Pontifícia Universidade Católica
do Rio de Janeiro

Gustavo Castro do Amaral

FPGA Applications on Single Photon Detection Systems

DISSERTAÇÃO DE MESTRADO

Dissertation presented to the Programa de Pós-Graduação em Engenharia Elétrica of the Departamento de Engenharia Elétrica, PUC–Rio as partial fulfillment of the requirements for the degree of Mestre em Engenharia Elétrica.

Advisor: Prof. Guilherme Penello Temporão

Rio de Janeiro
March 2014

Pontifícia Universidade Católica
do Rio de Janeiro

Gustavo Castro do Amaral

FPGA Applications on Single Photon Detection Systems

DISSERTAÇÃO DE MESTRADO

Dissertation presented to the Programa de Pós-Graduação em Engenharia Elétrica of the Departamento de Engenharia Elétrica do Centro Técnico Científico da PUC-Rio, as partial fulfillment of the requirements for the degree of Mestre.

Prof. Guilherme Penello Temporão
Advisor
Centro de Estudos em Telecomunicações – PUC-Rio

Dr. Miguel de Andrade Freitas
Centro de Estudos em Telecomunicações – PUC-Rio

Prof. Jean Pierre von der Weid
Centro de Estudos em Telecomunicações – PUC-Rio

Dr. Giancarlo Vilela de Faria
Departamento de Engenharia Mecânica – PUC-Rio

Prof. José Eugenio Leal
Coordinator of the Centro Técnico
Científico da PUC-Rio

Rio de Janeiro, March 28th, 2014

Gustavo Castro do Amaral

Gustavo Castro do Amaral graduated from the Pontifícia Universidade Católica do Rio de Janeiro (Rio de Janeiro, Brasil) in Electrical Engineering with both Computer Electronics and Telecommunications emphases. He is a member and an active participant of the Optoelectronics Laboratory and all its projects.

Bibliographic data

Amaral, G. C.

FPGA Applications on Single Photon Detection Systems / Gustavo Castro do Amaral; advisor: Prof. Guilherme Penello Temporão. — Rio de Janeiro : PUC–Rio, Departamento de Engenharia Elétrica, 2014.

v., 99 f: il. ; 29,7 cm

Dissertação de Mestrado - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica.

Inclui bibliografia

1. Departamento de Engenharia Elétrica – Dissertação. 2. FPGA;. 3. OTDR;. 4. Criptografia Quântica;. 5. Detecção de Fótons.. I. Temporão, G. P.. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Acknowledgments

To my advisor Guilherme Temporão for the support, constant discussions and friendship without which this project would not have been possible.

To the CAPES, CNPq and the PUC–Rio, for the financial support, without which this work would not have been realized.

To all my family, specially my mother and father.

To my girlfriend, Juliana, for the unconditional support, constant happiness and love which kept me going all the time.

To my colleagues and friends of PUC–Rio, specially Joaquim Dias Garcia, Mario Souto and Marcelo Jimenez for the support and ideas.

To my colleagues and friends of the Optoelectronics Laboratory, Diego, Luiz, Douglas, Guilherme, Thiago, Julio and Amalia for the support and friendship.

To professors Jean Pierre von der Weid, Carlos Kubrusly and Weiler Finamore for helping me discover my interests and for setting the examples of academic researchers.

To my friends, Gabriel and Jonas, for the unconditional friendship.

Abstract

Amaral, G. C.; Temporão, G. P. (Advisor). **FPGA Applications on Single Photon Detection Systems**. Rio de Janeiro, 2014. 99p. MsC Dissertation — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Despite the high sensitivity reached by Photon Detectors so far, the implementation of a background managing system often enforces the robustness of measurements thus creating a resourceful apparatus for specific applications. In this document, the management tools offered by Software Defined Hardware (SDHs) is put to test. By associating the power of FPGAs and Photon Detectors, enhanced measurement stations were assembled. Two different applications, a Bell State Projection Analysis Station and a Photon Counting Optical Time Domain Reflectometry (ν-OTDR) Automatic Setup, are presented. Even though both experiments involve the detection of single photons, the background technologies differ drastically.

Keywords

FPGA; OTDR; Quantum Cryptography; Photon Detection.

Resumo

Amaral, G. C.; Temporão, G. P. (Orientador). **Aplicações de FPGA em Sistemas de Detecção de Fótons Únicos**. Rio de Janeiro, 2014. 99p. Dissertação de Mestrado — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Apesar da alta sensibilidade alcançada por Fotodetectores comercialmente disponíveis, a implementação de circuitos de gerenciamento é capaz de fortalecer a robustez das medidas, criando um aparato com mais recursos em aplicações específicas. Duas aplicações práticas dessa hipótese são apresentadas em contextos diferentes, Criptografia Quântica e Monitoramento de Fibras Ópticas fazendo uso da plataforma FPGA.

Palavras Chave

FPGA; OTDR; Criptografia Quântica; Detecção de Fótons.

Contents

List of Figures

By the powers of truth I, while living, have conquered the Universe.

Johann Wolfgang von Goethe, *Faust.*

I
Introduction

Despite the high sensitivity reached by Photon Detectors so far, the implementation of a background managing system often enforces the robustness of measurements thus creating a resourceful apparatus for specific applications. In this document, the management tools offered by Software Defined Hardware (SDHs) is put to test. By associating the power of FPGAs and Photon Detectors, enhanced measurement stations were assembled.

Two different applications, a Bell State Projection Analysis Station and a Photon Counting Optical Time Domain Reflectometry (ν-OTDR) Automatic Setup, are presented. Even though both experiments involve the detection of single photons, the background technologies differ drastically.

While the first is a setup dedicated to the detection of qubit states fostered by the advent of the Measurement Device Independent Quantum Key Distribution, the second is a different approach to the classic OTDR inspection fomented by the development of Geiger-Mode Avalanche Photo Diodes. The sequence of technological advancements which enabled the experiments is presented in the following Time Line in which three different kinds of progress can be identified: Theoretical Physics; LASERs and Photodectors Engineering; and Optic Fiber Technology.

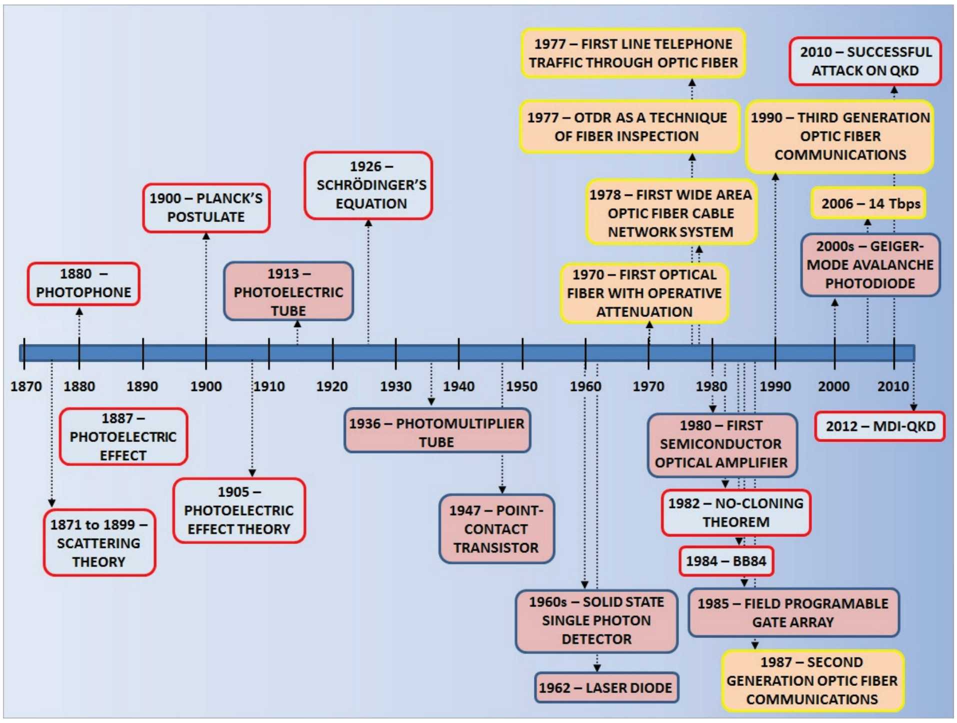

1977 – FIRST LINE TELEPHONE TRAFFIC THROUGH OPTIC FIBER
2010 – SUCCESSFUL ATTACK ON QKD
1977 – OTDR AS A TECHNIQUE OF FIBER INSPECTION
1990 – THIRD GENERATION OPTIC FIBER COMMUNICATIONS
1926 – SCHRÖDINGER'S EQUATION
1900 – PLANCK'S POSTULATE
1978 – FIRST WIDE AREA OPTIC FIBER CABLE NETWORK SYSTEM
2006 – 14 Tbps
2000s – GEIGER-MODE AVALANCHE PHOTODIODE
1880 – PHOTOPHONE
1913 – PHOTOELECTRIC TUBE
1970 – FIRST OPTICAL FIBER WITH OPERATIVE ATTENUATION
1870
1880
1890
1900
1910
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
1887 – PHOTOELECTRIC EFFECT
1936 – PHOTOMULTIPLIER TUBE
1980 – FIRST SEMICONDUCTOR OPTICAL AMPLIFIER
2012 – MDI-QKD
1905 – PHOTOELECTRIC EFFECT THEORY
1947 – POINT-CONTACT TRANSISTOR
1982 – NO-CLONING THEOREM
1871 to 1899 – SCATTERING THEORY
1984 – BB84
1960s – SOLID STATE SINGLE PHOTON DETECTOR
1985 – FIELD PROGRAMABLE GATE ARRAY
1962 – LASER DIODE
1987 – SECOND GENERATION OPTIC FIBER COMMUNICATIONS

Figure I.1: Time Line of the Leading Technologies Involved in the Project.

- 1871 to 1899: Lord Rayleigh's series of papers on the theory of scattering.
- 1880: Graham Bell and Charles Sumner create the Photophone and demonstrate the first optical transmission.
- 1887: Heinrich Hertz discovers the Photoelectric Effect.
- 1900: Planck's Postulate. Electromagnetic energy is quantized.
- 1905: Albert Einstein publishes a paper explaining Hertz's experimental results.
- 1913: Elster and Geiter invent the Photoelectric Tube enabling the detection of light.
- 1926: Schrödinger publishes his fourth and final paper with the non-relativistic version of the wave equation. Born interprets ψ as the probability amplitude.
- 1936: First demonstration of a Photomultiplier Tube, which permitted the detection of a single photon, by Harley Iams and Bernard Salzberg.
- 1947: Bardeen, Brattain and Schokley invent the first Point-Contact Transistor.
- 1960s: McIntyre and Haitz develop the Solid State Single Photon Detector.

- 1962: The group led by Robert N Hall demonstrates coherent light emission from a semiconductor.
- 1970: Corning Glass Works develops the first optical fiber with attenuation low enough for communication purposes. In the same year, the GaAs semiconductor LASER is developed.
- 1977: Barnoski, Rourke, Jensen and Melville propose and demonstrate the Optical Time Domain Reflectometry as a means of inspecting an optic fiber. In the same year, General Telephone and electronics sends the first live telephone traffic through optic fiber at 6 Mbps using 0.8 μm and GaAs semiconductor LASERs. Repeaters separated by 10 km.
- 1978: The first wide area optic fiber cable system network is installed by Rediffusion in Hasting, United Kingdom, with around 1000 subscribers.
- 1980: Development of the first Semiconductor Optical Amplifier.
- 1982: Wooters and Zurek and Diecks demonstrate the Non-Cloning Theorem.
- 1984: The first Quantum Key Distribution Protocol, the BB84, is proposed by Bennet and Brassard.
- 1985: Ross Freeman and Bernard Vonderschmitt invent the first commercially viable Field Programmable Gate Array.
- 1987: Second Generation of fiber optic communication operating at 1.3 μm with InGaAsP semiconductor LASERs. Repeaters separated by 50 km.
- 1988: TAT-8, the first transatlantic optic fiber telephone cable.
- 1989: Anti-reflection coating technology enables the fabrication of true travelling-wave Semiconductor Optical Amplifiers.
- 1990: Third Generation of fiber optic communication operating at 1.55 μm and 0.2 dB/km. Repeaters separated by 100 km.
- 2000s: Development of Geiger-Mode Avalanche Photodiodes.
- 2006: 14Tbps over a single 160 km line using optical amplifiers.
- 2010: Xu, Qi and Lo demonstrate the first successful attack on a QKD system.
- 2012: Curty, Qi and Lo propose the Measurement Device Independent QKD.

II
Theoretical Review

II.1 Semiconductors

In the Periodic Table of Elements, Dmitri Mendeleev classifies the atoms present in nature according to their electronic distribution. One direct consequence of different electronic configurations is variable electron to nucleus bonding and, ultimately, different energy band patterns. Three classes of elements can be identified in terms of energy band: insulators; conductors; and semiconductors.

The conduction band of a pure (intrinsic) semiconductor crystal is vacant at absolute zero and separated from the filled valence band by an energy gap E_g. An electronic band scheme leading to intrinsic conductivity is indicated in Figure II.1 [1]. In a semiconductor, the value of the band gap E_g, the difference in energy between the lowest point of the conduction band (or conduction band edge) and the highest point of the valence band (or valence band edge) [1], is comparable to k_BT, which translates into considerable gain in conductivity for slight changes in temperature. Band gaps of representative semiconductors are given in Table II.1 [1].

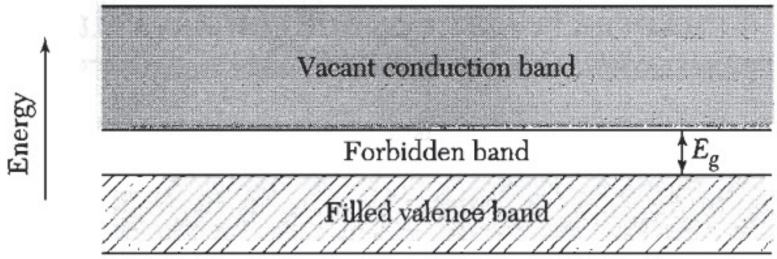


Figure II.1: Energy Band Scheme of an Intrinsic Semiconductor Crystal.

Table II.1: Energy Gap (eV) between the valence and conduction bands

Crystal	0K	300K	Crystal	0K	300K
Si	1.17	1.11	Ge	31	25
InSb	35	14	InP	35	144
GaP	35	144	GaAs	35	144
GaSb	35	144	InAs	45	300

The intrinsic conductivity and intrinsic carrier concentrations, i.e., the number of excited electrons from the valence band that populate the conduction band as the temperature increases, are largely controlled by E_g/k_BT, the ratio of the band gap to the temperature [1]. This behavior can be clarified in Figure II.2 [2] where the Fermi Function is considered. The Fermi function $f(E) = \left(e^{(E-E_F)/k_BT} + 1\right)^{-1}$ gives the probability that a given available electron state will be occupied at a given temperature. On the other hand, the addition of certain impurities and imperfections to a semiconductor crystal drastically affects its electrical properties [1], [3]. The deliberate addition of impurities to a semiconductor is called doping.

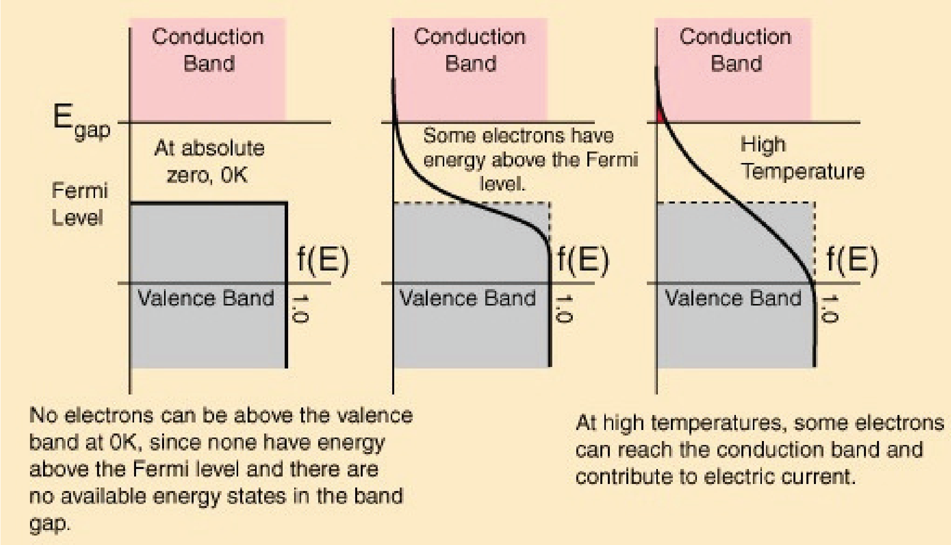

Conduction Band
Conduction Band
Conduction Band
E gap
Fermi Level
At absolute zero, 0K
Some electrons have energy above the Fermi level.
High Temperature
f(E)
f(E)
f(E)
Valence Band
Valence Band
Valence Band
1.0
1.0
1.0
No electrons can be above the valence band at 0K, since none have energy above the Fermi level and there are no available energy states in the band gap.
At high temperatures, some electrons can reach the conduction band and contribute to electric current.

Figure II.2: Illustration of the Implication of the Fermi Function on the Electrical Conductivity of a Semiconductor.

When a semiconductor material such as silicon crystallizes, each atom forms four covalent bonds, one with each of its nearest neighbors which corresponds to silicon's chemical valence four. In the case an impurity of valence five such as phosphorous is substituted in the lattice, there will be one valence electron left after the four covalent bonds are established. Impurity atoms that can give up an electron are called donors while atoms that take an electron from the lattice are called acceptors [1]. The role of an absent electron (also called *hole*) is fundamental and can be considered as that of an electron with positive charge in a simplistic approach. One important theoretical result regarding the behaviour of holes is that they behave as carriers in the valence band [1].

The last occupied energy state inside a semiconductor lattice is determined by the Fermi Level. It can be shown [1] that, by adding impurities of different natures (donors and acceptors) to a semiconductor lattice, it is possible to decrease or increase the Fermi Level of the crystal even at absolute zero. While for an intrinsic semiconductor the Fermi Level is in the middle of the energy gap, in a doped semiconductor, the Fermi Level is shifted depending on the type of dopant (p or n) as indicated in Figure II.3.

In Figure II.3 a), the addition of acceptor impurities contributes with hole levels low in the semiconductor band gap so that holes can be easily excited into the valence band from these levels (n-type semiconductor). In b), the addition of donor impurities contributes with electron energy levels high in the semiconductor band gap so that electrons can be easily excited into the conduction band (p-type semiconductor) [1].

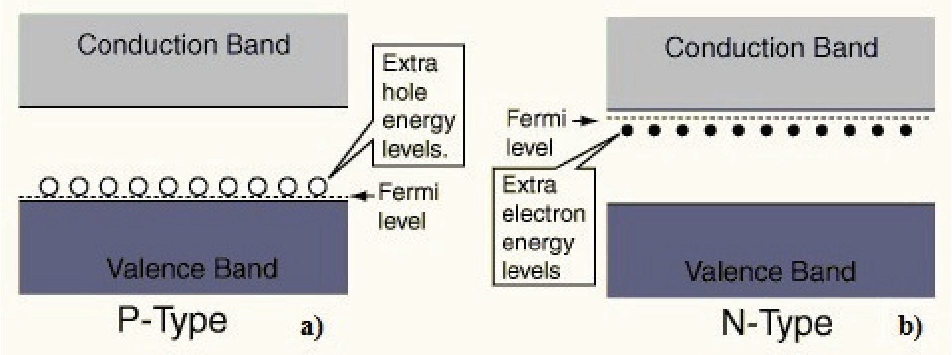


Figure II.3: Fermi Level Shift Due to the Addition of Impurities.

A p-n junction is created when two crystals, one doped with an acceptor element (p-type) and the other doped with a donor element (n-type), are connected. While the n region is filled with positively charged ionized donors and an equal concentration of free electrons, the p region is filled with negatively charged ionized acceptors and an equal concentration of free holes [1], [3].

When the junction is created, holes from p flow to n and electrons from n flow to p. This small charge transfer by diffusion leaves behind an excess of negatively charged ionized acceptors on the p side and an excess of positively charged ionized donors on the n side. An electric field directed from n to p is formed inhibiting diffusion and maintaining the separation of the two carrier types. The trade off region is called the Depletion Zone, indicated in Figure II.4.

In Figure II.4 a), ρ represents the volume charge density in the Depletion Zone. In b), the built-in electric field can be determined by integrating the volume charge density over the depletion region. In c), the electrical potential is proportional to the integral of the electric field over the depletion region. ΔV (or V_d) is the built-in potential barrier.

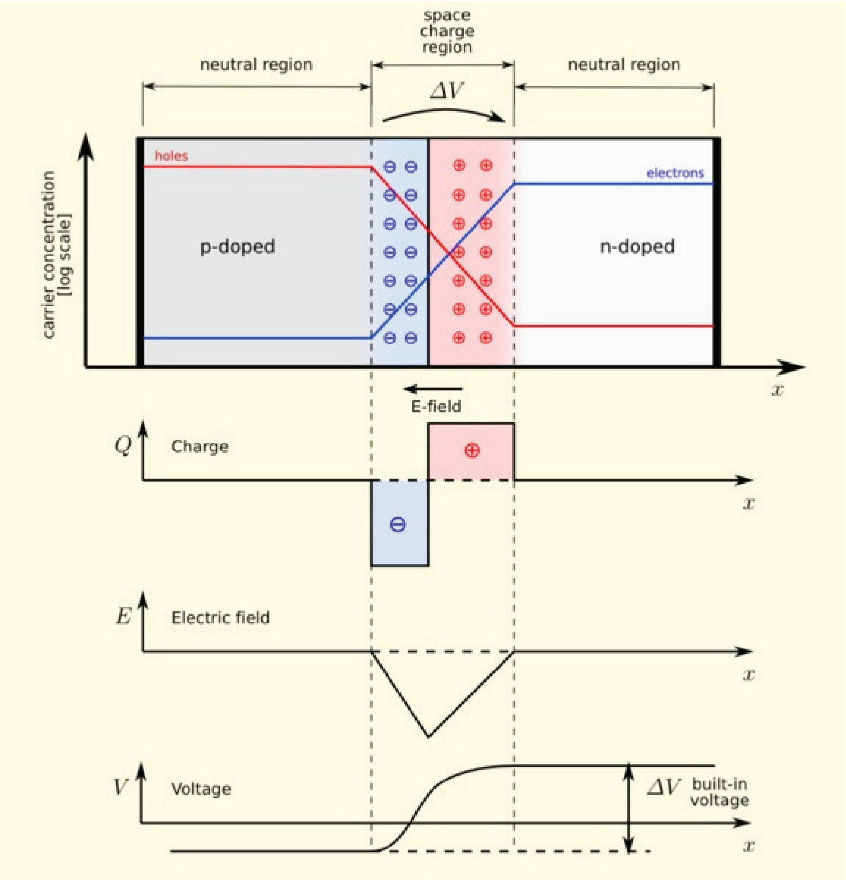


Figure II.4: Depletion Zone Representation of an Unbiased p-n Junction.

Following the schematic representation of Figure II.4, applying a positive voltage across the junction from n to p will contribute to the built-in potential barrier V_d making it more difficult for electrons or holes to cross the barrier, a process called reverse biasing. On the other hand, if a negative voltage is applied from n to p, the potential barrier will diminish and current will be more likely to flow through the junction from p to n, a process called direct biasing.

An important characteristic of p-n junctions is their I-V curve. When reverse-biased, aside from thermally-generated free carriers that flow through the junction by diffusion , hardly no carriers are exchanged between the n and p regions.When direct-biased, on the other hand, the resulting voltage across the junction is lowered so the amount of electrons and holes with sufficient energy to transpose the barrier grows as an exponential function of the applied voltage [4]. Equation (2) [1] describes this behaviour, where V is the applied bias voltage and I_S is the thermally-generated current. The term e/k_BT is simplified by:

$$V_T^{-1} = e/k_BT \tag{1}$$

a temperature dependent reference voltage of the junction [1]. Figure II.5 depicts the typical I versus V curve of a p-n junction.

The Dark Current I_S is the thermally-generated current which does not depend on the applied voltage and, thus, remain constant for reverse-biasing values of V. The Breakdown region is exploited for voltage regulation purposes since voltages after breakdown vary slightly with current changes. It is the region of operation of Zener Diodes and Avalanche Photodiodes.

$$I \cong I_S \left(e^{(eV/k_BT)}\right) \cong I_S \left(e^{(V/V_T)}\right) \tag{2}$$

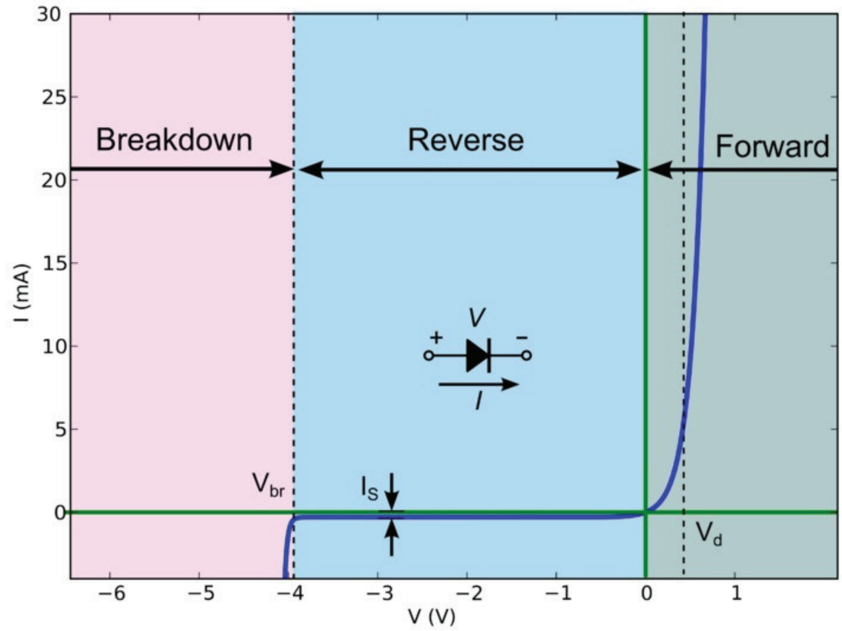


Figure II.5: Current-Voltage Curve in a *p-n* Junction.

