

Light Quantum Properties and Applications: Secure Key Distribution Systems

Beatriz Gomes Soares

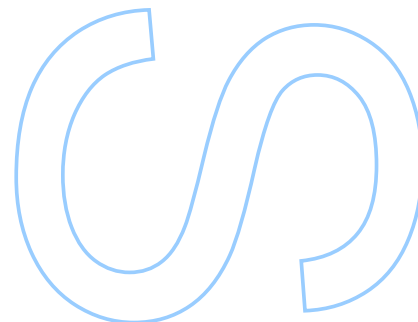
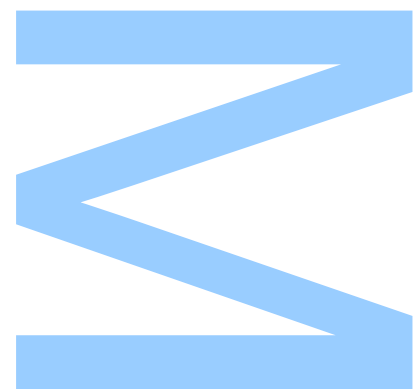
Mestrado Integrado em Engenharia Física
Departamento de Física e Astronomia
2021

Orientador

Prof. Orlando Frazão, Faculdade de Ciências

Coorientador

Prof. Ariel Guerreiro, Faculdade de Ciências



U. PORTO

FC FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Todas as correções determinadas
pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, ____ / ____ / ____

W

S

Q

UNIVERSIDADE DO PORTO

MASTERS THESIS

**Light Quantum Properties and
Applications: Secure Key Distribution
Systems**

Author:

Beatriz Gomes SOARES

Supervisor:

Orlando FRAZÃO

Co-supervisor:

Ariel GUERREIRO

*A thesis submitted in fulfilment of the requirements
for the degree of MSc. Engineering Physics*

at the

Faculdade de Ciências da Universidade do Porto
Departamento de Física e Astronomia

November 26, 2021

Acknowledgements

First, I would like to thank my supervisor, Professor Orlando Frazão, and my co-supervisor, Professor Ariel Guerreiro, for this opportunity and for the continuous assistance during the undertaking of this thesis. A special thanks to INESC-TEC, and in particular to Professor Henrique Salgado, and investigators Luís Pessoa and Joana Tavares, for helping during the research of the FWM section of this work. I would also like to thank IT-Aveiro and Professor Armando Pinto, from University of Aveiro, for allowing me to participate on their research team, as well as to Tiago Fernandes and Nuno Silva, for their crucial help during the experimental work on optical receivers. Finally, I would like to thank Paulo Robalinho, without whom, the work on UFL would have been quite difficult to achieve.

UNIVERSIDADE DO PORTO

Abstract

Faculdade de Ciências da Universidade do Porto

Departamento de Física e Astronomia

MSc. Engineering Physics

Light Quantum Properties and Applications: Secure Key Distribution Systems

by [Beatriz Gomes SOARES](#)

This thesis has as its main objective the study of optic applications in the area quantum information, in particular of quantum cryptography. The use of four-wave mixing (FWM) for development of quantum sources was studied, and the behavior of stimulated FWM, through employment of a highly non-linear fiber (HNLF), was verified. The obtained experimental data was used to characterize the HNLF, resulting in a non-linear parameter $\gamma = 9.6 \pm 1.8 \text{ W}^{-1}\text{km}^{-1}$, an attenuation coefficient $\alpha = 0.58 \pm 0.13 \text{ km}^{-1}$, and a zero-dispersion wavelength $\lambda_0 = 1539.93005 \pm 10^{-5} \text{ nm}$. The fit of the experimental data to the expected theoretical behavior was attained with a reduced χ^2 of 1.07×10^{-16} .

Further still, the use of optical receivers based on PIN photodiodes was studied. This type of optical receiver finds applications in the area of continuous variable quantum key distribution (CV-QKD). A theoretical model of the receiver and its noise sources was developed. The optical receiver was then studied experimentally, and its behavior compared with the expected results.

Finally, a classically based alternative to quantum key distribution protocols, based in an ultra-long fiber laser (UFL), was studied. A new configuration, based on a bi-directional amplifier between two users (Alice and Bob), was investigated, presenting itself as a viable and simple alternative to applications in optical communications. This protocol was implemented in the laboratory, and its resilience to *passive* attacks was tested. Possible vulnerabilities and improvements to the presented configuration were discussed.

