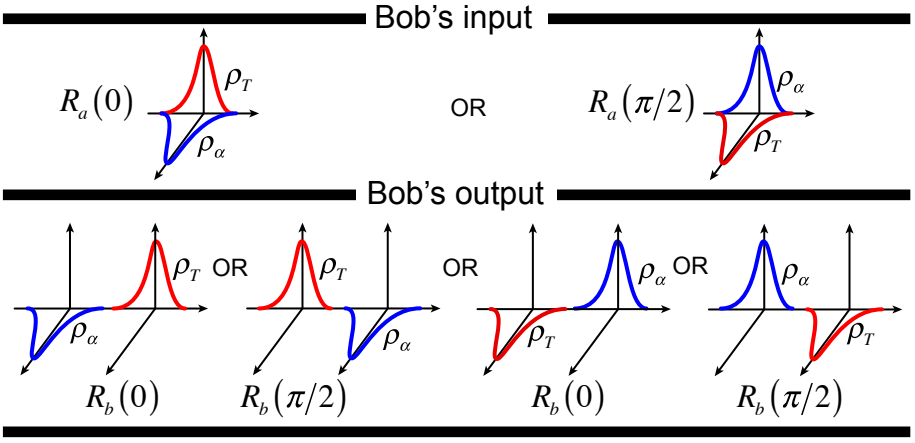


At Bob's side, the polarization rotators $R_b(\phi)$ and the polarizing interferometer formed by PBS_2, PBS_3 and the delay $\tau/2$, are used to mismatch temporally the polarization modes. Now, each pulse is splitted in two components in time mode, as in the bottom part of Figure. 3.4. The state at Bob's output is

$$\rho_B = \frac{1}{4}\left[\left(\rho_\alpha^1 \otimes \rho_t^2\right)_{HV} + \left(\rho_\alpha^2 \otimes \rho_t^1\right)_{HV} + \left(\rho_t^1 \otimes \rho_\alpha^2\right)_{HV} + \left(\rho_t^2 \otimes \rho_\alpha^1\right)_{HV}\right]. \tag{3.8}$$

The pulse structure in Bob's output might be tricky. However Figure 3.4 gives a visual explanation of all possibilities regarding Bob's choice to rotate his polarization by

Figure 3.4: Polarization scheme of Bob's incoming and outcoming pulses. ρ_α - coherent state and ρ_t - thermal state.



0 or $\pi/2$. For example, the second term in Equation (3.8) means the coherent state is at horizontal mode and time slot 2 and thermal state at vertical mode and time slot 1. The time slots 1 and 2 are separated by a time interval of $\tau/2$ and τ is the time interval between two consecutive pulses sent by Alice. It is obtained when Alice sends $(\rho_\alpha \otimes \rho_t)_{HV}$ and Bob uses $\phi = 0$ (bit 0) in both R_b. On the other hand, if Alice sends $(\rho_\alpha \otimes \rho_t)_{HV}$ and Bob uses $\tau = \tau/2$ (bit 1), the state at Bob's output is the first term in Equation (3.8). Hence, Bob's output is similar to Alice's output in the scheme shown in Figure 3.2, but now, instead of vacuum states, thermal states are used randomly in one out of two polarization modes.

The optical filter in Bob is used to avoid the possibility of an attack using a different wavelength not detected by Bob's single photon detector . It is natural for all QKD systems to limit the spectral range used to exchange pulses, as side-channels attacks exploit this breach for information leakage. The circulator and the single-photon detector are used to avoid a bidirectional path.

When the pulses arrive at Alice's setup she uses the polarization rotator R_a and the PBS_4 to separate the coherent and thermal states. The coherent state always emerges from H output while the thermal state always emerges from output V due the same rotation applied in both rotators. The coherent state is guided to an optical apparatus similar to the one used by Bob in Figure 3.2 while the thermal state is sent to an apparatus able to identify it, composed by a controllable delay, a single-photon detector and a spectrum analyzer. The one-way QKD is implemented in the traditional way but Alice and Bob play opposite roles when compared to the traditional one-way QKD. The security is the same provided by the classical one-way QKD improved by the security provided by the two-layer framework..

The crucial point in the scheme is the ability of Alice and Bob to detect Eve by analyzing the electrical power measured by a spectrum analyzer plugged at the single-

photon detector's output D_A. Let the coherent and thermal states produced by Alice have, respectively, the mean photon numbers $|\alpha|^2$ and μ_t. Their overlap is given by

$$\langle\alpha|\,\rho_t\,|\alpha\rangle = \exp\left[-|\alpha|^2/\left(1+\mu_t\right)\right]/\left(1+\mu_t\right). \tag{3.9}$$

Since they are not orthogonal for finite values of μ_t and $|\alpha|^2$, they cannot be perfectly distinguished with ta single measurement. However, if $\mu_t = |\alpha|^2$, the states ρ_α and ρ_t can be distinguished with high probability if one has a large enough number of samples of one of them. As explained in [41, 53] this task can be realized by a threshold single-photon detector. For simplicity, neglecting the afterpulsing, the probabilities of thermal and coherent states to fire an avalanche in a threshold single-photon detector are, respectively, given by

$$P_t = 1 - \frac{1}{1+\eta\mu_t}\left(1-p_d\right), \tag{3.10}$$

$$P_\alpha = 1 - \exp\left(-\eta|\alpha|^2\right)\left(1-p_d\right). \tag{3.11}$$

In (3.10) and (3.11), η and p_d are respectively the single-photon detector quantum efficiency and dark count probability. Using a spectrum analyzer to measure, in a fixed frequency band, the electrical power of the signal produced by a threshold single-photon detector, a large sample of thermal states can be distinguished of a large sample of coherent states. This happens because the electrical power in a fixed band is proportional to $(P - P^2)$ where P is the probability of an avalanche to be fired [53]. Since $|\alpha|^2$ and μ_t are chosen such that the probabilities of an avalanche to be fired are different, the electrical powers measured will also be different.

Applying this strategy, Alice and Bob can check if the quantum states they are receiving are in fact those they are expecting. Since Eve does not know the mean photon numbers used (this is a secret kept by Alice and she reveals it to Bob only at the end of the protocol), she does not know which state to use when she attacks Bob's apparatus. On the other hand, if Eve attacks the quantum states before or after Bob's coding, she will not be sure about the results because the impossibility to distinguish perfectly between coherent and thermal state.

3.4 Two-layer coherent-thermal QKD

Within the broad research scenario of quantum secure communication, two-way quantum key distribution (TWQKD) is a relatively new proposal for sharing secret keys that is not yet fully explored. We propose and analyze an optical setup of TWQKD scheme using the framework of two-layer QKD. The first paper of two-way QKD is [34] and here, an overview of the protocol is given. Here we propose a new protocol using the premisses of TWQKD, the codification scheme of the differential quadrature phase shift (DQPS-QKD)

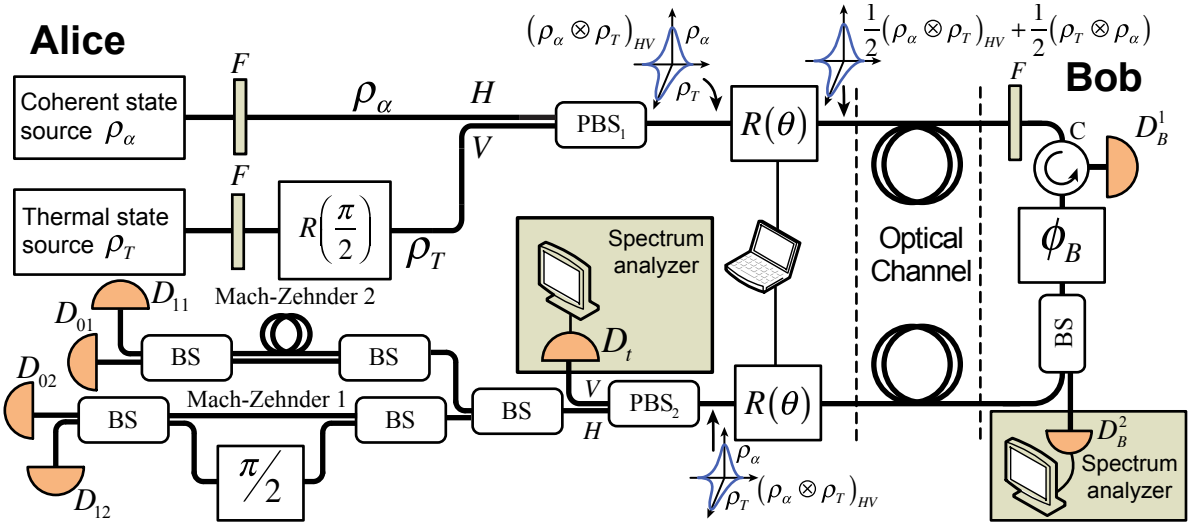
and the two-layer frame work, named CT-DQPS-QKD, where CT stands for Coherent and Thermal.

The CT-DQPS-QKD has some interesting properties. It is secure against beam splitter, intercept-resend, photon number splitting, unambiguous discriminations, external control and Trojan horse attacks. Furthermore, the eavesdropper's presence is denounced in two different ways: parameter (QBER) estimation in the QKD protocol and an electrical signal in the two-state protocol. Additionally, the two protocols are linked in such way that, depending on the attack strategy used by the eavesdropper, attacking one of them can cause errors in both. Another interesting point is the fact that the eavesdropper will never be sure about the value of the bits obtained during an attack.

3.4.1 Setup and protocol

The two-way QKD protocol was already overviewed in the previous chapter. In this section we are going to consider the two-way QKD with the framework of two-layer QKD employing the differential-quadrature- phase-shift QKD [39]. The optical scheme used to implement the CT-DQPS-QKD is shown in Figure 3.5.

Figure 3.5: Proposed optical scheme for CT-DQPS-QKD.PBS - polarization beam splitter; R -polarization rotator; ϕ_B - Bob's phase modulator; C - optical circulator; F - optical filters with central frequency at 1550 nm; BS - beam splitter and D_{ij}, D_T, D_B^1 and D_B^2 - single-photon detectors.



Comparing the scheme in Figure 3.5 with the description of two-layer QKD in Section 2.3, one can note that we chose $\rho_1 = |\alpha\rangle\langle\alpha|$ and $\rho_2 = \rho_T$. Furthermore, the unitary operation U is a phase-modulator, leading to the quantum operation in Bob's site $U = \exp(i\phi\hat{N})$, where $\hat{N}$ is the *Number operator*. One can readily observe that

$$U\rho_1 U^\dagger = e^{i\phi\hat{N}} |\alpha\rangle\langle\alpha| e^{-i\phi\hat{N}}, \tag{3.12}$$

$$U\rho_2 U^\dagger = e^{i\phi\hat{N}} \rho_T e^{-i\phi\hat{N}} = \rho_T. \tag{3.13}$$

Now, using (2.14) we note that the distinguishability between $|\alpha\rangle\langle\alpha|$ and ρ_T, and between $U(\phi)|\alpha\rangle\langle\alpha|U^\dagger(\phi)$ and $U(\phi)\rho_T U^\dagger(\phi)$ are the same

$$\left\langle \alpha e^{i\phi}\right| \rho_T \left|\alpha e^{i\phi}\right\rangle = \langle\alpha|\rho_T|\alpha\rangle = \exp\left[-|\alpha|^2/(1+\mu_T)\right]/(1+\mu_T). \tag{3.14}$$

Hence, the pair coherent and thermal states obeys the conditions (2.4) and (2.5). Moreover, due to (3.13), (2.6) is also satisfied. Finally, since the density matrix of the thermal state is a diagonal matrix with positive entries, it has a null kernel and, hence, (2.7) is also satisfied. Furthermore, a and b modes discussed in section 2.3 are the horizontal and vertical polarization modes. The mode separation in Alice is simply realized by a polarizing beam splitter. Finally, the ρ-detector is the setup with single-photon detector and spectrum analyzer discussed in Section 2.3.2. Initially, Alice produces optical pulses having a coherent state at the horizontal mode and a thermal state at the vertical mode, both of them having low mean photon number such that (2.4) is satisfied. Two optical filters (F) in Alice put the light from both sources inside the same spectral range. This avoids a side-channel attack in which Eve looks for photons in different frequencies aiming to identify from which source the photon came from. Following, Alice, randomly, sets her polarization rotator $R(\theta)$ in $\theta = 0$ or $\theta = \pi/2$. Thus, for each optical pulse produced by Alice, the total quantum state entering the optical channel is $1/2(\rho_\alpha \otimes \rho_T)HV + 1/2(\rho_T \otimes \rho_\alpha)HV$.

Bob has a polarization insensitive phase modulator and does not change the thermal state (since it has a diagonal density matrix), as is required by (3), but it adds the phase ϕ_B to the coherent state. Leaving Bob's place, the optical pulses return to Alice. For each pulse arriving, Alice applies the same polarization rotation she had applied when the pulse was leaving her place. Thus, before PBS_2, all pulses will have the coherent state at H-mode and thermal state at V-mode. These modes are separated by PBS_2 and the thermal state at the V-mode is monitored by a single-photon detector plugged to a spectrum analyzer that will measure the electrical power in a fixed band. On the other hand, the coherent state at H-mode is sent to Alice's QKD measurement setup composed by two fiber interferometers whose time difference between upper and lower arms, τ, is equal to the time separation between two consecutive pulses. The DQPS-QKD protocol can be readily implemented if Bob and Alice play the opposite roles as happens in traditional DQPS-QKD. Thus, Bob modulates each pulse that arrives at his place applying randomly one of the phases 0, $\pi/2$, π and $3\pi/2$. Alice, by its turn, is the one who has the interferometers placed at the coherent state output. The protocol rules follows the original paper and its security is increased by the use of thermal states.

3.4.2 Security analysis

A brief and introductory security analysis is realized for CT-DQPD-QKD. Most of the attacks strategy will explore the loopholes from the coding and measurement part, where

Eve can get some information of the raw keys. The analysis is performed based on the original paper and the attacks described in the paper.

The security of the CT-DQPS-QKD can be explained as follows: Without knowing if the coherent state is in the H- or V-mode, the beam splitter, intercept-resend and photon number splitting attacks will not be useful for Eve, since she will not be sure about the bit value obtained during the attack and she will introduce errors in Alice. All of these are type I attacks. Since the thermal state has a null kernel, the type II attack with unambiguous discrimination does not work.

As can be seen in Figure 3.5, the filter F in Bob avoids Eve to use light in a different wavelength not detected by Bob's single-photon detector . The optical circulator and the single-photon detector are used to avoid a bidirectional path. At last, the beam splitter BS with reflectivity r, the single-photon detector and the spectrum analyzer are used to check if the states modulated by Bob are in fact compatible the coherent and thermal states with the mean photon numbers chosen by Alice.

After the quantum communication, Alice informs Bob the mean photon numbers used. Bob checks if the electrical power value measured during the quantum communication is in accordance with the expected value for those mean photon numbers announced by Alice. If it is not, the key exchanged is discarded. Thus, if Eve changes the quantum states, without knowing the mean photon numbers used by Alice, with high probability she will change the electrical power measured by Bob. Moreover, since the QKD protocol used is the DQPS-QKD, in order to be sure about the quantum operation used by Bob, Eve has to use an optical pulse with at least two photons (if Eve sends to Bob the quantum state $|1\rangle$ the pulse at Bob's output will be the same produced by an ideal BB84). However, since Alice uses low mean photon numbers for the thermal and coherent states, the probability of having two photons in a pulse produced by her will be low. Thus, a two-photon state $|1\rangle_H |1\rangle_V$ will be easily distinguished from the state $1/2(\rho_\alpha \otimes \rho_T)HV + 1/2(\rho_T \otimes \rho_\alpha)HV$ produced by Alice. This is the type III attack. At last, if Eve tries to control externally Alice's single-photon detectors $(D_{01}, D_{11}, D_{02}, D_{12})$ sending to Alice strong (pulsed or CW) light [60], part of this light will be guided to the output 2 and the electrical power measured by Alice will be different from the expected value, indicating the attack. This is the attack type IV.

A simplified analysis of the secret-key rate (R_S) of the two-layer CT-DQPS-QKD consists in to consider (unrealistically) that, after her measurements, Eve knows when she attacked a thermal or a coherent state. In this case, one has $R_S = R_{sift}(I_{AB} - I_{AE}/2)$. The term 12 is due to the thermal states: having to choose randomly which mode to attack (horizontal or vertical), in average, half of the bits got by Eve (those obtained when a thermal state is attacked) will be completely uncorrelated with Alice's sequence, implying in $I_{AE} =$. The other half of the bits (those obtained when a coherent state is attacked) will imply in $I_{AE} \neq 0$. Using the equations forI_{AB} and I_{AE} described in [64]

one has

$$I_{AB} = 1 - \eta_{ec} H(QBER), \tag{3.15}$$

$$I_{AE} = \{(1 - \mu/2t)\,[1 - H(p)] + (\mu/2t)\} \,/\, [1 + (2p_d/\mu t\eta)]\,, \tag{3.16}$$

$$p_\mu = \mu t \eta t_B, \tag{3.17}$$

$$t = 10^{-\alpha L/10}, \tag{3.18}$$

$$R_{sift} = [1/2\,(p_\mu + 2p_d + p_{ap})\, f_{rep}] \,/\, [1 + \tau_{dead} f_{rep}\,(p_\mu + 2p_d + p_{ap})]\,, \tag{3.19}$$

$$p_{ap} = 0.008(p_\mu + 2p_d), \tag{3.20}$$

$$QBER = \frac{1}{2}\frac{p_\mu(1 - V) + 2p_d + p_{ap}}{p_\mu + 2p_d + p_{ap}}, \tag{3.21}$$

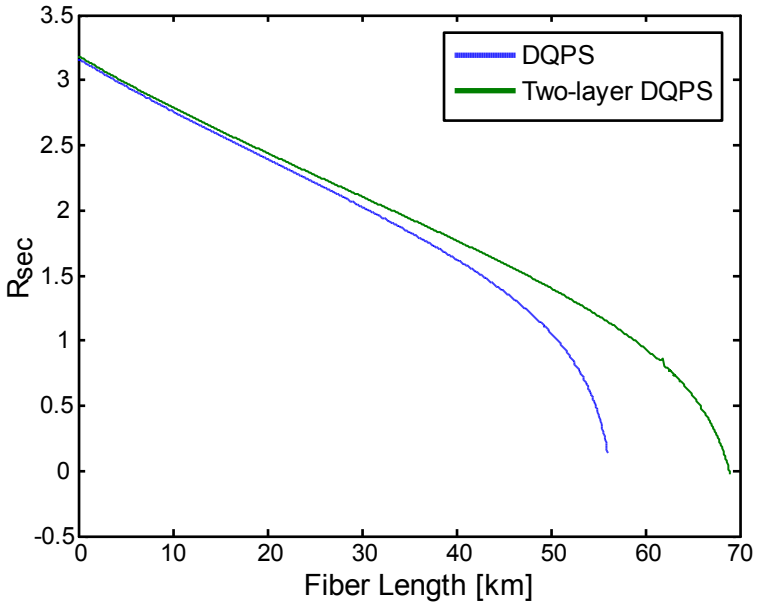
$$p = 1/2 + \sqrt{D(1 - D)}, \tag{3.22}$$

$$D = (1 - V)/(2 - \mu/t). \tag{3.23}$$

In (3.15)-(3.23), $\eta_{ec}(= 1.2)$ is the efficiency of the error correction protocol,$\mu(= 0.1)$ is the mean photon number of the coherent state used, $p_d(= 5.10^{-6})$ and p_{ap} are, respectively, the single-photon detector's dark count and afterpulsing probabilities, $\eta(= 0.07)$ is the single-photon detector's quantum efficiency, t is the transitivity of the optical link of length L between Alice and Bob, $t_b(= 0.543)$ takes into account the loss in Bob devices, $\alpha(= 0.21\ dB/\text{km})$ is the fiber coefficient loss, $f_{rep} = (5$ MHz) is the pulse repetition frequency, $V(= 0.98)$ is the visibility of the interferometers, $\tau_{dead}(= 1\ \mu\text{s})$ is the time during which the single-photon detector is unable to fire a new avalanche. At last, $H(\,\cdot\,)$ is the entropic function: $H(x) = -xlog_2(x) - (1 - x)log_2(1 - x)$. The comparison of the R_{sec} for DQPS-QKD with and without the second layer (thermal states) is shown in Figure 3.6.