If subject to an AC bias voltage, a *p-n* junction responds as a *rectifier*: near zero current flows in the negative cycle while a considerable amount of carriers cross the device in the positive cycle. The diode, therefore, is a direct application of the semiconductor *p-n* junction which also includes transistors, switches, photovoltaic cells, photodetectors and thermistors. One of the many advantages of doped semiconductor structures is that they may be used as single circuit elements (discrete elements) or as components of integrated circuits.

All the main effects of forward and reverse biasing of a *p*-*n* junction have been considered but one: when the reverse bias voltage is sufficiently high, thermally-generated electrons and holes which flow by diffusion gain so much kinetic energy due to the high electric field that they are able to ionize other electrons and holes causing a cascaded effect. In order to operate in the *Breakdown* Region, several precautions should be taken for circuitry protection since the high current and voltage may damage the device permanently.

The *Breakdown* Region is exploited in several devices technology such as the Zener Diode and Avalanche Photodiodes. In this operation mode, the significantly high current flows in the reverse direction, from *p* to *n*, in the direction of the reverse bias voltage.

II.2 Digital Circuits

Noble Prize winners John Bardeen, Walter Houser Brattain and William Bradford Shockley invented, in 1947, what is considered today a technological milestone: the transistor. As it was conceived, the transistor is a direct application of the semiconductor *p*-*n* junction with a few design modifications. Amongst other things, the development of transistors permitted the evolution of digital circuits [5].

The main difference between a conventional analog circuit and a digital circuit is the range of signal representation. It becomes clear when looking at Figure II.6 that while the red curve (analog representation) can assume a continuum of values in the amplitude range, the gray curve (digital representation) assumes only a few discrete values.

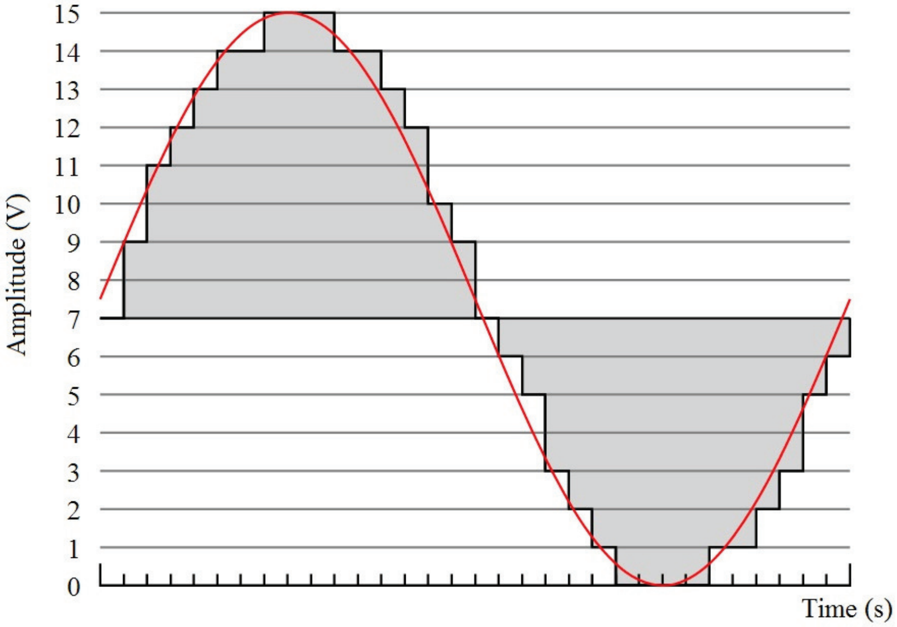
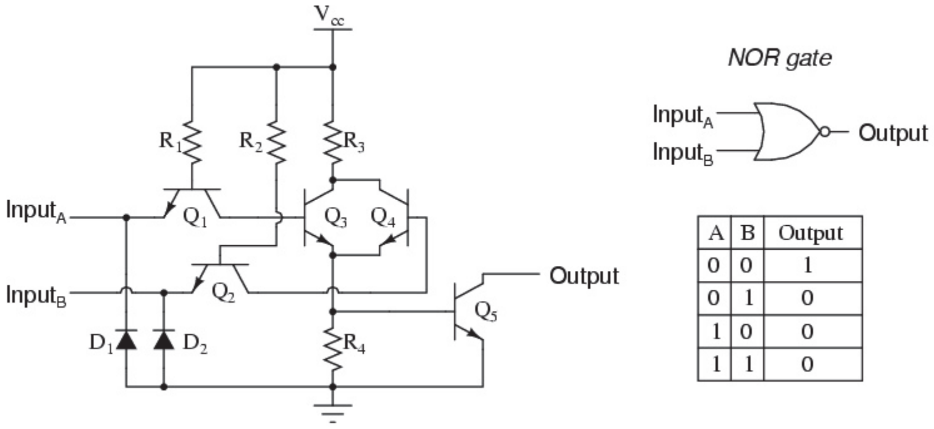


Figure II.6: Analog and Digital Representations of an Electrical Signal Varying in Time.

The most common type of digital circuit uses only two different voltage levels (commonly the supply voltage (high) and a reference or *ground* level (low)) that correspond to the true and false values of Boolean Algebra. Boolean functions that manipulate true/false values can be implemented based on the switching between the *saturation* and *cut-off* states of a transistor.

A simple NOR Transistor-Transistor Logic (TTL) structure along with its Truth Table is shown in Figure II.7 [6]. When Input A is set high, current flows through transistor Q1 which, in turn, saturates transistor Q3 and, consequently, transistor Q5, which outputs low. The same happens for Input B and transistors Q2 and Q4. If both inputs are set high, Q5 is also saturated due to the parallel connection of Q3 and Q4. The only case in which Q5 outputs high is when both A and B are set low [6].



A	B	Output
0	0	1
0	1	0
1	0	0
1	1	0

Figure II.7: Transistor-Transistor Logic Circuitry of a Simple NOR Gate and Its Truth Table.

Before the advent of transistors, digital circuits were assembled using structures called *valves* which could also be switched between operation modes. The transistor, nevertheless, rapidly substituted the valve because of simpler manufacturing process and smaller size.

The range of operations implemented by digital circuits can be divided into two categories: synchronous and asynchronous. As the name indicates, synchronous digital circuits operate according to a control signal often called *clock* which is implemented by a square voltage wave. All transitions between logical states of synchronous devices occur on the rising or falling edge of the clock signal. Asynchronous circuits on the other hand, are independent of clock signals and output transitions are determined by input transitions in the moment they occur.

An example of an asynchronous digital circuit is the NOR gate of Figure II.7 while the D-Latch (or D-type Flip-Flop) is an example of synchronous digital circuit. The combination of synchronous and asynchronous digital circuits is the basis for creating the powerful micro-processors present in the market today.

In the beginning of the Integrated Circuit technology, the number of transistors inside a chip was rather limited and, often, a chip was capable of implementing one simple digital function such as a NOR gate. Therefore, a complex digital project, with a high number of logic gates, demanded the manual connection of chips via wires or the creation of printed circuit boards.

As the technological enhancements in the field of *Photolithography* enabled greater transistor density inside a chip, the striving for a programmable platform capable of implementing different digital circuits according to its software definition rose. Software Defined Hardware structures were a natural development in the Very-Large-Scale Integration (VLSI) era.

II.3 FPGA

Software Defined Hardware (SDH) is the final frontier that divides hardware and software, allying the speed of the first and the facility and flexibility of the second. Its most successful representative, the Field Programmable Gate Array (FPGA), is a revolutionary concept that integrates most of the digital circuit projects, from the simplest to the most complex.

In 1985, the first commercially available integrated circuit capable of creating variable connections between programmable logic cells was assembled by Ross Freeman and Bernard Vonderschmitt, the founders of Xilinx, Inc [7] and, since, the industry's demand for such technology has increased.

The main idea behind an FPGA is the possibility to assemble any digital circuit inside a chip without the need to manually connecting wires. This is done by programming a memory structure that controls how the logic blocks are connected. For such, the Hardware Description Language (HDL), a novel programming language focused on SDHs, was developed with two main representatives, the VHDL and Verilog languages.

Differently from a conventional programming language such as C, the code is interpreted and a configuration file is created in a process known as Place And Route (PAR). This file contains the instructions necessary to control the elements in Figure II.8 and implement the desired circuit.

The Configurable Logic Blocks (CLBs) are interconnected through programmable Interconnection Nets. Inside the CLBs, Configurable Combinational Elements (CCEs) are connected to D-Latches and both output and input are created by the combination of internal and external signals in a digital multiplexer. All programmable and configurable structures are set by the Configuration Memory, implemented by a Static Random Access Memory (SRAM) [7].

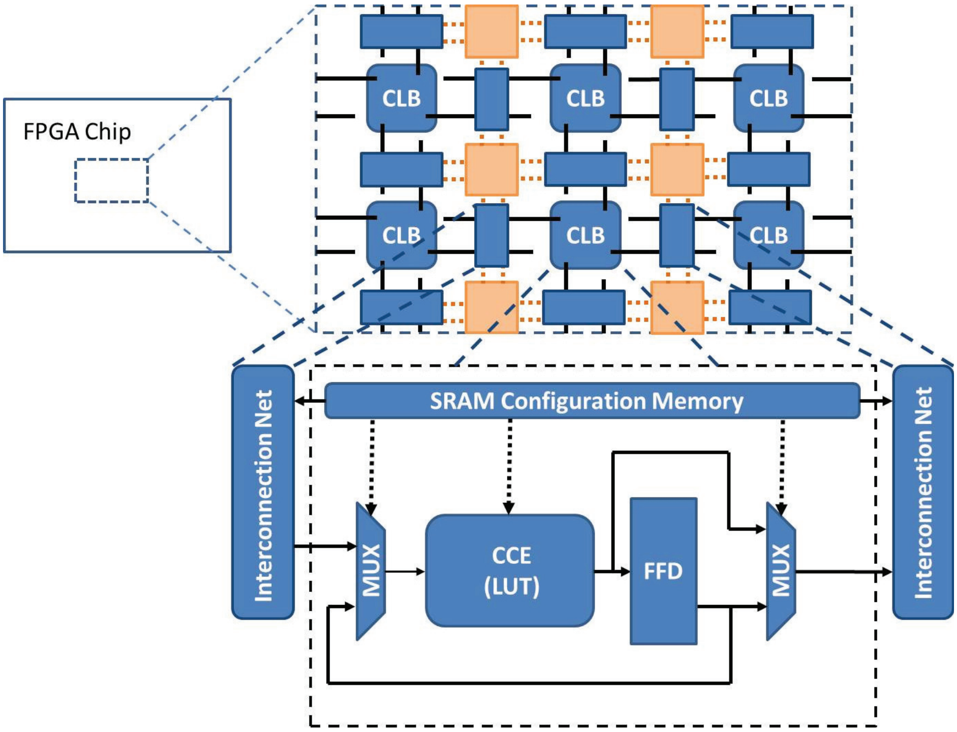


Figure II.8: Field Programmable Gate Array Internal Block Diagram.

The physical structure of an FPGA is as simple as the block diagram of Figure II.8. Aside from the Interconnection Nets, which work much like a remote keyboard, the CCEs are composed by simple digital structures such as D-Latches, Multiplexers and Look-Up Tables (LUTs) (the last can be implemented by a either a Multiplexer or an array of NAND gates). With enough cells, though, the processing power of an FPGA can match that of a modest microprocessor with parallel processing advantage.

One of the most interesting features of an FPGA when compared to a micro controller, for instance, is the parallel processing, i.e., the ability to simultaneously carry out multiple operations. An FPGA can, thus, be connected to multiple digital inputs and outputs and control each individual thread at the same time. In terms of processing, the power of an FPGA resides in the number of cells and the maximum clock frequency permitted by the structure.

The first generation of Xilinx FPGAs had up to 100 CLBs and supported up to 50 MHz clock frequency [7]. Table II.2 lists the developments in the area from the creation, in 1985, until 2001. Currently, commercially available boards such as the Virtex-7 support 2 million CLBs and up to 500 MHz clock frequency [7].

Table II.2: Evolution of FPGAs (1985 - 2001) [7]

Model	Number of CLBs	Max Clock Speed (MHz)
XC2000	100	50
XC3000	484	50
XC5200	484	50
XC4000	3136	80
Spartan	784	100
Virtex	6144	200
Spartan-II	1176	200
Virtex-E	16224	250
Spartan-IIE	3456	200
Virtex-II	11648	420
Virtex-II Pro	44000	420

Transceivers, RAM Blocks and DSP Slices are already built-in functionalities in the Virtex-7 [7], features that broaden the FPGA's application, still counting with the flexibility available in a SDH project.

II.4 FPGA Design

The role of FPGAs in electronic circuitry projects and different kinds of digital systems has been growing since their development due to a number of advantages, mainly: the practicality of designing and implementing a digital circuit as a software; the possibility of creating a prototype version which can be completely upgraded with a simple change of "'firmware" - which can be though of as the file containing the interconnection instructions for the chip; and, finally, the ease of testing - especially in the case of simulations.

This last aspect is, arguably, the most important feature of a digital circuit design and has been widely driven by the development of FPGAs since the possibility of defining all aspects of the behavior of the circuit via software - including debugging specific signals and processes - translates into faster and more reliable designs. In this sense, specific tools for the simulation of HDL codes is becoming so important that big companies are even subdividing the greater area of *FPGA Design* into *Simulation* and *Implementation* [8].

The importance of simulating all circuits in order to detect and work around design mistakes in a software level is obvious. Not only it makes easier for the whole project to have a safer implementation step - without too many hiccups, since they will always be present - but also so that a more profound understanding of how an electronics circuit operates.

Even though design strategies and directives can be found in great detail among the literature of HDL languages and FPGA Design - e.g. [8] -, the ones described here are of the author's preferences and reflect his point of view.

(a) FPGAs and Micro-Controllers

HDL differs drastically from software languages, but how and why? Any kind of code which is designed to be interpreted by a micro-controlled CPU rests on the premise that each line of code will be compiled and transformed into machine instructions and stored in the CPU memory from where they will be sequentially executed. Even though the micro-controlled structure of a computer can be much more complicated than the one presented, it can be condensed into the drawing of Figure II.9. The drawing shows the basic structures of a micro-controller: memory, data and address buses, registers, a program counter and a Arithmetic and Logic Unit (ALU). The main idea, as already stated, is that values can be stored during a definite number of clock cycles by the registers and used whenever it is necessary. The output of any computation is also stored when it completed and sent to the memory unit.

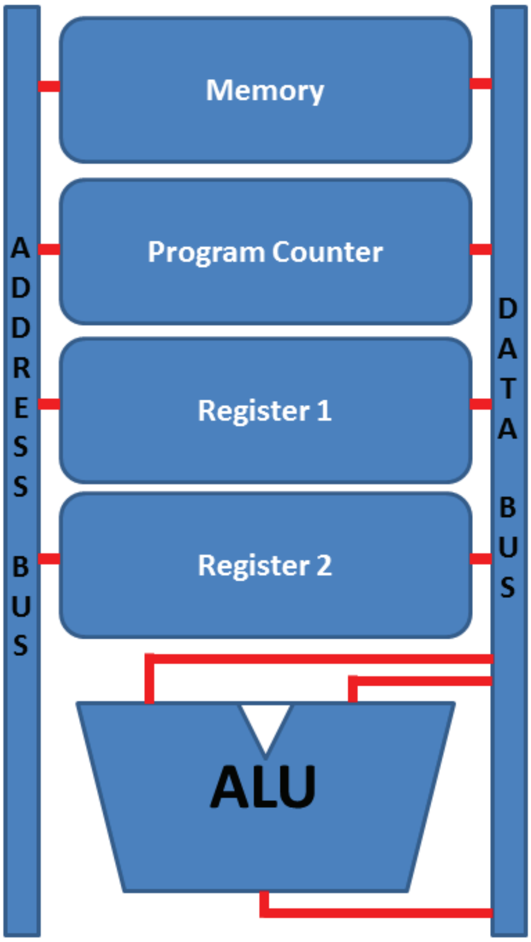


Figure II.9: Micro-controller basic structure.

The implications of writing a simple code in C, for example, like the following attribution *a = a + 1* in the micro-controller are of, at least, two clock cycles. In the first cycle, the value of a is identified among registers then sent into one of the ALU's inputs (the instruction stored in the memory unit controls the inputs and outputs to direct each of them to the correct port). In the second, the value of *1* can also be inputted - even though the majority of ALUs already have the *sum 1* operation as a default option - and the code for *sum* is selected in the ALU's chip and the output stored in a register.

What this simple example represents is that, in a micro-controller, the universal structure for algorithm implementation is already configured so logical attributions by the programmer are easily interpreted. When designing an HDL project, it is important to keep in mind that there are no logical attributions being made in the code, but rather the connection of wires.

The HDL attribution $a <= b$ does not take into account that a compiler is going to process the logical implications of the code and create an instruction to perform said operation. It will simply connect the output of a structure to the input of the other - more precisely, it will route one to the other since all inputs and outputs are already connected to the interconnection nets as previously mentioned.

It becomes very clear that the FPGA structure is far more general than that of a micro-controller and this can be very rewarding in some cases - when a parallel structure is needed - and not so much in many others - serial processing algorithms. In this sense the following statement makes sense and captures the essence of the discussion: it is possible to build a micro-controller out of an FPGA but it is not to possible to build an FPGA out of a micro-controller.

(b) FPGA Design Strategies and Directives

Since FPGAs are comprised of the building blocks of digital electronics and by connecting them greater structures can be created, it would make sense to structure an FPGA project design on that idea. For that, one of the first steps on each project is to define the hierarchy of the project. Let's take the example of a processing unit which receives serial input data (from a computer), stores, processes, and outputs the processed data serially (to a computer). The hierarchy, in this case, can begin with Figure II.10 where three main units are defined: input/output control; memory unit; and processing unit.

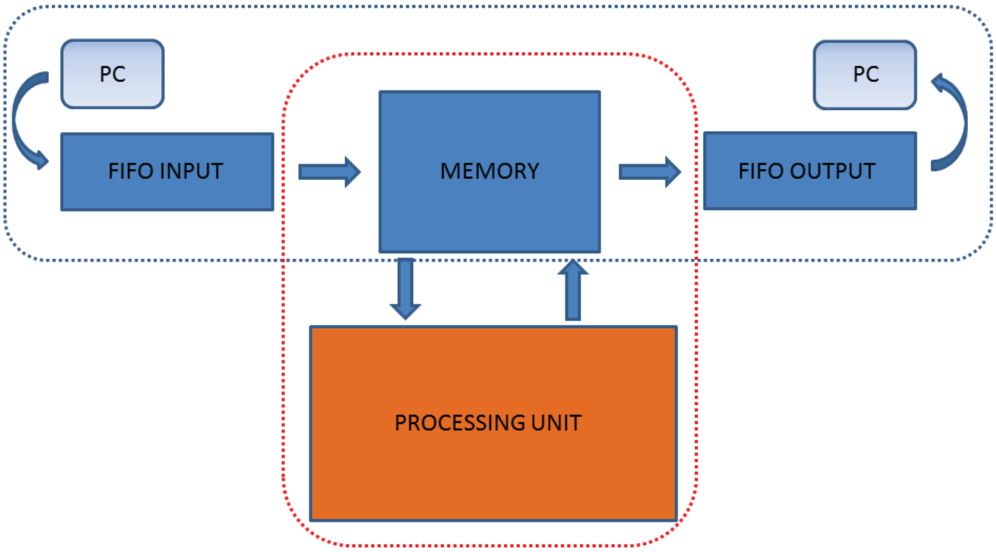


Figure II.10: Example of first step hierarchical definition.

Within each of these structures, more profound hierarchical subdivisions can be performed until the building blocks of the FPGA are reached. In the processing unit, for example, counters, adders, Finite State Machines (FSMs) and latches will be identified hierarchically and each of them will be defined and simulated. When all structures are behaving as expected, they can be merged into more complex structures until finally the processing unit is completed.

Practically, this strategy has the drawback of a slow start since it is in general necessary to unravel the entire hierarchy before starting to build the construction blocks of the final design. On the other hand, it gives a much clearer perspective on the project, enables task multiplexing - two designers could work on different structures at the same time - and also minimizes the number of simple mistakes that can lead to unexpected outcomes in the project's wider picture.

(c) Basic Digital Electronic Units

Despite the above mentioned strategy, it is clear that there is no necessity for creating components for each D-latch used in the design since that would render the design fragmentation completely obsolete. The definition, however, of how much logic a basic component - a building block in the design - should contain is a fine line that have many parameters often associated with each designer's practice. As in a C script, a function code with too many lines can be deceiving and hard to read, so too much information is always a problem. The number of counters, latches and multiplexers may as well turn the reading difficult.

In general, and along the projects here discussed, three structures considered basic are defined as to draw limits for the size of a component. These are: counters, FSMs and pipeline units. Counters are, as the name says, structures that increment their outputs in a previously defined fashion on a clock transition. FSMs, on turn, are structures that can jump from state to state on a clock transition given that the right input is selected. A state is associated with a different output, so counters can be thought of as very particular FSMs. Pipeline units are structures composed of serially connected processing elements where the output of one element is the input of the next one. An example is a chain of 1-bit full adders composing a 16-bit full adder. The important part of pipeline structures is the time taken by the process, i.e., the number of clock cycles after which the output be stable.

As a "rule of thumb" for the design, each of these structures should be associated with a different component and simulated for debugging. This imposes a parameter for hierarchical analysis of any project and contributes for the design strategy.

II.5 Avalanche Photodiodes

(a) Linear Operation

The first experimental demonstration of the Photoelectric Effect was developed by Heinrich Hertz in 1887. One might say that Hertz's experiments, together with Planck's Postulate, lead Albert Einstein to lay the milestones of Quantum Physics in the 1905 claimed paper *Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt* [9]. Besides the theoretical impact of Einstein's work, the theory behind the Photoelectric Effect permitted the construction of an apparatus capable of detecting light, a Photodetector.

The first Photodetector dates from 1913, when Elster and Geiter invented the Photoelectric Tube, a device based entirely in the effect demonstrated by Hertz and later explained by Einstein. Subsequent developments gave birth to the Photo Multiplier Tube (PMT), a more sensitive device which, until today is used in several fields of research such as nuclear and particle physics, astronomy and medical diagnostics.

Photodiodes are devices created with doped semiconductor junctions as described before and condensate, in a Solid State structure, the mechanism of light detection of the Photoelectric Tube. The basics of a Photodiode's operation are described in Figure II.11, in which an electron with sufficient energy ($h\nu = E_g$) excites an electron to the conduction band therefore creating an electron-hole pair which conduces current along the semiconductor proportional to the number of photons arriving at the junction. Each carrier then migrates in opposite directions under the influence of the electric field across the Depletion Region.

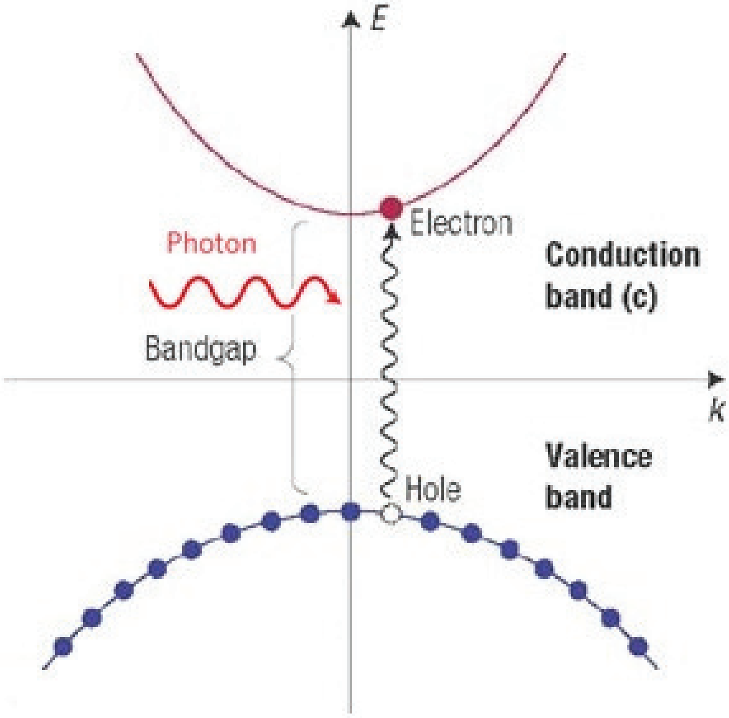


Figure II.11: Interaction Between an Incident Photon and the Semiconductor Junction in the Energy Domain.