UNIVERSIDADE DO PORTO

Resumo

Faculdade de Ciências da Universidade do Porto

Departamento de Física e Astronomia

Mestrado Integrado em Engenharia Física

Propriedades e Aplicações de Luz Quântica: Sistemas de Distribuição Segura de Chaves

por [Beatriz Gomes SOARES](#)

Esta tese tem como principal objetivo o estudo de aplicações de ótica na área de informação quântica, em particular criptografia quântica. Estudou-se o uso de four-wave mixing (FWM) para realização de fontes quânticas, e verificou-se o comportamento de FWM estimulado, gerado numa fibra altamente não linear (HNLF). Os resultados experimentais foram utilizados para caracterizar a HNFL, obtendo-se um parâmetro não-linear $\gamma = 9.6 \pm 1.8 \text{ W}^{-1}\text{km}^{-1}$, uma atenuação $\alpha = 0.58 \pm 0.13 \text{ km}^{-1}$, e um comprimento de onda de dispersão nula $\lambda_0 = 1539.93005 \pm 10^{-5} \text{ nm}$. O ajuste dos resultados experimentais ao comportamento teórico esperado, foi obtido com χ^2 -reduzido de 1.07×10^{-16} .

Estudou-se ainda o uso de recetores óticos baseados em fotodíodos tipo PIN. Este tipo de recetor ótico tem aplicações na área de distribuição de chave quânticas de variável contínua (CV-QKD). Um modelo teórico do recetor e das suas fontes de ruído foi desenvolvido. O recetor ótico foi estudado experimentalmente, e o seu comportamento comparado com os resultados esperados.

Estudou-se uma alternativa clássica aos protocolos de distribuição de chave quânticos, baseado em laser ultra-longos (UFL). Projetou-se uma nova configuração de chaves baseada no uso de um amplificador bidirecional conectado a dois utilizadores (Alice e Bob), apresentando uma solução viável e simples para uma aplicação em comunicações óticas. Este protocolo foi implementado experimentalmente e a sua resiliência a ataques passivos foi testada. Vulnerabilidades e melhoramentos à configuração estudada foram discutidos.

Contents

Acknowledgements	i
Abstract	ii
Resumo	iii
Contents	iv
List of Figures	vi
List of Tables	vii
Glossary	viii
1 Introduction	1
1.1 Motivation	1
1.2 Objectives	2
1.3 Structure	2
2 Brief review of quantum photon sources	3
2.1 Introduction	3
2.2 Applications for quantum photon	3
2.2.1 Quantum key distribution	4
2.2.2 Other applications	5
2.3 Characterization of quantum photon sources	6
2.3.1 Quantum and classical states of light	6
2.3.2 Experimental characterization of quantum photon sources	7
2.4 Quantum photon sources	9
2.4.1 Deterministic	10
2.4.2 Probabilistic	11
2.5 Conclusions	13
3 Four-wave mixing for use in quantum sources	14
3.1 Introduction	14
3.2 The Four-wave mixing effect	14
3.3 Generation of stimulated FWM using optical fibers	16
3.3.1 Theory	17

3.3.2	Experimental Setup	18
3.3.3	Experimental Results	18
3.4	Description of FWM quantum sources	21
3.4.1	Heralded single-photon source	21
3.4.2	Polarization-entangled photon pair source	22
3.5	Conclusions	24
4	Characterization and modeling of an optical receiver	25
4.1	Introduction	25
4.2	Continuous variable QKD	26
4.2.1	Coherent states and field quadratures	26
4.2.2	Principle of CV-QKD with coherent states	27
4.3	Theoretical model of an optical receiver	27
4.3.1	Photodiode	28
4.3.2	Transimpedance Amplifier	30
4.3.3	Photodetection noise sources	31
4.3.4	Detection scheme	34
4.4	Experimental characterization of an optical receiver	35
4.4.1	Experimental Setup	35
4.4.2	Experimental Results	36
4.5	Conclusions	40
5	Secure key distribution using a ultra-long fiber laser	42
5.1	Introduction	42
5.2	Principle of operation	43
5.3	Security of the system	44
5.4	Experimental Implementation of a UFL-KDS	45
5.4.1	Experimental Setup	45
5.4.2	Experimental Results	45
5.5	Discussion	48
5.5.1	Improvements to the system	48
5.5.2	Vulnerabilities	49
5.6	Conclusions	50
6	Final conclusions and future work	51
	Bibliography	52
	A Efficiency of the FWM process in optical fibers	62
	B Coefficients of the fits in Chapter 4	74