In the real case, Eve is never sure if she attacked a thermal or a coherent state. In this situation, the real mutual information between Alice and Eve will be lower than $I_{AE}/2$ and the curve of the secret-key rate will always be over those shown in Figure 3.6.

Figure 3.6: R_{sec}[bit/s](logarithmic scale) versus L for DQPS-QKD and two-layer DQPS-QKD.



3.5 Two-layer QKD using homodyne detection

In the past few years several quantum cryptographic schemes were developed mainly based on single-photon quantum systems. Recent events related to experimentation of these protocols have raised the need of new ways to overcome the unsecure scenario imposed by these technologies. As most schemes uses photon counting to detect weak light pulses, it is hard to avoid some imperfections in practical implementations, like multiphoton pulses, channel losses, low detection efficiency and dark counts of detector [65–70]. Another method for detecting weak light proposed to have a high accuracy faced to photon counting is the homodyne detection.

Sometimes called quadrature phase homodyne measurement, it is a well-established quantitative method for measuring the quadrature-amplitude operator of the radiation field [71]. It was first observed by Namiki and Hirano [72] that a quadrature measurement by a homodyne detection involves a phase shift operation and the most conventional light sources to do that are the coherent light sources. By that way, a combination of phase modulators and the homodyne detection scheme should provide a simple setup for QKD protocols using continuous variables [43]. Using this argumentation, they presented a protocol that the bits codification uses 4 coherent states with amplitude $\alpha > 0$, and phase shifts of $\pi/2$. The decodification was realized using one of the two quadratures X,Y of the field [18].

Another motivation for dealing with continuous variables in quantum information is the advantage in a more practical observation: efficient implementations of the essential steps in quantum protocols, namely, *prepare and measure* and the high efficiency imposed

by that implementation [73]. The use of four-state scheme instead of two orthogonal is based on two points: (i) the choice of basis is completely hidden from the other protagonist (the two bases correspond to the same density matrix), as well as from the eavesdropper, Eve [65]; and (ii) when Alice and Bob use different bases, there is no correlation between their bits.

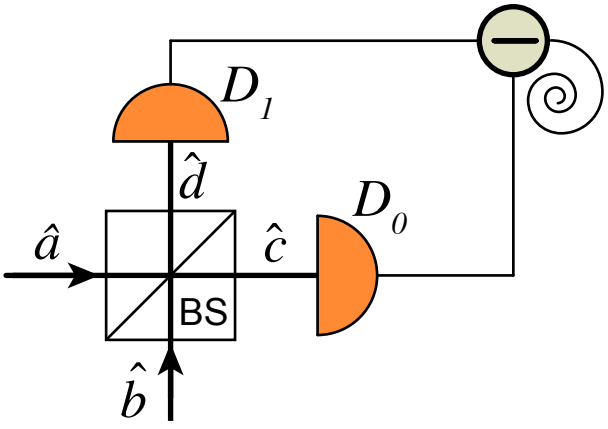
Most of the authors have proposed quantum key distribution schemes and protocols with homodyne detection using Einstein-Podolsky-Rosen type correlation or squeezed states [70, 74]. The main motivations to produce this hard work is to reduce the distress of the implementation by providing a simple and reliable scheme setup and to increase security throughout an adaptation of one of the most secure protocol produced.

3.5.1 Homodyne detection

The use of photodetectors for QKD schemes allow us to realize only a single measurement of the mean photon number or the superior statistical moments [71]. These intensity measurements are not enough to characterize completely a quantum light field, since it takes not account of the field phase. For instance, the detection of squeezed states requires a sensitive phase field scheme capable to realize quadrature variances measurements. In this case, ordinary homodyne detection can perfectly be used [75]. Differently from the balanced homodyne detection, most commonly used with coherent states, the frequency of both lights, the signal and the local oscillator, needs to be the same, what is reachable using the same transmittance media or the same channel and only one photodetector are needed. The local oscillator can also be produced in the same place the measurements are realized. Resuming, the ordinary homodyne detection allow us to obtain the necessary information.

In this work the balanced homodyne detection is used with coherent states, i.e. there is no need of phase and compression information. A simple model of balanced homodyne detection is shown in Figure 3.7.

Figure 3.7: Balanced homodyne detection scheme. $\hat{a}$ and $\hat{b}$ are BS inputs and $\hat{c}$ and $\hat{d}$ outputs connected to regular positive-intrinsic-negative diode(PIN) $D0$ and $D1$.



In the balanced homodyne detection, the reflectivity and transmissivity of the beam splitter must be exactly the same. This will cause the vanishing of the inherent quantum noise due to the local oscillator signal [76]. The equations expressing the relationship between input and output of the beam splitter regarded the amplitude operators are shown in (3.24) and (3.25).

$$\hat{c} = T\hat{a} + R\hat{b}, \tag{3.24}$$

$$\hat{d} = -R\hat{a} + T\hat{b}, \tag{3.25}$$

where R and T are the real values for the reflectivity and transmissivity of the BS. For each output, the number operator is given by

$$\hat{n}_c = \hat{c}^\dagger\hat{c} = \frac{1}{2}\hat{a}^\dagger\hat{a} + \frac{1}{2}\hat{b}^\dagger\hat{b} + \frac{1}{2}\left(\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right) \tag{3.26}$$

and

$$\hat{n}_d = \hat{d}^\dagger\hat{d} = \frac{1}{2}\hat{a}^\dagger\hat{a} + \frac{1}{2}\hat{b}^\dagger\hat{b} - \frac{1}{2}\left(\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right) \tag{3.27}$$

with $R = T = 1/\sqrt{2}$. As a combination of the output signals, the subtraction is obtained as:

$$\hat{n}_c - \hat{n}_d = \hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a} \tag{3.28}$$

and the measurement of this quantity is realized as:

$$\langle\hat{n}_c - \hat{n}_d\rangle = \left\langle\hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}\right\rangle = 2|\beta_{LO}|\left\langle\frac{1}{2}\left(\hat{a}^\dagger e^{i\phi_{LO}} + \hat{a}^\dagger e^{-i\phi_{LO}}\right)\right\rangle \tag{3.29}$$

with ϕ_{LO} as the projection angle of the local oscillator state onto the X quadrature. Then

$$\langle\hat{n}_c - \hat{n}_d\rangle = 2|\beta_{LO}|\left\langle\hat{X}_{LO}\left(\phi_{LO}\right)\right\rangle. \tag{3.30}$$

This approach is generally used to reduce the quantum noise, allowing higher amplitude for the local oscillator [77]. The operator described in Equation (3.29) is called the quadrature operator for X for a rotated axis of ϕ_{LO} and has the form

$$\hat{X}_{LO}\left(\phi_{LO}\right) = \hat{p}\cos\phi_{LO} + \hat{q}\sin\phi_{LO} \tag{3.31}$$

where $\hat{p}$ and $\hat{q}$ are the quadrature operators. Calculating the density operator for a coherent state, we have

$$|\left\langle x_\phi|\alpha\right\rangle|^2 = \sqrt{\frac{2}{\pi}}\exp\left[-2(x_\phi - \alpha\cos\phi)^2\right]. \tag{3.32}$$

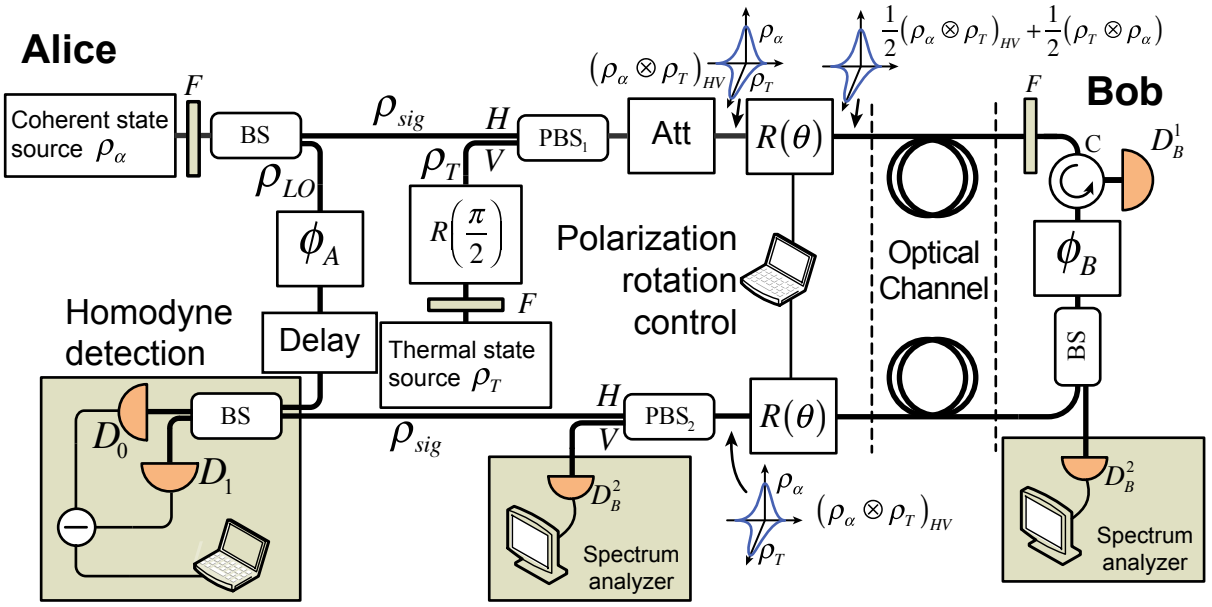
3.5.2 Setup and protocol

As we can see in Figure 3.8, the setup is implementable by simple devices found in any laser or quantum communication lab, as lasers, polarization modulators, phase modulators and photodetectors. The protocol can be understood as follows: initially Alice prepare a train of coherent pulses whose phase and amplitude are not necessarily modulated with Gaussian random numbers [76]. The density operator of the signal sent by Alice in terms of coherent states is described by

$$\hat{\rho}_c = (|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|)\,. \tag{3.33}$$

Our scheme uses four nonorthogonal states to implement a protocol using continuous variables (like the 4+2 protocol) [65], except for the detection method. In the output of the lasers, filters are regularly placed to avoid light returning. A beam splitter is positioned after the coherent source to generate the signal ρ_{sig} and ρ_{LO} components, each one with a few photons (typically less than one) and a large number (usually 10^6) respectively. Alice applies to the local oscillator a random phase shift ϕ_A of 0°, 90°($\pi/2$), 180°(π) and 270°($3\pi/2$). The delay line is used to compensate the time needed to the signal pulse to return to Alice's apparatus.

Figure 3.8: Scheme for two-layer QKD using homodyne detection.



The coherent pulses produced by a coherent laser usually have horizontal polarization; after crossing the BS, the signal joins the thermal pulses vertically polarized in PBS_1 . Note that the thermal pulses have their polarization states rotated by $\pi/2$ before the PBS_1. Now the pulses, with the signal and the thermal pulses onto the horizontal and vertical polarizations respectively, have the option to switch their polarization states, causing a

misunderstanding to Eve about which polarization state is the signal. In Bob's side, some components are placed to avoid or decrease the eavesdropping leakeage information. The optical filter is used to block the eavesdropper different wavelengths not detected by Bob's single photon detector . The circulator and the single-photon detector are used to avoid a bidirectional path. At ϕ_B the pulse can be randomly phase shifted by 0° or 90°, whether Bob decides to code a bit information of 0 or 1 respectively.

Back to Alice, the same polarization rotation must be applied to the pulses. On the other hand, a change in this configuration will cause a different measurement by D_t and the spectrum analyzer, indicating the eavesdropping presence. The signal and the local oscillator beams are joined in the last BS and two photodiodes D_1 and D_0 are used to realize the homodyne detection. The photocurrents produced by the photodetectors are then subtracted and the difference of photons determined. By that, the analysis is performed using the phase quadrature measurements. The total phase shift between the signal and LO is denoted by $\phi = \phi_A - \phi_B$. The bit sequence in Alice is created following the decision rules below:

$$\text{Phase difference} = \begin{cases} 0° & \text{if } x > X_D \\ 180° & \text{if } x < -X_D \\ \text{inconclusive} & \textit{otherwise} \end{cases} \tag{3.34}$$

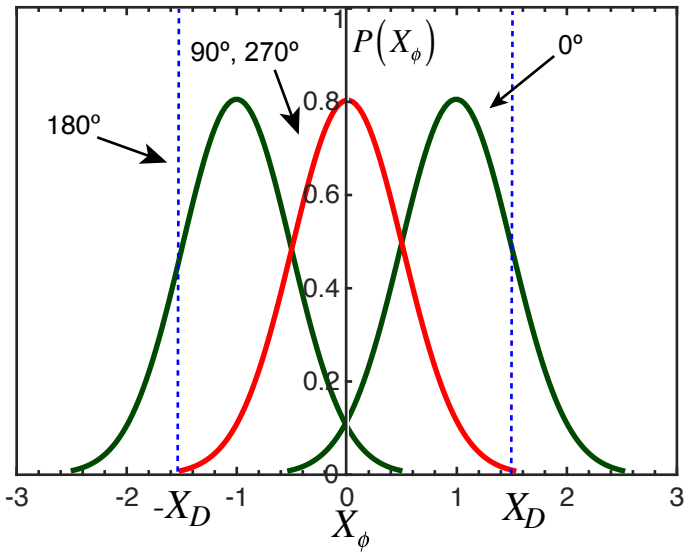
Based on the phase difference obtained in homodyne detection, the table 3.1 shows the bit assignment made by Alice and Bob:

Table 3.1: Bit assignment for homodyne detection.

Measurement	ϕ_A	ϕ_B	**Bit value**
$x > X_D$	0	0	'0'
$x > X_D$	90	90	'1'
$x < -X_D$	180	0	'0'
$x < -X_D$	270	90	'1'

When the signal is in a coherent state, $P(X_\phi)$ is given by a Gaussian function with a standard deviation of 1/2. If we plot graphs for the probabilities $P(X_\phi)$ for $\phi = 0°$, $90°(\pi/2)$, $180°(\pi)$, the probability distribution of $\phi = 90°$, $P(X_{90})$, and of $\phi = 270°$, $P(X_{270})$, are exactly the same, what make them impossible to distinguish, as in Fig 3.9; in this case, Alice chose the wrong basis [65]. Note that it is possible to differentiate between $P(X_0) = 0°$ and 180° by choosing two threshold values X_D and $-X_D$, corresponding the vertical dashed lines in Figure 3.9. Those values are defined as a limit for differentiation between acceptable values of measurement, where Alice is almost sure about the phase shift. Further this value is from "Zero", greater the certainty about the phase shift is. If the value obtained is in between $-X_D$ and X_D, an inconclusive result will make Alice abandon the judgment. As $P(X_0)$ overlaps $P(X_{180})$, there will be an intrinsic error probability e_{int}. This error probability depends on the chosen of the threshold value.

Figure 3.9: Theoretical probability distribution of the quadrature amplitude for total phase shifts of 0°, 90°, 180° and 270° when the signal is in a coherent state. Red line indicates wrong choice of basis and green line, distinguishable lines used for coding.



After a considerable number of transferred pulses, and differently from the reference [70], Alice does not need to disclose her phases, what decreases the leaking information to the spy. Only the time slots in which she had a reliable measurement of $X_\phi < -X_D$ or $X_\phi > X_D$ and if it was higher than X_D of less than $-X_D$ have to be public announced. Bob's key is coded by considering, for example, when the measurement is above X_D, the phase difference is with high probability 0°. This result is obtained when Bob and Alice pick up the same phase. So, if Bob modulates the pulse with $\phi_B = 0°$, the bit is '0'. For $\phi_0 = 90°$, the bit is '1'. By checking the table 3.1, if Alice's measurement is less than $-X_D$, Bob knows the phase difference is 180°. So, if Bob chose $\phi_B = 0°$, Alice certainly chose $\phi_A = 180°$. This is considered bit '0'. Quite the opposite, it is bit '1' when Alice pick up $\phi_A = 270°$. Summarizing, the phase correspondence by Alice is defined as: for bit '0', the phases to be send are ($\phi_A = 0°$ or 180°) and for bit '1' ($\phi_A = 90°$ or 270°). Finally, Alice and Bob can perform error correction and privacy amplification procedures.

3.5.3 Security analysis

The problems Eve has to face now are threefold. Beyond the problems inherent the protocol security, regarded to the 4+2 protocol [73], she has still to overcome one more barrier imposed by the new security layer. As explained in the beginning of the document, an improvement is proposed regarded the unknown state of polarization which the information is. Thus, it is safe to point out the invulnerability of this protocol. This means that the eavesdropper cannot acquire total information of the transmission no matter the eavesdropping strategy. In some cases, if Eve has a plenty of samples of the transmitted state, she is able to statistically determine the right polarization of the state with the

coded information. For these cases, the attack strategies are described now.

The main difference between the proposed protocol and the others in literature is that for Eve applies any attack strategy, she must initially identify the correct polarization state. Given the fact the eavesdropper possesses that information, she still has to face some improvements placed in scheme shown in Fig 3.8. The setup is composed with some devices used to block or vanish eavesdropping attacks. As explained, the optical filter placed in Bob's input is used to avoid the possibility of an eavesdropper to use a different wavelength not detected by Bob's single photon detector . The circulator and the single-photon detector are used to avoid a bidirectional path.

In Alice, a spectrum analyzer is positioned in the output of the thermal state to compare both initial and final electric power and deduce the presence of an eavesdropper. Finally, given all the circumstances, Eve still has to overcome the intrinsic security imposed by the protocol when using weak coherent pulses.

3.6 Conclusion

New QKD protocols are proposed in this chapter. They are designed using the *two-layer* QKD framework, which increases the security by adding an extra quantum state of light to run together with the coherent state. The second state is mixed with the first to scramble the polarization mode in where the information is. The protocols are based on the most promising ones, two-layer one-way QKD, CT-DQPS two-layer QKD and two-layer QKD using homodyne detetcion. Each one has their main features described and a basic security analysis stated.

For further experimental work, serious issues should be observed. The polarization of the states during the transmission should be controlled for a considerable discrimination; the time sincronization between the sources and the optical fibers refraction index should also have special attention.