The most important physical parameters of Photodiodes are listed bellow:

- Dark Current (I_S): The leakage current that flows through the junction when a bias voltage is applied to the material [10]. This concept had already been discussed previously in the *Semiconductors* section and addressed as the thermally-generated current.
- Quantum Efficiency (η): The rate of generated photoelectrons (n_e) divided by the rate of incident photons (e_{ph}): $\eta = \frac{n_e}{n_{ph}}$ or $\eta = \frac{I_{ph}/e}{P_0/h\nu}$ [11].
- Penetration Depth (δ): Incident light intensity inside the semiconductor varies with $I = I_0 e^{(-\alpha x)}$ where α, is a parameter of the material and is inversely proportional to the incident wave frequency. The Penetration Depth is defined as $\delta = 1/\alpha$ [11].
- Responsivity (R): The magnitude of electrical signal output from a Photodetector in response to a particular light power. $R = I_{ph}/P_0$ or $R = \eta \frac{e}{h\nu}$ [11].
- Response Time (τ): Dynamic performance of the photodetector calculated as the root mean square of the charge collection time (diffusion

and drift velocities) and the RC time constant dependent on the junction capacitance (due to the accumulation of carriers in the Depletion Region) [11].

- Noise Equivalent Power (NEP): The minimum detectable signal by a Photodetector, i.e., the minimum optical input power that yields a Signal to Noise Ratio of 1 ($SNR = 1$).
- Detectivity (D): Reciprocal of the Noise Equivalent Power, defined as $D = \frac{1}{NEP}$.
- Normalized Detectivity (D^*): Normalized Detectivity, taking into consideration the detector area and its bandwidth. It is defined as $D^* = \frac{\sqrt{A \times \Delta f}}{NEP}$.
- Shot Noise: Statistical fluctuation of the photocurrent due to the Poissonian Distribution of the photon stream. The photocurrent comprises a superposition of current pulses, each associated with a detected photon, so the mean value fluctuates.

Further evolution in the control of the semiconductor creation technology permitted enhancements in the Photodetector's design and led to the creation of *p-i-n* Photodiode, a structure with optimized detection area. Even though these structures exhibit higher gain when compared to regular *p-n* Photodiodes, the creation of the Avalanche Photodiode permitted a breakthrough in terms of photo-electric amplification.

Avalanche Photodiodes (APDs) are specially designed semiconductor structures that operate in the Breakdown Region. When a photon excites an electron pair in the Depletion Layer, the high built-in electric field intensified by a high reverse bias voltage provides enough kinetic energy to the carriers so that subsequent impact ionizations are possible, creating an avalanche process similar to the photo-multiplication of PMTs. APDs are, therefore, structures with internal gain since one photon produces more than one electron-hole pair.

As already mentioned, the APD is a Solid State Photomultiplier which exhibits many advantages when compared to PMTs. The physical structure of an APD and its operation principle may vary greatly depending on the application. Heterostructure APDs and Multiquantum-Well APDs are examples of technologies that were developed based on the conventional epitaxial APD which is depicted in Figure II.12 [11]. In a), the schematic structure of an Avalanche Photodiode is presented. b) Shows the net space charge density across the APD and c), the built-in electric field across the APD [11].

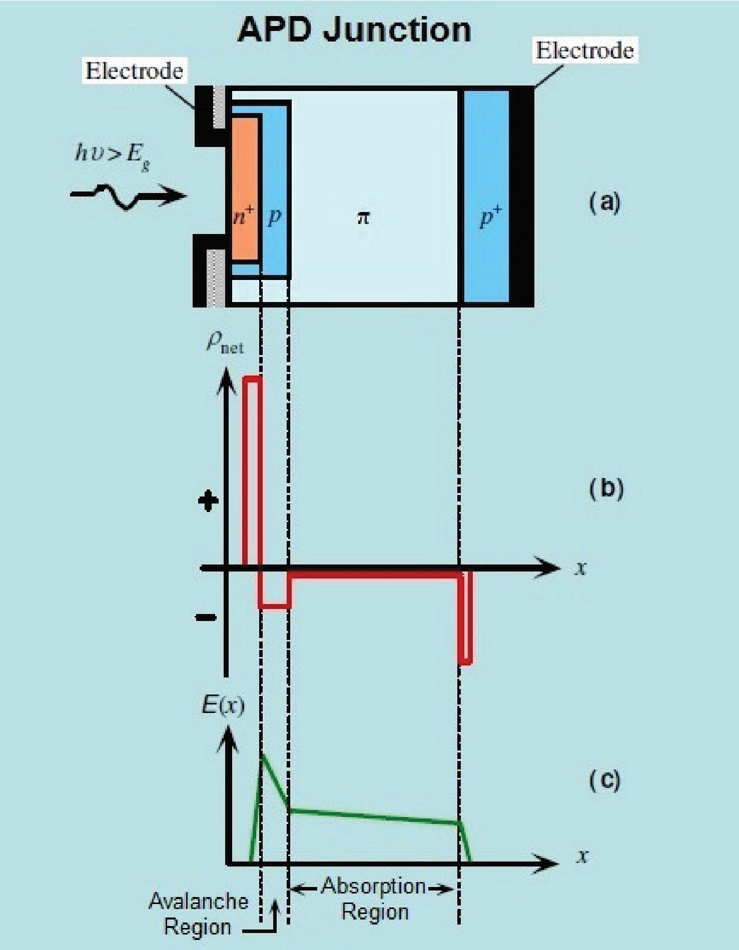


Figure II.12: APD Structure and Electrical Characteristics.

In such devices, incident light is mainly absorbed in the π region. From the π region, the photogenerated electrons drift into the n^+-p high field region where they undergo avalanche carrier multiplication [12]. It is important to notice that holes cannot be responsible for initiating the avalanche process since the electric field attracts these carriers in the p region direction away from the Avalanche Region. Usually, the n^+ contact under the optical window is made very shallow as to minimize both the carrier recombination and the hole injection from the n^+ region to the p region, which would increase the noise of the device [12].

Biasing the APD demands fine adjustment since, under the Breakdown voltage, the avalanche can be halted due to friction losses and, above the Breakdown, the device can be damaged by the high voltage and current produced. If the right bias voltage is applied, the acceleration of the charge carriers is high enough to sustain the avalanche process and single photons can be sufficient to generate a constant current which can be measured by external electronic equipment [13]. The photocurrent generated is calculated as shown in Equation (3) [13], where M is the APD internal gain.

$$I_{ph} = RMP_{in} \tag{3}$$

The Avalanche Multiplication M factor depends on the reverse bias voltage applied to the material and can be calculated as shown in Equation 4 [11], where n is the refractive index of the material, V_R is the reverse bias voltage and V_{BR} is the breakdown voltage of the n^+-p junction. The typical gain curve versus operating voltage for a Silicon APD is depicted in Figure (II.13) [13].

$$M = \frac{1}{1 - (V_R/V_{BR})^n} \tag{4}$$

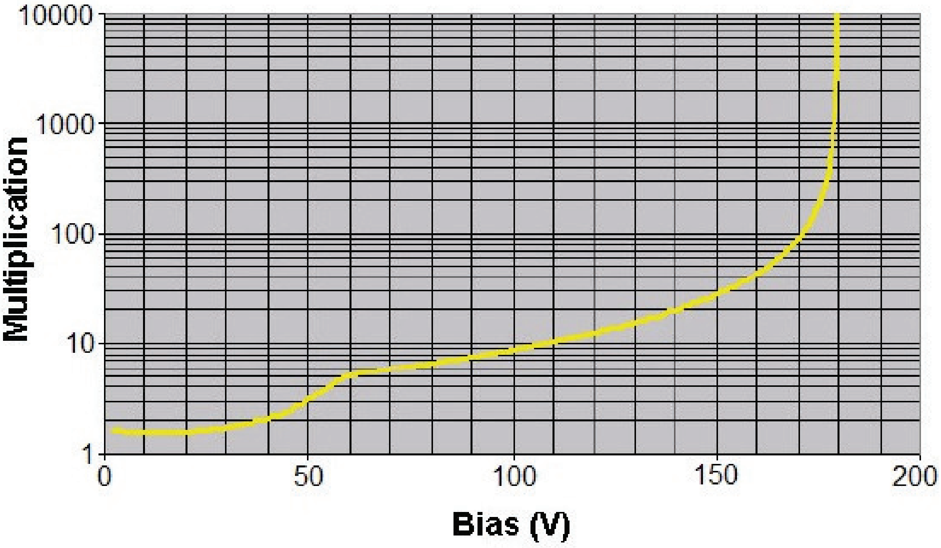


Figure II.13: Typical Gain Versus Operating Voltage for a Silicon APD.

To compare the efficiency of an APD with a p-i-n or p-n Photodiode, it is not sufficient to merely compare the noise of the detectors; the SNR of the entire system is crucial. For non-avalanche photodiodes, the respective preamplifier must always be considered since its noise characteristics are, among other things, frequency dependent and affect the response bandwidth. An APD is superior to a p-i-n Photodiode whenever the APD can substantially boost the signal level without significant increase of the overall system noise. In this sense, APDs are preferred in applications where light intensities at middle or high frequencies have to be detected. For APDs as well as for p-i-n Photodiodes, noise increases with bandwidth, therefore it is important to reduce it as far as it is practicable [13].

In an APD, Dark Current is created due to the thermally generated electron-hole pairs which are, then, multiplied in the Avalanche Region. The Avalanche or Multiplication Region of an APD plays a critical role in determining its performance since increasing the APD gain by increasing the external bias voltage also increases the Dark Current [14], a phenomena illustrated by Figure II.14 [14] in which M_{opt} signalizes the optimal reverse bias voltage for maximal Signal to Noise Ratio. Because the internal gain of the APD also affects the Shot Noise, the SNR decreases for M grater than M_{opt}. The APD multiplication process also produces an additional noise component, known as Excess Noise, a consequence of the random nature of impact ionization during avalanche which depends on the rate $\kappa = \alpha/\beta$ of electrons (α) and holes (β) ionization coefficients [15].

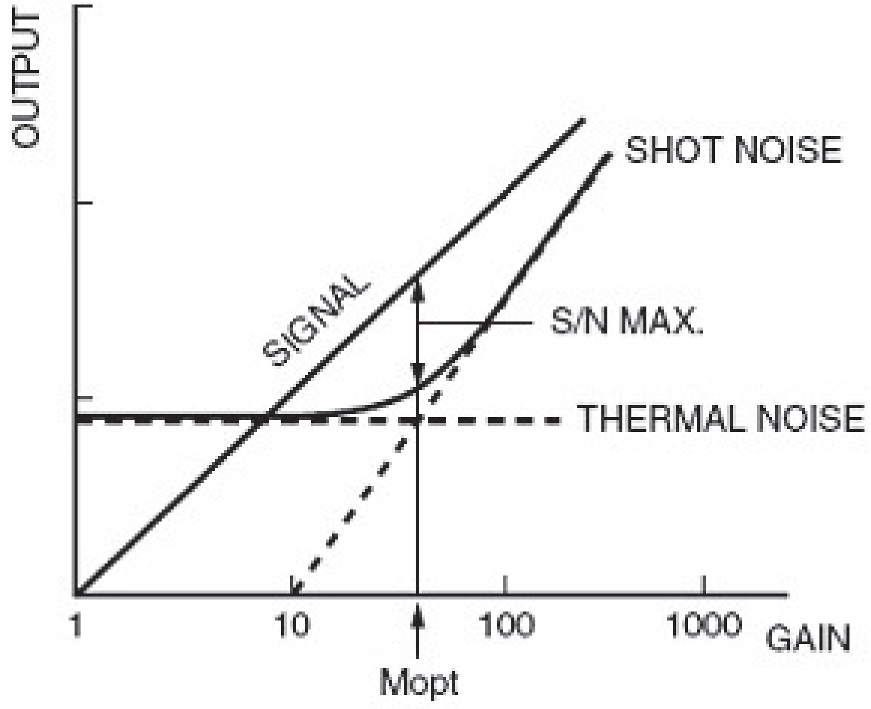


Figure II.14: Signal and Noise Characteristics of a Conventional APD.

In free space and fiber optical data transmission, rise and fall times of 300 ps at a gain of up to 100 make APDs the components of choice for use in high-speed receivers. Small area, low noise InGaAs APDs serve as key components for the construction of highly sensitive receivers, enabling data transfer across several kilometers at 12.5 Gbps [13]. A list of different APD structures and its characteristics is presented in Table II.3 [13]. Specially selected Si APDs can also be used as Photon Counters in the “Geiger Mode” [13].

Table II.3: Different APD Structures Characteristics [13]

Structure Type	Bevelled Edge	Epitaxial	Reach Through
Absorption Region	large	low	middle to large
Multiplication Region	large	low	middle to large
Typical Size (diameter)	up to 16 nm	up to 5 nm	up to 5 nm
Gain	50-1000	1-100	15-300
Excess Noise Factor	very good ($\kappa = 0.0015$)	good ($\kappa = 0.03$)	good to very good ($\kappa = 0.02$ to 0.002)
Operating Voltage	500-2000 V	80-300 V	150-500 V
Rise Time	slow	fast	fast
Capacitance	small	large	small
Blue Sensitivity	good	poor	good
Red Sensitivity	good	good	good
Near IR Sensitivity	vary good	good	very good

The three possible APD structures detailed in Table II.3 are presented in Figure II.15 [13]. M indicates the Multiplication Region of the APD structure and A indicates the Absorption Region [13].

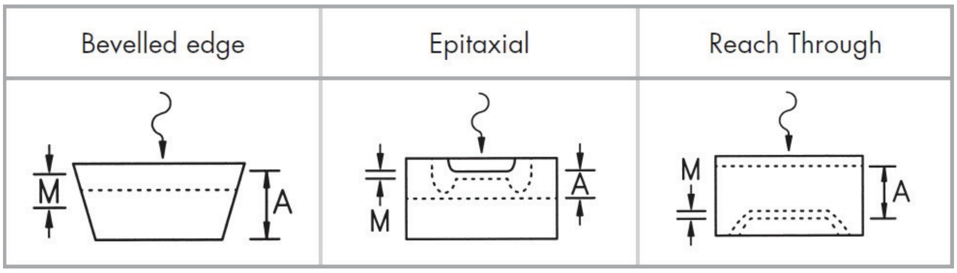


Figure II.15: Three Possible APD Structures.

The spectral operating range of APDs is very wide, in the range from 300 nm to 1700 nm. Silicon APDs are, depending on their structure, suitable between 300 nm and 1100 nm, Germanium between 800 nm and 1600 nm and InGaAs from 900 nm to 1700 nm, making InGaAs the most suited for telecom operation. Compared to Germanium, InGaAs APDs have significantly lower noise characteristics, a higher bandwidth relative to the active area and advantages due to the extended spectral response to 1700 nm. A disadvantage is that InGaAs APDs are more expensive than Germanium APDs [13].

(b) Geiger Operation

Avalanche Photodiodes are Photomultipliers devices that undergo an avalanche process whenever a photon reaches the absorption region and excites an electron-hole pair that collects sufficient kinetic energy from the applied electric field to start an impact ionization cascaded effect. The basis of this effect is an operation at the Breakdown Voltage, so the avalanche may be sustained. Geiger Mode APDs (G-APDs) go further into the Breakdown Region of a Photodiode.

Two distinct modes of operation of the G-APD can be defined according to the device's characteristics:

- IDLE: The device is reverse biased over the breakdown voltage with a discharged junction and ready for a detection.
- ACTIVE: A constant detection current flows through the device after any number of photo-excited carriers initialize the avalanche.

When biased above the Breakdown Voltage, electrons and holes are ionized faster than they can be extracted from the semiconductor lattice so, eventually, the junction becomes saturated [16], [17]. G-APDs operate at saturation, therefore the photocurrent is independent of the number of incident photons since it reaches the saturation value in every detection. This behavior differs from that of other photodetectors in which the photocurrent is proportional to the number of photons. For that reason, a gain factor is not defined for G-APDs [17].

The effects of a photoexcited electron-hole with enough energy to produce cascaded ionization is an exponential growth in the population of holes and electrons in the Multiplication Region and of the associated photocurrent. This goes on for as long as the electric field in the device is not altered by the photocurrent growth, i.e., until the space charge effect limits the photocurrent to a constant value leading the circuit into a steady-state condition [16], [17].

In order to bring the device back from the steady-state, it is necessary to discharge the device's saturated junction in a process called *quenching*, which can be active or passive. Different circuits can be employed in order to perform passive or active quenching. Figure II.16 pictures the schematic diagram of a Quenching Circuit using a transistor configuration. After a photon arrives, the voltage T_S reaches a peak and is forced to return to zero when transistor M_1 is activated. V_{SEL} controls the recharging of the APD. Transistor M_7 signalizes the photon arrival [18].

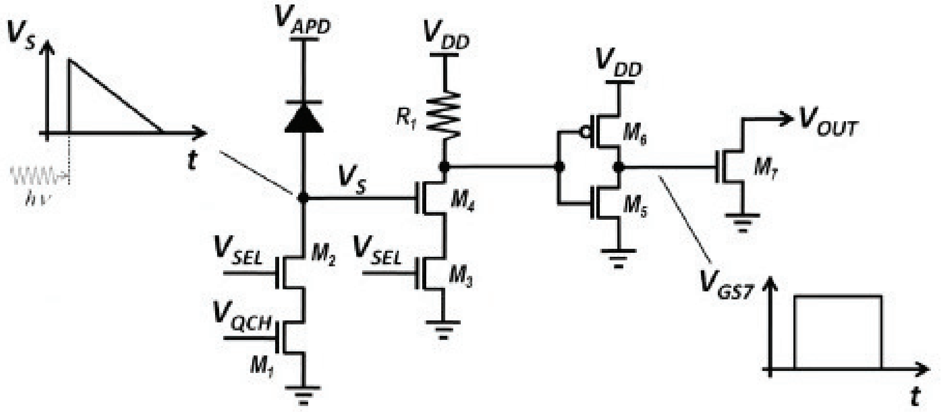


Figure II.16: Schematic Diagram of an Active Quenching Circuit with a Detection Signalling System.

Aside from higher sensibility to single photons reached by G-APDs, the binary behavior of these devices introduces two new parameters of operation: Dead Time and Afterpulsing. Dead Time is the period between an avalanche and the end of the quenching process during which the photodetector is inoperative [19]. Since G-APDs become unresponsive during the Dead Time, active quenching is more suited for fast detection applications [16], [17].

Although already present in other photodetector devices, the Afterpulsing effect is more critical in G-APDs. The probability of a Dark Count, i.e., a false avalanche, is higher right after a detection due to carrier trapping [17] and delayed release inside the semiconductor junction. This period might last several microseconds [19]. One drawback of Afterpulsing is that, in order to diminish the probability of thermally generated avalanches, the temperature of the photodetector is often decreased which leads to longer delayed releases and, thus, to longer periods of high Afterpulsing probability [19].

More than one G-APD may be used in an array configuration which is desirable in various applications [19], [20]. In these cases, the Optical Crosstalk is an effect that may degrade the device's response. During an avalanche process, photons may be re-emitted due to the high energy electrons crossing the junction and may be re-absorbed by other detectors, creating an undesirable Dark Count effect. This might be overcome by tailoring the device.

The physical parameters and the design of the photodetector structure has direct implication on the operation of the device. The doping concentration of each layer and its thickness, for instance, affect the range of sensitive wavelengths and the operating voltage, respectively. Dark Counts and Afterpulsing, on the other hand, can be reduced by controlling the impurities and crystal deffects [19].

Other features of Geiger-Mode Avalanche Photodiodes include [19]:

- High gain (independent of the input optical power).
- Low bias voltage ($\sim 50V$).
- Low power consumption.
- Compactness and ruggedness.

The application of G-APDs is vast, including High Energy Physics, Astroparticle Physics, Medical Applications [20], in which various of such devices are used in an array, and Quantum Information, where the G-APD is used to build a structure called the Single Photon Counter (SPD). The technology enhancements in SPD design is one of the reasons for the rediscovery of techniques such as the Photon-Counting OTDR [21], [22]. The simplified schematic design of IDQuantique's *id210* is depicted in Figure II.17 [23].

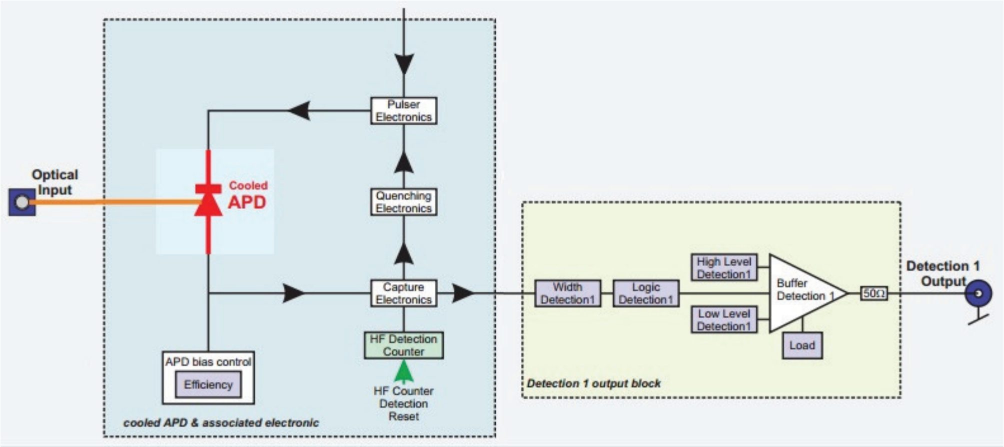


Figure II.17: Simplified Schematic Siagram of the *id210* Single Photon Detector.

II.6 Lasers and Optical Amplifiers

The acronym LASER (Light Amplification by Stimulated Emission of Radiation) often stands for devices that emit light through a process of optical amplification based on the stimulated emission of electromagnetic radiation when, in fact, the acronym refers to the process itself. The theoretical foundations of Laser (and Maser) theory were described by Einstein [24] in 1917 where he re-derived Planck's law of radiation using a formalism based on the probability coefficients for the three kinds of interaction between photons and atoms: absorption; spontaneous emission; and stimulated emission (Figure II.18) [10]. In memory of Einstein, these coefficients are now known as Einstein Coefficients.

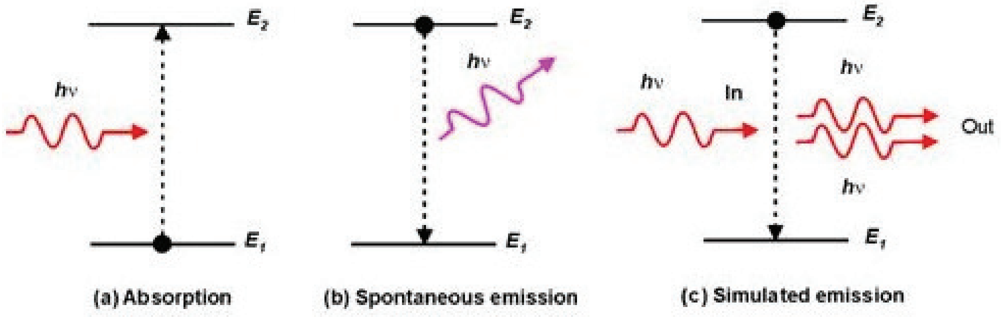


Figure II.18: Possible Interaction of Light and Matter.

Lasers are strongly dependent on the phenomena of *population inversion*, a condition in which the number of excited members of a system exceed that of the non-excited ones. The main concept is to give enough energy to a system (atoms, solids, molecules) in a process called *pumping* so the members can reach the Excited State and, by achieving the *population inversion* condition, stimulate a simultaneous decay to the Ground State as depicted in Figure II.19. The simultaneous decay leads to the generation of a coherent light beam since the emitted photons share the same characteristics of the original incident photon [10]. This process can be considered an optical amplification since the light intensity grows after the interaction.

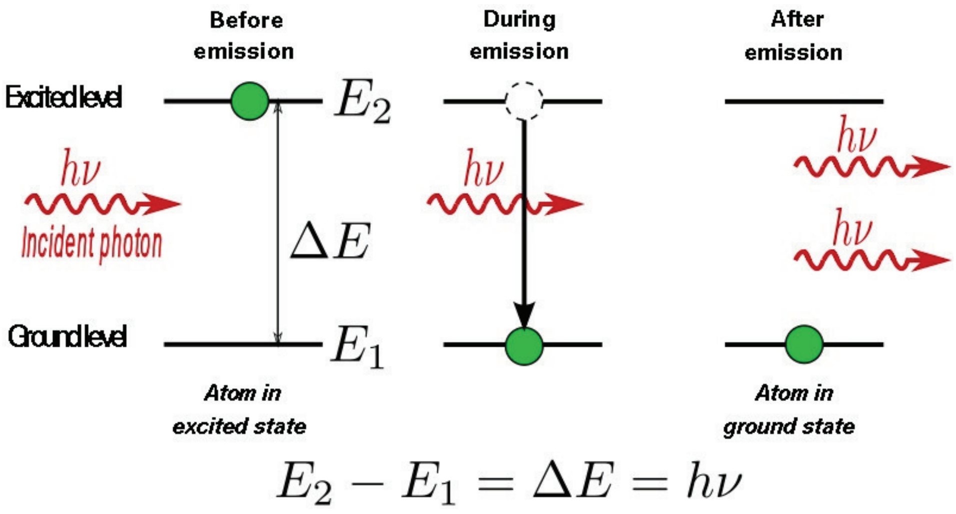


Figure II.19: Diagram of the Steps of the Stimulated Emission Process.