List of Figures

2.1	Setup of the Hanbury-Brown-Twiss single-photon source characterization experiment.	7
2.2	The Hong-Ou-Mandel (HOM) effect.	8
2.3	Setup of a single-photon source characterization experiment based on the HOM effect.	9
2.4	The SPDC process and its different types of phase-matching.	12
3.1	Schematic representation of the (a) non-degenerate and (b) degenerate FWM process.	15
3.2	Schematic representation of the degenerate (a) stimulated and (b) spontaneous FWM process.	16
3.3	Experimental setup used in order to obtain stimulated FWM.	18
3.4	Some of the experimental optical spectra of stimulated FWM obtained with the OSA	19
3.5	Experimental results and theoretical fit for the idler optical power vs. distance between signal and pump wavelengths	20
3.6	Basic setup of a single-photon source based on spontaneous FWM	22
3.7	Basic setup of a polarization-entangled photon-pair source using the counter-propagation scheme.	23
4.1	Schematic representation of a (a) PN and (b) PIN photodiode.	28
4.2	Schematic representation of a photodiode equivalent circuit	30
4.3	Schematic representation of the studied optical receiver	31
4.4	Experimental setup used to characterize a PIN photodetector.	36
4.5	Experimental results, data fits, and expected behavior for the average power and noise variance, in the direct and balanced detection schemes.	37
4.6	Experimental results and improved expected behavior, for the average power and noise variance, in the direct and balanced detection schemes.	40
5.1	Schematic setup for secure key distribution using a ultra-long fiber laser.	43
5.2	Lab setup and internal schematic of the bidirectional EDFA utilized.	46
5.3	Optical spectrum of the four states of the UFL-KDS	46
5.4	Cavity signal when transitioning from non-secure to secure states and vice-versa	47
5.5	Cavity signal filtered at λ_0 and λ_1 for several transitions of UFL states.	48
A.1	Impact of different values of the parameter C_1 on (a) $\Delta\beta_{eff}L$ and (b) the idler power	73

List of Tables

2.1	BB84 protocol for quantum key distribution (QKD)	5
3.1	Specifications of the HNLF used.	18
3.2	Values obtained from the theoretical fit	21
4.1	Specifications of the optical receiver used.	36
4.2	Parameters calculated from the experimental fits.	39
5.1	Protocol for key distribution using a ultra-long fiber laser (UFL).	44
B.1	Calculated fit and theoretical values for the <i>average power</i> measured in the <i>direct detection</i> scheme	74
B.2	Calculated fit and theoretical values for the <i>noise variance</i> measured in the <i>direct detection</i> scheme	74
B.3	Calculated fit and theoretical values for the <i>noise variance</i> measured in the <i>balanced detection</i> scheme	75

Glossary

CP	Counter-Propagating
CV-QKD	Continuous Variable QKD
DSF	Dispersion-Shifted Fiber
DV-QKD	Discrete Variable QKD
EDFA	Erbium Doped Fiber Amplifier
FBG	Fiber Bragg Grating
FWM	Four-Wave Mixing
HNLF	Highly Non-Linear Fiber
HOM	Hong-Ou-Mandel effect
KDS	Key Distribution System
LOQC	Linear Optic Quantum Computing
NEP	Noise-Equivalent Power
OSA	Optical Spectrum Analyzer
PBS	Polarization Beam-Splitter
PCF	Photonic Crystal Fiber
QD	Quantum Dot
QKD	Quantum Key Distribution
RD	Research and Development
RIN	Relative Intensity Noise
RSA	Rivest-Shamir-Adleman scheme
SFWM	Spontaneous Four-Wave Mixing

SL	Sagnac-Loop
SNR	Signal-to-Noise Ratio
SPDC	Spontaneous Parametric Down-Conversion
SPM	Self-Phase Modulation
SWW	Silicon Wire Waveguides
TIA	Transimpedance Amplifier
UFL	Ultra-long Fiber Laser
VOA	Variable Optical Attenuator
WCP	Weak Coherent Pulses
WDM	Waveguide Division Multiplexing
XPM	Cross-Phase Modulation
ZDW	Zero-Dispersion Wavelength