4 PHOTOMULTIPLIER TUBES

Abstract

Recently, non-destructive and non-invasive measurements using light is becoming more popular in diverse fields including biological, chemical, medical, material analysis, industrial instruments and home appliances. For quantum information technology, two main features are relevant: detectability(detection efficiency) and security(robustness against eavesdropping attacks). Two options are available for such a high (low-level light sensitivity) detectability: photomultiplier tubes (PMT) and avalanche photodetectors (APD). The technology advances have reached such a low sensibility level, becoming possible to detect a single-photon. Regarding security, the experimental systems still have not reached their theoretical models. Here in this work, there are proposals to positively contribute to the practical quantum communication systems security, specially to QKD. This chapter shows experimental results for one issue so far not largely explored: the backflash emission. Its importance for the security scenario is also discussed.

4.1 Introduction

Light detection technology is a powerful resource used to provide a deeper and more sophisticated understanding of nature phenomena. Measurements using light offers several advantages, for example, non-destructive analysis of substances, high-speed properties discrimination and extremely high detectability. Recently, advanced research fields like scientific measurements, medical diagnosis and treatment, high energy physics, spectroscopy, astrophysics and biotechnology require detectors of light that exhibit the ultimate in various performance parameters [78].

Photodetectors or light sensors can be broadly divided by their operating principle into three main categories: external photoelectric effect, internal photoelectric effect and thermal effect. The external photoelectric effect is a phenomenon in which when light strikes a metal or a semiconductor placed in vacuum, electrons are emitted from its surface into the vacuum. Photomultiplier tubes (PMT) make use of this external effect, turning them into superior devices regarding response speed and sensitivity (low-level-light detection). They are widely used as industrial and academic measurements, medical equipment and analytical instruments.

Light sensors utilizing the internal photoelectric effect are further divided into photoconductive types and photovoltaic types. Photoconductive cells represent the former, and PIN photodiodes the latter. Both types feature high sensitivity and miniature size, making them well suited for use as sensors in camera exposure meters, optical disk pickups and in optical communications. The thermal types, though their sensitivity is low, have

no wavelength-dependence and are therefore used as temperature sensors in fire alarms, intrusion alarms and water alarms.

Unfortunately, given several issues regarding those devices, most of them are not suitable for quantum information systems. As PMT's have higher sensitivity than its former partners, a few systems are still designed for them. This chapter describes the PMT types and their main features, as well experimental measurements of the breakdown (backflash) emission and its influence in the security scenario.

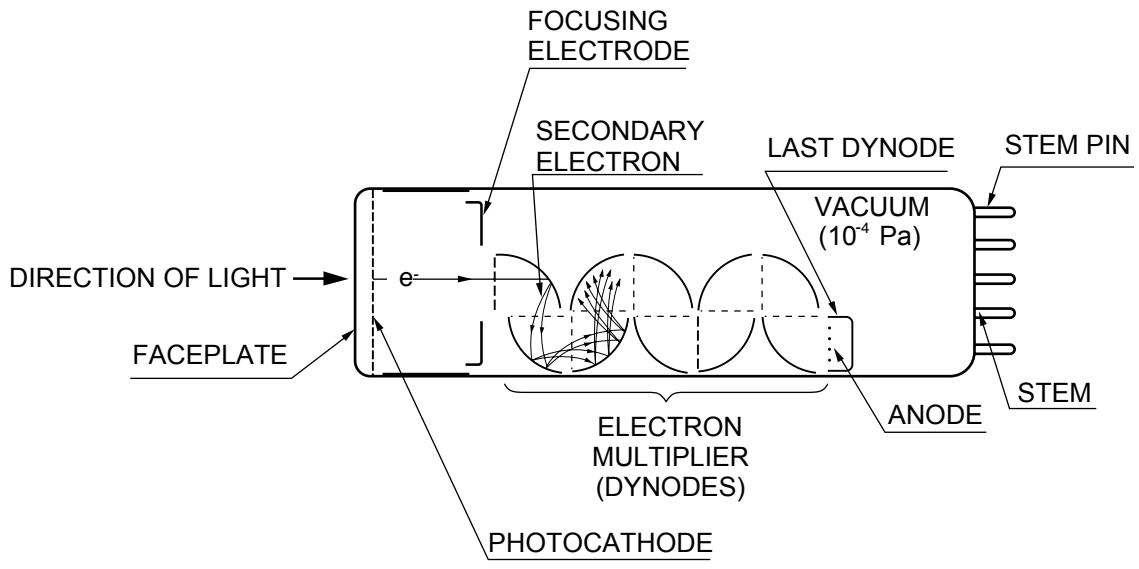
4.2 Photoelectron emission in PMTs

Among the photosensitive devices in use today, the photomultiplier tubes (PMT) are versatile devices that provides extremely high sensitivity and ultra-fast response. A typical photomultiplier tube has a photoemissive cathode (photocathode) followed by focusing electrodes, an electron multiplier and an electron collector (anode) in a vacuum chamber as Figure 4.1. When light enters the tube and strikes the photocathode, photoelectrons are emitted into the vacuum made inside the unit. They are guided through electrode voltage towards the electron multiplication stage. Dynodes [1] are found in the photoelectrons path and generate secondary emissions. The secondary photoelectrons are collected by the anode in the end path of dynodes as an output signal. The stem pins are responsible to send pulses to a circuit board, which threat and amplify the output pulses levels.

The photocathode plays the main role of the device: converting photons in photoelectrons. The photoelectric conversion is broadly classified into external photoelectric effects by which photoelectrons are emitted into vacuum from the material and internal

[1] Electrode that produces a significant number of electrons after the collisions of other electrons.

Figure 4.1: Detailed description of a PMT's. Circular types follow the same structure.



photoelectric effects by which the photoelectrons are excited into the conduction band of a material. The photocathode of the units used in this thesis has the second effect. Since they are semiconductors, it can be described using band models as shown in Figure 4.2.

In a semiconductor band model, there exist a forbidden-band gap or energy gap (EG) that can not be occupied by electrons. The other energy bands are joined into an electron affinity (EA) band, which is the energy difference between the conduction band and the vacuum level barrier. Also there is the work function (ψ) which is the band between the Fermi level and the vacuum level. When photons strike a photocathode, electrons in valence band absorb photon energy (hν) and become excited, diffusing toward the photocathode surface. If the diffused electrons have enough energy to overcome the vacuum level barrier, they are emitted into vacuum as photoelectrons. This can be expressed in a probability process by the quantum efficiency $\eta(\nu)$, i. e., the ratio of output electrons to incident photons, given by

$$\eta(\nu) = (1 - R)\,\frac{P\nu}{k}\left(\frac{1}{1 + 1/kL}\right)P_s \tag{4.1}$$

where

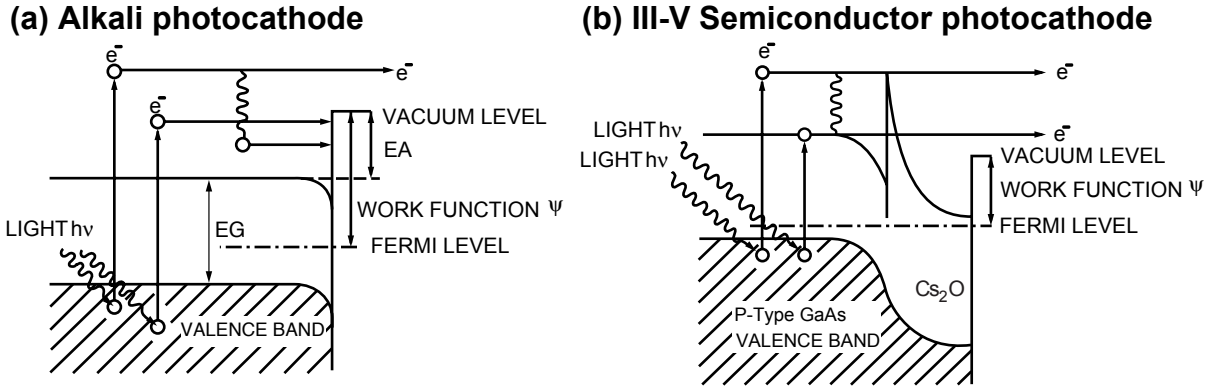
- R: reflection coefficient
- k: full absorption coefficient of photons
- Pν: probability that light absorption may excite electrons to a level greater than the vacuum level
- L: mean escape length of excited electrons
- Ps: probability that electrons reaching the photocathode surface may be released into vacuum
- ν: frequency of light

In the equation above, if we have chosen an appropriate material which determines parameters R, k and Pν, the factors that dominate the quantum efficiency will be L (mean escape length of excited electrons) and Ps (probability that electrons may be emitted into vacuum). L becomes longer by use of better crystal and Ps greatly depends on electron affinity (EA).

Figures 4.2a and b show the band model of a photocathode Alkali compounds and III-V semiconductor compound [79–81]. If the surface layer of electropositive material such as Cs_2O is applied to a photocathode, a depletion layer is formed, causing the band structure to be bent downward. This bending can make the electron affinity negative. This state is called NEA (negative electron affinity). The NEA effect increases the probability (Ps) that electrons reaching the photocathode surface may be emitted into the vacuum. In particular, it enhances the quantum efficiency at long wavelengths with lower excitation

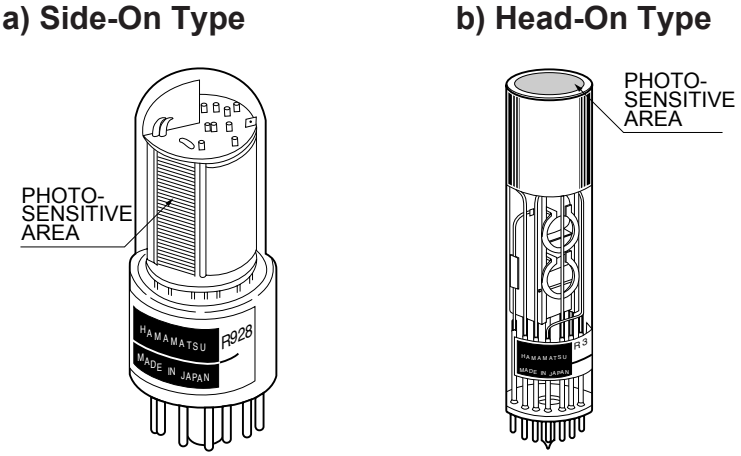
energy. In addition, it lengthens the mean escape distance (L) of excited electrons due to the depletion layer.

Figure 4.2: Photocathode band models. (a) Metal-alkali type and (b) III-V compound semiconductor type.



Photocathodes can also be classified by its photoelectron emission process into: a side-on type and head-on type as in Figure 4.3. The side-on type receives incident light from the side of the glass bulb, while in head-on type, it receives through the end of the tube. In general, the construction inside is based on a few types of circular and box geometry types. Most of the side-on types are relatively low priced, widely used in spectrophotometers and general photometric systems. They also employ opaque photocathodes and circular-type structures increasing sensitivity at relatively low supply voltage.

Figure 4.3: Photocathodes classification types by emission process. Extracted from [4].



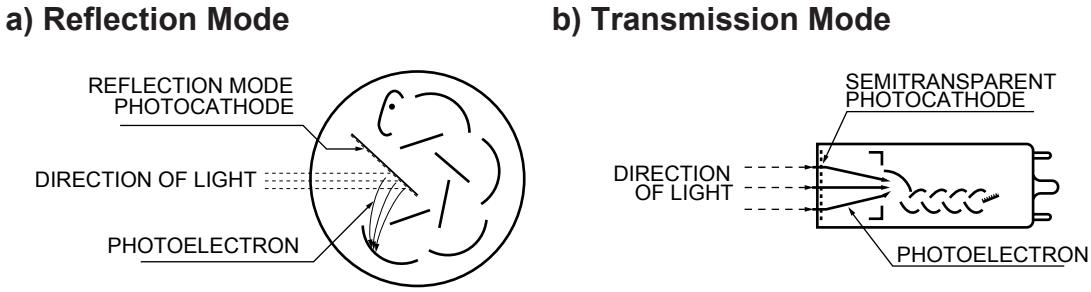
The head-on type (or the end-on type) has semitransparent photocathodes deposited upon the inner surface of the entrance window. They also provide better spatial uniformity [2] and allow the choice of the photosensitive area, from tens of square milimeters to

[2]Uniform sensitivity thoughtout the photocathode area.

hundreds of square centimeters. The modules used in this work are head on types with electronic board outside the main module.

Regarding photocathode generation layer, there are two types: one working in reflection mode and transmission mode. In the reflection mode Figure 4.4a, the incident light produces in the photocathode reflected photoelectrons, which are guided to the dynodes in the electron multiplication stage. On the other hand in transmission mode Figure 4.4b the incoming light generates photoelectrons in the opposite layer of the photocathode.

Figure 4.4: Types of photocathode regarding the photogeneration.



The photocathode is a photoemissive surface usually consisting of alkali metals with very low work functions. Based on the construction material of the photocathode, the most commonly used types are described below:

1) Ag-O-Cs The transmission mode photocathode using this material sensitive from visible to infrared range (300-1200 nm). They are mainly used for detection in the near infrared region with the photocathode cooled.

2) GaAs(Cs) GaAs activated with cesium is also used as a photocathode. The spectral response of this photocathode usually covers a wider spectral response range than multialkali, from ultraviolet to 930 nm. This is the photocathode type of the PMT's units used in this thesis. However, the type is activated with phosphorus (P), which increases to 40% the quantum efficiency.

3) InGaAs(Cs) This photocathode has greater extended sensitivity in the infrared range than GaAs. Moreover, in the range between 900 to 1000 nm, InGaAs has much higher S/N ratio than Ag-O-Cs.

4) Sb-Cs This is a widely used photocathode and has a spectral response in the ultraviolet to visible range. This is not suitable for transmission-mode units and mainly used for reflection mode photocathodes.

5) Bialkali (Sb-Rb-Cs, Sb-K-Cs) They have a spectral response range similar to Sb-Cs photocathode, but higher sensitivity and lower noise than Sb-Cs.

6) Multialkali (Na-K, Sb-Cs) They have a high and wide spectral response from ultraviolet to near infrared region. It is widely used for broad-band spectrophotometers.

A few other types are less frequently used.

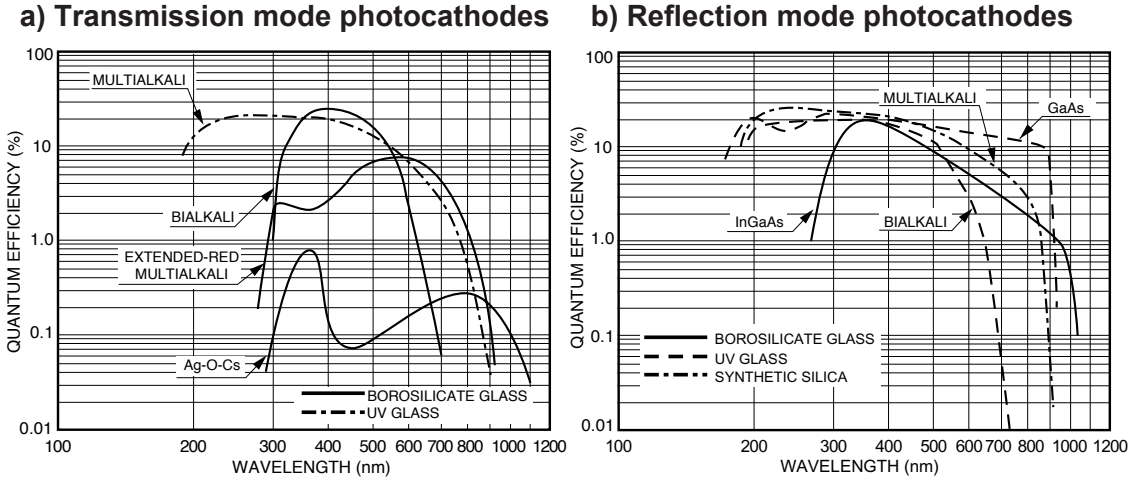
4.2.1 Radiant sensitivity

The spectral response is usually expressed in terms of radiant sensitivity or quantum efficiency as a function of wavelength, as in Figures 4.5a and 4.5b. Radiant sensitivity S is the photoelectric current from the photocathode, divided by the incident radiant power at a given wavelength, expressed in A/W (amperes per watt). The quantum efficiency is the number of photoelectric emitted from the photocathode divided by the number of incident photons. It is customary to present quantum efficiency in percentage by the following relationship per wavelength:

$$QE = \frac{S \times 12400}{\lambda} \times 100\% \tag{4.2}$$

where S is the radiant sensitivity in A/W at a given wavelength λ in (nm) nanometers.

Figure 4.5: Typical spectral response characteristics of the photocathodes.



4.3 Backflash emission

4.3.1 Device under test (DUT)

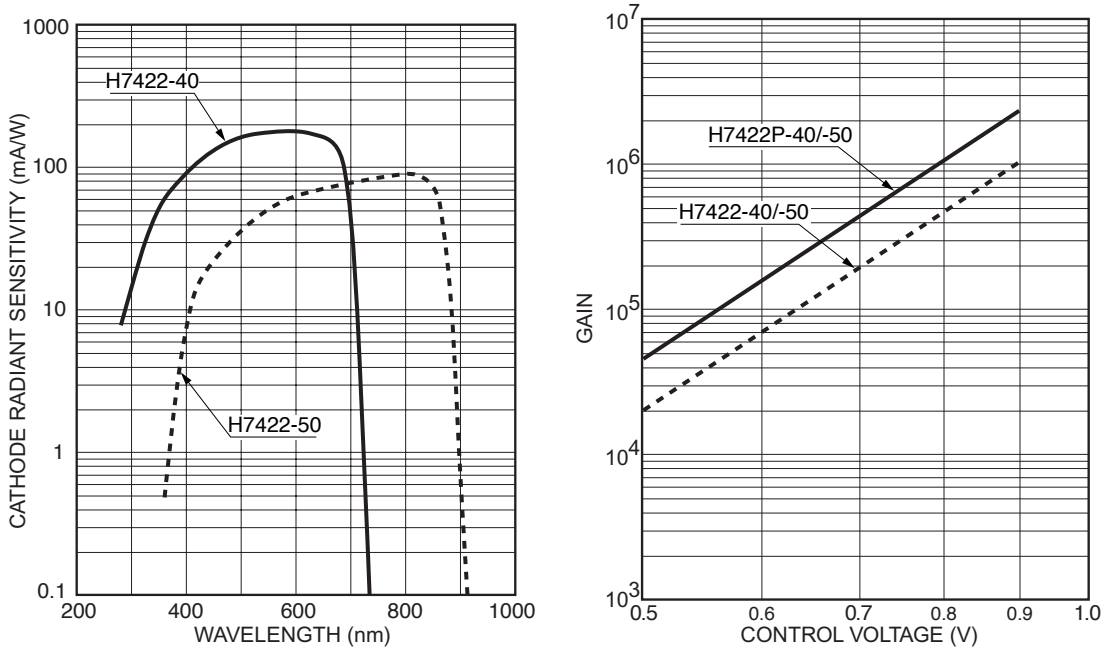
The devices used in the experiments are photosensors modules from Hamamatsu® series H7422, with real picture in Figure 4.6. They have internal high-voltage power supply circuit and a cooler installed in the metal package photomultiplier tube. The input is a free-space C-mount lens adapter protuding 4mm or more from the flange-back

with the option to add an FC type optical fiber connector. To achieve best performance, low thermal noise and high S/N ratio, the cooling system is made with a heatsink and a fan attached to the module.