Population inversion, however, is a delicate phenomena which depends on the rates of transition between Energy Levels inside a system and, in thermal equilibrium, cannot exist [25]. This behavior is clarified by Equation (5), which describes the dependence of the density of occupied states in a two levels system, N_1 (Ground State) and N_2 (Excited State), with Temperature [25]. This equation is a derivation of the Boltzmann Distribution, which governs systems in thermal equilibrium [26]. Hence, Lasers operate in a non-equilibrium regime.

$$\frac{N_2}{N_1} = e^{-\Delta E/k_B T} \tag{5}$$

Even though two level Lasers as described above have been created and are possible, *Continuous Wave* (CW) operation is difficult because of the limit imposed by population inversion. These devices operate in a *Pulsed Mode* (PM) regime, where the pumping takes members of the population to the Excited State then Stimulated Emission is induced taking all the members to the Ground State and the process repeats. Intelligent designs which make use of more than two energy levels and can operate in both conditions, PM and CW, are presented in Figure II.20 [10].

In Figure II.20 a), the three Level Laser schematic is presented. Atoms in the Ground State (1) are excited via Pumping to a high energy state (3) from where there is fast Spontaneous Emission to a lesser energetic state (2). Atoms in this level are more stable so the Population Inverse can be induced continuously (CW mode). In b), the Four Level Laser schematic is presented. Atoms in the Ground State (0) are excited via Pumping to a high energy state (3) from where there is fast Spontaneous Emission to a lesser energetic state (2). The Stimulated Emission occurs from level 2 to level 1 so *population inversion* has to be achieved between these two levels [10].

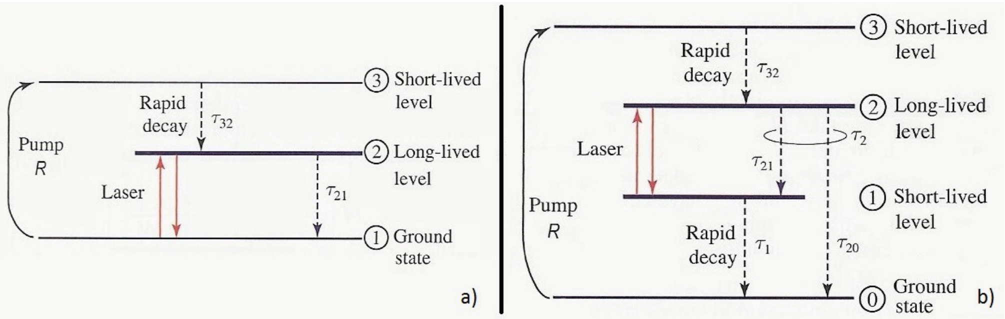


Figure II.20: Three and Four Level Laser Schematics.

In the *population inversion* condition as described above, Stimulated Emission dominates over Spontaneous Emission and the system exhibits optical gain. For semiconductor Lasers, *population inversion* is achieved inside a *p*-*n* junction which is called Active Region [25]. In order to form the Active Region the *p*- and *n*-type semiconductors must be heavily doped so that the Fermi-Level separation exceeds the Band Gap under forward biasing as seen in Figure II.21. In a) is the band diagram with no external bias voltage applied and in b), the band diagram with the application of an external bias voltage [27].

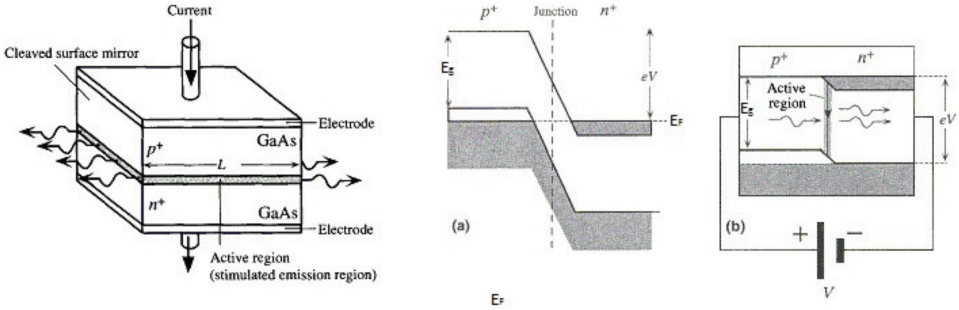


Figure II.21: Active Region Formation Due to High Doping of a *p*-*n* Junction.

Heterostructures such as the one depicted in Figure II.22 [27] (*n*-AlGaAs, GaAs, *p*-AlGaAs), with an Active Region formed by a lower Band Gap intrinsic semiconductor between a *p*-*n* junction, are commonly used in Laser design since it improves the rate of Stimulated Emission and also the efficiency of the optical cavity [27]. In Figure II.22 b), a sufficiently large forward bias leads to a large injection of electrons from the Conduction Band of the *n*-AlGaAs into the GaAs which are confined to the Conduction Band of the GaAs since there is a potential barrier (ΔE) between the GaAs and the *p*-AlGaAs [27].

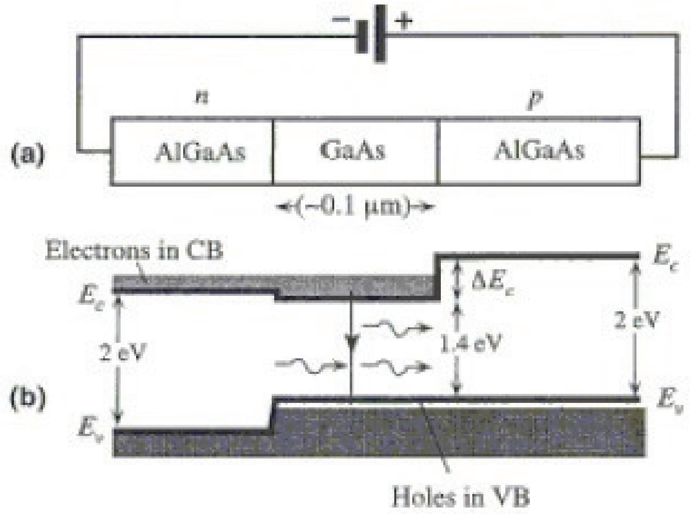


Figure II.22: Forward Biased Heterostructure Schematic.

Semiconductor Optical Amplifiers (SOAs) share the same principal of Lasers in terms of the amplification of light and even in terms of physical structure. The main difference, however, is the absence of the *optical feedback*, which converts an amplifier into an oscillator [25]. In non-semiconductor Lasers, the feedback is provided by placing the gain medium inside an optical cavity formed by two mirrors. In the case of semiconductor Lasers, external mirrors are not required since the cleaved semiconductor facets act as mirrors [25].

Since the concentration of injected electrons in the Active Region can be increased quickly even with moderate increases in forward current if it is made thin [27], SOAs are well suited for any optical amplification process. Also, an optical dielectric waveguide that confines photons to the Active Region is created due to the Heterostructure's different refractive indexes [27].

Figure II.23 depicts a typical SOA structure. Light entering in $z = 0$ stimulates emissions along the length of the device so the output power at $z = L$ is sensitively higher than at the input. The core of the waveguide is formed by the intrinsic active region due to the difference of refractive indexes between InP and InGaAsP [28].

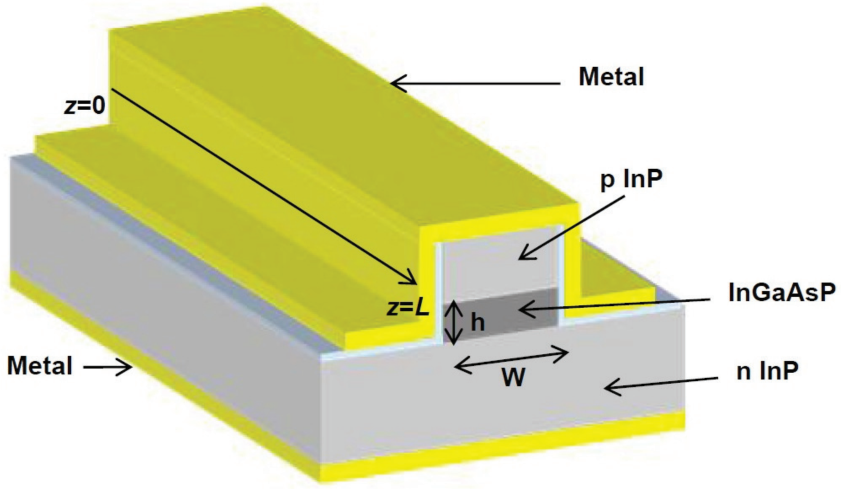


Figure II.23: Typical Semiconductor Optical Amplifier Structure.

II.7 Optical Fibers

Optical Fibers are structures that guide light due to *total internal reflection* which is a consequence of a difference in refractive indexes. Total internal reflection is one of the many possible outcomes of light encountering an abrupt change in refractive indexes which are accounted for by Equation (6) (Snell's Law) and depicted in Figure II.24. The angle that the incident beam of light forms with the normal of the incident plane is of total relevance in the interaction's result as well as n_1 and n_2.

$$n_1 sin\theta_1 = n_2 sin\theta_2 \tag{6}$$

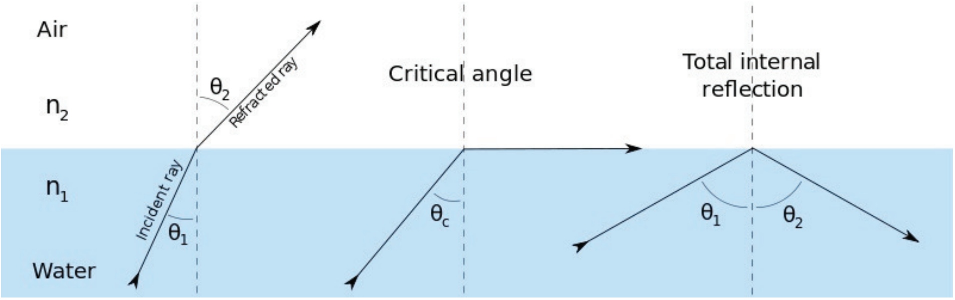


Figure II.24: Different Outcomes of Light Interacting with an Abrupt Change in Refractive Index.

If the first total internal reflection is guaranteed, further propagation inside the waveguide is safeguarded since the reflected angle is equal to the incident angle and the behaviour repeats itself. Thus, in order to guarantee the propagation, a minimum angle of incidence in the fiber is defined as the fiber's Numerical Aperture. The Numerical Aperture defines a cone of acceptance for the fiber, i.e., light beams inside the cone will be coupled to the fiber as depicted in Figure II.25. With little manipulation of Equation (6) it is possible to find Equation 7.

$$NA = \left(n_1^2 - n_2^2\right)^{\frac{1}{2}} \tag{7}$$

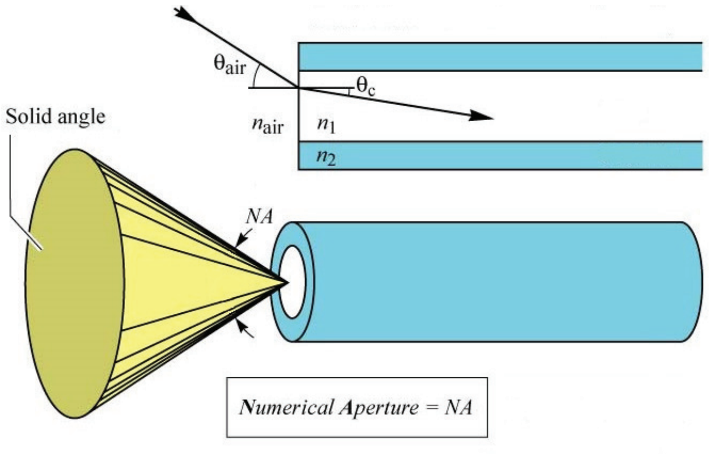


Figure II.25: Cone of Acceptance Defined by an Optic Fiber's Numeric Aperture.

In general, an Optic Fiber consists of a cylindrical core of silica glass (n_1) surrounded by a cladding (n_2) whose refractive index is lower than that of the core so that light can be guided. The difference in refractive index is usually very small for communication purposes since the phenomenon of *multipath dispersion* can be diminished by that. Another technique for canceling the loss due to *multipath dispersion* is that of Graded-Index fibers, in which the refractive index changes smoothly [25] in contrast with the Step-Index fibers described previously and shown in Figure II.25.

An important characteristic of Optic Fibers, which is a characteristic of every waveguide, is the capacity to guide more than one propagation mode. This result arises theoretically from the different particular solutions of the Wave Equation [10] given the boundary conditions of the waveguide. Due to a high Dispersion coefficient inherent of Multimode guiding, Single-Mode fibers are preferable for communication, even though the amount of data supported being smaller [25].

In the present time, Fiber-Optic communications are the dominant data transport medium, with rates of up to 15 Tbps at $1.55\mu m$ when employing the technique of Dense Wavelength Division Multiplexing enabled by the development of robust Optical Amplifiers [29]. The evolution of Fiber-Optic communications is, thus, a joint work between the Fiber, Transmitter, Detector and Amplifier technologies which is detailed in Table II.4.

Table II.4: Fiber-Optic Communications Evolution [25]

Optic-Fiber Communications Generation	Optical Fiber Technology	Tx, Rx and Amplifier Technology	Year	Bit Rate and Distance
First Generation	850 nm 4 dB/km	AlGaAs Laser 800 - 890 nm	1980	45 Mbps 10 km
Second Generation	1300 nm 0.5 dB/km	InGaAsP Laser 900 - 1700 nm	1987	1.7 Gbps 50 km
Third Generation	1550 nm 0.2 dB/km	InGaAsp Laser 900 - 1700 nm	1990	2.5 Gbps 60-70 km
Fourth Generation	1550 nm 0.2 dB/km	EDFA + WDM 900 - 1700 nm	1996	5 Gbps 11300 km

The initial separation between the Second and Third Windows (1300 nm and 1550 nm) was due to an absorption peak of the *Hydroxyl* (OH), a contaminant in the fabrication of the optical fiber [30]. This contaminant could later be removed by more advanced optical fiber manufacturing processes and the two windows were substituted by a broad wavelength spectrum. The wavelengths from 1260 to 1675 are subdivided according to Table II.5 [30].

Table II.5: Fiber-Optic Operational Bands [30]

Band	Description	Range
O Band	Original	1260-1360 nm
E Band	Extended	1360-1460 nm
S Band	Short Wavelengths	1460-1530 nm
C Band	Conventional	1530-1565 nm
L Band	Long Wavelengths	1565-1625 nm
U Band	Ultralong Wavelengths	1625-1675 nm

II.8 Optical Time Domain Reflectometry

(a) Basic Operation

The success of Optical Fibers as data carriers was unmatched and soon exceeded electrical waveguides, free-space Radio Frequency transmissions and electric cables in terms of distance, bandwidth and cost [25]. The mechanical fragility of glass fibers, though, impose a serious drawback since breaks and faults may jeopardize the data transmission eventually rendering the link inoperative.

Based on the theory of light backscattering introduced by John William Strutt (Lord Rayleigh) in the late 1800s [31], [32], and since its demonstration in 1976 [33] the Optical Time Domain Reflectometry technique offers a method for detecting and evaluating fiber faults without the need of end-to-end measurements [33] thus providing a valuable tool to support the operation of Fiber-Optic links [21]. A simple OTDR schematic which makes use of an *optical circulator* is depicted in Figure II.26.

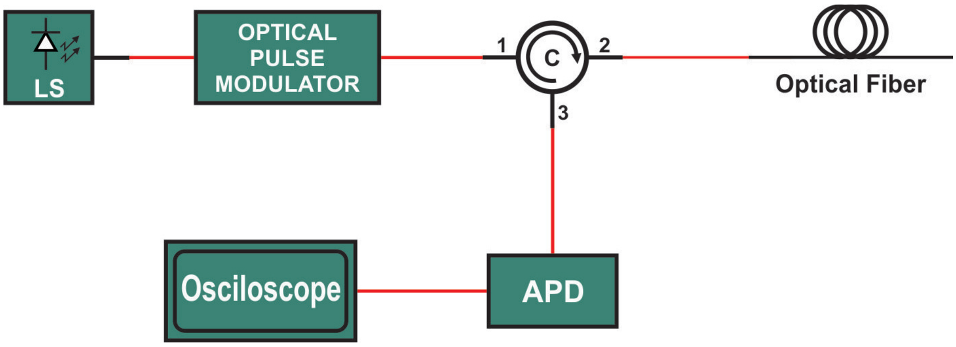


Figure II.26: Basic OTDR setup.

During the period of 1854 to 1879, John Strutt published several papers discussing the phenomenon of light scattering from atomic nuclei which depended on the wavelength of the incident light [32]. Rayleigh Scattering is the excitation of the electric dipole of the atom by light with wavelength much smaller than the atomic radius. The excited dipole then radiates photons in the same wavelength in every direction. In an Optic Fiber background, if the backscattered light falls inside the Cone of Acceptance defined by the fiber's Numerical Aperture, it is guided back.

The backscattered light can then be detected and used to create a profile of the fiber according to the power level received. Since the waveguide's attenuation is dependent on the distance, the OTDR trace produced by an optical pulse traversing it is a descending line with angular coefficient equal to the fiber's attenuation. Any event which causes optical power loss is interpreted accordingly as shown in Figure II.27. Fiber connectors, for instance, are characterized by a higher reflection coefficient in a specific point along the fiber, i.e., a reflected power peak. Fiber faults, connectors and defective fiber splices can also be identified.

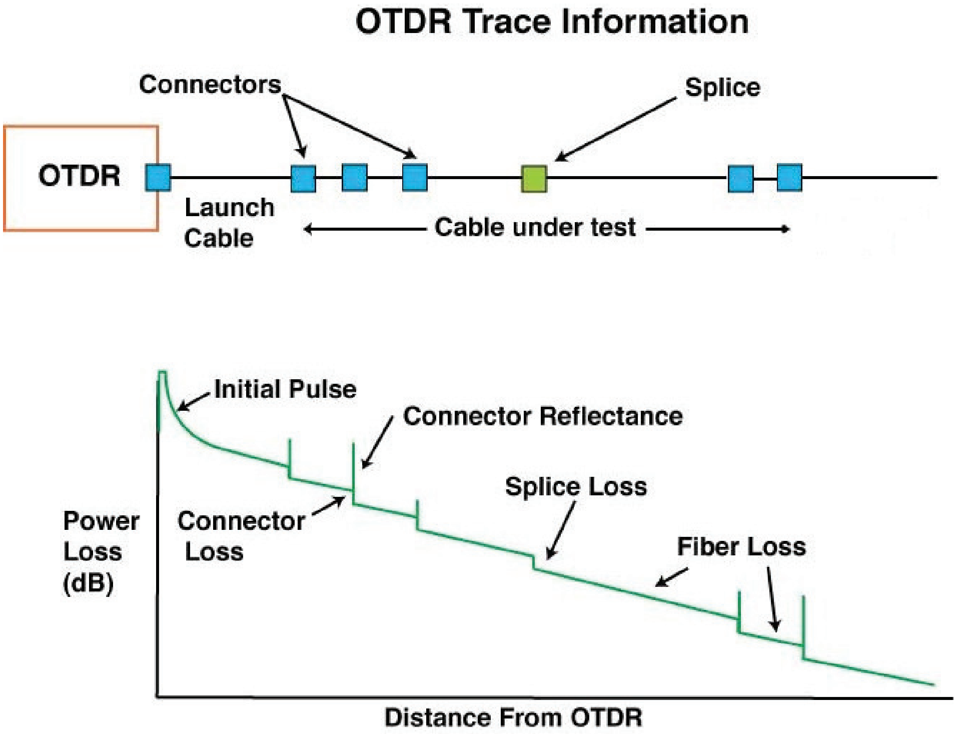


Figure II.27: Information Retrieved from the OTDR Trace.

(b) Fiber Losses

Fiber loss is one of the most important properties of an optical fiber as it largely determines the maximum distance from one optical repeater to the other and, thus, the number of repeaters in any fiber optic communication link. Three loss mechanisms play the major role in fused silica glass fibers (SiO_2): absorption, scattering and bending. As already mentioned, absorption is very low in the telecommunication wavelength range, from the O to the U band, but still inflicts an attenuation of approximately 0.2 dB/km at the C band. Stress, pressure, tension and twist along with manufacturing imperfections can inflict losses due to micro-bending so it is common that the fiber is protected by either a loose or tight buffer [34].

In terms of scattering, three distinct phenomenons can be present in the fiber: Raman, Brillouin and Rayleigh. While the first two are nonlinear effects that occur only at higher power levels thus limiting the maximum optical power at the fiber's input, the third arises from light interacting with density fluctuations in the fiber. Variations in material density and compositional fluctuations during fiber manufacture can cause random inhomogeneities that give rise to refractive index variations. This isotropic phenomenon is termed Rayleigh scattering if the size of the defect is much smaller than the wavelength of the incident light, as proposed by John Strutt [34], [32].

(c) Backscatter Signal

As a result of the attenuation effects, light travelling along the fiber exhibits an exponentially decreasing power level with the distance. This is clarified by Equation (8):

$$P\left(z\right) = P_0\, e^{-\alpha z} \tag{8}$$

where the attenuation coefficient α is measured in km^{-1}. Also, α is regarded as a composition of the absorption and scattering coefficients.

$$\alpha = \alpha_a + \alpha_s \tag{9}$$

Since the backscatter coefficient of Single-Mode fibers is at least one order of magnitude smaller than the absorption coefficient [34], α can be approximated by α_a.

In a scattering event along the fiber, the scattered power dp_s at a position z within an infinitesimal small interval dz is proportional to the pulse power $P\left(z\right)$, the scattering coefficient α_s, the numerical aperture NA and the refractive index of the fiber core center n_0. Equation (10) describes this behaviour.

$$dp_s = \alpha_s \left(\frac{NA}{2.13\, n_0}\right)^2 P\left(z\right) dz \tag{10}$$

The quadratic term is usually referred to as the backscattering capture coefficient S, which describes the amount of optical scattered power that is guided back in the fiber and can be detected.

If a light pulse with duration τ travelling through the fiber is considered, light is scattered from a fiber element of length W which depends on the pulse duration, the speed of light c and the group index of the fiber n_{gr}.

$$W = \tau \frac{c}{n_{gr}} \tag{11}$$

The total optical power received by the measurement apparatus of the OTDR from a given distance L is the integral of the scattered power at position z along the fiber element W.

$$P_s\left(L\right) = \int_0^W S \cdot \alpha_s \cdot P_0 \cdot e^{-2\alpha(L+z/2)} dz \tag{12}$$

This expression can be further approximated, yielding Equation (13), which provides sufficient accuracy when dealing with pulsewidths typical in OTDR applications [34].

$$P_s\left(L\right) = S \cdot \alpha_s \cdot W \cdot P_0 \cdot e^{-2\alpha L} \tag{13}$$

(d) Spatial Resolution and Dynamic Range

The goal of spatially resolved optical reflectometry such as the OTDR is to measure optical reflectivity as a function of distance. An optical probe signal, generally an optical pulse, is sent into the fiber and the reflected signal returns after various time delays depending on the locations of the reflective sites which was previously deduced. With information about the time delay and the speed of light within the Fiber Under Test (FUT) it is straightforward to determine the reflection positions [34].

In this context, two characteristics of the measurement apparatus have to be considered: Spatial Resolution and Dynamic Range. Spatial Resolution, or Two-Point Spatial Resolution, refers to the minimum distance between two reflectors that can still be resolved by the measurement system. It reflects how sensible an OTDR system is and with what precision a fault can be detected. The Spatial Resolution has a strong correlation to Equation 11, for it becomes clear that narrower pulses yield better sensitivity.

Dynamic Range, on the other hand, refers to the maximum length of fiber which is measurable or, conversely, to the amount of attenuation along the fiber such that a SNR of 1 is still possible. The Dynamic Range is strongly correlated to Equation (13) since this equation states that the amount of optical power originated at distant portions of the fiber may be attenuated to the point where a detection is impossible. A fundamental limitation for any conventional OTDR is the tradeoff between Dynamic Range and Spatial Resolution.

For high Spatial Resolution, the probe pulsewidth has to be as small as possible with a correspondingly wide receiver bandwidth, which leads to reduced SNR. Increasing the strength of the received signal by using long probe pulses and low noise (low bandwidth) receivers leads to improved Dynamic Range with correspondingly less Spatial Resolution [34].

(e) Photon Counting OTDR

In the classical OTDR technique, detection involves the use of *p*-*i*-*n* and Avalanche Photodiodes [35] since the backscattered optical power is continuous at the detector. The maximal Spatial Resolution, i.e., the minimum distance detectable between two events, therefore, is dependent on the detector's bandwidth. Unfortunately, as already discussed, the reduction of the bandwidth has a direct consequence on the NEP which is high for linear photodetectors and imposes a limitation to the measurement precision [34].

An alternative to increased Spatial Resolution is the Photon-Counting OTDR, which employ single photon detectors. Such devices offer better sensitivity [35] since the NEP is minimal given that a single photon is capable of generating a detection current. Several applications of Photon-Counting OTDR can be found in [35], [22], [21], [36] and [37].

II.9 Classical Criptography

Criptography is the art of rendering a message unintelligible to any unauthorized party [38]. Together with its counterpart, Cryptoanalysis, which is the art of breaking codes, constitutes the broader field of Cryptology. In order to achieve confidentiality, a *cryptosystem* is used to combine the message with additional informationless data (key), such as in a channel coding scheme, producing a *cryptogram*. The success of a *cryptosystem* is dependant on the difficulty in accessing the message's information without the right key, i.e., how much effort should a cryptoanalist put into deciphering the *cryptogram* [38].