Chapter 1

Introduction

1.1 Motivation

The application of quantum mechanics to the field of information processing has been a relatively new development [1, 2], with the first proposal of quantum computing dating back to the 1980s [3]. Interest in the field grew with the introduction of Shor's algorithm in the 1990s, which, if implemented, would pose a threat to some of the most widely used encryption systems [1, 3]. The most common of these, the Rivest-Shamir-Adleman (RSA) scheme, is a public key cryptosystem, that relies on the difficulty to invert the encryption of a message, with access to only the freely available public key. Hypothesis which depends on a classical computer's prohibitively hard time in factoring large numbers, something which would theoretically disappear for a quantum computer running Shor's algorithm [1]. Accordingly, quantum cryptography emerges as a potential solution, with schemes such as quantum key distribution (QKD) being proposed, and providing *theoretically* unconditional security [2–6]. In this context, the past several decades have seen significant progress in quantum systems applications, and under the broader umbrella of quantum information science, fields such as quantum processing, communication, networking, sensing and metrology driving considerable interest in research and development (R&D).

Appropriately, photons, namely single-photons, have proven to be some of the more useful quantum objects [4, 7], and proper R&D of single-photons sources and detectors therefore becomes crucial.

1.2 Objectives

In this thesis we aim to study the generation, detection and characterization of single-photons, having in mind its possible applications. Additionally, we aim to study a proposed classically-based alternative to the QKD encryption scheme.

1.3 Structure

The structure of this thesis is as follows:

- Chapter 1 presents the main motivations, objectives and structure of this thesis.
- Chapter 2 presents a review of quantum photon sources, their main applications, principal theoretical descriptions, and most common implementations.
- Chapter 3 discusses the process of four-wave mixing (FWM) for use in quantum sources. The main theoretical principles are presented, and an experimental setup of stimulated FWM is implemented and its results compared with the expected behavior. A description of the use of spontaneous FWM in single-photon and entangled-photon sources is also discussed.
- Chapter 4 shows the theoretical description and experimental characterization of an optical receiver, for use in continuous variable QKD.
- Chapter 5 introduces and tests a secure key distribution scheme based on an ultra-long fiber laser (UFL). Its feasibility as a classical based alternative to QKD is discussed.
- Chapter 6 summarizes the main results of this thesis and presents suggestions for future work.

Chapter 2

Brief review of quantum photon sources

2.1 Introduction

The search to fully explore the promise of quantum technologies, requires the ability to work with single quantum objects. With this in mind, this chapter presents a brief review of quantum photon sources: first discussing some of its applications, with special attention to quantum key distribution (QKD), then on how to characterize them, theoretically and experimentally, and lastly, a description of some of the most common types of quantum photon sources is presented.

2.2 Applications for quantum photon

The main driver behind the current interest in the research of single/quantum photon sources and single photon detectors derives from their applicability in the fields of quantum information and metrology [4, 7]. Photons, which can form a quantum qubit by being encoded through several degrees of freedom such as polarization, momentum, energy, and others, are thus very useful objects in such fields [5]. They are especially good candidates for the transmission of quantum information, since they can travel at fast speeds and, being chargeless and massless particles, interact weakly with neighboring photons, leading to a reduction of loss and noise [5, 7]. In this section we discuss some of this applications, with special emphasis on quantum key distribution.

2.2.1 Quantum key distribution

One of the most advanced applications for quantum photon is its use in quantum key distribution (QKD) [4], a quantum cryptography method that in its ideal implementation allows for unconditionally secure communication [2, 5]. QKD protocols enable the distribution of a secret, random key between two parties, which then can be used to encrypt a message through classical encryption schemes [4]. Important to note that QKD refers only to the transmission of the key and not the actual message. The first QKD protocol, the BB84 protocol, was introduced by Bennett and Brassard in 1984 [8] and utilizes the polarization of photons to encode information [2, 4, 5]. However, other ways to encode the qubits, such as time-bin qubits, are possible [5]. In the BB84 protocol the sender, which will be referred to as Alice, sends a string of single photons to the receiver, referred to as Bob, each with their polarization randomly encoded with one or zero. For this process to be secure Alice switches randomly between two different sets of polarization bases. As an example, we can have one of the basis with horizontal and vertical polarization basis states (\uparrow and \downarrow) and the other rotated 45° from it (\nearrow and \searrow), each assigned with the classical bit values of “0” (for ex. \uparrow and \searrow) and “1” (for ex. \downarrow and \nearrow). Bob, not knowing the basis chosen by Alice, will also choose the basis in which to measure each polarization randomly. Whenever Alice and Bob, by chance, choose the same basis they will obtain perfectly correlated results. However, when they happen to choose different basis sets, they will obtain uncorrelated results, as measurement in a different basis will yield, statistically speaking, the wrong result half of the time. Alice and Bob will therefore have to exchange their choice of basis to each other, over a classical communication channel. Important to notice that the exchange of basis does not reveal information about the bit value sent. With this information Alice and Bob will then discard the bits in which they used a different basis, which happens, on average, half the time, and thus obtain a sift-key. This sift-key is completely random, with neither Alice nor Bob being able to influence it, but both know it with certainty, thus allowing them now to send highly secure encrypted messages using classical protocols. This protocol is schematically depicted in table 2.1.