Figure 4.6: PMT series H7422 with external cooler.

The photocathode is the GaAsP, with QE of 40% at peak wavelength and it is designed for the spectral range of 300 nm to 720 nm. The spectral response and the gain of the unit are respectively shown is Figure 4.7.

Figure 4.7: Cathode radiant sensitivity on the right and the gain on the left for the H7422 series. Bold lines indicate the module used in this work.

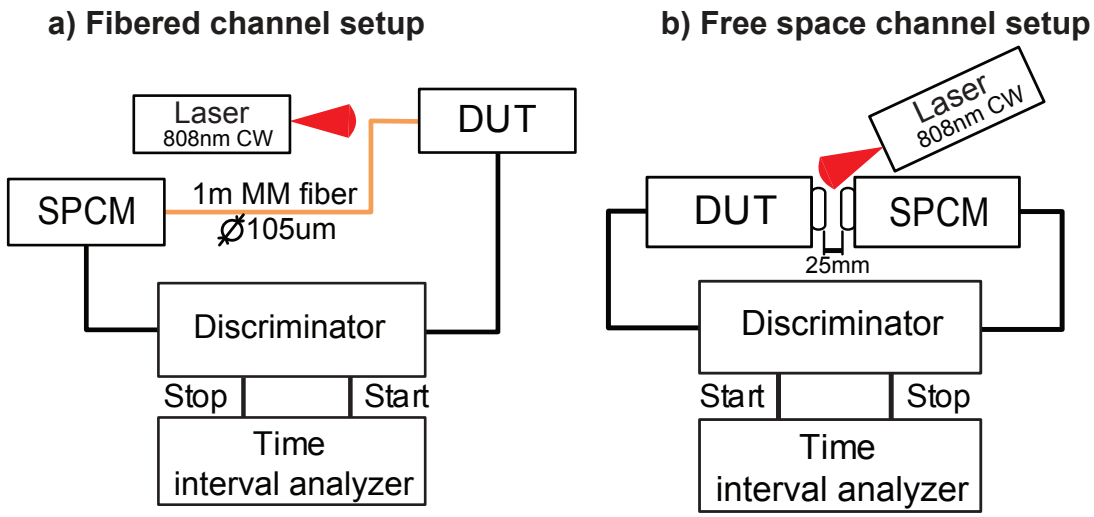


4.3.2 Time analysis

The investigation of the backflash emission in PMT's started by the setups shown in figs. 4.8(a) and 4.8(b). By quantifying the emission in two possible scenarios, with free space and optical fiber, a strategy to explore the potentialities of the phenomenon can be

developed. The starting point was to design a proof-of-principle setup able to measure and quantify the emission. The setup in Figure 4.8a has two units of the same type connected by a 105 μm core multimode fiber. Given the low number of darkcounts, the DUT unit had the count-rate increased by a free-space laser of 808 nm operating in CW regime to generate a high number of backflash photons. For the best coupling of the laser into the fiber, a hijack 20 cm close to the unit was enough, otherwise a significant count-rate could not be reached. The optimal count-rate was reached at 180 kcounts, slightly lower than its saturation level, which was 200 kcounts. After the assembling and alignment, the DUT and SPCM units had the count-rates of respectively of 180 kcounts±1kcounts and 16 kcounts±0.5kcounts. The difference in the count rates was due the position of the laser and the proximity of the hijack with the DUT unit. The backflash emission is then measured by a unit of the same type in the SPCM place.

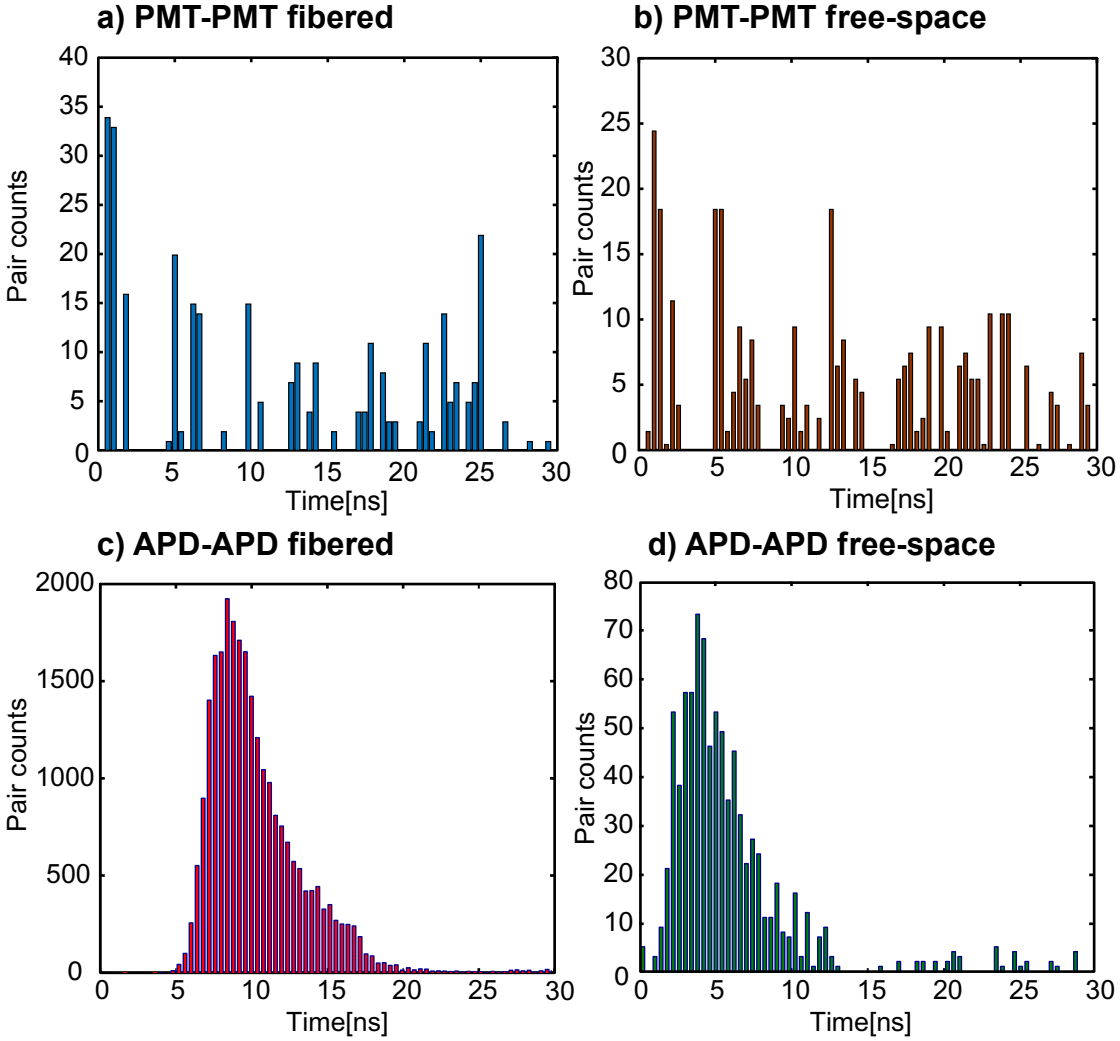
Figure 4.8: Setups for the investigation of backflash emission by PMT's.



For each click, a NIM (The nuclear instrumentaion module standard defines a NIM pulse as a negative logic pulse) pulse is generated with 2 mV amplitude and 3 ns width. The strategy to check the emission is explained as follows: a time interval analyzer model SR-620 records the arrival time of the pulses from both units. If the time difference between clicks are proportional to the travel time of the photons, the second click was caused by a photon produced in the opposite unit. In the case presented, as the output pulses of modules are undetected by the SR-620, a discriminator device model SR-400 had to be used. Clicks from the DUT unit starts an internal clock in the time interval analyzer and clicks from the SPCM stops the clock. The data is presented in histogram form, respectively in Figure 4.9(a) and 4.9(b).

All histograms represents only the coincidence points from the data collected. The time scale presented is only 30 ns, which is long enough to show the emission that should happen around 5 ns, the approximate travel time of a photon in a silicon fiber channel or

Figure 4.9: Histograms of backflash emission by different experiments with PMT's and APD's in four different scenarios.



125 ps corresponding to 2.5 cm of free-space propagation. As previously stated, the output levels of the units are not detectable by our time interval counter, SR-620. The SR-400 was set up with negative slopes and discriminator levels of -10 mV. A negative pulse of -1 V and 7 ns is generated for every count. The START/STOP configuration was adjusted for negative slopes and -200 mV for each channel, with DUT sending START pulses. It is noticeable the random pattern presented by the results and the low average pair count-rate. Comparable to the darkcount rate, in the order of 15-25 cps, the conclusion is the total absence of emission.

A few other experiments were conducted to double-check the emission with the same setups, but replacing the units by Si-APD. Three possible replacement scenarios were tested, as explained below:

1. Using free-space channel with a PMT unit as DUT and a APD as SPCM: by replacing the SPCM unit by an APD, we tested the PMT unit for any measurement abnormality or malfunction.

2. Using free-space channel with a APD unit as DUT and a PMT as SPCM: this scenario was not possible to be tested due the FC connector in front of the APD unit, which reduces significantly the number of coupling photons.

3. Using fibered and free-space channel replacing the units by two APD's: by comparing these two with the ones of first experiment, the conclusions are validated.

The histograms showed in Figures 4.9c and 4.9d compares only scenarios with two units of the same type, which excludes scenario 2 and 3. The table II shows the upper-bounds for all configurations using the setups in Figure 4.8. Based on the table upperbound values, the APD-APD setups show histograms with considerable coincidence points and the PMT-PMT histograms have a few points, indicating the absence of backflash photons.

Table 4.1: Statistical results for backflash experiments with PMT and APD units.

Description		Total counts	Pair counts	Upperbound
APD-APD	Fibered	10^6	25290	5.06×10^{-2}
	Free-space	10^6	806	1.61×10^{-3}
PMT-PMT	Fibered	10^6	71	1.42×10^{-4}
	Free-space	10^6	93	1.83×10^{-4}

4.4 Conclusion

Photomultiplier tubes had a special place in quantum optics experiments before the photodiodes popularization. The small darkcount rate added to other features were the reason. Nowadays, APD's and superconducting detectors have replaced them given their ability to measure single-photons and the capacity of geiger-modes.

This chapter started with a brief explanation of PMT theory. After that, the experimental method and the results are showed. The experimental results enlight that PMT's do not produce backflash. With a brief look at the theory, we realize that the photocathode has null chances of ejecting photons to the opposite side that it was designed. Another reason is that the strikes on the dynodes can eject electrons not photons.

Also, based on the histograms in Figures 4.9, the number of coincidence pairs is considerable low, making the distinguishability of them between darkcounts and sporadic clicks not possible. This conclusion discards further investigation. The PMT units analyzed had shown considerable null backflash emission in the spectral range measured with no apparent pattern, which characterizes the device as ***secure*** for this kind of security loophole. Regarding quantum cryptography, or QKD, the emission can be neglected and no other modifications are necessary for the optical systems.

5 SILICON AVALANCHE PHOTODETECTOR

Abstract

This chapter describes the experimental verification of breakdown (backflash) emission in a silicon avalanche photodetector unit. Initially, an overview of the Si-avalanche photodetector is shown. After that, possible measurement regimes using APD's are discussed. The experiment procedures and results from the backflash emission verification and a brief security analysis are explained in the sequence.

The absorption of photons by a material causes electronic transition to higher energy levels, resulting in free charge carriers [82]. Under the effect of an electric field, these carriers move and produce a measurable electric current. The photoeffect takes two forms: external and internal. The **external photoeffect** involves photoelectric emission, in which the photogenerated electrons escape from the material as free electrons. The **internal photoeffect** involves photoconductivity, in which the excited carriers remain within the material and serve to increase its conductivity.

The thermal detector operates by converting photon energy into heat. As a result of the time required to effect a temperature change, thermal detectors are generally inefficient and slow in comparison with photoelectric detectors. This chapter is devoted to one particular type of semiconductor photoelectric detector that rely on the internal photoeffect, the **avalanche photodiodes**. After a brief review of the device used and measurement regimes, experimental methodology and results are showed. To conclude the chapter, a preliminary theory about the backflash effect and the influence in quantum cryptography is elucidated.

5.1 Introduction

The use of photon counting mitigates against gain noise and circuit noise because the detector response is still normalized and discrete. Photon counting can be achieved by using **single-photon avalanche photodetector** (SPAD), also known as **Geiger-mode avalanche detector** [82].

Silicon SPAD's operate in the visible near-infrared regions ($\lambda_0 = 400 - 1000$ nm) and offer high efficiency ($\eta \approx 75\%$), low dark-count rates (≈ 75 $counts$/s) and sub-nanosecond timing resolution (≈ 100 ps). In the optical fiber communication band ($\lambda_0 = 1300 - 1600$ nm), InGaAs/InP are the devices of choice, but performance is far less impressive than at shorter wavelengths: typical parameters are $\eta \approx 75\%$, dark-count rate ≈ 5000 $counts$/s, timing resolution of ≈ 500 ps. Si and Si-Ge are occasionally used in this region. At yet longer wavelengths ($\lambda_0 < 4$ μm), devices relying on an InAsSb absorption layer together with an AlGaAsSb multiplication layer, on GaSb substrate, have been used. Devices fabricated from GaN and SiC have found use in ultraviolet. SiC has the

Figure 5.1: Encapsulated Silicon avalanche photodetector model.

particular merit that it can tolerate high temperatures and hostile environments. In all cases, SPAD's are subjected to a tradeoff between efficiency and bandwidth.

Photon counting can also be achieved by making use of **superconducting single-photon detectors** (SSPDs), which are broadband, low-noise, and fast although they require extreme cooling capacity and control. Basically the arrival of a photon locally creates a nonsuperconducting hotspot that gives rise to a response signaling the ocurrence of an event. Applications using superconductiong detectors require an expensive and specif equipment, demanding an extreme controlled environment. Here in this work, only Si-APDs are used for quantum communications.

In this work, a series of experiments were conducted to analyze the emission of photons during the avalanche breakdown in one model of Si-photodetector(SPD), as previous realized with photomultiplier tubes (PMT). The unit tested was the standard commercial model SPCM-AQRH-12-FC from Excelitas as detailed explanation before. The emission of light from Si-semiconductors junctions is not recent. The first report was published by Newman [27], which described the emission from silicon p-n reverse bias junctions. Subsequently Chynoweth and McKay [83] released a detailed study of the phenomenon and concluded that the light emitted originated from recombinations occurring between energetic electrons and the holes in the avalanche breakdown region. After that, several other papers were release stating distinct possible causes for the phenomenon and trying to quantify this emission[25, 26, 84–88]. However, in 2001 Kurstsiefer[28] raised a question about the connection between the emission and quantum cryptography. He mentioned if the light emitted could induces a security loophole in quantum communication.

Quantum key distribution (QKD) is the most famous branch of the quantum communication field. It has the premise of perfect security by exchanging cryptography keys secured by the laws of the quantum mechanics[16, 89]. Nowadays, a countless number of experimental systems are available [3, 29–31, 54, 90–92] and the security issue still causes

tumult in the quantum community. The theory predicts an unconditional security, given the fact that all the components in the system follows his most optimistic premises of functionality[17] . However the current technology is far behind the theory. In practical quantum key distribution (QKD), the most vulnerable part is the receiver which concentrates most of the attacks. Basically most of its structure has already been exhaustively investigated in search for loopholes. However, light emission from photon detectors [28] has not yet been well studied. In this direction, this work investigates light emission from a QKD receiver which can leak secret information into the optical channel to an eavesdropper. The goals here are to perform a good estimation of the emission in terms of the number of carries, characterize the amount of emission into the channel of one specific type of receiver, upper-bound the light emitted, measure the emission spectrum in order to prevent side-channels and check for a possible "backflash attack" by checking the leakage of information.

Based on the physics behind the backflash emission in avalanche photodetectors, the state of the backflash photons might not be in coherence with the state of the photon that caused the click. Unfortunately, after the creation stage, they might pass back through other components inside the receiver, such as PBS, which encode the polarization of that specific channel and carry those information out to the channel. If this happens, Eve can intercept each backflash photon and perform measurements to determine which channel those photons were created. Eve can also estimate the time delay between her detector and Bob's APD to find which pulse caused the backflash, which enhances the knowledge about the key.

To verify those speculations, a few tests should be realized on a QKD system. First, the probability that a click would generate a photon backflash that pass out of the channel. Second, test whether those backflash photon are able to carry out some channel's information that can be distinguished by an eavesdropper.

In this chapter, Silicon avalanche photon detectors are described and the experiment performed to quantify the breakdown emission or gently called **backflash emission** stated. The effect considered in the context of quantum security was so far considered by [28], and no effective analyses was made. Here, a new analyzes is performed, boundaries are defined to explain possible information leakage in quantum communication systems.

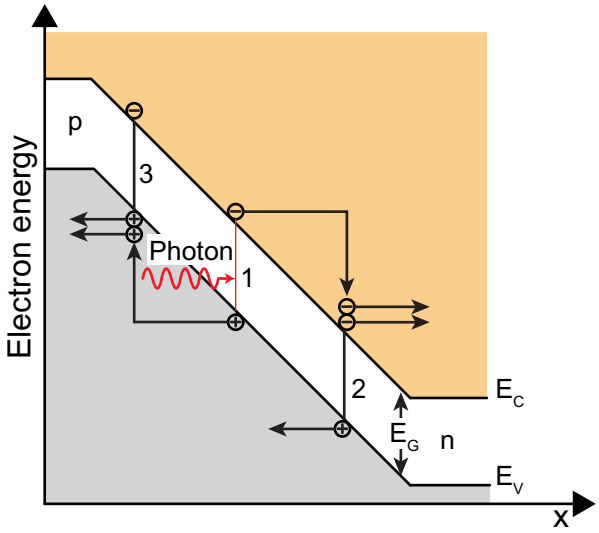
5.2 Si-avalanche photodetector

Avalanche photodiodes (APD) operates by converting incoming photons into a *cascade* of moving carrier electrons. Each cascade is called **avalanche** because it creates a burst of ejected electrons inside the junctions. Each electron ejected gives rise to a new avalanche process. The process grow exponentially until the amount of electrons current is sufficiently measurable. The charge carriers can therefore acquire sufficient energy to be

free by a process called **impact ionization**. The device is configured as a strong-reversed biased photodiode, in which the electric field in the junction increases.