Cryptosystems come in two main classes which correspond to the use of the key by the two communicating parties, Alice and Bob. If Alice and Bob share the same key, the scheme is termed Symmetrical - or Secret-key - Cryptosystem. The process used by Alice to encrypt the message using the key is invertible, i.e., by use of the same key, Bob is capable of retrieving the message. The most important representative of the Symmetrical Cryptosystem class is probably the *One-Time Pad*, proposed by Gilbert Vernam in 1926, since it was proved secure via Information Theory [39], [40] and is the only completely secure cryptosystem known today [38].

The *One-Time Pad* takes a string of bits m which represents the message Alice wants to transmit to Bob and a randomly generated key k which must be of the same length of m. In order to encrypt her message, Alice must perform a bit-by-bit binary addition of m and k ($s = m \oplus k$) which produces s, the scrambled text which is transmitted to Bob. The same operation over s gives Bob and, assuming no one else possesses the key k, only to Bob, the message m ($s \oplus k = m \oplus k \oplus k = m$). Even though secure, the *One-Time Pad* is hardly implemented in practice for reasons that will be discussed shortly. To overcome such practical impossibilities, less reliable schemes with asymptotic security are used [38].

Cryptonalists resort to classical super-computers in order to faster decipher a cryptosystem since these are the most powerful processing tools available in present days. By creating problems which are hard to solve even for classical super-computers, modern cryptography has found a way to be asymptotically successful, i.e., capable of maintaining the information protected with a high probability. Ultimately, the main question behind computational complexity "*Is P equal to NP?*" secures most of the modern cryptosystems used in e-mails and bank accounts.

The RSA [41] is an example of such schemes which are known as Asymmetrical, or Public-Key, Cryptosystems. Since no fast classical (implementable to the present date) algorithm for factoring large numbers have yet been developed, protection of confidential information is based on the computational hardness of solving this mathematical problem.

In the Asymmetrical Cryptosystem paradigm, and following the description of Figure II.28, instead of encrypting the message and sending to Alice, Bob first chooses a private key P_p which is kept secret. Then, he computes, from this private key, a public key P_b which he discloses to any interested party. Alice uses this public key to encrypt her message which is then transmitted to Bob, who decrypts it with his secret private key [38].

The analogy of padlocks can be used in order to explain the mechanism. Bob produces padlocks and sends them to whoever wants to send secret messages to him. The open padlock distributed by Bob can be seen as a public key P_b which is produced using a private key P_p. Once the padlock is locked by Alice, only Bob can open it with the private key [38].

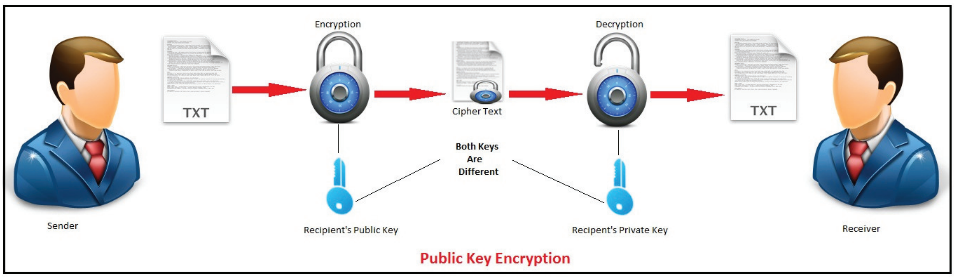


Figure II.28: Public Key Cryptosystem Scheme.

II.10 Quantum Information and Quantum Cryptography

(a) Quantum Superposition

The superposition principle plays the most central role in all considerations of quantum information and in the paradoxes of quantum mechanics. Its understanding can be accessed through the analysis of a simple physical experiment known as the Double-Slit Experiment. In this experiment (Figure II.29), a source of particles ranging from photons, electrons, neutrons or even atoms is aimed at a double-slit assembly and interference fringes are formed in an observation screen. These fringes may be understood once a wave property of the particles emerging from the source is assumed [42]. The interference pattern created in the observation screen follows the probabilistic distribution which corresponds to the intensity of the fringes.

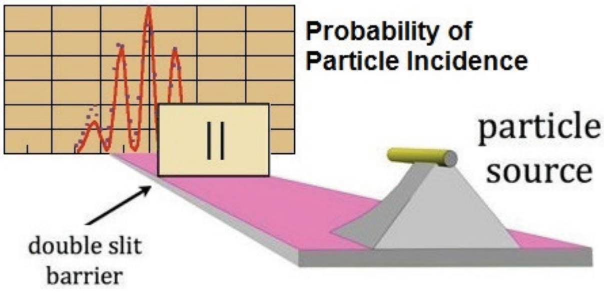


Figure II.29: Double-Slit Experiment Setup.

If one of the slits is kept close, no interference pattern is observed since there would be just one wavefront emerging from the barrier. Quantum mechanically, the state with both slits open is the coherent superposition

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_a\rangle + |\Psi_b\rangle\right) \tag{14}$$

where $|\Psi_a\rangle$ and $|\Psi_b\rangle$ describe the state with only slit a or slit b open. The interesting feature of this experiment is that it can be observed even when the source is set at such a low intensity that only one particle interferes with itself [42].

Like the Schrödinger's Cat analogy, any measurement over the superposition state created in the Double-Slit Experiment leads to decoherence, i.e., interaction with the particle is destructive to superposition. If a detector is positioned at any of the slits in order to determine which path the particle took, the interference pattern is lost and a classical particle behaviour is once again observed [42].

(b) Qubits

The most fundamental entity in information science is the bit, a system which carries two possible values, "0" and "1", for example. In its classical realisation, the bit is designed to have two distinguishable states, since any state transition would be detrimental. Therefore, classically, once the state of a bit is determined, measurement of the system yields that particular result [42].

In Quantum Physics, the fundamental concept is that of *state* which can be described as a wave function. The condition upon the wave function is that it satisfies Schrodinger's Equation which basically translates the law of energy conservation. One of the postulates of Quantum Physics states that *Every Quantum System can be described by a complex separable Hilbert Space.* In that sense, and according to the Spectral Theorem, the wave function that represents a *state* (Quantum System) can be written as an infinite weighted sum of orthogonal projections:

$$\Psi\left(x_1\right) = \sum_{i=1}^{\infty} \psi_n\left(x_1\right) E_n\left(x_1\right) \tag{15}$$

The set of orthogonal projections $E_n\left(x_1\right)$ and their corresponding weights $\psi_n\left(x_1\right)$ are determined by the physical quantity - e.g., linear momentum, position, spin, polarization, etc.. - chosen to describe the Quantum System. A measurement on $\Psi\left(x_1\right)$ leads to the collapse of the wave function into one of the orthogonal projections - *reduction of the wave packet* - so that the *state* becomes merely $\psi_n\left(x_1\right) E_n\left(x_1\right)$ for some n.

An equivalent representation of a *state* is Dirac's notation which uses $\langle|$ and $|\rangle$ to denote functions in the Hilbert Space that describes the Quantum System. The above equation is written, in Dirac's notation as:

$$|\Psi\rangle = \sum_{i=1}^{\infty} \psi_n \left|E_n\right\rangle \tag{16}$$

The *Qubit* can be thought of as the quantum analog of a classical bit and, since, is a two-level *state*. The *Qubit*, nevertheless, is defined over a Hilbert Space of dimension two which renders its representation completely different from its classical counterpart, the first being the possibility of state superposition. A *Qubit*, differently from a bit, has no definite state, rather, it is in a superposition of states and exhibits probabilities of being measured in one state or the other.

The general *Qubit*

$$|Q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{17}$$

with $|\alpha|^2 + |\beta|^2 = 1$ represents a system in the coherent superposition of states $|0\rangle$ and $|1\rangle$. Mathematically speaking, the state $|Q\rangle$ is written as a linear combination of the basis vectors $|0\rangle$ and $|1\rangle$. Upon measuring, the output can either be the state $|0\rangle$ with probability $|\alpha|^2$ or the state $|1\rangle$ with probability $|\beta|^2$. This can be visualized in a Block Sphere like the one presented in Figure II.30. While classical bits could only be at the "North" and "South" Poles in the locations of states $|0\rangle$ and $|1\rangle$, a *Qubit* can be at any point on the surface of the sphere.

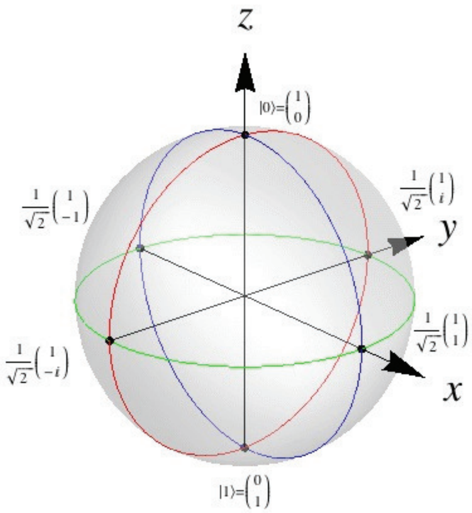

z
$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$
y
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$
x
$|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$

Figure II.30: Bloch Sphere.

A crucial difference from bits to Qubits is that any measurement of a bit yields the same result while for a Qubit, depending on the measure basis used the result can differ completely. A Qubit encoded in the polarization of photons, for example, in the state $|Q'\rangle$ defined in terms of the Vertical and Horizontal polarizations (Rectilinear Basis)

$$|Q'\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \tag{18}$$

exhibits 50% probability of being measured as $|H\rangle$ or $|V\rangle$. However, if this photon is measured in the Diagonal Basis, which corresponds to a rotation of 45 degrees of the photon's polarization, it yields the state $|45^o\rangle$ deterministically. The result follows the matrix representation of each measurement in a Hilbert Space of dimension two with all elements represented in the Rectilinear Basis.

$$\langle Q'|Rect|Q'\rangle = \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix} = \begin{pmatrix}1/2\\1/2\end{pmatrix} \tag{19}$$

$$\langle Q'|Diag|Q'\rangle = \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \tag{20}$$

(c) No-Cloning Theorem

If a state $|Q'\rangle$ is measured in the Rectilinear basis, the result should be the state $|H\rangle$ or $|V\rangle$ each with equal probability. Once measured, however, the quantum superposition state previously describing the Qubit is lost and no distinction can be made between a Projective, e.g. Equation 19, and a Deterministic, e.g. Equation 20, Measure.

The No-Cloning Theorem [43], [44] states that no non-orthogonal quantum system can be duplicated due to the intrinsic loss of information during measure. Take the normalised states $|H\rangle$ and $|45^o\rangle$, for instance, which are non-orthogonal, i.e., $\langle H|45^o\rangle \neq 0$, and a supposedly quantum cloning machine which operates as follows

$$|H\rangle\,|blanck\rangle\,|machine\rangle \rightarrow |H\rangle\,|H\rangle\,|machine_0\rangle \tag{21}$$

$$|45^o\rangle\,|blanck\rangle\,|machine\rangle \rightarrow |45^o\rangle\,|45^o\rangle\,|machine_1\rangle \tag{22}$$

where “blanck” is an initial state of a particle which, after the machine’s operation, becomes the clone. This operation must be unitary and should preserve the inner product, or

$$\langle H|45^o\rangle = \langle H|45^o\rangle\,\langle H|45^o\rangle\,\langle machine_0|machine_1\rangle \tag{23}$$

which is only possible when $\langle H|45^o\rangle = 0$ (the two states are orthogonal) or when $\langle H|45^o\rangle = 1$ (the two states are indistinguishable) [42].

Both conditions, however, lead to contradictions. The first one contradicts the very first assumption of non-orthogonality between the two states. The second renders this system useless for communication since, with indistinguishable states, no information can be transmitted. Making use of non-orthogonal (no-cloning) states and the unavoidable modification of the original quantum state after measurements, it is possible to devise Quantum Cryptography protocols that, instead of depending on computation hardness, base their security on the laws of physics.

(d) Entanglement, Bell’s Inequality and Bell States

Entanglement is a condition where a number of quantum systems share an intrinsic and very strong correlation. When a measurement is performed over one portion of an entangled state, information regarding the rest of the system is automatically gained independently of how separated are the elements.

Several sources of entangled photons are available based on Spontaneous

Parametric Down Conversion (SPDC) which create entanglement based on time, momentum or polarization. In the SPDC process, the nonlinear effects produced by the inelastic scatter of strong electromagnetic fields at frequency ω_p (pump photon) in crystal lattices are responsible for the spontaneous generation of photons at frequencies ω_1 and ω_2. Due to the conservation of energy, the relationship between these frequencies obey $\omega_1 + \omega_2 = \omega_p$ [42].

On Time Entanglement Sources, the entanglement relies on the fact that the two photons in a pair are created simultaneously and that the energy conservation rule is satisfied. On Momentum Entanglement Sources, the phase-matching conditions $\kappa_1 + \kappa_2 = \kappa_p$ inside the crystal lattice cause the two photon in a pair to be emitted in different directions. Finally, on Polarization Entanglement Sources, again the phase-matching conditions cause the two photons to be emitted with orthogonal polarizations, e.g, horizontal and vertical.

Equation 24 is the mathematical representation of a two-qubit polarization state such as one exiting a Polarization Entanglement Source based on SPDC.

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2 \right) \tag{24}$$

What this equation states is that the polarization on spatial mode 1 can either be H or V but, independently on the result, the polarization on spatial mode 2 will be the complement of the first.

The fact that entanglement is such a strong relation between quantum states capable of even disagreeing with Einstein's Theory of Relativity was one of the motivations for Einstein, Podoslky and Rosen to write the 1935 paper [45] in which they contest the completeness of Quantum Physics. In 1964, however, John Bell produced an article in which he states, through Bell's inequality, an inequality that demonstrates that some correlations predicted by quantum mechanics cannot be reproduced by any local theory, that Quantum Physics in a non-local theory.

Bell's inequality, later generalized to the Bell-CHSH Inequality due to Clauser, Horne, Shimony and Holt, draws classical limits for the correlations between the detections of two separated detection stations each at one end of a Entangled State Source such as depicted in Figure II.31.

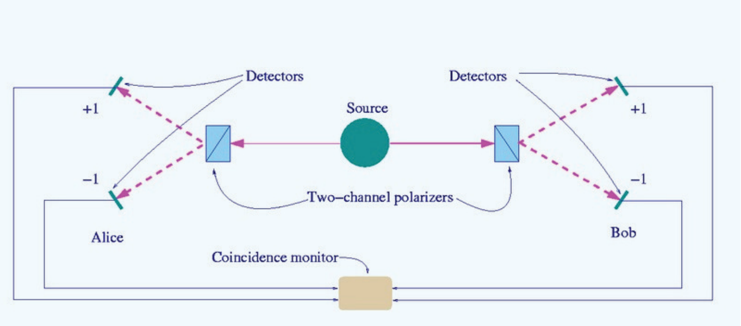


Figure II.31: Diagram of the Bell-CHSH Inequality Test Experiment Using Polarization Entanglement Sources.

Using a Polarization Entanglement Source as in Figure II.31 and Polarization Beam Splitters, both stations save and compare each result searching for coincidences which represent the degree of correlation between measurements. Even though Bell used the mathematical formalism of the Bell's Inequality on a fictitious experiment proposed by David Bohm [45] which was based on an entangled spin state called the *singlet state*, the same formulation can be developed using the polarization entangled *singlet state*.

Using a background such as the one depicted in Figure II.31, Bell proposed that quantum physics could be described by a local theory of "hidden variables" if the correlation between measurements of Alice and Bob was governed by the same classical parameter λ [45]. It is important to note that correlation is thought of in the quantum physicist's sense, i.e., the expected value of the product of the two binary outcomes (± 1) [45].

Taking the expectation of the measurement with respect to λ yields Equation 25 for the *singlet state*, which is the generalized Bell-CHSH Inequality. Symbols a, a', b and b' represent Alice's detection on detector 1 and 2 and Bob's detection on detector 1 and 2 respectively [45].

$$\rho\,(a,b) + \rho\,(a,b') + \rho\,(a',b) - \rho\,(a',b') \leq 2 \tag{25}$$

If the "hidden variables" model was correct, the result of this description should equal the quantum mechanical expectation. The inner product of the projection operators on each detector yields the expectation value and, due to the commuting of these operators, the result of Equation 26 is the violation of the Bell-CHSH Inequality, which confirms the hypothesis that Quantum Physics is not a local theory [45].

$$\langle a,b\rangle + \langle a',b\rangle + \langle a,b'\rangle - \langle a',b'\rangle = \frac{4}{\sqrt{2}} = 2\sqrt{2} \tag{26}$$

Entangled states disobey classical predictions of physical systems and, for that, are the center of the Quantum Theory's conundrum. Not all entangled states, however, exhibit maximal entanglement and the ones that give the upper bound of $2\sqrt{2}$ are maximally entangled states. Two-qubit states that yield this maximum correlation are known as the Bell States and are shown in Equations 27 and 28.

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1 \left|V\right\rangle_2 \pm \left|V\right\rangle_1 \left|H\right\rangle_2\right) \tag{27}$$

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1 \left|H\right\rangle_2 \pm \left|V\right\rangle_1 \left|V\right\rangle_2\right) \tag{28}$$

II.11 Quantum Key Distribution - The BB84 Protocol

The first protocol for Quantum Cryptography was proposed in 1984 by Charles H. Bennett, of IBM, and Gilles Brassard, of the University of Montreal, hence the name BB84 as this protocol is now known. The protocol involves four quantum states that constitute two bases of any two-level quantum system, e.g., photon polarization. The goal of the BB84 is to provide a means to exchange a common key between two parties that wish to communicate secretly. Based on the No-Cloning Theorem, the protocol offers a secure way to overcome the main issue in the "One-Time Pad" protocol, that of Key Distribution [42].

Usually, the Rectilinear and Diagonal bases are used due to the ease of usage and the availability of equipments. One particularity of these bases is that they are maximally conjugate, i.e., the projection of one of the vectors onto the other base yields the same result.

$$|\,\langle H|45^o\rangle\,|^2 = |\,\langle V|45^o\rangle\,|^2 = |\,\langle 45^o|H\rangle\,|^2 = |\,\langle -45^o|H\rangle\,|^2 = \frac{1}{2} \tag{29}$$

The binary 1 and 0 values are attributed to one vector of each base, such that $|H\rangle = |45^o\rangle = 0$ and $|V\rangle = |-45^o\rangle = 1$ for instance, in order to create a correspondence between the transmitted quantum state and the value of the common key of Alice and Bob [38].

Alice sends polarized photons to Bob chosen randomly among the four Rectilinear and Diagonal states. As long as both parties can keep a correspondence between the transmitted and received photons, the method of transmission (serial or parallel) is irrelevant. Bob measures each incoming photon in a randomly chosen basis so, for those chosen in the same basis as Alice, he gets a Deterministic Measure and, for the others, he gets Projective Measures.

At the end of transmission, Bob resorts to a public channel and, for each received Qubit, announces to Alice in which basis he performed the measurement so that Alice can reveal if the sent state was in a compatible basis. All Deterministic Measures are kept and all Projective Measures are discarded. The conjunction of both Alice's and Bob's random decisions produces the key, so neither parties can decide which key will result from the protocol.

The No-Cloning Theorem assures the security of the protocol when a third party Eve, which wishes to spy on the transmission between Alice and Bob, makes use of a simple attack. Eve measures the Qubits sent by Alice in one of the two possible bases like Bob would and resends another Qubit in the state corresponding to her measurement result. Eve will get the right basis in about half of the cases and the retransmission to Bob will be successful but in the other half of the cases, the states sent to Bob will be in an overlap of 1/2 with the correct states originally sent by Alice.

The intervention can be noticed in half of the cases where Bob and Alice got uncorrelated results. After removing the cases in which they used incompatible basis, there is still a 25% error rate (Quantum Bit Error Rate - QBER) when the resulting bit string is compared. For error assessment, Alice and Bob sacrifice some of the bits in their string and determine if the transmission was compromised. In order to best certify the security of the private key, a process called *Privacy Amplification* is further employed [38].

After the process is completed, and assuming that no eavesdropper were detected, Alice and Bob share a common binary key which can be used in order to communicate secretly using the "One-Time Pad" Protocol. All subsequent transmissions must be preceded by another Quantum Key Distribution since the binary key used in the "One-Time Pad" must only be used once.

(a) Attacks on the BB84

Several experimental imperfections impose difficulties to the use of the quantum channel, mainly the actual impossibility to fabricate a single photon source which is crucial for the BB84. If Alice eventually sends pulses of light with more than one photon, Eve can measure one of them and let the other travel directly to Bob. This way, she would have information on the key without introducing any QBER.

Although the implementation of the protocol has been successful even when taking such imperfections into account, attacks on the BB84's setup such as the Bright Illumination Attack [46], the Time-Shift Attack [47] and the Phase-Remapping Attack [48] were capable of disproving the complete security of the protocol. Attacks focused on the device's performance used in practice require either a new approach to the key distribution protocol or improvements on the device's physical structure.

The Time-Shift Attack

The Time-Shift Attack exploits the gated-mode of APDs. In this mode, the APD works as in the Geiger Mode with the difference that it is only triggered during a small time window, normally around a few nanoseconds. In this mode, even though the Dark Count rate is rather diminished since the amount of time in which the APD is polarized is small, the synchronization between two parties in a QKD system is critical [47].

Owing to the different responses of Bob's two APDs and other imperfections in electronics, the time-dependent efficiencies of these two SPDs are not identical. Because the width of the SPD's open window (a few ns) is often substantially larger or at least not shorter than the laser pulse duration (a few hundreds ps), Alice and Bob can synchronize the laser pulse with the center of the SPD's open window as depicted in Figure II.32 [47]. This ensures that the small detector efficiency mismatch will not affect the normal operation of the QKD system [47].

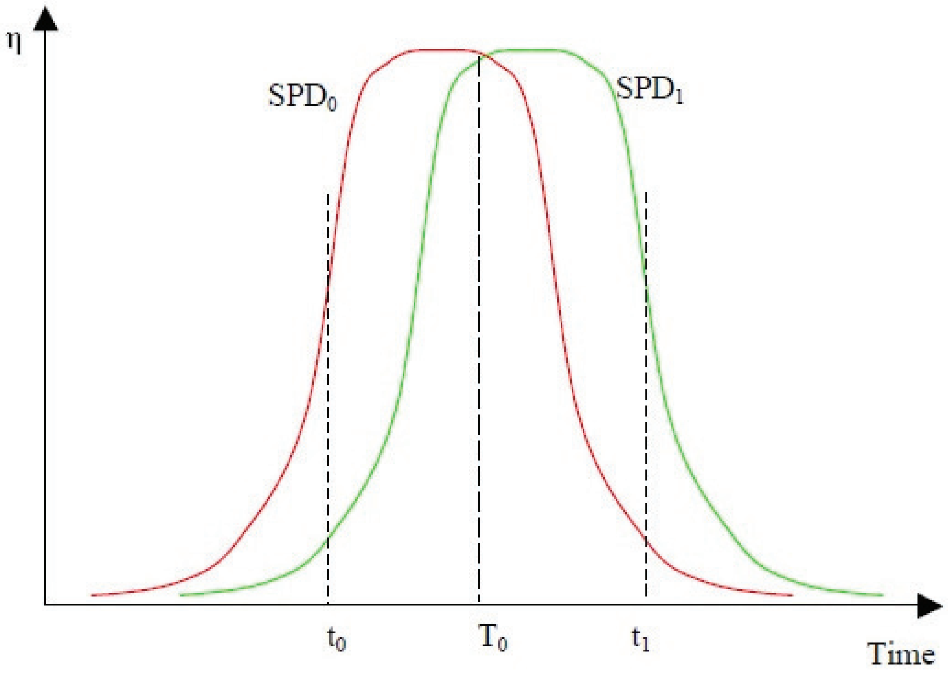


Figure II.32: The Time-Dependence Efficiencies of Bob's SPDs.

In order to exploit this time-dependent efficiency, the eavesdropper utilizes the "intercept-resend" attack described shortly as follows [47]:

- Eve intercepts the quantum states sent from Alice with the same detection scheme used by Bob, i.e., she performs measures in a randomly chosen basis.
- According to the measurement result, Eve prepares a new quantum state (a faked state) and sends it at different times so that it arrives at Bob's SPD at either time t_0 or t_1 depending on the result she intends to induce.

It is clear that the farthest in time the efficiencies, the more control Eve can have over Bob's detections. On the worst case, at time t_0 only detector SPD$_0$ is active and at time t_1 only detector SPD$_1$ is active so Eve has complete control over the results and full access to the key [47].

The Bright Illumination Attack

In 2010, Lydersen, Skaar and Makarov developed the Bright Illumination Attack which exploits the linear mode of APDs. The technique is based on the demonstrations that passively, actively and gated APDs can be induced to the linear operation mode by the use of blinding illumination [46].

Once the Photon Detectors are in the linear operation mode bright light pulses can be tailored in order to trigger the detectors of choice. Eve can, then, implement the “intercept-resend” attack and control Bob’s results, i.e., Eve measures the states from Alice using a copy of Bob’s measurement device to obtain a detection event. She then uses a faked state generator (FSG) to generate a bright pulse tailored to cause the same detection event in Bob. These attacks are specially designed against distributed-phase-reference (DPS) protocols [49] since Eve can use a phase modulator in order to choose which SPD will be triggered via the amplitude of light reaching each detector as depicted on Figure II.33 [46].