The safety of this protocol arises from the fact that it's impossible to measure a quantum state without perturbing it [2]. Let's suppose an eavesdropper called Eve tries to intercept a qubit sent from Alice to Bob. If the source used is not a true single photon source, Eve can perform a photon-number splitting attack, measuring part of the photons in a pulse and letting the rest reach Bob [4]. However, if the source is single photon, Eve needs to

TABLE 2.1: BB84 protocol for QKD. Only when Alice and Bob choose the same basis are the bits kept in order to obtain the sift-key.

Alice's chosen basis	\uparrow	\uparrow	\times	\times	\uparrow	\times	\uparrow	\uparrow
Alice's bit value	0	1	1	0	0	0	1	0
Sent Polarization	\uparrow	\rightarrow	\searrow	\nearrow	\uparrow	\nearrow	\rightarrow	\uparrow
Bob's chosen basis	\times	\uparrow	\uparrow	\times	\times	\uparrow	\times	\uparrow
Bob's bit value	0	1	0	0	1	0	1	0
Sift-key		1		0				0

measure the qubit and then replicate it to send to Bob, so he does not notice the attack and stops the communication. Due to the no cloning theorem, Eve cannot make a perfect copy of an unknown quantum system. Indeed, as Eve measures the qubit in one of the two basis at random, she will only choose the correct basis half the time, thus only sending an accurate copy of the original qubit half the time. Altogether, Eve will only get 50% of the information and Alice and Bob get an error rate of 25%, which they can detect by comparing a sample of the obtained sift-key [2]. In practice, though, the source, detectors and transmission line are not perfect, opening a possibility for Eve to disguise her attack as communication noise [2]. However, the better the equipment used, the more difficult this becomes [2].

2.2.2 Other applications

Another application for quantum photon includes the realm of linear optic quantum computing (LOQC), with the first notable proposal for the building of all-optical quantum gates described in the paper [9] by Knill, Laflamme and Milburn (KLM) [2, 4] (a review on LOQC systems can be found in [10]). Quantum photons can also be used, among other applications, to generate truly random numbers [2, 5], perform quantum teleportation [2, 7] and in the field of quantum metrology build an accurate standard for the intensity of a light source [4]. Finally, single/quantum photons are also popular in experiments of fundamental ideas and principles of quantum mechanics, such as the violation of Bell's inequality [7].

2.3 Characterization of quantum photon sources

In an ideal world a single photon source would be one which could emit one and only one photon at any arbitrary moment in time, with any rate of emission necessary and whose emitted photons would be indistinguishable from each other. However, deviations from this ideal behavior are obviously present in real life systems and is therefore necessary to properly characterize single photon sources according to their proximity to this idealized theoretical case. To achieve this we will first briefly discuss some quantum theory in order to distinguish between classical and quantum states and then we will describe some of the experimental setups used to characterize single photon sources.

2.3.1 Quantum and classical states of light

The Hamiltonian of electromagnetic energy can be defined as an infinite sum of harmonic oscillator Hamiltonians, such as

$$\hat{H} = \sum_{\lambda} \hat{H}_{\lambda} = \sum_{\lambda} \hbar\omega_{\lambda} \left(\hat{a}_{\lambda}^{\dagger} \hat{a}_{\lambda} + \frac{1}{2} \right) \quad (2.1)$$

where $\hat{a}_{\lambda}^{\dagger}$ and \hat{a}_{λ} are the creation and annihilation operators associated with photons of mode λ . Since the number operator, defined as $\hat{n}_{\lambda} = \hat{a}_{\lambda}^{\dagger} \hat{a}_{\lambda}$, commutes with the Hamiltonian, its eigenstates, called Fock states ($\hat{n}_{\lambda} |n_{\lambda}\rangle = n_{\lambda} |n_{\lambda}\rangle$), are also eigenstates of \hat{H} . Therefore, the variance of the number of photons for a certain Fock state is exactly zero. This property contrasts with that of observed classical light, such as that emitted by, for instance, a laser or a black body. Hence, to properly describe the statistical properties of this types of sources, one needs to resort to different types of states. As it is common practice to use attenuated laser sources as substitutes for single photon sources, we will focus our attention on the states that describe the light emitted by a stable laser, i.e. coherent states, which are defined from Fock states as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad (2.2)$$