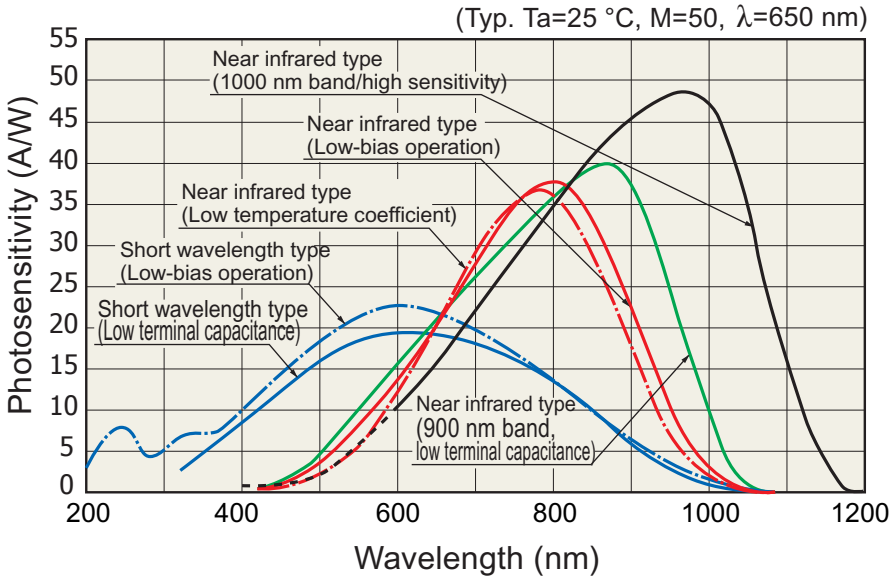
The current of electrons generated by successive avalanches is called **photocurrent**. The photogeneration mechanism of an avalanche photodiode is the same for other photodiodes and it is depicted in Figure 5.2. When light enters a photodiode, eletron-hole pair are generated at point 1. The electron accelerates under the influence of strong electric field, thereby increasing its energy with respect to the bottom of the conduction band. The acceleration process is constantly interrupted by random collisions with the lattice in which the electron lose some of its acquired energy. These competing processes cause the electron to reach an average saturation velocity. Should the electron be lucky and acquire an energy larger than E_G at any time during the process, it has the opportunity to generate a second electron-hole pair by impact ionization (say at point 2). The two electrons then accelerate under the effect of the field, and each of them may be the source for a further impact ionization. The holes generated at points 1 and 2 also accelerate, moving toward the left. Each of these also has a chance of creating an impact ionization whether they acquire sufficient energy, thereby generating a hole-initiated electron-hole pair (e. q., at point 3).

Figure 5.2: Photocurrent generation within the standard semiconductor structure. Top layer: conduction layer and bottom layer: valence layer.



The APD model used in the experiments is the one shown in Figure 5.1. It is inside the newly improved SPCM (Single Photon Counting module) from Excelitas Technologies company (www.excelitas.com). The model used is the SPCM-AQRH-12C. It uses a unique silicon APD, SliK type, with a circular active area, achieving a peak of photondetection efficiency grater than 70% at 700 nm over a 180 µm diameter with unmatched uniformity over the full active area. The photodiode is both thermoelectric cooled and temperature controlled, ensuring stabilized performance despite ambient temperature changes. Figure 5.5 shows a privileged view of a decapsulated dead sample. TEC plates are shown with

Figure 5.3: Photosensitivity expressed in therms of spectral range for several models of silicon avalanche photodetectors.

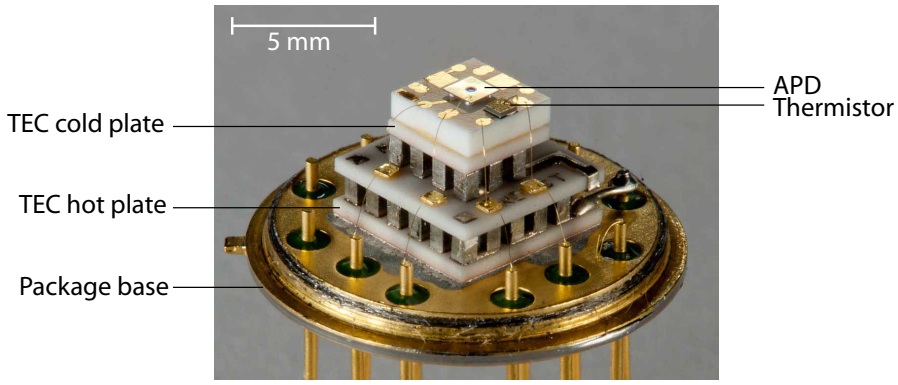


several stages, the APD itself and the thermistor, responsible to measure the inner temperature. Temperature operation has been increased and the module (case temperature) will function between 5°C and 70°C. A real picture of the module is shown in Figure 5.4.

Figure 5.4: SPCM module from Excelitas, model SPCM-AQRH with an encapsulated Si-APD attached.

Inside the model, a modern electronic circuitry is responsible for controlling and outputting. Recent electronic circuit improvements have reduced the minimum dead time to 20 ns, thereby increasing linearity and improving dynamic range and performance of the module. A few other key features are given: typical supply voltage of 5V; the dark count rate around 500 *counts*/s for the module used; afterpulse probability of 0.5%; single-photon time resolution of 350 ps; TTL output pulse. As explained before, given several advantages between the avalanche photodiode and the regular diodes, and based on the modern electronic circuit inside the module, the photodetection efficiency is higher than

Figure 5.5: SPCM module from Excelitas, model SPCM-AQRH with an encapsulated Si-APD attached.



its counterpart, around 70%.

5.2.1 Avalanche active quenching regime

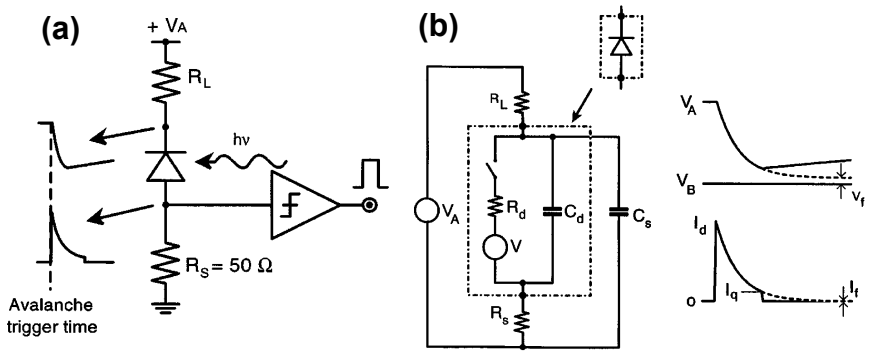
Silicon APD's have been extensively investigated and are nowadays well developed. Considerable progress in the single photon detection field has been achieved regarding efficiency, desing and fabrication technique. A wide range of good modules are commercially available, each one well designed for a variety of applications. For quantum communication applications, APD's operating above the breakdown voltage are well suited.

Avalanche photodiodes usually operating above the breakdown voltage (Geiger mode) need to be connected with avalanche-quenching circuits to detect single photons [5, 93]. Two main types of circuit configuration are used: passive quenching circuits (PQC), which are simple to implement, but limited by passive electronic components. Active quenching circuits (AQC) is a suitable option to exploit the best performance of the APD. Each on has their use specifically designed by each company. The modules used in this work operates with a modern version of active quenching circuit.

A few drawbacks are detected in SPAD's working in PQC: slow recovery form avalanche pulses and uncertainties in the quenching time parameters. The idea of the PQC is to develop a voltage drop on a high impedance load to make the avalanche current quech itself. The circuit is pretty simple and widely used today. The SPAD is reverse biased through a high balast resistor $R_L = 100$ kΩ or more, C_d is the junction capacitance (typically 1pF), and the C_S is the stray capacitande (capacitance to ground of the diode terminal connected to R_L, typically in the order of a few picofarads). The diode resistance R_d is given by the series of space-charge resistance of the avalanche junction and of the ohmic resistance of the neutral semiconductor crossed by the current. Basic circuit schemes are shown in Figure 5.6.

The avalanche current discharges the capacitances so that V_d and I_d exponentially fall toward the asymptotic steady-state values of V_f and I_f, as in Figure 5.6b. Avalanche quenching corresponds to opening the switch in the diode equivalent circuit, so that

Figure 5.6: Basic passive quenching circuits: (a) configuration swith current-mode output and (b) equivalent circuit of the current-mode output configuration. The avalanche signal is sensed by the comparator that produces a standard signal for the pulse counting and timing. Extracted from [5].



the capacitances are slow recharged by the small current balast resistor R_L. The diode voltage exponentially recovers toward the bias voltage and the the time is given by the capacitances and the balast resistor values.

In the active quenching circuit (AQC), a few drawbacks can be avoided by sensing (detecting) the avalanche level. It means basically to sense the rise of the avalanche pulse and react back on the SPAD, forcing, with a controlled bias-voltage source, the quenching and reset transitions in the appropriate short time [6]. The first AQC application dates back to 1975 [94], but it was in 1981 before its application to photon timing was attempted, fast gating of the detector was demonstrated [22].

Figure 5.7: (a) Principle of active quenching: current-voltage I-V characteristic curve of SPAD and switch load line (dashed lines) of the AQC controlled voltage source. The Q arrow denotes the quenching transition and the R arrow the reset transition. (b) Output pulses from AQC designed for minimum dead time that operates with a standard SPAD, biased 0.9 V above breakdown voltage, displayed on a fast resolution oscilloscope at 5 ns/*div*. Extracted from [5].

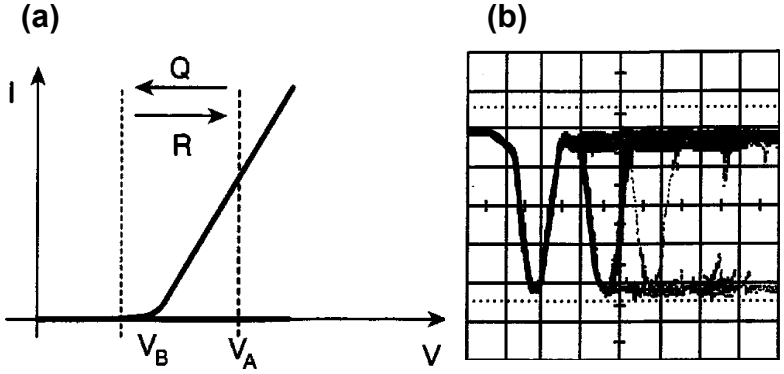
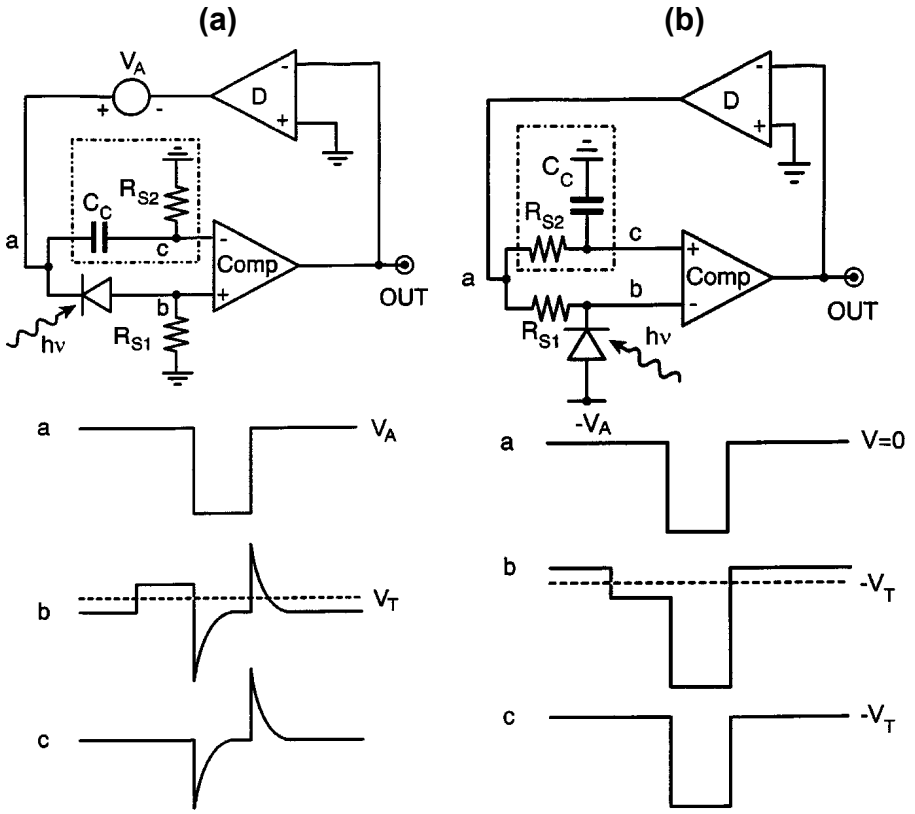


Figure 5.7a illustrates the idea of the active quenching method. The rise of the avalanche pulse is sensed by a fast comparator whose output switches the bias voltage source to breakdown voltage V_B or below. After an accurate controlled hold-off time, the

bias voltage is switched back to operating level V_A. A standard synchronous pulse to the avalanche rise is derived from the comparator output to be employed for photon counting and timing. The basic advantage offered by the AQC approach are the fast transitions (from quenched state to operation level and vice versa) and the short and well defined duration for the avalanche current and dead time.

Two basic configurations are inherently linked to the SPAD in AQC mode, one with a quenching terminal opposite the sensing terminal (Figure 5.8a) and the other with a coincidence and sensing terminal (Figure 5.8b). In any case the sensing terminal has a quiescent voltage level at ground potential or not far from it, since it is directly connected to the AQC input [95].

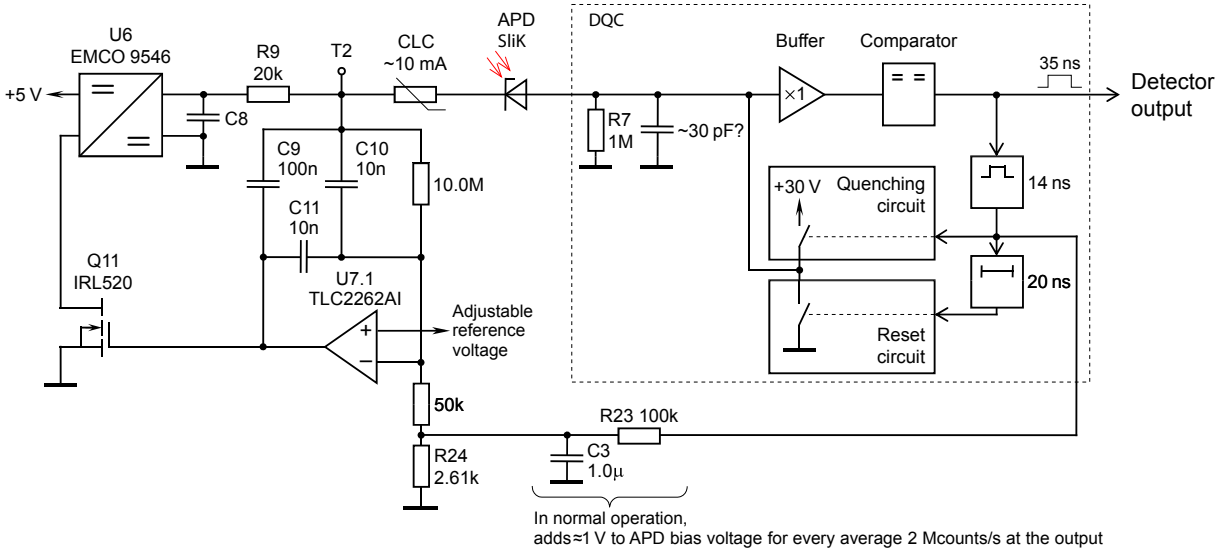
Figure 5.8: Simplified diagrams of the basic AQC configurations with (a) opposite quenching and sensing terminals of the SPAD and (b) coincident quenching and sensing terminals. Voltage waveforms for both diagrams represent the circuit nodes marked with the same letter. Extracted from [5].



In figure 5.8a, the network in the dotted box compensates the current pulses injected by the quenching pulse through the SPAD capacitance, thus avoiding circuit oscillation. On the other hand, the dotted box in Figure 5.8b is employed to avoid (i) locking of the circuit n the triggered state by the quenching pulse, and (ii) circuit oscillation due to small overshoots and ringing of the quenching pulse. The quenching and the reset driver, labeled D in both diagrams of Figure 5.8, can be implemented with either a pulse-booster [23, 94, 96–98] or electronic switches [93, 98–100] connected to two different dc voltage

sources that correspond to the operating and quenching voltage levels. With fast switches the AQC can be simpler, more compact, and have lower power dissipation, since the driver dissipates power only during the transitions. With a pulse-booster circuit the AQC output can be better approximate a SPAD operation, better control and fine adjustment of the pulse waveform is usually obtained.

Figure 5.9: Circuit diagram of the simplified reverse-engineered of PerkinElmer SPCM-AQR module. Nowadays, the PerkinElmer company was bought by Excelitas and adopted definitely the new name. Extracted from [6].



The AQC circuit used by the Excelitas models are not available due commercial restrictions. Fortunately, a paper released in 2011 [6] used reverse-engineered to analyze a few steps and components around the avalanche time and directly connected to the APD. The circuit depicted in Figure 5.9 shows a modern version of an AQC, with separate circuits for quenching and reset the avalanche. For normal operation, the APD cathode (superlow-k SliK type) is biased at a constant high voltage, stabilized by a feedback loop containing an opamp U7.1 (Texas Instruments TLC2262), a field-effect transistor Q11 and a high-voltage DC/DC converter module U6 (EMCO custom model no. 9546). The anode of the APD is connected to a detection quenching circuit (DQC). The DQC senses charge flowing through the APD during the avalanche, then briefly connects the APD anode to +30 V to lower the voltage across the APD below breakdown and quench the avalanche. The APD anode voltage is subsequently reset to 0 V, and the detector becomes ready for the next avalanche.

5.3 Breakdown emission analysis

The simplest methodology possible of experimental analysis was adopted in first place, the direct emission and measure system. The setup in Figure 5.8a has one device under

test (DUT), generating detections (only due to darkcounts) and possibly emitting some light. To quantify that light, another detector unit (SPCM) is connected with a multimode fiber patch cable of 105 μm core (Thorlabs M43L01). Both units are connected to a time interval counter, model SR620 from Princeton Technologies. The direct approach to verify the emission of light from those units is to check on the time difference between two consecutive detection pulses using the time mode function of the SR620. In this mode, two pulses are necessary to START the timer and consequently to STOP it. For both experiments in Figure 5.10, the START and the STOP pulses are sent by the DUT and SPCM units respectively. The trigger level used was 0.8 V with positive slope due to the nature of TTL output pulses of the units [excellitas SPCM datasheet]. A 40 ns delay line was inserted in the SPCM electric cable, which reason is explained later in this work.

Figure 5.10: Setups for measurement of breakdown emission from Si-APD units. (a) Face-to-face fibered setup and (b) setup for distinct wavelength analysis.