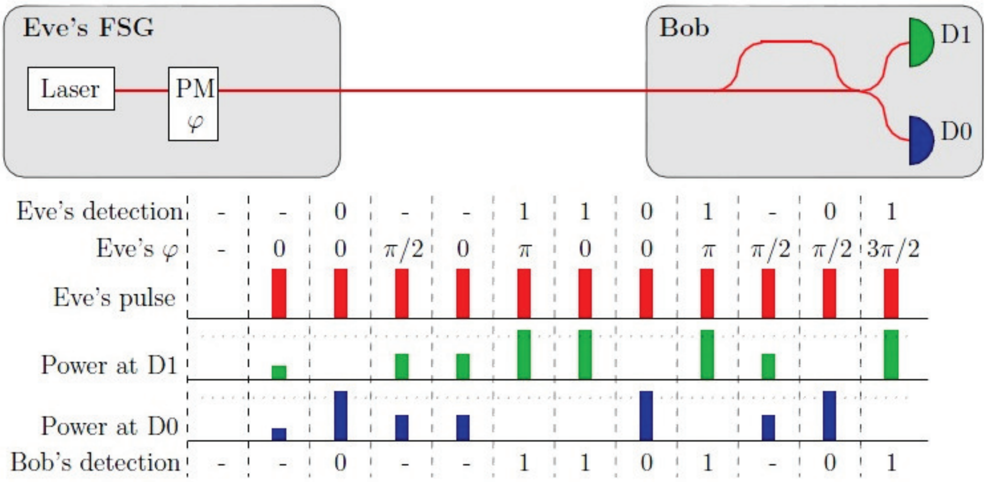

Eve’s FSG
Laser
PM
φ
Bob
D1
D0
Eve’s detection - - 0 - - 1 1 0 1 - 0 1
Eve’s φ - 0 0 $\pi/2$ 0 π 0 0 π $\pi/2$ $\pi/2$ $3\pi/2$
Eve’s pulse
Power at D1
Power at D0
Bob’s detection - - 0 - - 1 1 0 1 - 0 1

Figure II.33: Bright Illumination Attack: Detector Control in a DPS Implementation.

(b) Practical QKD Systems

Despite of its often praised unconditional security, quantum cryptography also relies on some assumptions. Some of them are quite natural, such as the validity of quantum mechanics, the existence of true random number generators, or to assume that the legitimate users are well shielded from the eavesdropper. Other assumptions are more severe, like considering that the honest parties have an accurate and complete description of their physical devices [50].

Obviously, if the functioning of the real setup differs from that considered in the mathematical model, this may become completely vulnerable to new types of attacks not covered by the security proof [50]. Two practical setups that aim at overcoming the real characteristics of QKD mathematical models are presented below, namely the Device Independent and the Measurement-Device Independent QKD.

Device Independent QKD

The Device Independent protocol is a modification of the EPR Protocol proposed by Ekert in 1991 [51]. The idea is to use an entangled qubit source between Alice and Bob so the results in the detectors are correlated and in violation of the Bell-CHSH Inequality. It then becomes possible to identify any local disturbance during transmission. Even though the protocol is proved to be secure [52], it also introduces a problem known as the Detection Loophole.

Curty and Moroder presented a setup in order to bypass the Detection Loophole which can be exploited to attack the system. Because the efficiency of detection in SPDs is not perfect (i.e., $\eta \leq 100\%$), the violation of the Bell-CHSH Inequality is modified to the following expression where the only valid detections are the ones that yield coincidences:

$$E\left(\langle a,b\rangle\left|C\right)+E\left(\langle a',b\rangle\left|C\right)+E\left(\langle a,b'\rangle\left|C\right)-E\left(\langle a',b'\rangle\left|C\right)=\frac{4}{\eta}-2 \qquad (30)$$

This way, depending on the detector's efficiency, no violation occurs and, ultimately, Alice and Bob would not be able to differ from an attack and the loophole's effect over the final QBER of the QKD transmission.

The EPR Protocol and the Measurement-Device Independent QKD

Curty, Qi and Lo [53] proposed, in 2012, a new setup of the QKD, namely the Measurement-Device Independent (MDI) QKD, in which physical imperfections of any measurement device inherent to the practical implementation, such as Photodetectors, are ignored. The physics behind this protocol relies on the “bunching” (Hang-Ou-Mandel Effect) of two indistinguishable photons at a 50:50 Beam Splitter [53].

The protocol is based on an idea from Artur Ekert which, in 1991 [51], proposed an EPR-based(or entanglement based) Quantum Cryptography Protocol. Differently from the BB84, in this proposition a common source between Alice and Bob emits maximally entangled qubits. After Alice and Bob perform measurements, the source announces the bases used and they keep the data only when they happen to have made their measurements in the compatible basis [38], [51].

The EPR Protocol for Quantum Cryptography relies on Bell’s Inequality to assure the security of the channel since no local physical operation can reproduce the correlations that arise from the use of maximally entangled Bell States [38]. Once Alice and Bob are confident that the source emits such states (which can be done by the use of an extra basis apart from the Rectilinear and Diagonal bases), any intervention created by Eve is a local perturbation and modifies the result’s correlations which can be detected.

If Alice and Bob got Qubits on their own and wished to determine what original Bell State sent by the source produced such Qubits they could perform a Bell State Projection, the result of the detection of previously uncorrelated quantum states into one of the four maximally entangled Bell States [54]. This is the idea behind the Measurement-Device Independent Protocol, a time-reversed version of Ekert’s EPR Protocol in which Alice and Bob create Qubits and send to a central Bell State Analysis Station.

The method makes use of weak coherent pulses (WCPs) which has been shown [53], [55] to exhibit Hang-Ou-Mandel interference at the Beam Splitter of a Bell State Analysis Station [56]. Using the linear optics based structure of Figure II.34, it is possible to make use of the interference of Alice’s and Bob’s photons to generate different detection patterns and associate each to a different Bell State.

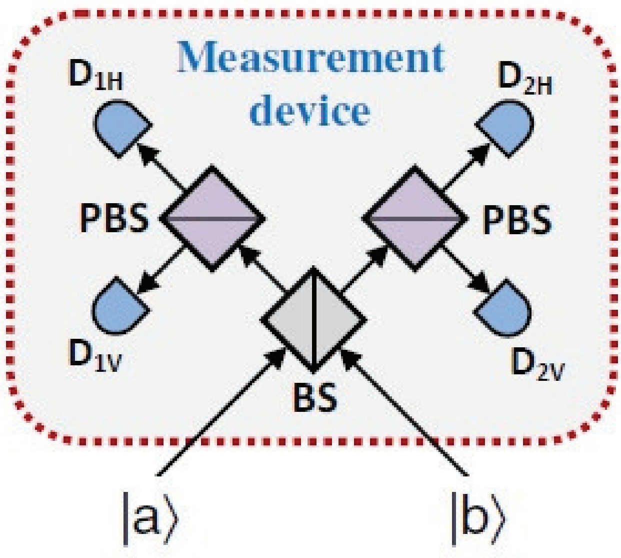


Figure II.34: Linear Optics Based Bell State Projection Structure.

A simple example of the method is as follows. Both Alice and Bob prepare WCPs in the four possible BB84 polarization states and send them to an untrusted relay Charlie (or Eve) located in the middle, who performs a Bell state measurement. Furthermore, Alice and Bob apply decoy state techniques [57] to estimate the gain (i.e., the probability that the relay outputs a successful result) and quantum bit error rate (QBER) for various input photon numbers [53].

Once the quantum communication phase is completed, Charlie uses a public channel to announce the results. Moreover, as in BB84, Alice and Bob post-select the events where they use the same basis in their transmission.

III
Experiments

III.1 Automatic Photon-Counting OTDR Using FPGA and Digital Signal Processing for Fault Position Estimation

In this section a methodology is proposed that aims to ally the high sensitivity of ν-OTDR's with higher data harvesting rates using an integrated system based on Software Defined Hardware. This implementation takes into account the parallel processing advantages and flexibility of Field Programmable Gate Arrays (FPGAs), so a single board is employed capable of managing multiple devices at high speed while gathering detection information from a Single Photon Detector.

In order to overcome the low detection rate at long distances, a feedback system with a Variable Optical Attenuator (VOA) enables the zooming over a designated portion of the fiber, which translates into faster inspection of statistically relevant data.

Furthermore, the possibility of selecting the portion of the fiber to be monitored allied with an attenuation control capable of keeping a high detection rate is a relevant tool that can be applied in many different areas, such as centralized monitoring of Passive Optical Networks (PONs). In such links, the maximum supervision reach is hindered due to the losses in splitters with high split ratio [58]. Being able to divide the fiber into two or more zones (e.g., before and after the splitters) overcomes this limitation.

(a) A-PC-OTDR Experimental Setup

In Figure III.1, the block diagram that represents the implemented system is depicted. The FPGA board accesses the Semiconductor Optical Amplifier (SOA) Driver and the Single Photon Detector while it buffers each backscattered detection in an on-board RAM structure. The saved data is transmitted through an USB cable to a computer interface capable of communicating with the VOA. The attenuation is set based on the results of Digital Signal Processing from a $\ell 1$ Trend Filter [59] implementation over the received data.

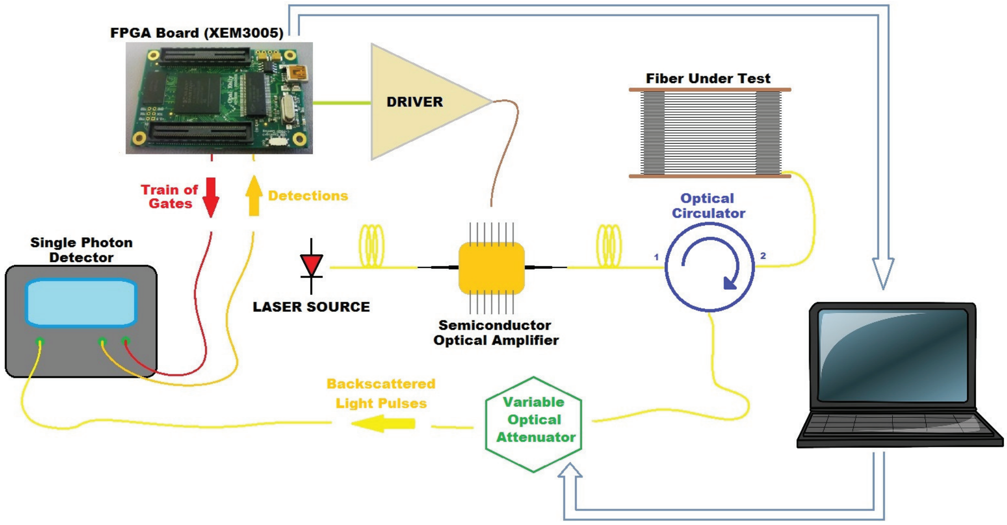


Figure III.1: Block Diagram of the Experimental Setup.

After the first batch of data is processed, the $\ell 1$ Trend Filter detects break points which can be associated with losses. The FPGA performs a “zoom” over the area near the break points while the Optical Attenuator is set so the detection rate is optimal in order to best estimate the fault’s position. After each break point is thoroughly examined, the entire fiber is once again inspected and a full result can be presented.

(b) Photon Counting OTDR and FPGA

The OTDR technique consists of sending a light pulse into an optical fiber and measuring the Rayleigh Backscattered light. Although classical OTDR has been successful, ν-OTDR, which employs an SPD as the detection apparatus, presents a number of advantages such as better sensitivity and the absence of Dead Zones [36], [21].

A main issue in ν-OTDR measurements is the time necessary for one light pulse to exit the fiber before the next pulse can be sent, which substantially increases the monitoring period. An approach already discussed in [21] is to use a train of gates in the SPD to maximize the number of detections per pulse. As the gating period corresponds to the SPD’s Dead Time, for a single pulse traversing the fiber, the system is capable of checking whether there was a reflection or not on positions determined by the Dead Time. A time shift for each new pulse guarantees that the whole fiber is analyzed.

The FPGA board is responsible for managing the train of gates and the delays between pulses as well as enabling the light pulses through the (SOA) Driver which works as a light switch. In order to optimize the memory usage, which is limited by the board's configuration, only detection events are stored so, for each new detection, a 16 bit word is created by the composition of the gate number and the delay number. This way, every new event can be instantly stored by the board without loss of information regarding the position of the fiber which generated the event. Figure III.2 illustrates this process.

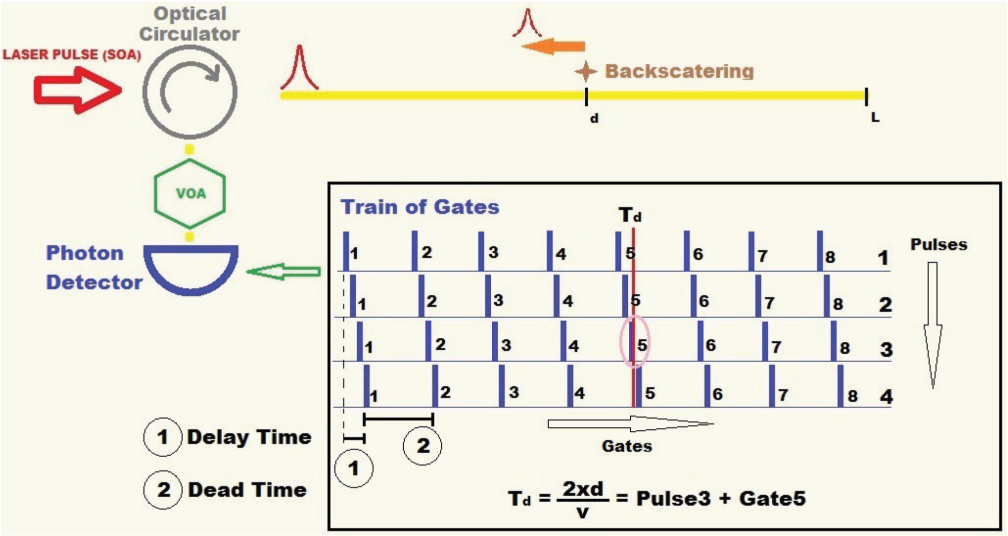


Figure III.2: Detection Storage Scheme.

Although not as fast as an Application Specific Integrated Circuit (ASIC), an FPGA's flexibility, the possibility of modifying the Hardware according to the application's necessities and an accessible simulation software make it a powerful and reliable tool for this project [60]. Also, the simulation software offers an easy platform to implement the design as well as an easy method for checking timing inconsistencies.

(c) Semiconductor Optical Amplifier and Driver

The setup proposed by [61], with a Semiconductor Optical Amplifier and an electronic Driver, fits perfectly into the design of FPGA integrated ν-OTDRs not only because of its high extinction ratio but also because of the capability of digitally triggering a light pulse. The FPGA controls the Driver via a TTL input so no further adaptation is necessary.

Still according to [61], a Laser source in Continuous Wave (CW) operation is connected to the SOA which operates as an optical switch. Figure III.3 depicts the output signal characteristics when the SOA is active and inactive in which the CW Laser power spectrum serves as reference. In the operational wavelength of 1550 nm, the Peak Pulse Power is 23 dBm with 78 dB extinction ratio. This characterizes a good application of the SOA as a switch but, although the advantages of this characteristic are a breakthrough in terms of extinction ratio, its use hinders the spatial resolution. A maximal spatial resolution of 6 meters is achieved when setting the Driver's pulse width to its minimum of 60 ns.

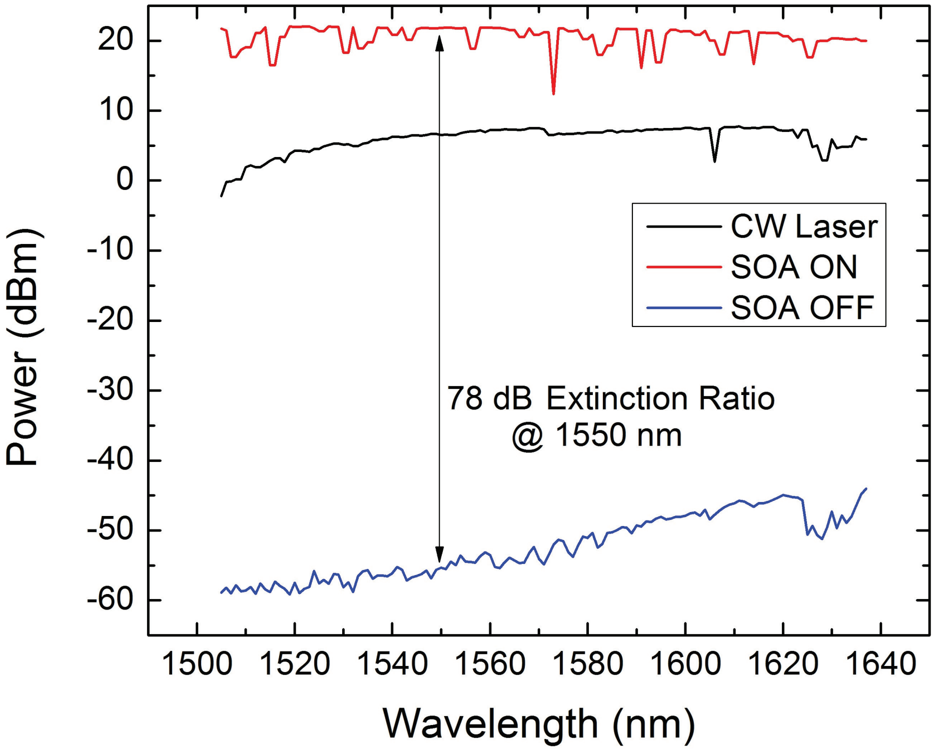


Figure III.3: SOA Characteristics for Different Wavelengths.

(d) Saturation and Timing Analysis

Saturation is a phenomenon often regarded as a system reaching its maximum capacity. On a ν-OTDR background, this happens when the system is incapable of differentiating whether a portion of the fiber has higher reflectivity than the other. Since a single photon pulse is capable of triggering a detection in an SPD, this is the case when a light pulse has a high probability of containing more than one photon. The control of the number of photons and, thus, of the power level in the reception, is therefore necessary for a linear operation.

Individual photon detections can be treated as independent events that follow a random temporal distribution. As a result, photon counting is a classic Poisson process, and n, the number of photons detected by an SPD, is described by the discrete probability distribution of Equation (1) where λ is the expected number of photons per detection, which is proportional to the incident optical power [62].

$$P(n = k) = \frac{e^{-\lambda}(\lambda)^k}{k!} \tag{1}$$

In order to stipulate the reception's power level so the system can operate linearly, it is common to set λ such that Inequality (2) is satisfied.

$$P(n = 1) \gg \sum_{j=2}^{\infty} P(n = j) \tag{2}$$

In other words, the probability of having a light pulse with one photon in the reception must be much greater than the probability of having light pulses with more than one photon. Considering "much greater" as at least one order of magnitude greater, i.e, a 10% relation between these two probabilities, we can write Inequality (3) as follows.

$$\lambda e^{-\lambda} > 10\left(1 - e^{-\lambda} - \lambda e^{-\lambda}\right) \tag{3}$$

The values of λ that solve this inequality are in the range $0 < \lambda < 0.18$ as seen in Figure III.4 a) which depicts the linear operation region in terms of the mean number of photons per pulse. In order to decrease the detection period, λ can be raised at the cost of non-linear operation. In Figure III.4 b), the number of photons and number of detections per pulse in the pulse reflected at the first position of the fiber as a function of the VOA's attenuation level is depicted. Linear operation region is annotated at approximately 19 dB.

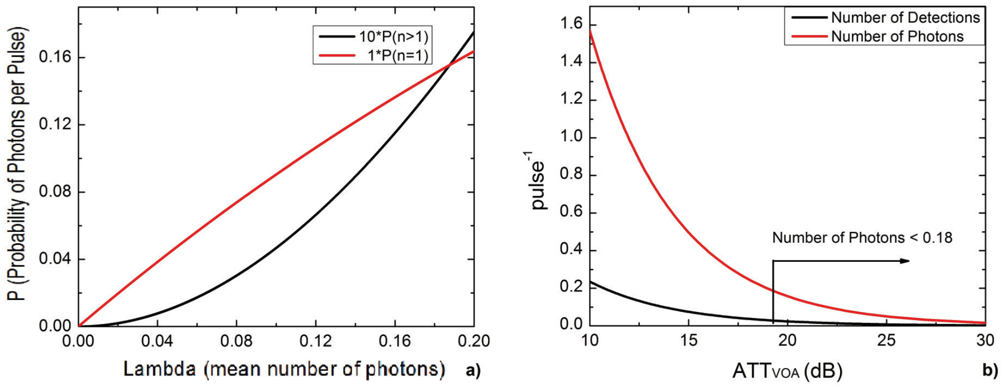


Figure III.4: Number of Photons per Pulse and Number of Detections.

The number of photons arriving at the SPD (N_D) can be estimated using the information of the peak pulse power at the fiber's input as a function of the reception attenuation which is controlled by a VOA.

$$N_D = \eta N_{ph} = \eta \frac{P_{in} W_{gate}}{h\nu} \tag{4}$$

Where η is the detector's efficiency, W_{gate} is the Gate Width and P_{in} is the Rayleigh Backscatter input power at the SPD which, for a 4 ns Gate Width and according to [63], is 76 dB below the 23 dBm of P_{peak} shown in Figure III.3. Connector and insertion losses sum up to 9 dB in the present experimental setup regardless of the VOA's attenuation. Figure III.4-b exhibits the required VOA's attenuation for near region analysis.

Distant positions of the fiber can be analyzed without extended periods of detection when the power loss along the fiber is reimbursed by the control of the VOA's attenuation. As seen in Equation (13), the optical signal along the fiber decays exponentially so P_{in} is replaced by $P_{in}(L)$ in Equation (4) when a different portion of the fiber is analyzed. Also, the FPGA unit is programmed so that triggers associated with nearer positions are disregarded in order to protect the SPD from the elevated optical input power when using the zoom functionality. This guarantees that the power level at the input of the photodetector remains the same even when distant positions are accessed. The result is that the total amount of time per measure does not decrease due to lower optical power since the VOA counterbalances the fiber's attenuation effect.

Using equations (4), (13) and inequality (3) it is possible to automatically calculate the attenuation levels for new measurements taking into account the previous losses due to splitters and connectors, such as the ones depicted in Fig. III.5 and update the VOA with these new values. Even though the operation regime may be pushed towards saturation as a means to lessen the detection period, this method is used only in order to diminish statistical inaccuracies and best estimate Break Points locations during the zoom functionality.

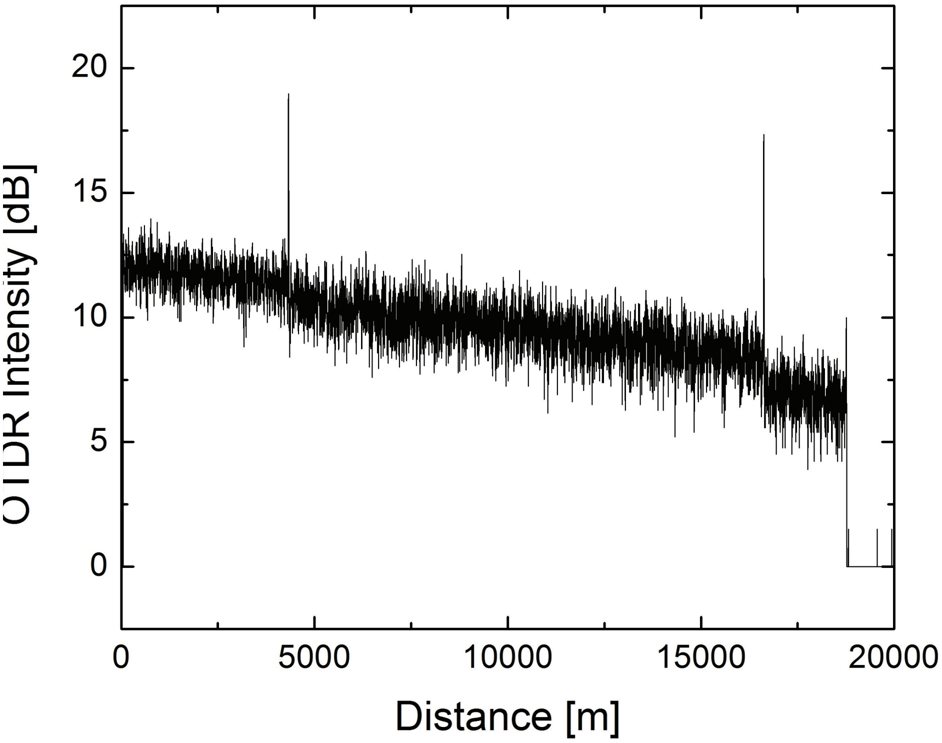


Figure III.5: Typical trace result of the described Setup for one minute long inspection of a 20 km composition of fibers.

It is interesting to note that the 10% relation, i.e, the threshold of one order of magnitude between probabilities for 1 or more photons per pulse - characterized by 3 - , yields a 0.4 dB saturation at the photon launching point. Results from [64] consider a 2% relation which yields a 0.1 dB saturation. Since the monitoring position and the VOA's attenuation are set automatically, the linear operation is assured at the break point locations even with the proposed level of saturation.

Another result from [64] is regarding the maximum Dynamic Range for fixed power Photon Counting OTDR schemes which is that of 17 dB. Naturally, controlling the VOA's attenuation, the fiber can be sectioned and further distances can be achieved through the zoom functionality. Given that the total attenuation necessary for linear operation at the beginning of the fiber is around 18 dB, the total Dynamic Range achieved by this scheme is of 35 dB, an unparalleled result given that, in this case, tunability of the PC-OTDR scheme is considered [64].