where from now on we drop the mode index λ . The number of photons of coherent states follows a Poissonian distribution, where the probability of finding m photons is given by

$$p(m) = \frac{\langle n \rangle^m}{m!} e^{-\langle n \rangle} \quad (2.3)$$

with the average number of photons being $\langle n \rangle = |\alpha|^2$ with a respective variance of $\Delta n^2 = |\alpha|^2$. A consequence of the fact that the photon number variance is non-zero is that attenuated laser sources or weak coherent laser pulses (WCP), cannot be used as a “true” source of single photons.

To characterize the type of states emitted by a source, one often employs an important measurement called the second order correlation function, $g^{(2)}$, defined as

$$g^{(2)}(\tau) = \frac{\langle a^\dagger(t) a^\dagger(t+\tau) a(t+\tau) a(t) \rangle}{\langle a^\dagger(t) a(t) \rangle^2} \quad (2.4)$$

This function relates the number of photons in a certain state at two different moments in time, which will remain constant in Fock states, yet vary for both coherent and thermal states. With this we can now describe the most common experiments used to indicate the quality of a given single photon source.

2.3.2 Experimental characterization of quantum photon sources

Photon anti-bunching

A characteristic of Fock states that distinguishes them from classical/near-classical states is the effect of anti-bunching. To study it, it is common to use the Hanbury-Brown-Twiss setup represented in figure 2.1 a).

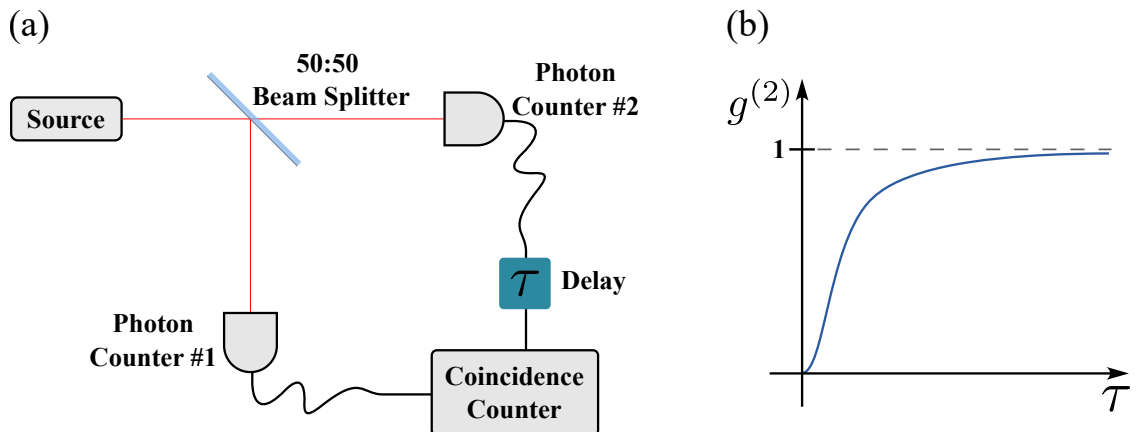


FIGURE 2.1: (a) Schematic setup of a Hanbury-Brown-Twiss experiment and (b) the expected second-order correlation function obtained by the coincidence counter for an ideal single-photon source.

In the setup shown, light is incident in one of the input ports of a 50/50 beam splitter and the second order correlation function with delay τ is measured between the two output ports. If a single photon is emitted by the source, then it can exit from either output of the beam splitter, but not from both, as a photon is indivisible. Therefore, at zero-time delay, there cannot be simultaneous detection in both outputs, and we have that $g^{(2)}(\tau = 0) = 0$. After the emission of the first single photon the source can emit once again, consequently, as the time delay between both arms is varied, simultaneous detection of photons at the coincidence counter is expected and we have that $g^{(2)}(\tau) > g^{(2)}(0)$. The fact that for a true single photon source arbitrarily short delays between the emission of two photons is forbidden and thus they are emitted one at a time is referred to as photon anti-bunching. This contrasts with the properties of attenuated laser light where any delay is allowed due to the poissonian distribution of the photons. In fact, for coherent states like this we have that $g^{(2)}(\tau) = 1$ for all τ . It is still important to mention that, in practice, the time response and dark counts of the detectors determines a minimum $g^{(2)}(0)$ allowed to be measured, even for a perfect $g^{(2)}(0) = 0$ source.