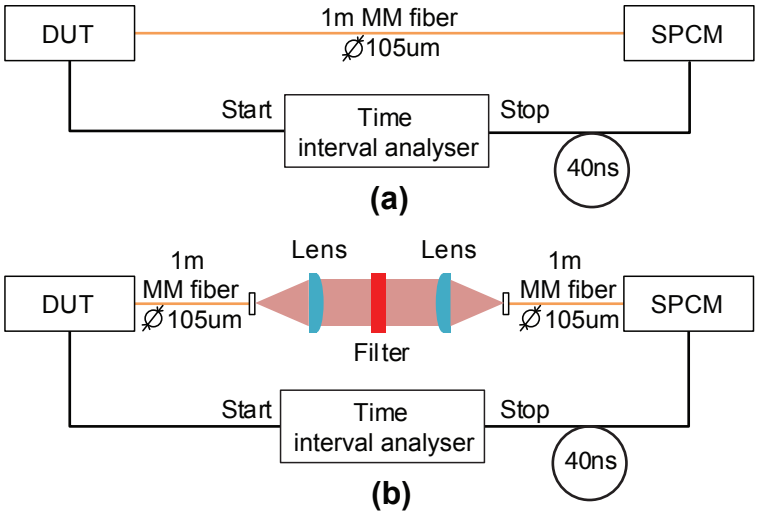


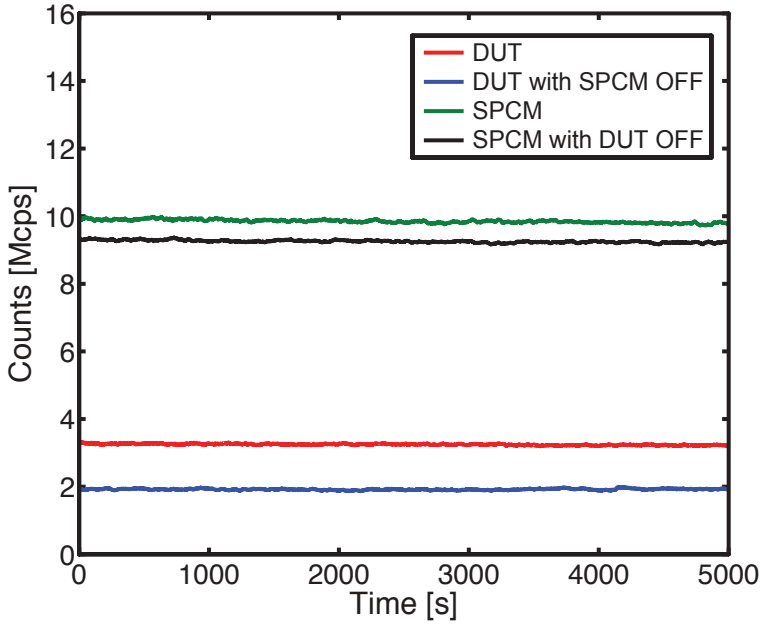
Figure 5.10b presents a slightly modified setup in comparison with the setup in Figure 5.10a. The objective of the free-space arrange is to analyze the emission in specific bands of the spectrum by using spectral filters. The DUT and the SPCM units are linked to the optical path by the use of 1 m multimode fiber patch cables each. The free-space optical assembly is composed by: two aspheric A-coated lenses, one (Thorlabs A397TM-A) of 11 cm focal distance and NA of 0.22 responsible to collimate the beam and one(Thorlabs C280TME-A) with focal distance of 18.5 cm and NA of 0.15, placed to couple the collimated beam into another multimode fiber optic to the measurement unit. Filters are inserted in between the lenses, which are separated by 20.5 cm. As for the previous experiment, the DUT and the SPCM provide the START and the STOP pulses respectively, with same electric cables length configuration. For both setups, the time interval analyzer is connected to the computer through GPIB port, which uses an automated algorithm to control the acquisition.

5.3.1 Time analysis

To precisely identify the origin of the clicks in the DUT unit, whether caused by backflash emission or thermal darkcount, the travel time of the photons between the units was observed. The scenario where the backflash emission takes place is: a photon generated by an avalanche breakdown causes a detection in the SPCM unit within a time based on the travel time of a photon in that specific channel. By checking the travel time in the SR620, which has to be sufficient for the photons travel between both devices, all the electronics processing and for the output electrical signals to reach the time counter, it is expected a high number of events non-uniformly distributed in a small range around it.

In Figures 5.10a and 5.10b, two photodetection units of the same type were used and connected facing each other. So, any photon produced by the units will run through the same channel, regardless of direction. Beforehand, a count-rate check was realized using the setup in Figure 5.10a. The count-rate of each unit was recorded to check for discrepancies possible caused by mal-function or environment disturbance. As shown in Figure 5.11, the number of counts is considerably constant in time and based on the availability of the other unit, the first signs of backflash emission are verified. The increase in the units count-rates point out extra counts only due to photons emitted by each other unit.

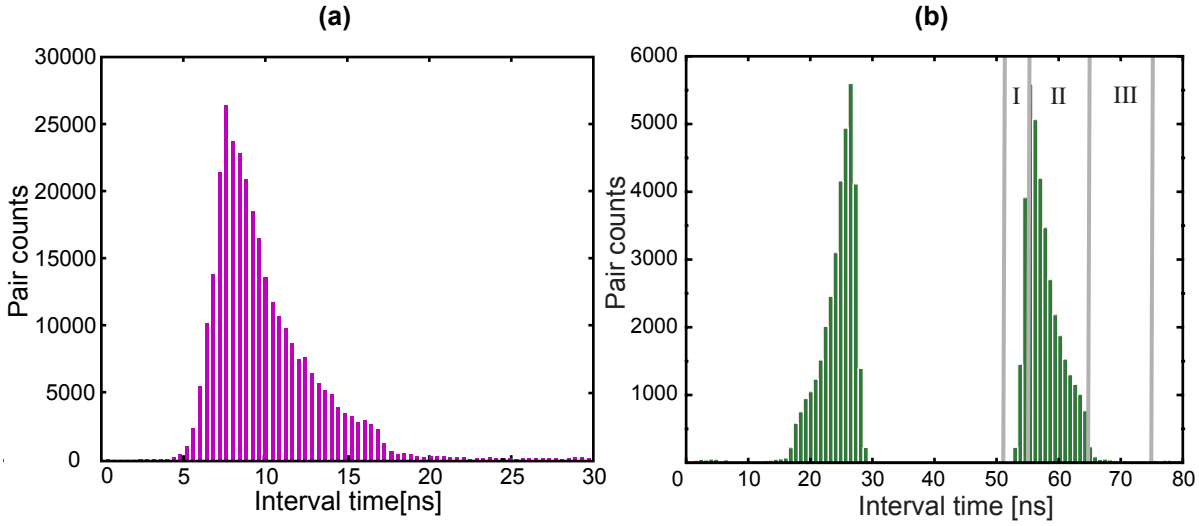
Figure 5.11: Units count-rates verified during a interval of 5000 s.



For the experiments in Figure 5.10a, two slightly different configurations were prepared: the first using both electrical cables (connecting the photodetection devices to the counters) with the same length, equal to 10 ns and second with a cable delay inserted after the SPCM of 40 ns. With this configuration, using only the darkcount rate as source

of clicks, 14 hours were necessary to get a dataset of 1 Million records. Histograms in Figure 5.12 show the emission for the setups in Figure 5.10. The histogram on the left hand shows the pair counts for the first scenario, where no delay line is included. Only one chart represents two distinct emissions overlapped, one from each unit. Each click starts the clock and a later click in the other unit stops. The starting point ($\geq$ 5 ns) of the chart agrees with the delay incurred by the fiber path. No information about the characteristic of the pulse can be inferred by the overlapped chart in Figure 5.12a.

Figure 5.12: Histograms of pair counts for setup in Figure 5.10a (a) with no delay line and (b) with 40 ns delay line. The peak difference in (b) is due to the darkcount of the units, which was at the time 352 *counts*/s for the DUT unit and 474 *counts*/s for the SPCM.



The distribution in Figure 5.12b is the result of the setup in Figure 5.10a with 40 ns delay line included. This feature enable us to analyze separately two events which happen simultaneously: one is when the DUT unit clicks first and cause a second click in the SPCM because of the backflash emission (represented by the second peak on the right), and the second one is the opposite, when a click in the SPCM happens first and causes a later click in the DUT unit (first peak on the left). The average for the second peak happens in about 59 ns, which shows a clear sign of clicks happening faster than the darkcount rate, which is 500 *counts*/s. Based on DUT darkcount-rate, it is supposed to have random clicks in about 2.25 ms. In the absence of backflash emission, the time range analyzed should present only a uniform distribution with a few or no points at all, which is not the case. Each peak resembles the avalanche peak for SPAD current profile, with each peak representing the emission from one unit. The right peak is selected and marked with three vertical lines to indicate three distinct regions to explain the shape. The region I indicates the avalanche rapid development, an exponential grow in the number of carriers released by consecutive impact multiplication processes. The region II shows

an exponential decay due to the recombination of most of the carriers, a process intrinsic to the photodiode and also caused by a rapid discharge of the parasite capacitors in the electronics. Finally the region III is the avalanching quench caused by the electronic system of the unit, actively quenched.

The emission probability can then be calculated separately for each peak (each unit), just by subtracting the darkcount rate and dividing by the quantum efficiency of the detector, which is ≈ 0.55. For the peak to the left, the sum of pair counts is 12122 $counts/s$, which gives an emission probability of 0.0206. For the peak to the right, with a total pair count of 11683 $counts/s$, the emission probability is 0.0212.

In Figure 5.10b, optical free-space filters were used to check the backflash emission in specific wavelength windows. Two 532 nm filters were used in the first run, one shortpass filter with cutoff in 770 nm, model FESH0700 of Thorlabs and a bandpass with 90% transmittance in 532 nm, model LL01-532-12.5 from Semrock. It was observed in the range of $0 - 100$ ns the absence of emission, as the number of samples in this range was very low and uniformly distributed, with an average of 1 $count/$ns, it can be categorized as sporadic, due to random click emission nature. Following, emission in the 808 nm window was observed using a 8 nm bandpass filter in 808 nm of LOT-Oriel for two scenarios, one with the same length for electric cables and other with a 40 ns delay line. To calculate the emission probability, the efficiency of the optical setup should be considered. Table 5.1 show the emission probabilities.

Table 5.1: Emission probability for the setup in Figure 5.10b. The calculation of the spectral filter probabilities, the photodetection efficiency used was 0.55 limited to a spectral range of $510 - 860$ nm.

Description	**Total counts**	**Pair counts**	**Emission probability**
No spectral filter	10^6	37643	1.08×10^{-1}
3 nm spec. filter of 532 nm	10^6	5	1.41×10^{-5}
8 nm spec. filter of 800 nm	10^6	2306	6.50×10^{-3}

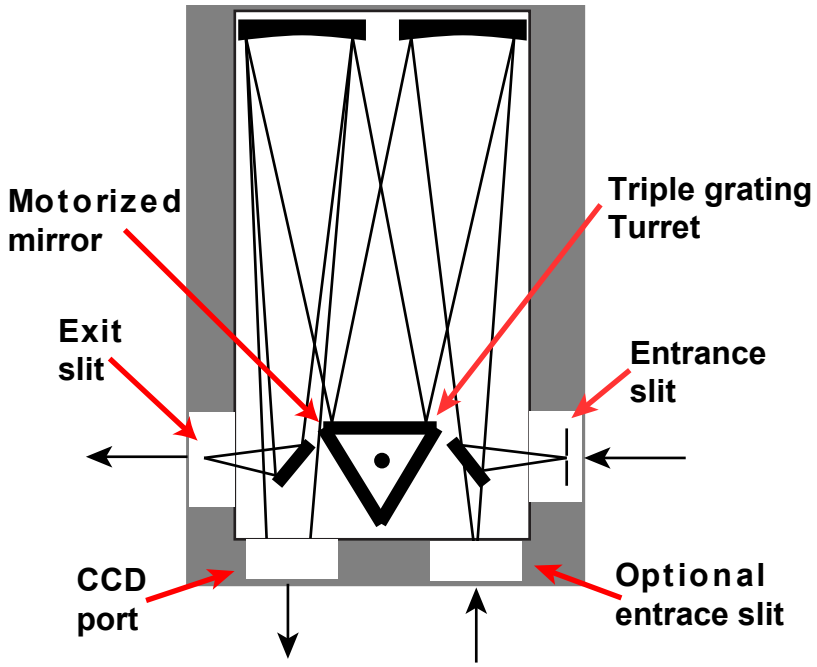
Based on the histograms presented in Figures 5.12 and the emission probability, the existence of backflash emission is far from negligible. For instance, in a BB84 QKD scheme, with a passive receiver, if an eavesdropper can get returning photons from the measurement setup, they carry polarization information about the path followed inside the receiver and the detector which it was originated, breaking the entire security of the protocol.

5.3.2 Spectral analysis

The spectral distribution of the emission provides a useful knowledge, for instance to create counter-measures for systems sensible to the emission in other wavelengths. For the measurements performed in this work, the model SpectraPro-750i from Acton research

corporation was used. It is composed by a monochromator with a triple grating setup, an output to a CCD cryogenic camera, and a flat slit connected to a FC/PC connector as input connected before the slit. The monochromator is a system of two parabolic lenses that reflects the input light to the grating system and to the CCD sensor, as shown in Figure 5.13. The gratting used had 600grooves/mm planed rule. The sensor is cooled down by liquid N_2, reaching operating temperature of $-70°C$ to $-120°C$, which reduces to minimum the number of darkspots. It has a sensor format array of 1320×100 image pixels. The measurements were realized using the procedure called "step-and-glue", used to measure wide spectral ranges. The maximum spectral interval measured by the spectrometer was 80 nm. So, to cover the entire spectrum band, several exposures had to be taken, each one taking 120 s, and placed together at the end of the measurements. Because of the laser radiation over the monochromator due to reflections on the optical table, two limitations were implemented. The exposure time had to be short, avoiding saturation and damage. And the second, cut off the laser wavelength due to saturation in thar specific wavelength. As it is shown ahead, the measurements charts had to start after 532 nm, in a multiple wavelength of 80 nm, the exposure time window and to finish before 1064 nm, the second harmonic of the laser.

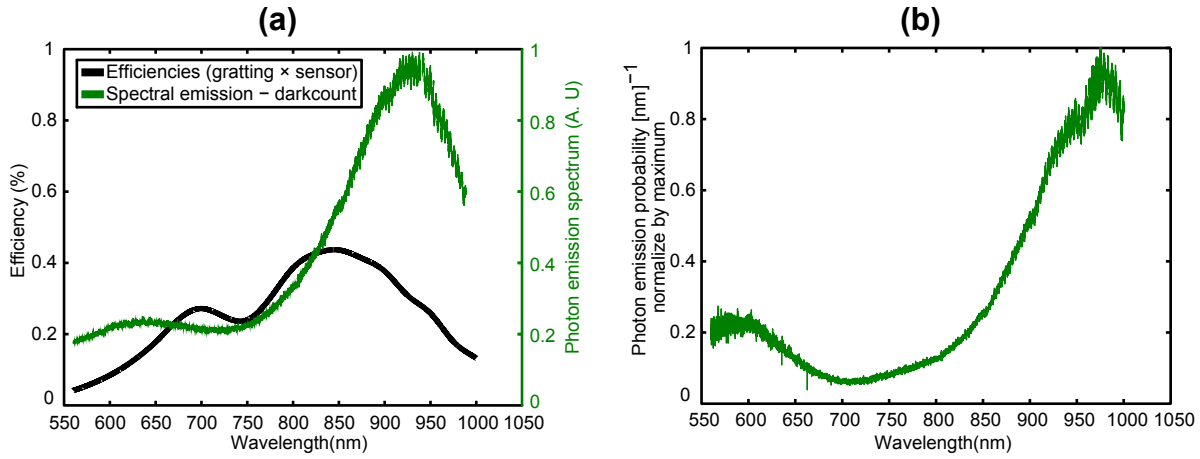
Figure 5.13: Monochromator design Model SP-555 from SpectraPro-750i series manufactured by Acton research corporation.



To increase the visibility of the measurements, a free-space laser of 532nm operating in CW had to be used. It was pointed out to the input of the unit to increase the count-rate of the breakdown emitted photons. The unit was connected to the monochromator by a 1m multimode fiber, the same used in the previous experiments. The count-rate was increased to the maximum possible due to the low laser power, about 150mW pointed out

to the fiber cladding. The number reached was 22×10^6 counts, almost half-way to the saturation, which is 40×10^6 counts. Two sources of loss were found in the monochromator: the grating and the CCD sensor. Both have a detection efficiency dependent on the wavelength. So, the correct spectral measurements has to take into account those features. Figure 5.14 shows the spectral measurements for the system efficiency and the final result after considering efficiencies and darkcount.

Figure 5.14: (a) Spectral backflash emission in green subtracted the darkcount and in black the efficiencies of the sensor and gratting combined. (b) the final spectrum.



The starting point of the measurements was 560 nm, for two reasons: 1- the laser light in 532 nm pointed out to the optical fiber saturated the spectrometer, which has a single-photon sensibility. 2- the efficiency range of the grating starts in 500 nm, so the first 60 nm had to be cutted off. The measurement curve was normalized for the efficiencies and for the maximum of the measurements, that was 1905 photons for 941 nm. Each measure windows was exposed for 2 min, and had the width of 80 nm. A process of step-and-glue was responsible to gather the absorption windows. The highest emission window was found to be $850 - 1000$ nm, with the maximum peak of 6940 counts in 975.2 nm. One can also identify false peak at 572.6nm, in the beginning of the scale, due to the high efficiency of the CCD sensor in that range (not shown in Figure 5.14). However, the efficiency of the detector is less than 30% for 560 nm , what makes impracticable the use of that specific wavelength. That specific emission pattern is only shown due to the unusual shape of the CCD sensor efficiency, which starts to be sensitive at 200 nm and has a peak of $\approx 95\%$ in 550 nm.

Comparing the emission of the breakdown emitted photons with the photodetector efficiency, we noticed a non coincident scenario. The peak of measurement do not the agree with the peak of detection efficiency, which is around 700 nm. The results show that only half of the emission happen due to the peak of detection efficiency, meaning that countermeasures to block the breakdown emitted photons should consider the range

around the peak of 941 nm. Finally, considering the final shape of the chart, we believe that emission higher than 1 μm should be highly considered.

5.4 Eavesdropping experiments

The realization of future safe communication is entirely conditioned to the investigation and solution of the security problems actually presented. There are several papers showing loopholes and their specific countermeasures. It is a common sensus that the main problems of the quantum communication systems are located into their detection apparatus. And the main pieces of those apparatus are the photodetectors. Most of the eavesdropping attacks are originated due to its imperfections, like trojan horse attack [101] and blinding attack [60]. However, a failure point presented several years ago did not attract too much attention, the breakdown emission, known as the backflash emission.