(e) Number of Detections and RAM Capacity

In order to estimate the average number of detections needed in relevant data analysis and also the timing associated with such a measure, a brief study on the detection apparatus is proposed. Given a 20 km fiber, 20 ns detection windows and a 500 ns dead time for the detector, the following data can be extracted:

- Time Between Optical Pulses: $\frac{20[km]\cdot 2}{2\cdot 10^8[m/s]} = 0.2[ms]$
- Number of Gates per Optical Pulse: $\frac{0.2[ms]}{500[ns]} = 400$

Assuming that the power level at the insertion point is calculated so the number of photons per pulse does not exceed 0.18, the number of detections per pulse can be calculated using the detector's efficiency of 15%. This yields 0.027 detections per pulse at the insertion point.

Given that two gates are separated in time by 500 nanoseconds, the corresponding spatial separation is that of 100 meters. The overall fiber's attenuation is known to be 0.2 $[dB/km]$ which, for 100 meters, corresponds to a 0.02 dB attenuation. This yields the following equation for determining the number of detections within an optical pulse, in which it was assumed that the average number of detections per pulse does not vary widely from one optical pulse to the other, even with the 20 nanoseconds delay between each.

$$0.002 = 10 \cdot \log_{10} X \rightarrow X \cong 1.004 \tag{5}$$

$$N_D = 0.027 + \sum_{i=1}^{399} \frac{0.027}{(1.004)^i} \cong 5 \tag{6}$$

Considering a total of 5000 optical pulses per second, given that the spacing between optical pulses is 0.2 milliseconds, the average number of detections per second is approximately 25000. For a 28K Bytes RAM as is supported by the XEM3005 FPGA [7], it means that, considering the data storing process described before - *subsection b* - , on average for this setup, the board's memory is filled in approximately 1.1 seconds.

In the above table, similar calculations for different fiber lengths are showed in order to best evaluate the setup's performance.

The increasing measurement time as a function of the monitored fiber length is one of the motivations of using the zoom function in order to achieve better timing for longer distances. Also, the limitation of the 17 dB Dynamic Range imposed by the Photon-Counting technique [64] renders the monitoring of any fiber with more than 85 km impossible, which is another motivation for the zoom function.

Table III.1: Detection Time

Fiber Length (meters)	Detection Period (seconds)
1000	0.54
2000	0.56
5000	0.64
10000	0.79
20000	1.13
40000	1.95
80000	3.81
100000	4.76
200000	9.52

Detection Period and Number of Samples for Fault Analysis

In order to determine the average number of samples which yields a statistically relevant measurement and enables fault detection and analysis, a 10 dB SNR is considered for the last measuring position. It is known that the noise component for Photon-Counting measures is a function of the number of samples, and grows with the square root of detections.

A 10 dB SNR, therefore, is achieved when approximately 100 samples are gathered. This result comes from the fact that, in a Poisson process, the number of observed ocurrences fluctuates about its *mean* with a *standard deviation* $\sigma = \sqrt{\lambda}$, often called Poisson Noise. For 100 samples, the corresponding Poisson Noise would be 10 and, in turn, the SNR would be 10dB. The average number of detections per optical pulse at the last position can be calculated as the last component of the sum in Equation 6, i.e.

$$N_D^{400} = \frac{0.027}{(1.004)^{399}} = 0.0043 \tag{7}$$

The number of filled RAMs (N_Rams) necessary for yielding a 10 dB SNR for the last position is, then, calculated as follows, where 5000 optical pulses per second are considered:

$$N_{Rams} = \frac{100}{5000 \cdot 0.0043} \cong 5 \tag{8}$$

Considering the time that takes for the FPGA board to unload the RAM's contents to the computer as, on average, equal to 1 second (measured), this yields a total monitoring time of approximately 11 seconds. These results can be added to Table III.1, generating Table III.2.

The results from Table III.2 indicate clearly that not only the Dynamic

Table III.2: Timing Characteristics

Length (meters)	Full RAM Timing	10 dB SNR (Full RAMs)	Total Timing
1000	0.54	1	1.54
2000	0.56	1	1.56
5000	0.64	1	1.64
10000	0.79	1	1.79
20000	1.13	5	10.66
40000	1.95	59	174.34
80000	3.81	4675	22500
100000	4.76	36867	–
200000	9.52	–	–

Range limitation of Photon-Counting measures imposes a limitation on the monitored distance, but also the timing needed for statistically relevant sampling.

Although the results from Table III.2 state the minimum sampling rate, it is often advantageous to gather more data in order to better locate and analyze faults. A 13 dB SNR, for instance, is achieved, for a 20 km fiber, for approximately 400 samples, which yields a Total Timing of 40 seconds. These results are carried out in the protocol as will be seen later, i.e., all the measurements are based on 13 dB SNR 20 km fibers.

(f) l1 Level Filter

Given a typical fiber profile such as the one presented in Figure III.5 one can treat the data as a composition of three elements: Linear Trend, Level Shifts and Statistical Noise. While the Linear Trend reflects the fiber's power attenuation along the fiber, the Level Shifts indicate the presence of faults such as splitters, connectors or fiber defects. In order to determine the position of Level Shifts and the power loss associated with each, a signal processing technique called the $\ell 1$ Level Filter is applied.

Mathematical programming has been widely used in signal processing and time series analysis to filter signals and remove its trends and seasonality. The ν-OTDR data series is extremely similar to time series, though indexed by spatial position instead of time. In [59] it is proposed the $\ell 1$ Trend Filter, designed to obtain piecewise linear trends of time series. Formulation of the $\ell 1$ Trend Filter follows

$$\min_{w_i,x_i} \sum_{1}^{N} (y_i - x_i - w_i)^2 + \rho \sum_{2}^{N} |w_i - w_{i-1}| + \lambda \sum_{2}^{N-1} |x_{i-1} - 2x_i + x_{i+1}| \tag{9}$$

where y_i are counts from the original series, x_i are points from the linear trend component, w_i are points from the level shit component and λ and ρ are real numbers that control the frequencies of the linear trend and level shift respectively.

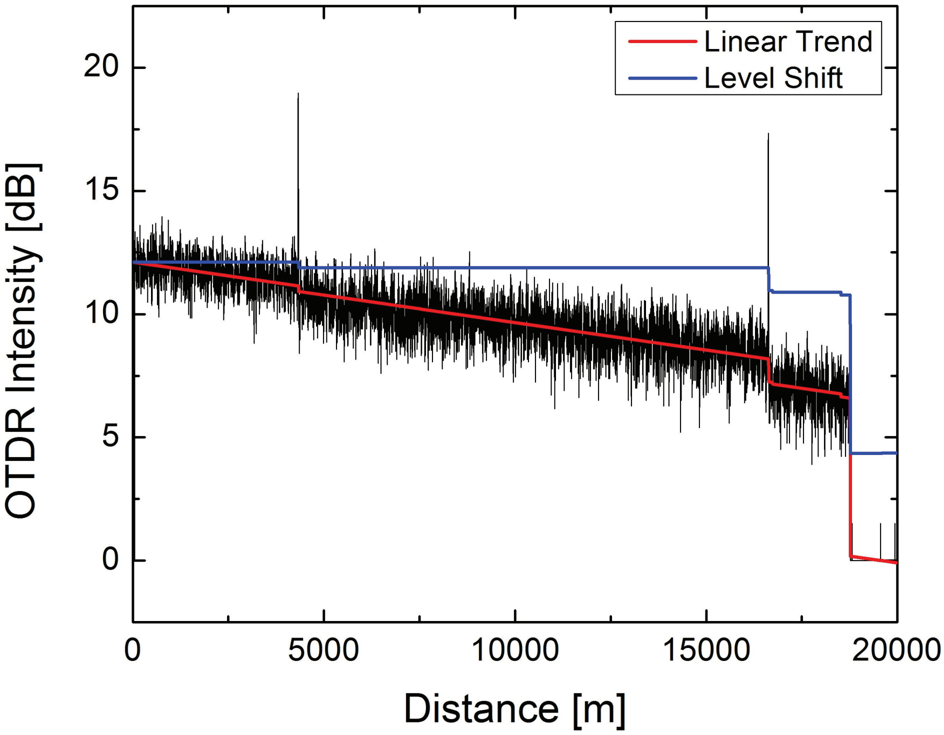


Figure III.6: Gurobi Optimizer Results Running the $\ell 1$ Level Filter.

The goal is to design a linear program capable of capturing the data's Level Shifts that represent Break Points as shown in Figure III.6. In the graphic depicted, two faults localized at approximately 3.9 and 16 km should be detected by the program. The red component is the OTDR Intensity curve fitting and the Level Shift component is in blue. The following model, where the piecewise linear component is substituted by a simple linear component, is proposed

$$\min_{w_i,a} \sum_{1}^{N} (y_i + az_i - w_i)^2 + \rho \sum_{2}^{N} |w_i - w_{i-1}| \tag{10}$$

This modification halves the number of variables, consequently reducing the computational cost of solving the program. Aiming at faster processing time, the quadratic term is substituted by the absolute value in Eq.(10), also yielding less computational effort.

$$\min_{w_i,a} \sum_{1}^{N} |y_i + az_i - w_i| + \rho \sum_{2}^{N} |w_i - w_{i-1}| \tag{11}$$

When solved to optimality, this program minimizes the random error in the L^1 norm taking into account a penalization for Level Shifts. Different methods implemented in the linear program solver Gurobi Optimizer [65] are compared in terms of running time. Depending on the number of samples, the program is solved via the Simplex or Barrier Methods [66] as seen in Table III.3.

Table III.3: Processing Time (seconds)

Number of Samples	Barrier Method	Presolve and Simplex	Primal Simplex
40000	6.59737	7.0404	56.73624
1000	0.053	0.061	0.034
100	0.01	0.009	0.002

In solving the proposed model, Break Points locations, as well as power loss, are retrieved via the Level Shift (related to steps) component. Statistical imprecision should be soften by the zoom tool.

(g) A-PC-OTDR Experimental Results

The following images depicted in Figure III.7 show the steps taken by the program while inspecting the fiber. In this case, two faults were detected and both positions and power losses were estimated. The monitoring period of the ν-OTDR/FPGA is 3 minutes for a 20km fiber, a result that is four times faster than what was achieved in [36] even though the spatial resolution is poorer.

In Figure III.7 a), the initial measurement of the fiber is depicted. The optimizer software detects potential Break Points at approximately 4, 16 and 20 km. In b) is the analysis of the first Break Point at $\sim$ 4 km. It becomes clear that the software was to detect the fault in the Step Trend. The Break Point is confirmed and stored. In c) is the analysis of the second Break Point at $\sim$ 16 km. It is noticeable that two steps were detected which are processed in order to determine the fault's position. In d) is the analysis of the third Break Point at $\sim$ 20 km. The software detects the end of the fiber and enables the final measurement.

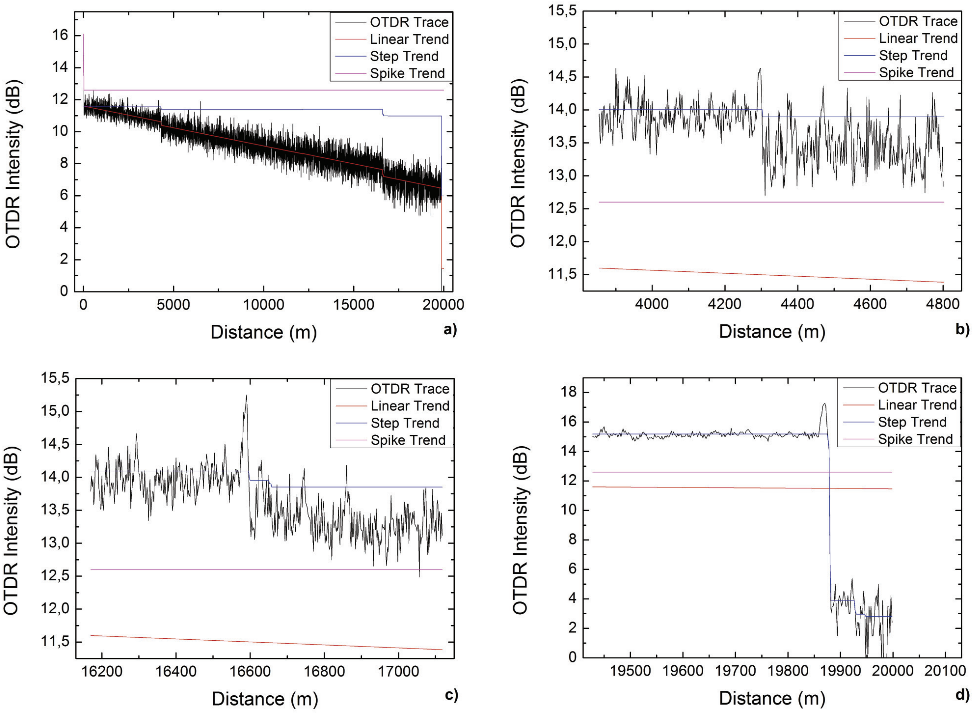


Figure III.7: Steps of Fiber Measurement.

By combining the information returned by the Step Trend, the software is able to successfully detect Break Points caused by connectors or fiber defects, while maintaining precision and fast measurement times due to the zoom functionality, allowing the presentation of a full profile with the exact location of losses (up to the spatial resolution of 6m). Once all Break Points are determined, the software runs one last profile and presents all faults positions.

In order to determine how close to the actual fault position this technique has gotten, classical OTDR traces were computed for the same fibers used in the example. As it has already been discussed, the fiber profile measured in this case study was created connecting three different fibers, so the fiber faults should appear in positions relative to the length of each of the fibers. In Figure III.8, the classic OTDR traces with the respective lengths (3.351, 4.463 and 12.560 km respectively) is shown.

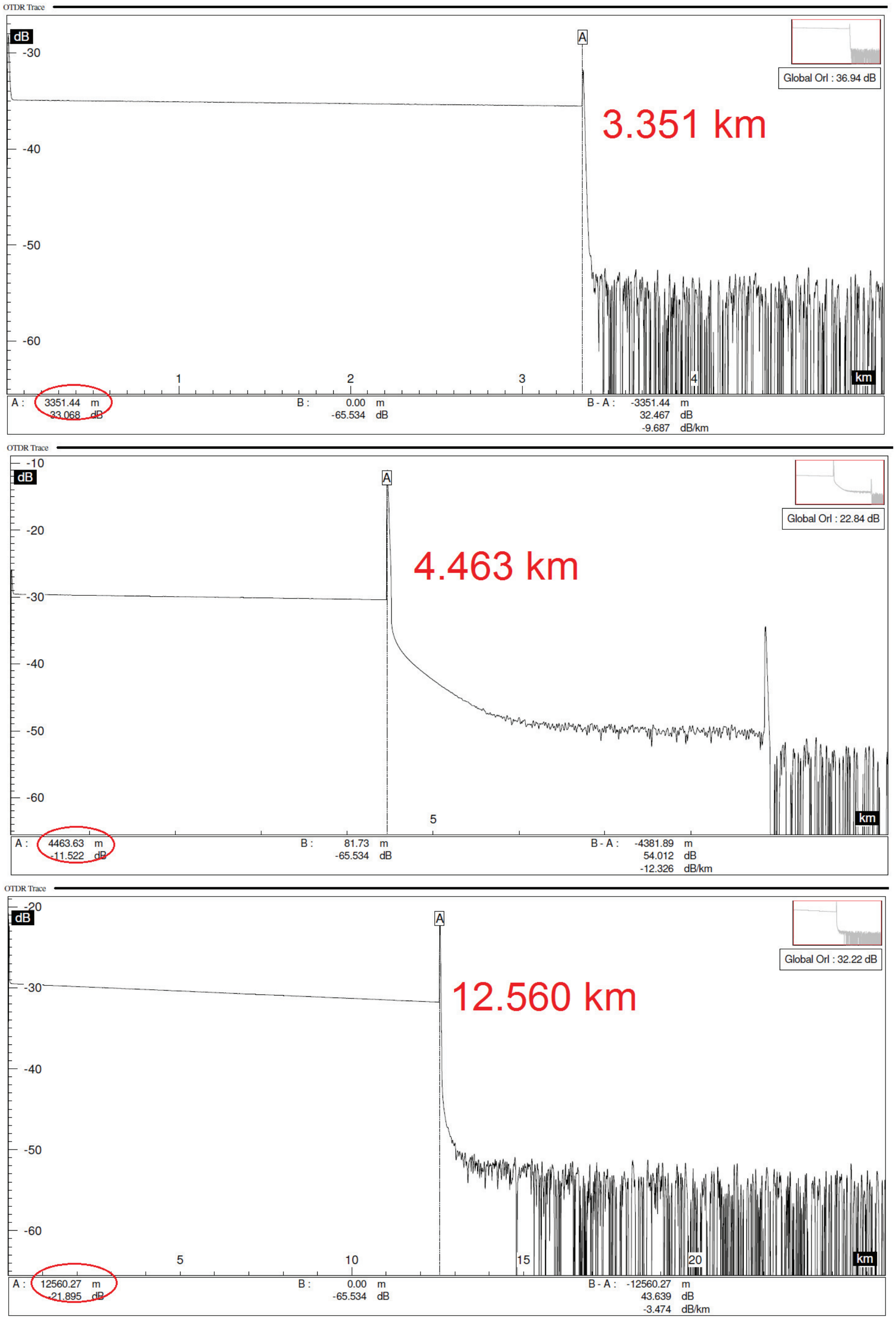


Figure III.8: A-PC-OTDR reference traces.

In the complete profile, the expected results for break points would be 4.463, 17.023 and 20.362 kilometers respectively. The results found by the software after the steps presented in Figure III.7 were . Even though at first sight these results exceed the spatial resolution commented previously (6 meters), a factor has to be considered which is the refraction index taken into account by each procedure. The classical OTDR instrument uses $n = 1.4682$ as a default value for the refractive index while the program developed to work in the A-PC-OTDR uses $n = 1.5$. The normalization is easily done, however, as seen in the following development:

$$d = v \cdot t = \frac{c}{n_1} \cdot t = \frac{c}{n_1} \cdot \frac{n_1}{n_2} \cdot t = d \cdot \frac{n_1}{n_2} \tag{12}$$

where n_1 is the A-PC-OTDR value of 1.5 and n_2 is the OTDR default value of 1.4682 so

$$d_{norm} = d \cdot \frac{1.5}{1.4682} = d \cdot 1.021 \tag{13}$$

Table III.4 lists and compares the results of the employed technique and the well-established classical OTDR.

Table III.4: A-PC-OTDR Results against Reference Traces

A-PC-OTDR Results [km]	Normalized Results [km]	Classical OTDR Results [km]	Discrepancy [m]	Status
4.330	4.420	4.463	43	Outside Tolerance
12.294	12.552	12.560	8	Inside Tolerance
3.280	3.348	3.351	3	Inside Tolerance

The high discrepancy found for the first fiber can be attributed to some Dead Zone effects due to the measurement apparatus which has not been taken into account. Since the fiber lengths are being calculated based on the first break - the first fiber length -, the discrepancy which would be taken for the whole fiber appears as an effect of the first.

Even though timing characteristics of the proposed experimental setup are in accordance with other ν-OTDR systems, the choice of using a SOA driver for pulse generation harshly limits the spatial resolution. The SOA itself is capable of producing very narrow pulses of up to 1 nanosecond width [67] but, the limitation of both the driver's electronics (60 nanoseconds) and of the board's clock frequency (50 MHz) lead to a maximal spatial resolution of 6 meters for this particular setup. The actual setup has a 6 meters resolution, but commercially available FPGAs and driver electronics would be able to reach at least 50 centimetres based on the SOA's limitations.

(h) FPGA Implementation

The hardware design is a crucial step on the experiment and, in this setup, three main structures can be defined: Input Structure, Output Structure and Signal Managing Structure. Following the sketch presented on Figure III.9, these three structures can be identified by different arrow colors - purple, blue and green respectively. The Front Panel Application Programming Interface [68] which is embedded in OpalKelly's XEM3005 board offers an easy communication channel between the computer and the FPGA, so both Input and Output Structures communicate to the computer interface through an USB cable. The schematic is also presented in Figure III.9[1].

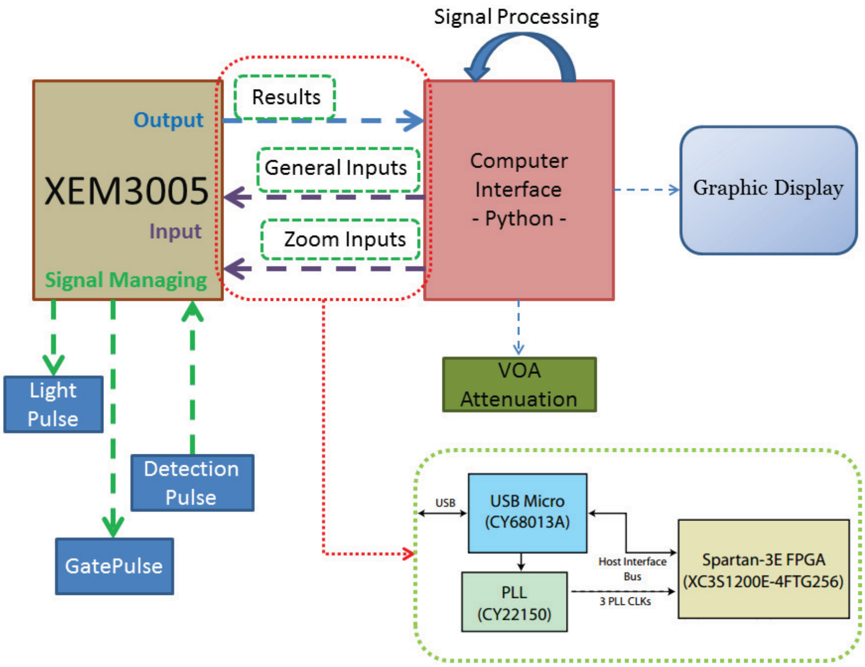


Figure III.9: Sketch of the FPGA design highlighting the three main structures.

The role of the Python Interface is to, after passing all the inputs needed for the protocol - which are user defined -, wait until the board signals a transmission. This, as has been described in previous sections, happens when the board's memory reaches its maximum capacity. While data is being transferred, all processes of detection and triggering are halted.

The internal structure of the hardware consists of a number of counters, each corresponding to a specific delay. After the threshold of a counter is reached, a control unit enables the following counter. This way, the number of

[1] Image taken from the actual document [68] and later edited.

gates and delays is controlled and, in the case of a detection, the outputs of the counters are directed to the memory and the information is stored.

(i) A-PC-OTDR Conclusions

An integrated fault analysis system is proposed in this experiment. Making use of variable optical attenuation and digital processing tools as well as an FPGA unit capable of communicating with the SPD, the SOA and a PC, the system is intended to function automatically and. Through the use of attenuation control, it can show considerable gain in timing during relevant data acquisition, i.e., information regarding faults is the fiber.

The system is capable of automatically detecting faults as small as 0.1 dB with a spatial resolution limited by the electronic driver. Zoom over different portions of the fiber associated with an attenuation control permits faster and more flexible fiber characterization.

A point that has already been discussed is that the time taken by the communication protocol to send information from the board to the computer and vice-versa is the timing bottleneck of the procedure. In this sense, a interesting approach to the problem would be to implement the signal processing tools of the $\ell 1$ filter inside the board. Apart from the timing boost gained by this approach, the fact that the board would be even more independent from the computer is an important step in the direction of creating a commercially available instrument based on the technique here presented.

III.2 FPGA Based Bell State Projection Analysis Station

In this section a simple Software Defined Hardware implementation is described that aims at improving the data acquisition system of a Bell State Projection. Once again, the parallel processing capability and flexibility of Field Programmable Gate Arrays is of main interest since the information from four Single Photon Detectors is simultaneously gathered and processed.

The simultaneous analysis enabled by the FPGA removes the need for a post-selective event handling at the detection unit of a Measurement Device Independent Quantum Key Distribution system. Ultimately, this advantage permits the detection of coincidences that could not be detected in a post-selective measurement system and thus improve the experimental secret-key generation rate of the QKD apparatus.

(a) BSA-AS Experimental Setup

Although only the Bell State Analysis unit is regarded in the FPGA project proposed, an overview of the entire experimental setup is depicted in Figure III.10 [69]. Both Alice and Bob are separated from Charlie by a 8.5 km fiber link which is shared by the synchronizing signal, the polarization control signal and the quantum channel. Charlie's synchronizing signal controls both Alice and Bob and the delay generator that triggers the Gated-Mode Single Photon Detectors [69].

In Figure III.10: AM: amplitude modulator, PD: photodetector, VOA: variable optical attenuator, SOP: polarization controller to SOP preparation, M: WDM, APC: automatic polarization controller, MC: master clock, d: delay generator [69].

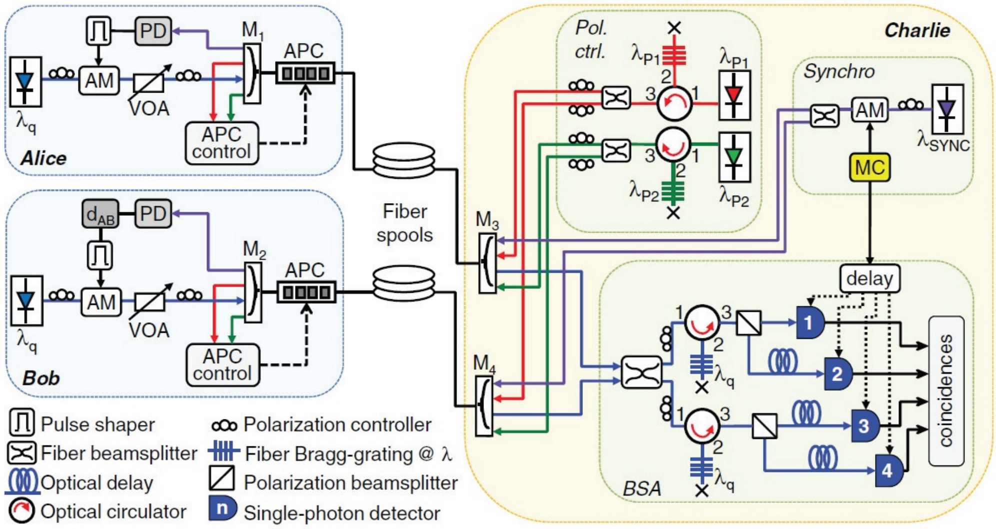


Figure III.10: Block Diagram of the MDI-QKD Experimental Setup.