The HOM effect

The Hong-Ou-Mandel (HOM) effect occurs when two indistinguishable photons impinge on the two input ports of a 50/50 beam splitter. Due to second order interference effects, the possibility of one photon exiting each output port cancels out and only the possibility of both photons exiting together by one of the output ports remains (figure 2.2).

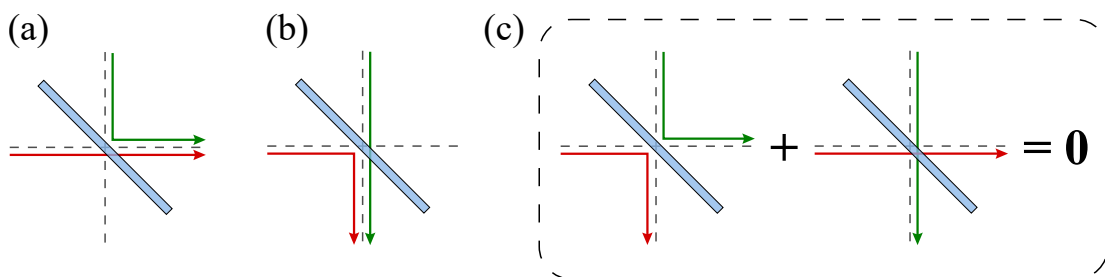


FIGURE 2.2: The HOM effect. Two independent photons arrive at the exact same time to the two input ports of a beam-splitter. Due to second order interference effects, the two paths shown in (c) cancel out and only the possibility where both photons exit by the same output port, like shown in (a) and (b), remains.

However, if there is some distinguishability between both input photons, such as a delay in arrival (see figure 2.3 a)), then the chance of the photons exiting by a different output port is non-zero. As such, if we measure $g^{(2)}$ in function of the delay in arrival time to the beam splitter between photons, we expect to obtain a graph similar to figure 2.3 b).

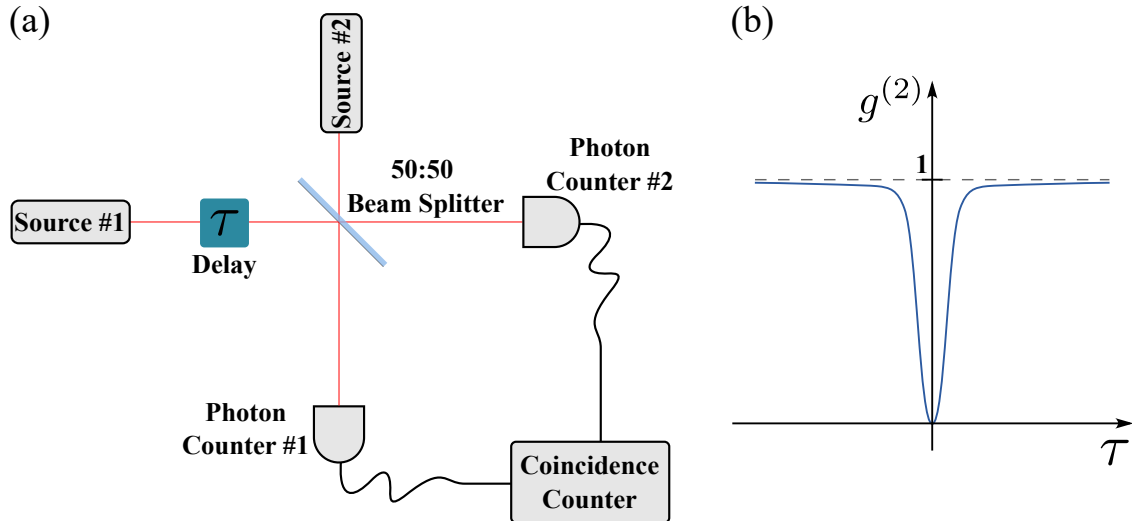


FIGURE 2.3: (a) Schematic setup of an experiment based on the HOM effect and (b) the expected second-order correlation function obtained by the coincidence counter for two indistinguishable, ideal single-photon sources.

The size of dip at zero time delay is proportional to the indistinguishability of the photons [4]. Important to note that this property is required for some quantum photon applications, such as linear quantum computing, but not for others, such as QKD [4]. Therefore, for applications where indistinguishability is unimportant, the Hanbury-Brown-Twiss experimental setup described above is sufficient to evaluate the quality of the source.