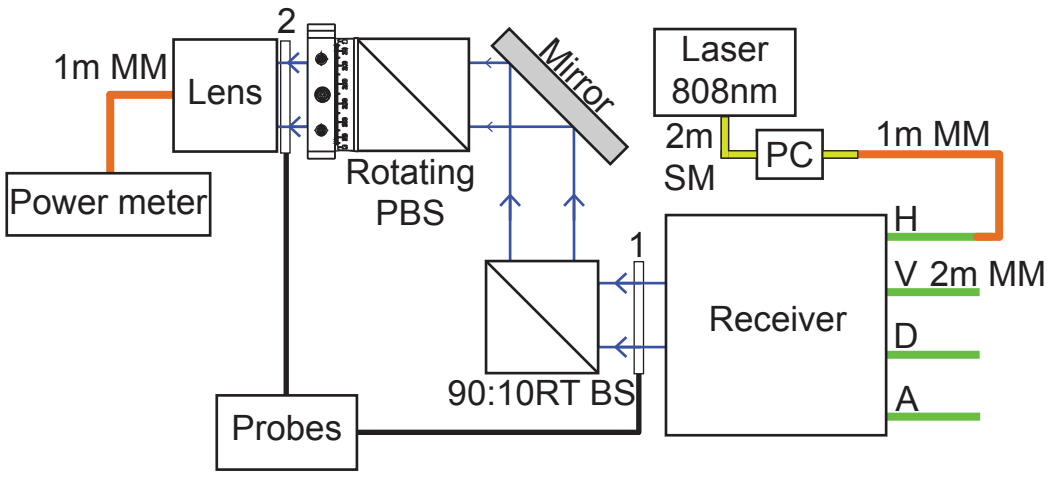
The structure of the security investigation applied nowadays works as follows: a loophole for some device or system is discovered, then an attack strategy is proposed using the advantage over that specif breach. After a few prof-of-principle realizations, several counter-measures are proposed in counterpart. Usually after the step of discovering a counter-measure, a new loophole is found. As showed previously in this work, there is a sporadic emission caused by impact ionization during the avalanche in the photodiode that may be a new loophole for most of the systems using photodetectors. This phenomenon causes ejection of some photons backward from the photodetector that may be back into the channel (Eve's domain). In this section, we investigated the ability of Eve to distinguish the click between different channels or detector units and hence, gain information of Bob's key.

5.4.1 Loss analysis

The setup shown in Figure 5.15 was designed to calculate the loss for the counter propagating light. The photons generated in the photodetectors have to travel from the unit backwards to the channel passing through the entire system. The idea is to make some light travel back to the channel and measure the loss. The system uses a CW laser in 808 nm, which is close enough to the receiver's wavelength 785 nm, connected to a polarization controller (PC), responsible to decrease the loss caused by variations in the polarization. The laser and the PC are then connected via 105 μm core 1 m of multimode fiber to a receiver that works as a passive basis choice setup (regular Bob). More details about the receiver later in this section.

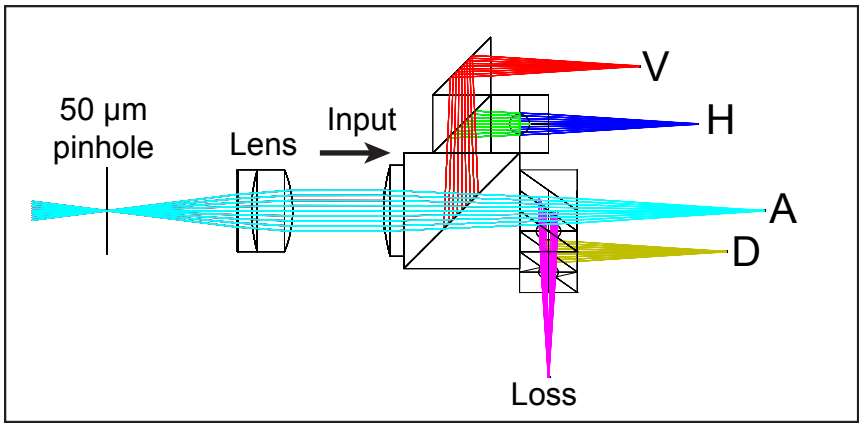
After the receiver, a 90:10 (R:T)BS will drive the light to a regular dielectric broadband mirror, then to a rotating PBS. After the PBS, an achromatic lens focus the light into a MM fiber connected to a power meter. The receiver used in this setup was an integrated receiver by INO company designed for a free-space polarization encoding QKD

Figure 5.15: Setup for measurement of the loss due to the back propagating light.



systems running at 785 nm. Figure 5.16 shows a picture of the device, with its four green multimode fibers, each one connected to the output of one polarization path dependent (A, D, H and V). The scheme represents the internal structure of the crystal designed to work as a passive selecting basis setup.

Figure 5.16: Receiver model designed by INO working on 785 nm. Crystal structure within the model and light paths based on polarization state.



A diverged beam of 500 µW with mixed polarization light was injected through each channel of the receiver. The light was coupled to the receiver through each multimode fiber at the end of receiver. It was sent to Eve setup by a 90:10RT beam splitter (BS). Then, passed through a polarizing beam splitter (PBS) to a power meter which represent Eve measurement device. We adjust all components to maximized the coupling between Eve and the receiver. After that, the PBS was rotated to find the orientation where the light coupled from H-channel was maximum and where it was minimum. The ratio between the input power and Eve's power meter was recorded. This process was repeated for all four channels, then the extinction ratio of Eve receiver could be calculated and it is showed in Table 5.2. In real eavesdropping, Eve can split the backflash photon into

four PBS oriented in 'Max' angle for each channel to get a real information of where the photons came from.

Table 5.2: Extinction ratio of loss setup.

Channel	**Max**		**Min**		**Ext. Ratio**	**Loss(%)**
	Angle(deg)	Power (μW)	Angle(deg)	Power(μW)		
H	3	25	91	0.15	166.67	99.60
V	94	19.8	1	0.03	660.00	99.85
D	315	20.7	223	1.94	10.67	91.63
A	49	23.5	141	3.69	6.37	85.30

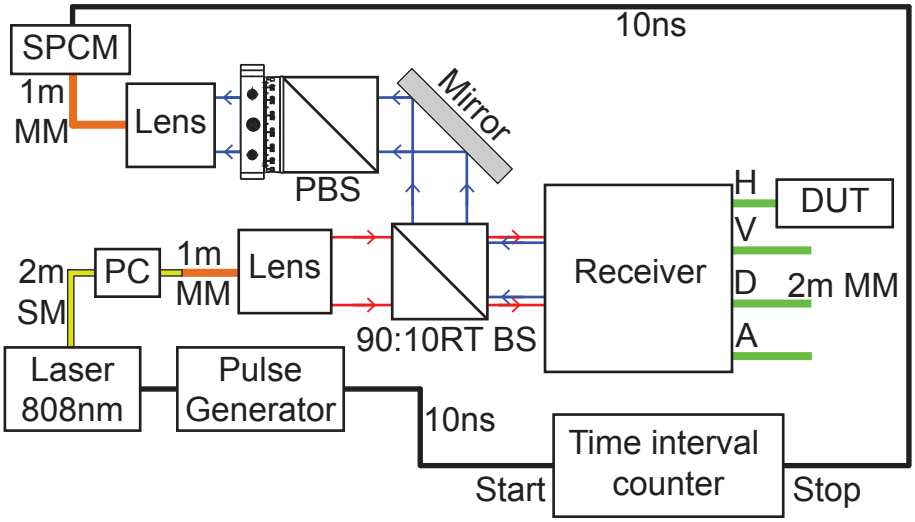
The drastically lower of distinction ratio of D and A polarization was due to the use of mirror which was essential for the alignment. In real eavesdropping, Eve can replace this mirror with a tip-tilt piece for a better alignment setup. As the system is not designed for back propagation, it is expected that the loss is high. Instead of the loss caused by the crystal polarization selection, another sources of loss can be outlined: the fiber-air coupling, which has no proper alignment in the opposite way; the output lens, caused by an unknown diameter beam and the pinhole, by the same reasons as the lens. It is also expected that the smaller loss is found for A channel, given the geometry of the crystal. Given the extinction ratios presented, with a better apparatus, an eavesdropper can distinguish between the polarization states H and V, but not A and D.

5.4.2 Backflash photons time resolution

The previous experiment showed that Eve can distinguish the polarization of the backflash photon. In real life, Eve's detection might not solely depend on the backflash. It can be a result of stray light in the channel, or the reflection of the signal photon in Bob's optical components which did not cause a click. The solution for Eve is to synchronize with Alice and Bob'a signal pulses and activate her detector at a specific time where she expects the backflash photon to arrive. The synchronization part can be done by monitoring Alice and Bob signal prior the eavesdropping. The next part, as shows in Figure 5.17, is to find the delay between Bob's clicks and backflash arrival at Eve's detector.

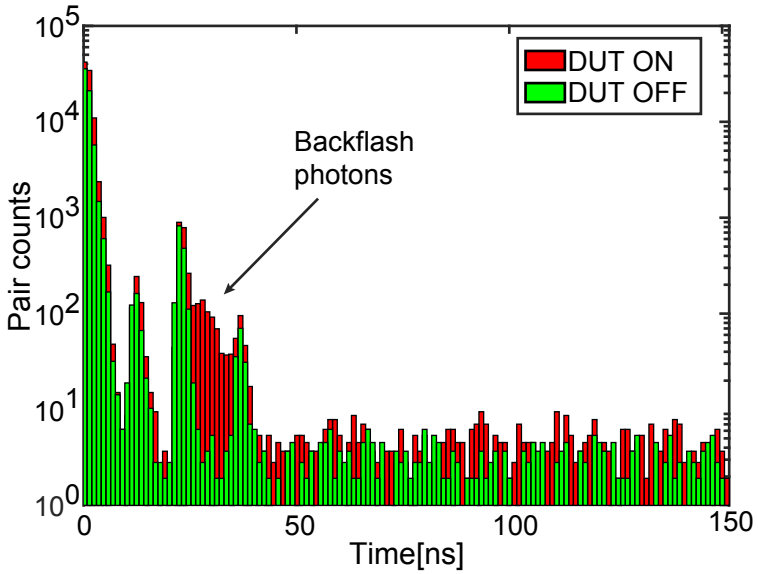
We simulated Alice's signal with attenuated laser pulses with width of 3 ns and 200 ns interval. In principle, Alice followed the same emission setup of the Figure 5.15 with the addition of a pulse generator model P-400 from Highland Technologies. The light was sent to the receiver through a 90:10RT BS. The eavesdropping apparatus was kept the same, but now instead of a power meter, a SPCM unit was used to send an output pulse heralding its detection. The interval time between the signal produced time sent out to Bob and the time when Eve SPCM clicked was recorded. Two sets of scenarios of these interval were analyzed. First, the case where the SPAD, marked as device-under-test

Figure 5.17: Experimental setup designed to measure the time correlation between backflash and reflected photons.



(DUT), in Bob was not activated. All data in this case were the results of dark count in Eve's SPCM, reflection in Bob or stray light in the channel. The second set was with the DUT activated. Any extra cross clicks out of the first set was the result of the backflash. This is showed by the histogram in Figure 5.18. Subtracting the delay between Alce's signal sent out and Bob's click we found that the delay between Bob's click and Eve's detection due to the backflash was around 25-30 ns.

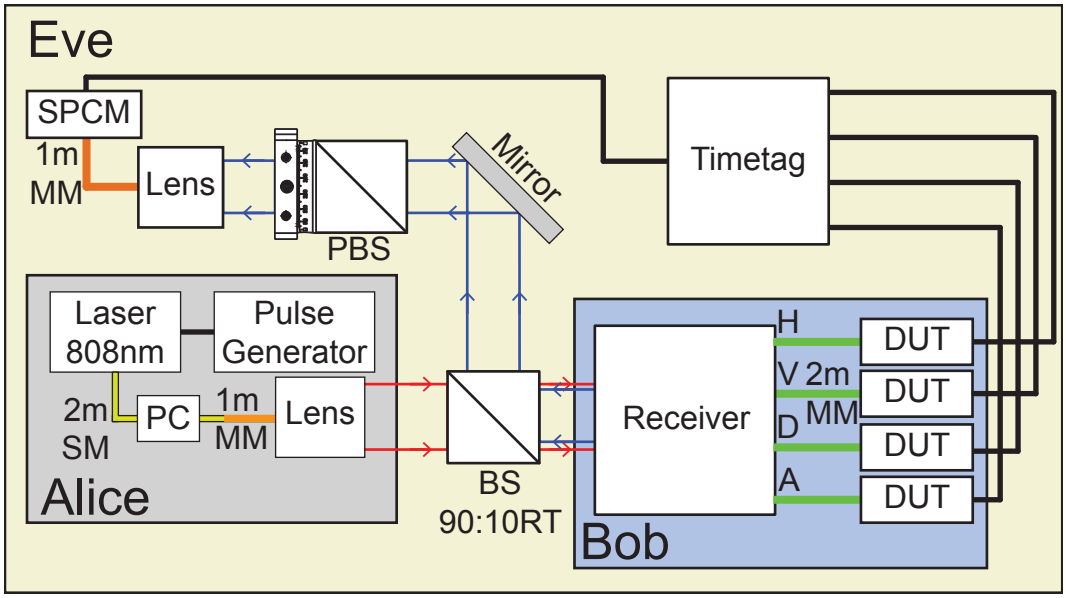
Figure 5.18: Histogram of timing resolution of clicks in Bob's DUT unit for two scenarios: with DUT On and Off.



5.4.3 Eavesdropping attack

After verified the ability of Eve to detect and distinguish the backflash signal, this section will put Eve's setup in an operational condition of the receiver. With a setup in Figure 5.19, the experiment was conducted as follows: Alice produces attenuated pulses with width of 3 ns delayed by 200 ns. These pulses are sent to Bob to simulate the signal pulse in a regular QKD protocol. The Timetag unit was set to register the time of clicks of five different DUT's, four for each channel of Bob and one from Eve. We recorded four sets of data for each Max angle of Eve's PBS for each polarization orientation in Bob.

Figure 5.19: Experimental setup to calculate time correlations between clicks on the DUT's and SPCM units.



Eve's information about H channel acquired from this setup is calculated by setting Eve's PBS to Max angle of H and running the system as stated above. The incidence number, E_{HH}[1] indicates that Eve's detector clicked within the interval of 25-30 ns after Bob's H detector click and no other detector in Bob click within 5 ns of H. We counted this and the total clicks on Bob's H detector, B_H, over 10 *seconds*. The ratio $R_{HH} = E_{HH}/B_H$ is the probability of Eve to get the right detection for each click in Bob's H. We repeated this process with the PBS angle adjusted to Max angle for V. From this measurement, we get $R_{HV} = E_{HV}/B_H$ which is the probability of Eve getting a wrong bit value when H detector in Bob clicked. The extinction ratio for H channel is $E_H = \frac{E_{HH}}{E_{VH}}$. Table 5.3 shows the result for H and V channel. The result in D and A channels are omitted since they are indistinguishable under this specific setup.

Taking the probability of an APD to produce the backflash from table 5.3, $P_b = 10.8\,\%$, the mutual information of Eve to H detection in Bob under this specific setup is $I_H =$

[1]Here, E_{ij} represents the number of incidence where the cross-click was a result of detector i in Bob and j orientation of Eve's PBS

Table 5.3: Cross-click rate and extinction ratio of the attack.

PBS angle(deg)	**Bob's click**	
	H	V
87 (V Max)	3.66E-03	5.69E-03
2 (H Max)	5.00E-02	1.45E-03
Extinction ratio (Ei)	13.67347	3.928571

$P_b(\frac{E_{HH}-E_{VH}}{E_{HH}+E_{VH}}) = 0.09$. Similarly, the mutual information for V is $I_V = 0.06$. If we assume that the distribution between the key in each polarization orientation are identical, this means that Eve knows up to 7.5% of the key in HV basis without inducing any error.

5.4.4 Theory

In this section we will discuss about possible countermeasure to this backflash effect. By characterizing the SPCM as shown in the previous section, the upper bound of Eve's knowledge can be estimated. Let P_b be the probability that a click in an APD causes backflash, η_b the transmission efficiency of the APD to the front end of the receiver. This η_b takes into account all built-in loss such as wavelength mismatch between component's coating and backflash photon, also any physical countermeasures of Bob such as loss in optical isolator that might be inserted in the channel.

It is safe to assume the worst case where all photons that left the receiver carry out the information that allows Eve to fully determine which channel clicked ($E_{ij} = 0$ for all $i \neq j$). The portion of the key that Eve gains full information is $P_{flash} = \eta_f P_b$. This portion of key can be taken care of as the same fashion as the multi-photon part in the weak coherent pulse under PNS attack[102]. For example, the key rate equation of BB84 protocol with weak coherent pulse and backflash photon is given as

$$r = \frac{A}{2}(1 - h(E/A) - leak_{EC}), \tag{5.1}$$

where E is error rate, $leak_{EC}$ is the portion of bits disclosed in the error correction step, $A = \frac{P_{det}-P_{multi}-P_{flash}}{P_{det}}$ where P_{det} is probability of detection on Bob, P_{multi} is the probability of multi-photon pulse generated by Alice, and P_{flash} is the probability of backflash photon that left the receiver as discussed previously.

It can be seen that if P_{flash} is too high, the system can no longer generate secure key. This can be solved by characterizing the SPCM and insert an optical isolator with reverse transmittance $T < 1$ in the front-end of the receiver. It will reduce the value of P_{flash} to $T\eta_f P_b$. The suitable value of T for each specific SPCM as well as finite key size analysis for the system with backflash is left for further study.

5.5 Conclusion

This chapter is devoted to experimentally show the existence of an sporadic emission of photons from SPD devices and to check whether this photons can be used by an eavesdropper to learn something about the transmission or the key when the devices are used in quantum key distribution systems. The first sections briefly reviewed the fundamentals of photodiodes and avalanche photodiodes used in photodetectors. After that, an analysis of the emission of a silicon avalanche photodetector (APD) working in active quenching regime was performed. It was showed that the emission is measurable, as shown in table 5.2 and by the spectrum in Figure 5.14b.

In the sub-sequence sections, the ability of Eve to detect the emitted photon and find the correlation between those photons and its originated detector in Bob was tested. A prove-of-concept setup for an attack was demonstrated. We also discussed about the way to improve that attack scheme. Lastly, we gave a sketch for the treatment of backflash effect on QKD systems both in theory and physical apparatus. The results have shown that Eve can get partial information about the photodetectors clicks in HV basis. With a improved and better alignment setup, or different optical setup, the eavesdropper can surely get more information. This is a situation one should avoid by using optical filters, circulators or a monitoring detector in Bob's input.

6 CONCLUSION

6.1 Conclusions

The topics covered in this thesis were essentially *two-layer QKD* as a framework to increase security to another level and the investigation of the breakdown emission in photodetection, specially their influence in quantum cryptography.

6.1.1 Two-layer QKD

- New protocols were designed to increase the security of the current QKD protocols using on two-layer framework and the consolidated two-way QKD.
- A new one-way protocol with time-bin coding is proposed. Using a new quantum state of light, the security is increased with a mixing of the two states and other countermeasures.
- A new DQPS QKD is proposed. It has the main features of the original protocol added the secure advances of the two-layer QKD and also a few other countermeasures.
- A new QKD protocol using homodyne detection is also proposed. The homodyne detection is a well-established quantitative method for measuring quadrature-amplitudes. Using two-layer QKD, improvements to the original protocol were made and other eavesdropping countermeasures were also added.

6.1.2 Breakdown measurements and quantum cryptography

- Measurements of this phenomenon were performed in two-distinct devices: a photomultiplier tube and a Silicon APD.
- Using direct time correlation measurement, PMTs demonstrated no emission during its multiplication process. The reason is based on the internal structure, even if there are ionization impact, the photons can not surpass the opposite voltage barrier neither the photocathode layer.
- Several experiments were conducted with Si-APDs. Using direct time correlation measurement, Si-APDs demonstrated emission during its avalanche process in a wide spectrum range. The emission is not negligible and has the avalanche current shape.
- Spectral measurements were also realized in a range from $560 - 980$ nm. Based on the efficiency of the detector and the spectrometer, the highest emission was found around 900 nm.