The digital signals corresponding to a detection on any of the SPDs are sent to the FPGA which processes possible coincidental detections. The information regarding the number of detections on each SPD and the total number of coincidences are sent via USB to a computer interface which outputs the results for the user. Since most of the polarization control of the quantum channel is adjusted by maximizing the number of detections on each of the SPDs, the experimental procedure demands a user's interface with fast response [70].

(b) Bell State Projection Analysis and FPGA

Formally speaking, a Bell-state analysis is the projection of any incoming quantum state onto the Bell state basis, composed by the four Bell States $|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^+\rangle$ and $|\Phi^-\rangle$. Repeating the experiment, it is possible to determine with which probability the original state could be found in one of the Bell states [42].

The goal of this procedure in the MDI-QKD protocol is to determine how the states prepared by Alice and Bob were related by projecting them onto the Bell state basis. By doing so, when Charlie announces the projection results, Alice and Bob can determine what state was sent by the other party when analyzing the state sent by themselves. Any other party listening to the result broadcast can gain no information since knowledge of the original states is not accessible.

A drawback of the use of polarization encoded Qubits is the fact that the linear optics based Bell State Projection as depicted in Figure II.34 is not able to identify the states $|\Phi^{\pm}\rangle$ since they trigger detections on the same SPD which is not sensitive to multiple photons [42]. A $D_{1H}D_{1V}$ or a $D_{2H}D_{2V}$ detection indicate a projection on $|\Psi^{+}\rangle$ while a $D_{1H}D_{2V}$ or a $D_{1V}D_{2H}$ detection indicate a projection on $|\Psi^{-}\rangle$.

The method previously employed for Bell-State projection, which consisted in the post-selection based on triggers in one of the SPDs (Figure III.11-a), did not available the detection of all possible coincidences between detectors since if no photons arrived in, say, reference SPD D_{1H}, all other detections would be discarded. The FPGA based Bell State Analysis enables such detections because the time-bin of photon arrival is set by Charlie's synchronizing signal (Figure III.11-b) and, within this time-bin, the detections are processed simultaneously by the FPGA.

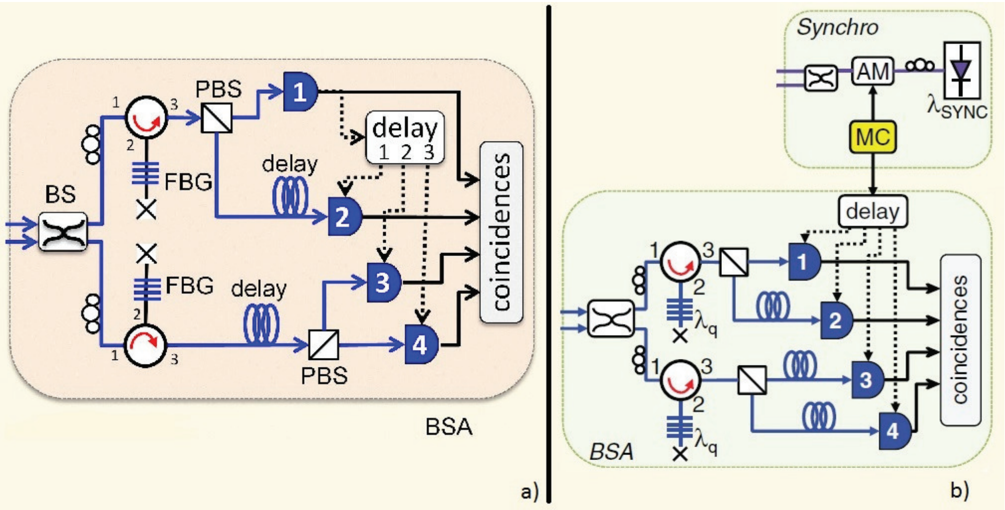


Figure III.11: Diagram of the Experimental Implementation of the Bell-State Analysis Station.

(c) Time Bin and Coincidence Detection

In order to detect coincidences within Charlie's Time Bin, the board utilizes three parallel structures: Delay Generation Unit, Coincidence Unit and Coincidence Counter Unit. Apart from these three structures, there is also the Window Generation Unit which, depending on the application's necessities, enables a less constrained detection. For the purposes of the MDI protocol, though, the window of detection is always set as the minimal pulse duration of 10 ns.

Following the description of Figure III.12, the user can set the parameters of the Delay Unit as to match each pulse's physical delay, enabling coincidences between detectors. Originally, the Time Bin set by Charlie would be interpreted by the board as a trigger signal. However, this course of action was disregarded since all the calculated and measured delays did not exceed 300 ns, which, for a 1 MHz clock on Charlie, does not allow for spurious coincidences.

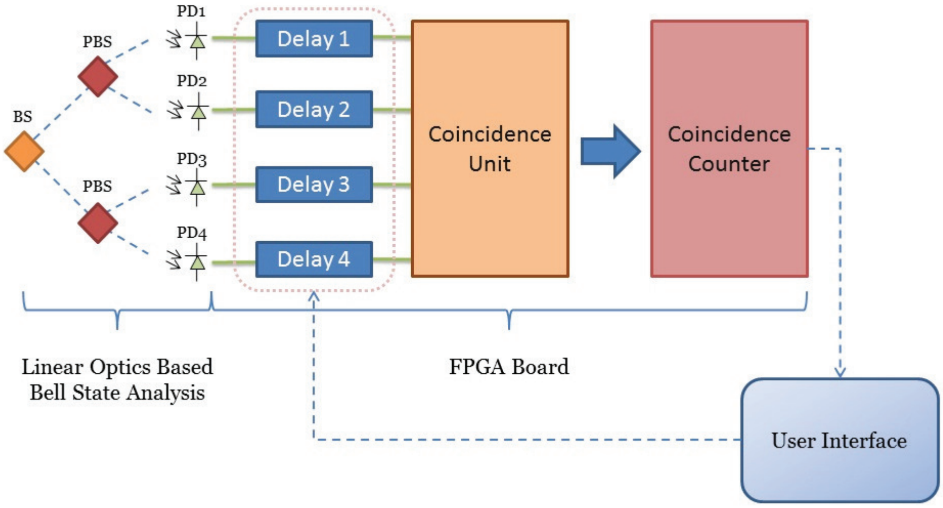


Figure III.12: FPGA Based Bell State Analysis Station.

On the event of a detection, a TTL pulse arrives at the board and, after the designated time interval, a new pulse reaches the Coincidence Unit which, on turn, checks for all the possible coincidences between pulses. Because there are 4 pulses arriving at the board, the total number of coincidences is 11, 6 doubles, 4 triples and 1 quadruple coincidence. Individual counters receive confirmations from the Coincidence Unit and update their values on each Time Bin.

The results are stored in a RAM memory unit and, at the user's demand, are transmitted to the interface. Because this method only enables a total amount of coincidences after a number of Time Bins, without the discrimination of what coincidence occurred at which Time Bin, a second and more robust BSA station was envisioned and is depicted in Figure III.13.

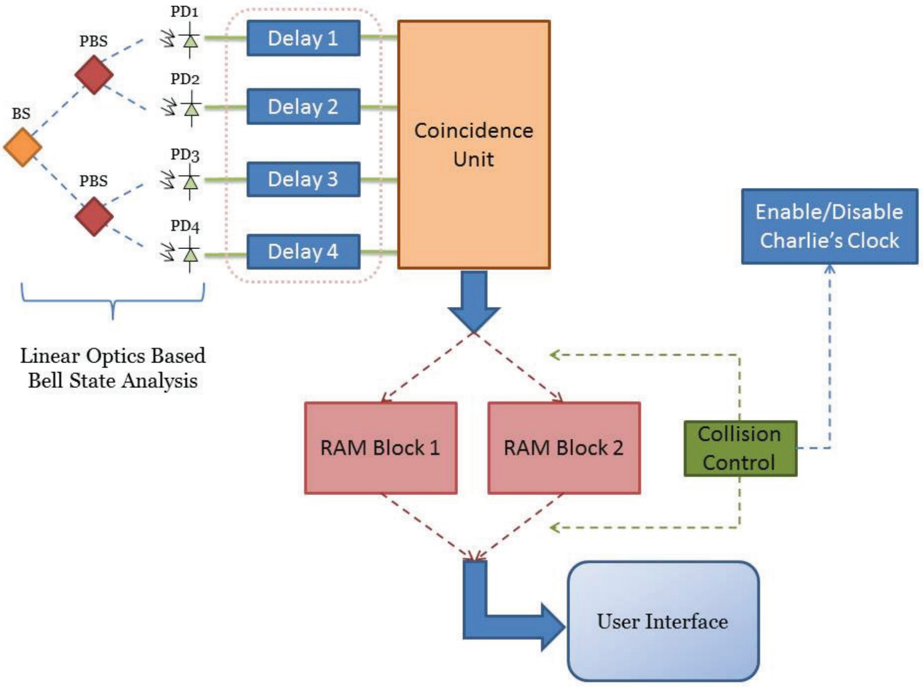


Figure III.13: FPGA Based Synchronous Bell State Analysis Station.

This synchronous station stores the coincidences sequentially utilizing more RAM resources and, since the transmission time between two data transfers cannot exceed the time of pulse arrivals, the station controls Charlie's clocking. In the eminence of a collision, the clock is disabled until the board can again store results. Although this station would fit in a complete QKD system, for the sake of the project [69], the non-synchronous station is sufficient.

(d) BSA-AS Experimental Results

The implementation of the FPGA based Bell-State Analysis permits an optimal gate frequency in all detectors since the trigger is dependent only on the synchronizing signal (Figure III.14). The possibility of detection of previously inaccessible states raised the coincidence generation rate, leading to a 3dB gain of the quantum channel. Also, the optimal operation frequency of 1 MHz can be set on all detectors by the synchronizing signal since detections are no longer dependent on a reference SPD.

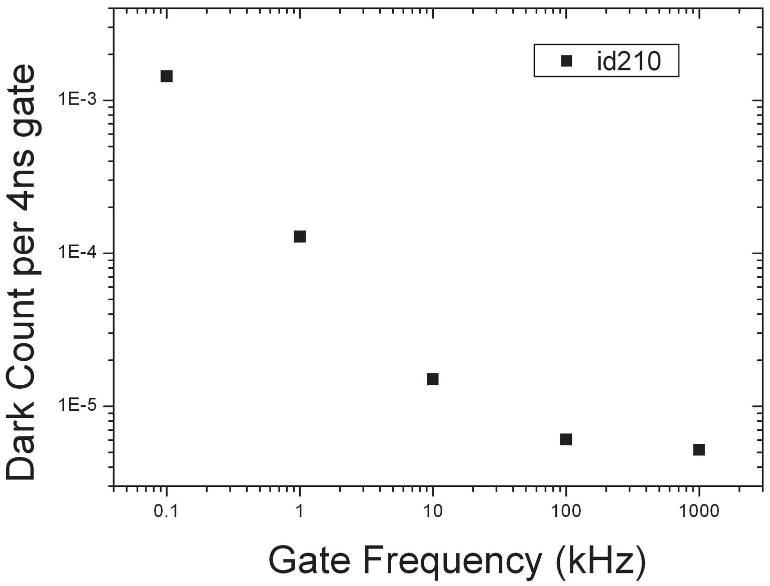


Figure III.14: Dark Count Versus Gate Frequency of the SPDs.

The immediate result is that the secret key generation threshold defined by [71] could be overcome thus permitting the adequacy of the experiment to actual quantum communication channels. The protocol operates at a $1.59 \cdot 10^{-6}\,[bits/pulse]$ rate, above the $1.04 \cdot 10^{-6}\,[bits/pulse]$ minimum acceptable rate.

(e) BSA-AS Conclusions

A FPGA based Bell-State Analysis structure is presented. Its usage in an experimental MDI-QKD protocol shows a number of benefits, including the increase of secret key generation rate. The visual display containing information of all detections and coincidences also provides ease of use to the experimenter specially regarding polarization alignments.

The overall results are included in the article entitled “Proof-of-Principle Demonstration of Measurement-Device-Independent Quantum Key Distribution Using Polarization Qubits” [69].

Even though the objective of the mentioned article is to prove that MDI can indeed be used for QKD purposes offering means to circumvent the present limitations of practical instruments, the structures developed throughout the procedure entice their use in an actual automatic QKD link. An interesting development of this work would be, in this sense, to transform the whole apparatus - using the Synchronous BSA station - into a QKD session with real key exchange.

Bibliography

[1] C. Kittel, **Introduction to Solid State Physics**. John Wiley & Sons, Inc, 2005. II.1, II.1, II.1, II.1, II.1, II.1

[2] Hyper Physics, *Fermi Level and Fermi Function* - `http://hyperphysics.phy-astr.gsu.edu/`. II.1

[3] R. Eisberg and R. Resnick, **Quantum Physics of Atoms, Molecules, Solids, Nuclei and Particles**. John Wiley & Sons, Inc, 1974. II.1, II.1

[4] University of Colorado, *Principles of Semiconductor Devices* - `http://ecee.colorado.edu/`. II.1

[5] A. S. Sedra and K. C. Smith, **Microelectronic Circuits**. Pearson Prentice Hall, 2007. II.2

[6] All About Circuits, *TTL NOR Gate* - `http://www.allaboutcircuits.com`. II.2

[7] Xilinx Inc, *Xilinx FPGAs* - `http://www.xilinx.com`. II.3, II.3, II.2, II.3, III.1(e)

[8] A. Rushton, **VHDL for Logic Synthesis**. John Wiley & Sons, Inc, 1999. II.4

[9] A. Einstein, *Über einen die Ezeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt*, **Annalen der Physik**, vol. 332, 1905. II.5(a)

[10] B. E. A. Saleh and M. C. Teich, **Fundamentals of Photonics**. John Wiley & Sons, Inc, 2007. II.5(a), II.6, II.6, II.6, II.7

[11] Dragica Vasileska - Arizona State University, *Photodetectors* - `https://nanohub.org/groups/dragica_vasileska/`. II.5(a), II.5(a)

[12] H. Melchior, A. R. Hartman, D. P. Schinke, and T. E. Seidel, *Planar Epitaxial Silicon Avalanche Photodiode*, **The Bell System Technical Journal**, vol. 57, 1978. II.5(a)

[13] Laser Components, *Avalanche Photodiodes* - `www.laser-components.com`. II.5(a), II.5(a), II.5(a), II.5(a), II.3, II.5(a), II.5(a)

[14] T. Stokes - Photonics Online, *Avalanche Photodiodes: Theory and Applications* - `http://www.photonicsonline.com/`. II.5(a)

[15] J. C. Campbell, *Recent Advances in Telecommunications Avalanche Photodiodes*, **Journal of Lightwave Technology**, vol. 25, 2007. II.5(a)

[16] B. F. Aull, A. H. Loomis, D. J. Young, R. M. Heinrichs, B. J. Felton, P. J. Daniels, and D. J. Landers, *Geiger Mode Avalanche Photodiodes for Three-Dimensional Imaging*, **Lincoln Laboratory Journal**, vol. 13, 2002. II.5(b), II.5(b)

[17] S. Cova, N. Ghioni, A. Lotito, I. Rech, and F. Zappa, *Evolution and Prospects for Single-Photon Avalanche Diodes and Quenching Circuits*, **Journal of Modern Optics**, vol. 15, 2004. II.5(b), II.5(b)

[18] C. Niclass, K. Ito, M. Soga, H.Matsubara, I. Aoyagi, S. Kato, and M. Kagami, *Design and Characterization of a 256x64-pixel Single Photon Imager in CMOS for MEMS-base Laser Scanning Time-of-Flight Sensor*, **Optics Express**, vol. 20, 2012. II.5(b)

[19] D. Renker, *Geiger-Mode Avalanche Photodiodes, History, Properties and Problems*, **Nuclear Instruments and Methods in Physics Research A**, vol. 567, 2006. II.5(b)

[20] N. Otte. *The Silicon Photomultiplier - A new device for High Energy Physics, Astroparticle Physics, Industrial and Medical Applications.* in **SNIC Symposium**, 2006. II.5(b)

[21] M. Wegmuller, F. Scholder, and N. Gisin, *Photon Counting OTDR for Local Birefringence and Fault Analysis in the Metro Environment*, **Journal of Lightwave Technology**, vol. 22, 2004. II.5(b), II.8(a), II.8(e), III.1(b)

[22] F. Scholders, J. D. Gautier, M. Wegmuller, and N. Gisin, *Long-Distance OTDR Using Photon Counting and Large Detection Gates at Telecom Wavelength*, **Optics Communications**, vol. 213, 2002. II.5(b), II.8(e)

[23] IDQuantique, *id210 - Advanced System for Single Photon Detection*, Specifications Sheet, **Technical Report**. II.5(b)

[24] A. Einstein, *Zur Quantentheorie des Strahlung*, **Physikalische Zeitschrift**, vol. 18, 1917. II.6

[25] G. P. Agrawal, **Fiber-Optic Communication Systems**. John Wiley & Sons, Inc, 1997. II.6, II.6, II.6, II.7, II.4, II.8(a)

[26] S. M. Rezende, **A Física dos Materiais e Dispositivos Eletrônicos**. Universidade de Pernambuco, UFPE, 1996. II.6

[27] S. O. Kasap, **Optoelectronics and Photonics: Principles and Practices**. Prentice Hall, 2001. II.6, II.6, II.6

[28] Farhan Rana - Cornell University, *Semiconductor Optoelectronics* - `https://courses.cit.cornell.edu`. II.6

[29] J. Elmirghani and H. Mouftah, *All-Optical Wavelength Conversion: Technologies and Applications in DWDM Networks*, **IEEE Communications Magazine**, vol. 38, 2000. II.7

[30] RP Photonics Encyclopedia - Optical Fiber Communications, *Semiconductor Optoelectronics* - `http://www.rp-photonics.com/`. II.7, II.5

[31] J. Strutt, *On the Light from the Sky, Its Polarization and Colour*, **Philosophical Magazine**, vol. 41, 1871. II.8(a)

[32] J. Strutt, *On the Scattering of Light by Small Particles*, **Philosophical Magazine**, vol. 41, 1871. II.8(a), II.8(a), II.8(b)

[33] M. K. Barnoski, M. D. Rourke, S. M. Jensen, and R. T. Melville, *Optical Time Domain Reflectometer*, **Applied Optics**, vol. 16, 1977. II.8(a)

[34] D. Derickson, **Fiber Optic - Test and Measurement**. Prentice Hall, 1998. II.8(b), II.8(c), II.8(c), II.8(d), II.8(e)

[35] P. Eraerds, M. Legré, J. Zhang, H. Zbinden, and N. Gisin, *Photon Counting OTDR: Advantages and Limitations*, **Journal of Lightwave Technology**, vol. 28, 2010. II.8(e)

[36] E. Diamanti, C. Langrock, M. M. Feyer, and Y. Yamamoto, *1.5 μm Photon-Counting Optical Time-Domain Reflectometry with a Single-Photon Detector Based on Upconversion in a Periodically Poled Lithium Niobate Waveguide*, **Optics Letters**, vol. 31, 2012. II.8(e), III.1(b), III.1(g)

[37] G.-L. Shentu, Q.-C. Sun1, X. Jiang, X.-D. Wang, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, *217 km Long Distance Photon-Counting Optical Time-Domain Reflectometry Based on Ultra-Low Noise Up-Conversion Single Photon Detector*, **Optics Express**, vol. 21, 2013. II.8(e)

[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, **Reviews of Modern Physics**, vol. 74, 2002. II.9, II.11, II.11(b)

[39] C. E. Shannon, *A Mathematical Theory of Communication*, **Bell System Technical Journal**, vol. 27, 1948. II.9

[40] C. E. Shannon, *The Mathematical Theory of Communication*, **The University of Illinois Press**, 1949. II.9

[41] R. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, **Communications of the ACM**, vol. 21, 1978. II.9

[42] D. Bowmeester, A. Ekert, and A. Zeilinger, **The Physics of Quantum Information**. Springer, 2001. II.10(a), II.10(a), II.10(b), II.10(c), II.10(d), II.11, III.2(b)

[43] W. Wootters and W. Zurek, *A Single Quanta cannot be Cloned*, **Nature**, vol. 299, 1982. II.10(c)

[44] D. Diecks, *Communication by EPR Devices*, **Physics Letters A**, vol. 92, 1982. II.10(c)

[45] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, **Physical Review**, vol. 47, 1935. II.10(d), II.10(d), II.10(d)

[46] L. Lydersen, J. Skaar, and V. Makarov, *Tailored Bright Illumination Attack on Distributed-Phase-Reference Protocols*, **Journal of Modern Optics**, vol. 58, 2011. II.11(a), II.11(a)

[47] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Time-Shift Attack in Practical Quantum Cryptosystems*, **Quantum Information and Computation**, vol. 7, 2006. II.11(a), II.11(a), II.11(a)

[48] F. Xu, B. Qi, and H.-K. Lo, *Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System*, **New Journal of Physics**, vol. 12, 2010. II.11(a)

[49] K. Inoue, E. Waks, and Y. Yamamoto, *Differential Phase Shift Quantum Key Distribution*, **Physical Review Letters**, vol. 89, 2002. II.11(a)

[50] M. Curty and T. Moroder, *Heralded Qubit Amplifiers for Practical Device-Independent Quantum Key Distribution*, **Physical Review A**, vol. 84, 2011. II.11(b)

[51] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, **Physical Review Letters**, vol. 67, 1991. II.11(b), II.11(b)

[52] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-Independent Quantum Key Distribution Secure against Collective Attacks*, **New Journal of Physics**, vol. 11, 2011. II.11(b)

[53] H.-K. Lo, M. Curty, and B. Qi, *Measurement Device Independent Quantum Key Distribution*, **Physical Review Letters**, vol. 108, 2012. II.11(b), II.11(b)

[54] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, **Physics**, vol. 1, 1964. II.11(b)

[55] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporao, and J. P. von der Weid, *Long-Distance Bell-State Analysis of Fully Independent Polarization Weak Coherent States*, **Journal of Lightwave Technology**, vol. 31, 2013. II.11(b)

[56] P. G. Kwiat and H. Weinfurter, *Embedded Bell-State Analysis*, **Physical Review A**, vol. 58, 1998. II.11(b)

[57] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, **Physical Review Letters**, vol. 91, 2003. II.11(b)

[58] G. P. Temporao, G. V. de Faria, P. J. Urban, and J. P. von der Weid. *Feasibility of Centralized PON Monitoring Using PON-Tuned OTDR.* in **FOAN 2012**, 2012. III.1

[59] S.-J. Kim, K. Koh, S. Boyd, and D. Gorinevsky, *l1 Trend Filtering*, **SIAM Review**, vol. 51, 2010. III.1(a), III.1(f)

[60] R. Wiśniewski, *Synthesis of Compositional Microprogram Control Units for Programable Devices.* PhD thesis, University of Zielona Góra, 2009. III.1(b)

[61] D. V. Caballero, J. P. von der Weid, and P. J. Urban. *Tuneable OTDR Measurements for WDM-PON Monitoring.* in **IMOC 2013**, 2013. III.1(c)

[62] S. W. Hasinoff - Google Inc, *Photon, Poisson Noise* - `http://people.csail.mit.edu/hasinoff/`. III.1(d)

[63] W. V. Sorin and D. M. Baney, *Measurement of Rayleigh Backscatering at 1.55 μm with a 32 μm Spatial Resolution*, HP Labs Technical Reports, **Technical Report**. III.1(d)

[64] G. C. do Amaral, L. E. Y. Herrera, D. Vitoreti, G. P. T. ao, P. J. Urban, and J. P. von der Weid, *WDM-PON Monitoring with Tunable Photon Counting OTDR*, **Photonics Technology Letters**, vol. 26, 2014. III.1(d), III.1(e)

[65] Zonghao Gu, and Edward Rothberg, and Robert Bixby - Google Inc, *Gurobi Optimizer* - `http://www.gurobi.com/`. III.1(f)

[66] D. P. Bertserkas, **Nonlinear Programming**. Athena Scientific, 1995. III.1(f)

[67] ThorLabs, *SOA1013SXS Polarization Independent Optical Shutter/Switch*, ThorLabs, **Technical Report**. III.1(g)

[68] OpalKelly, *XEM3005 User Manual*, OpalKelly, **Technical Report**. III.1(h), 1

[69] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporao, and J. P. von der Weid, *Proof-of-Principle Demonstration of Measurement-Device-Independent Quantum Key Distribution Using Polarization Qubits*, **Physical Review A**, vol. 88, 2013. III.2(a), III.2(c), III.2(e)

[70] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporao, and J. P. von der Weid. *Polarization-Stable Long-Distance Interference of Independent Photons for Quantum Communications.* in **OSA Research in Optical Sciences**, 2012. III.2(a)

[71] X. Ma, C.-H. F. Fung, and M. Razavi, *Statistical Fluctuation Analysis for Measurement-Device-Independent Quantum Key Distribution*, **Physical Review A**, vol. 86, 2012. III.2(d)