- Regarding quantum cryptography, the question was there all the time: is the breakdown emission a real concern for quantum cryptography? The answer is no.
- So far the results found in this work shows low distinguishability between photons coming from different detectors.
- We tested a passive setup designed for small systems (like satellites) with a crystal inside responsible for passive basis choice. The loss of the backward propagation is on average 90%.
- Given the high loss and the low emission rate, the eavesdropping chance of getting information performing an attack is around 7.5% for the HV basis. For AD, the mutual information is null.

6.2 Further investigation

6.2.1 Two-layer QKD

- As further investigation, two-layer QKD framework can be used for another protocols and implemented.
- A full security analysis of each enhanced protocol can be done.
- A more sophisticated study of the framework can be realized considering quantum memories, nondemolition quantum measurements and eavesdropping attacks.

6.2.2 Breakdown measurements and quantum cryptography

- The breakdown emission has to be investigated in another devices.
- A full spectrum analysis can be done considering a wider spectral range.
- An eavesdropping investigation has to be done in another quantum systems, using another protocols and setups, for instance, the differential phase-shift QKD has a serious flaw regarding breakdown emission: as its setup is quite simple, a time correlation measurements of this photo emission can increase the chances of information leakage.
- Another attacks can be joined with the “backflash attack”.

BIBLIOGRAPHY

[1] ENGGSTUDENT. **Enggstudent Blog**. 2016. Disponível em: <http://ppt netsec. blogspot.com.br/>. Acesso em: 20 dez 2017.

[2] BOSTRÖM, K.; FELBINGER, T. Deterministic secure direct communication using entanglement. **Physics Review Letters**, v. 89, n. 18, Oct 2002.

[3] PINHEIRO, P. V. P.; RAMOS, R. V. Two-layer quantum key distribution. **Quantum Information and Computation**, v. 14, n. 6, p. 2111–2124, Jun 2015.

[4] HAMAMATSU, P. **Photomultiplier tubes: construction and operation characteristics**. 2nd ed., Jan 1998.

[5] COVA, S. et al. Avalanche photodiodes and quenching circuits for single-photon detection**. Applied Optics**, OSA, v. 35, n. 12, p. 1956–1976, 1996.

[6] SAUGE, S. et al. Controlling an actively-quenched single photon detector with bright light**. Optics Express**, v. 19, p. 23590–23600, 2011.

[7] DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE transactions on information theory**, IT-22, n. 6, p. 644–654, November 1976.

[8] BAR-YOSEF, N. **Understanding Public Key Cryptography and the History of RSA**. February 2012. Disponível em: <http://www.securityweek.com/understanding-public-key-cryptography-and-history-rsa>. Acesso em: 20 mar 2018.

[9] WIKIPEDIA. **History of cryptography**. November 2015. Wikipedia, the free encyclopedia. Disponível em: <https://en.wikipedia.org/wiki/history_of_cryptography>. Acesso em: 20 mar 2018.

[10] LEARNCRYPTOGRAPHY.COM. **The Enigma Machine**. November 2015. Disponível em: <http://learncryptography.com/the-enigma-machine/>. Acesso em: 20 mar 2018.

[11] ELGALAM, T. A public-key cryptosystem and a signature scheme based on discrete logarithms. **IEEE transactions on information theory**, v. 31, n. 4, p. 469–472, 1985.

[12] MERKLE, R. C. Secure communications over insecure channels. **Communications of the ACM**, v. 21, n. 4, p. 294–299, Apr 1978.

[13] SMART, N. **Cryptography: An introduction**. [S.l.]: Mcgraw-Hill College, 2007.

[14] DIFFIE, W.; HELLMAN, M. E. **Exhaustive cryptanalysis of the NBS data encryption standard**. Computer, v. 10, n. 6, p. 74–84, June 1977.

[15] ROBSHAW, M.; MURPHY, S. Essential algebraic structure within the AES. **Proceedings on Crypto 2002**. Crypto, 2002. v. 1. Disponível em http://www.isg.rhul.ac.uk/mrobshaw/rijndael/rijndael.html. Acesso em: 20 mar. 2018.

[16] BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing**. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing**. Bangalore, India: IEEE Press, New York, 1984. p. 175–179.

[17] LÜTKENHAUS, N. Estimates for practical quantum cryptography. **Physics Review A**, American Physical Society, v. 59, n. 5, p. 3301–3319, 1999.

[18] BRASSARD, G. et al. Limitations on practical quantum cryptography. **Physics Review Letters**, American Physical Society, v. 85, n. 6, p. 1330–1333, 2000.

[19] DIAMANTI, E. et al. 100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors. **Optics Express**, OSA, v. 14, n. 26, p. 13073–13082, 2006.

[20] CHIANGGA, S.; ZARDA, P.; JENNEWEIN, T. & WEINFURTER, H. Towards practical quantum cryptography**. Applied Physics B**, 1999, 69, 389-393

[21] SILVA, T. F. da et al. Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems. **Optics Express**, v. 20, n. 17, p. 18911–18924, 2012.

[22] COVA, S.; LONGONI, A.; ANDREONI, A. Towards picosecond resolution with single-photon avalanche diodes. **Review Scientific Instrumentation**, v. 52, p. 408–412, 1981.

23 COVA, S. et al. A semiconductor detector for measuring ultra-weak fluorescence decays with 70 ps FWHM resolution. **IEEE Journal of Quantum Electronics**, QE-19, p. 630–634, 1983.

[24] COVA, S.; LACAITA, A.; RIPAMONTI, G. Trapping phenomena in avalanche photodiodes on nanosencond scale. **IEEE Electronic device letters**, v. 12, n. 12, p. 685–687, Dec 1991.

[25] LACAITA, A. et al. Photon-assisted avalanche spreading in reach-throught photodiodes. **Applied Physics Letters**, v. 62, n. 6, p. 606–608, Feb 1993.

[26] PACELLI, A.; SPINELLI, A. S.; LACAITA, A. L. Impact ionization in silicon: A microscopic view. **Journal of Applied Physics**, v. 83, n. 9, p. 4760–4764, May 1998.

[27] NEWMAN, R. Visible light from a silicon p - n junction. **Physics Review**, American Physical Society, v. 100, p. 700–703, Oct 1955.

[28] KURTSIEFER, C. et al. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? **Journal of Modern Optics**, v. 48, p. 2039–2047, 2001.

[29] EKERT, A. K. Quantum Cryptography Based on Bell's Theorem. **Physics Review Letters**, v. 67, n. 6, p. 661–663, 1991.

[30] BENNETT, C. H. Quantum cryptography using any 2 nonorthogonal states. **Physics Review Letters**, v. 68, n. 21, p. 3121–3124, 1992.

[31] BENNETT, C. H.; BRASSARD, G.; MERMIN, N. D. Quantum cryptography without Bell's theorem. **Physics Review Letters**, v. 68, p. 557–559, 1992.

[32] BENNETT, C. H. et al. Experimental quantum cryptography. **Journal of Cryptology**, v. 5, p. 3–28, 1992.

[33] SCARANI, V. et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. **Physics Review Letters**, v. 92, n. 5, p. 057901, 2004.

[34] LUCAMARINI, M.; MANCINI, S. Secure deterministic communication without entanglement. **Physics Review Letters**, v. 94, n. 140501, Apr 2005.

[35] STUCKI, D. et al. Fast and simple one-way quantum key distribution. **Applied Physics Letters**, AIP, v. 87, n. 19, p. 194108, 2005.

[36] LO, H.-K.; MA, X.; CHEN, K. Decoy state quantum key distribution. **Physics Review Letters**, v. 94, n. 23, p. 230504, 2005.

[37] INOUE, K.; WAKS, E.; YAMAMOTO, Y. Differential phase shift quantum key distribution. **Physics Review Letters**, v. 89, n. 3, p. 037902, 2002.

[38] INOUE, K.; WAKS, E.; YAMAMOTO, Y. Differential-phase-shift quantum key distribution using coherent light. **Physics Review A**, American Physical Society, v. 68, n. 2, p. 022317, 2003.

[39] INOUE, K.; IWAI, Y. Differential-quadrature-phase-shift quantum key distribution. **Physics Review A**, v. 79, n. 0223119, 2009.

[40] LO, H.-K.; CURTY, M.; QI, B. Measurement-device-independent quantum key distribution. **Physics Review Letters**, v. 108, p. 130503, 2012.

[41] MENDONÇA, F. A.; BRITO, D. B. de; RAMOS, R. V. An optical scheme for quantum multi-service network. **Quantum Information and Computation**, v. 12, n. 7&8, p. 0620–0629, Apr 2012.

[42] GROSSHANS, F. et al. Quantum key distribution using gaussian-modulated coherent states. **Nature (London)**, v. 421, n. 238, 2003.

[43] SILVA, M. B. C. e et al. Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol. In: Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series. [S.l.: s.n.], 2006. (Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, v. 6343), p. 63431R.

[44] WANG, X.-B. et al. General theory of decoy-state quantum cryptography with source errors. **Physics Review A**, APS, v. 77, n. 4, p. 042311, 2008.

[45] ROSENBERG, D. et al. Practical long-distance quantum key distribution system using decoy levels. **New Journal of Physics**, v. 11, p. 045009, 2009.

[46] BENNETT, C. H.; WIESNER, S. J. Communication via one-and-two-particle operators on Einstein-Podolsky-Rosen states. **Physics Review Letters**, v. 69, n. 20, p. 2881–2884, 1992.

[47] CAI, Q.-Y. The “ping-pong” protocol can be attacked without eavesdropping. **Physics Review Letters**, v. 91, n. 109801, p. 109801–1, SEP 2003.

[48] WÓJCIK, A. Eavesdropping on the “ping-pong” quantum communication protocol. **Physics Review Letters**, v. 90, n. 15, Apr 2003.

[49] RUDOLPH, T.; SPEKKENS, R. W.; TURNER, P. S. Unambiguos discrimination of mixed states. **Physics Review A**, v. 68, n. 010301(R), 2003.

[50] ELDAR, Y. C. Mixed-quantum-state detection with inconclusive results. **Physics Review A**, American Physical Society, v. 67, p. 042309, Apr 2003.

[51] FIURÁŠEK, J.; JEŽEK, M. Optimal discrimination of mixed quantum states involving inconclusive results. **Physics Review A**, American Physical Society, v. 67, p. 012321, Jan 2003.

[52] BARNETT, S. M.; CROKE, S. Quantum state discrimination. **Advances in Optics and Photonics**, v. 1, p. 238–278, Feb 2009.

[53] CAVALCANTI, M. D. S.; MENDONÇA, F. A.; RAMOS, R. V. Spectral method for characterization of avalanche photodiode working as single-photon detector. **Optics Letters**, OSA, v. 36, n. 17, p. 3446–3448, Sep 2011.

[54] PEEV, M. et al. The SECOQC quantum key distribution network in Vienna. **New Journal of Physics**, v. 11, n. 7, p. 075001, 2009.

[55] YUAN, Z.; SHIELDS, A. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. **Optics Express**, OSA, v. 13, n. 2, p. 660–665, 2005.

[56] KHIR, M. F. bin A. et al. Implementation of two-way free space quantum key distribution. **Optics Enginnering**, v. 51(4), n. 045006, p. 842–845, Apr 2012.

[57] QI, B. et al. Polarization insensitive phase modulator for quantum cryptosystems. **Optics Express**, v. 14, p. 4264–4269, 2006.

[58] TAKESUE, H. et al. Differential phase shift quantum key distribution experiment over 105 km fibre. **New J. Physics**, v. 7, n. 1, p. 232, 2005.

[59] DIAMANTI, E. **Security and Implementation of Differential Phase Shift Quantum Key Distribution**. Tese (Doutorado) — Stanford University, June 2006.

[60] LYDERSEN, L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. **Nature Photonics**, v. 4, p. 686–689, 2010.

[61] LYDERSEN, L. et al. Thermal blinding of gated detectors in quantum cryptography. **Optics Express**, v. 18, p. 27938–27954, 2010.

[62] MAKAROV, V. Controlling passively quenched single photon detectors by bright light. **New Journal of Physics**, v. 11, n. 6, p. 065003, 2009.

[63] YUAN, Z. L.; DYNES, J. F.; SHIELDS, A. J. Avoiding the blinding attack in QKD. **Nature Photonics**, v. 4, p. 800–801, 2010.

[64] ERAERDS, P. et al. Quantum key distribution and 1 gbps data encryption over a single fiber. **New Journal of Physics**, v. 12, p. 063027, 2010.

[65] GROSSHANS, F.; GRANGIER, P. Continuous variable quantum cryptography using coherent states. **Physics Review Letters**, v. 88, p. 057902, 2002.

[66] ANDERSEN, U. L.; LEUCHS, G.; SILBERHORN, C. Continuous-variable quantum information processing. **Laser Photonics Review**, v. 4, p. 337, 2010.

[67] BRAUNSTEIN, S. L.; LOOCK, P. van. Quantum information with continuous variables. **Review of Modern Physics**, American Physical Society, v. 77, n. 2, p. 513–577, Jun 2005.

[68] FOSSIER, S. et al. Field test of a continuous-variable quantum key distribution prototype. **New Journal Physics**, v. 11, n. 4, p. 045023, 2009.

[69] RALPH, T. C. Continuous variable quantum cryptography. **Physics Review A**, v. 61, n. 1, p. 010303, 1999.

[70] HIRANO, T. et al. Quantum cryptography using pulsed homodyne detection. **Physics Review A**, v. 68, p. 042331, 2003.

[71] LEONHARDT, U. **Measuring the quantum state of light**. UK: Cambridge University Press, 1997.

[72] NAMIKI, R.; HIRANO, T. Security of quantum cryptography using balanced homodyne detection. **Physics Review A**, v. 67, p. 022308, 2003.

[73] HUTTNER, B. et al. Quantum cryptography with coherent states. **Physics Review A**, v. 51, p. 1863–1869, 1995.

[74] FRANZEN, A. et al. Experimental demonstration of continuous variable purification of squeezed states. **Physics Review Letters**, v. 97, p. 150505, 2006.

[75] SEMMLER, M. et al. Single-mode squeezing in arbitrary spatial modes. **Optics Express**, v. 24, n. 7, p. 7633–7642, Apr 2016.

[76] PRAXMEYER, L.; ENGLERT, B.-G.; WÓDKIEWICZ, K. Violating of Bell's inequality for continuous-variable epr states. **European Physics Journal D**, v. 32, p. 227–231, 2005.

[77] SOUZA, D. D. de. **Quantum cryptography with squeezed states of light**. Dissertação (Mestrado) — Gleb Wataghin Physics Intitute, State University of Campinas, Brazil, 2011.

[78] HAMAMATSU, P. **Photomultiplier tubes: basics and application**. 3rd ed., 2007.

[79] SONNENBERG, H. InAsP-Cs_2O, a high-efficiency infrared-photocathode. **Applied Physics Letters**, v. 16, n. 245, 1970.

[80] ADACHI, S. GaAs, AlAs, and $Al_xGa_1 - xAs$: Material parameters for use in research and device applications. **Journal of Applied Physics**, v. 58, n. 3, p. R1–R29, 1985.

[81] SPICER, W. E.; BELL, R. L. The III-V photocathode: A major detector development. **Publications of the Astronomical Society of Pacific**, v. 84, n. 497, p. 110, 1972.

[82] SALEH, B. E. A.; TEICH, M. C. **Fundamental of photonics**. Wiley, 2007.

[83] CHYNOWETH, A. G.; MCKAY, K. G. Photon emission from avalanche breakdown in silicon. **Physics Review**, v. 102(2), n. 2, p. 369–376, Apr 1956.

[84] WALDSCHMIDT, M.; WITTIG, S. Backscattering and bremsstrahlung of electrons in a silicon detector. **Nuclear instruments and methods**, v. 64, p. 189–191, May 1968.

[85] CHILDS, P. A.; ECCLESTON, W. Impact ionization induced minority carrier injection by avalanching pn junctions. **Journal of Applied Physics**, v. 55, n. 12, p. 4304–4308, 1984.

[86] GAUTAM, D. K.; KHOKLE, W. S.; GARG, K. B. Photon emission from reverse-biased silicon p-n junctions. **Solid-state Electronics**, v. 31, n. 2, p. 219–222, 1988.

[87] HUANG, T. et al. Photon emission characteristics of avalanche photodiodes. **Optics Engineering**, v. 44(7), n. 074001, p. 1–4, Jul 2005.

[88] AKIL, N. et al. Photon generation by silicon diodes in avalanche breakdown. **Applied Physics Letters**, v. 73, n. 7, p. 871–872, 1998.

[89] BENNETT, C. H.; DIVINCENZO, D. P. Quantum information and computation. **Nature**, v. 404, p. 247–255, 2000.

[90] CHUANG, I. L. et al. Experimental realization of a quantum algorithm. **Nature**, v. 393, p. 143–146, 1998.

[91] PAPPA, A. et al. Experimental plug and play quantum coin flipping. **Nature Communications**, v. 5, p. 3717, 2014.

[92] MARCIKIC, I.; LAMAS-LINARES, A.; KURTSIEFER, C. Free-space quantum key distribution with entangled photons. **Applied Physics Letters**, AIP, v. 89, n. 10, p. 101122, 2006.

[93] DAUTET, H. et al. Photon counting techniques with silicon avalanche photodiodes. **Applied Optics**, OSA, v. 32, n. 21, p. 3894–3900, 1993.

[94] ANTOGNETTI, P.; COVA, S.; LONGONI, A. A study of the operation and performances of an avalanche diode as a single photon detector. In: EURATOM PUBL. EUR 537E 1 (OFFICE FOR OFFICIAL PUBLICATIONS OF THE EUROPEAN COMMUNITIES, LUXEMBOURG, BELGIUM, 1975). Proceedings of the Second Ispra Nuclear Electronics Symposium, 1975. p. 453–456.

[95] MAKAROV, V.; ANISIMOV, A.; SAUGE, S. Can Eve control PerkinElmer actively-quenched single-photon detector? **arXiv:0809.3408v1**, 2008.

[96] NIGHTINGALE, N. S. A new silicon avalanche photodiode photon counting detector module for astronomy. **Express Astronomic**, v. 1, p. 407–422, 1991.

[97] RIPAMONTI, G.; LACAITA, A. Single-photon semiconductor photodiodes for distributed optical fiber sensors: state of the art and perspectives. Distributed and Multiplexed Fiber Optic Sensors II, J. P. Dakin and A. D. Kersey, n. **Proceedings SPIE 1797**, p. 38–49, 1993.

[98] MIGDALL, A. et al. Single-photon generation and detection. 1st ed. **Academic Press of Elsevier**, 2013. (Experimental methods in the physical sciences, v. 45).

[99] BONACCINI, D. et al. Novel avalanche photodiode for adaptive optics. Adaptatative Optics in Astronomy, M. Ealey and F. Merkle, n. **Proceedings SPIE 2201**, p. 650–657, 1994.

[100] SZE, S. M.; NG, K. K. **Physics of semiconductor devices**. 111 River Street, Hoboken, NJ - USA: Wiley-Interscience, 2007.

[101] GISIN, N. et al. Trojan-horse attacks on quantum-key-distribution systems. **Physics Review A**, v. 73, n. 2, p. 022320, 2006.

[102] GOTTESMAN, D. et al. Security of quantum key distribution with imperfect devices. **Quantum Information and Computation**, v. 4, n. 5, p. 325–360, 2004.