2.4 Quantum photon sources

In this section we briefly describe some of the most studied types of quantum photon sources. As per common convention, we divide the photon sources into two categories based on their availability: deterministic or probabilistic. Probabilistic sources, while at first glance may seem impractical, rely on the generation of photon pairs and can thus use one of the photons to herald the arrival of the other. This knowledge of when a photon has been produced, through the use of a heralding photon, is sufficient for some quantum photon applications. Finally, it's important to mention that, in practice, the distinction between deterministic and probabilistic sources is not as clear cut, as real life limitations implicate that some sources that are classified as deterministic are not reliable 100% of the time.

2.4.1 Deterministic

Single atom, ion and molecule sources

In these types of sources, emission of a single photon occurs when there is a transition from a higher to a lower energy level of one and only one emitter, whether it be an atom, ion or molecule [5, 7]. Thus, when the emission of a single photon is required, an external source places the system upon an excited state, so that the single photon can be emitted upon the system's relaxation. The main technological challenges of this type of source are to first isolate a single particle and then have it efficiently emit in a chosen direction [7]. A common way to achieve this is described in article [11]. In it a magneto-optical trap (MOT) is used to cool and trap ^{85}Rb atoms. They are then subsequently released, in a controlled manner, from the MOT and enabled to fall down into an optical cavity, where they are subjected to a sequence of laser pulses and thus placed in an excited state. The optical cavity alters the density of states in such a way that the emission rate is enhanced in a chosen direction and suppressed in all others, through the Purcell effect [2, 4]. This turns the isotropic nature of the subsequent spontaneous emission into a highly anisotropic, i.e. unidirectional, process [4]. This process of trapped single particles and coupling to cavity modes allows for narrow emission linewidths and low probability of multiple photon emission [7]. While this type of source is experimentally very challenging [5] and therefore not ideal for technological applications, they are still good options for experiments on fundamental quantum principles and quantum metrology [7].

Quantum dots

Quantum dots (QD) are semiconductor particles or nanocrystals that are often referred to as "artificial atoms" as, despite usually containing several hundred of thousand of atoms, have an energy structure that resembles that of an atom's discrete level energy system [7, 12]. One advantage of using quantum dots is the ability to use nano-engineering. This allows QDs to be designed to work in wavelengths which can range from infrared to ultra-violet, making them compatible with already available telecom components [12]. Quantum dots can also operate with either electrical or optical pumping [5, 7]. The optical pumping scheme relies on the absorption of photons by the system to set electrons from the valence to the conduction band, while the electrical scheme relies on directly moving electrons into the quantum dot itself [5]. This creates electron-hole pairs, or excitons, that

then emit photons upon their return to the ground state. Depending on the number of electron-hole pairs we can have emission from exciton, bi-exciton or multi-exciton states [5, 7]. Theoretically they can all be used in single photon sources, with the employment of spectral filters, though its most commonly to use either exciton or bi-exciton states [7]. Like in the previously discussed quantum photon sources, quantum dots are commonly coupled to cavities in order to control the direction of emission through the Purcell effect.

Color centers

Color centers are formed by defects on the crystal structure of an inorganic material, leading to a change in the electronic states surrounding it [2, 5, 7]. One of the more promising color centers for single photon generation is that of a nitrogen-vacancy (NV) center in diamond. This center is formed by the substituting two neighboring carbon atoms in the diamond crystal lattice with a nitrogen atom and a vacant space [2, 7]. Other color centers of diamond, such as the nickel-nitrogen (NE8), have also been proposed for the purpose of single photon generation. An important advantage of using such diamond color centers is their stability at room temperature, which arises from the rigidity of the diamond lattice [2, 5].

2.4.2 Probabilistic

Spontaneous parametric down-conversion

The phenomenon of spontaneous parametric down-conversion (SPDC) is a consequence of a non-zero second-order term of a given material's susceptibility ($\chi^{(2)}$) [5, 13, 14]. This term, when a material is pumped with a high enough electric field, will lead to a non-negligible non-linear response in the polarization of the medium. Among other possible phenomena, this polarization term will lead to the generation of two additional frequencies, called signal and idler, that follow the rules of energy and momentum conservation, such that:

$$\omega_{pump} = \omega_{idler} + \omega_{signal} \quad (2.5)$$

$$\vec{k}_{pump} = \vec{k}_{idler} + \vec{k}_{signal} \quad (2.6)$$

These two equations, that must be observed in order for SPDC to happen, are referred to as phase-matching conditions.

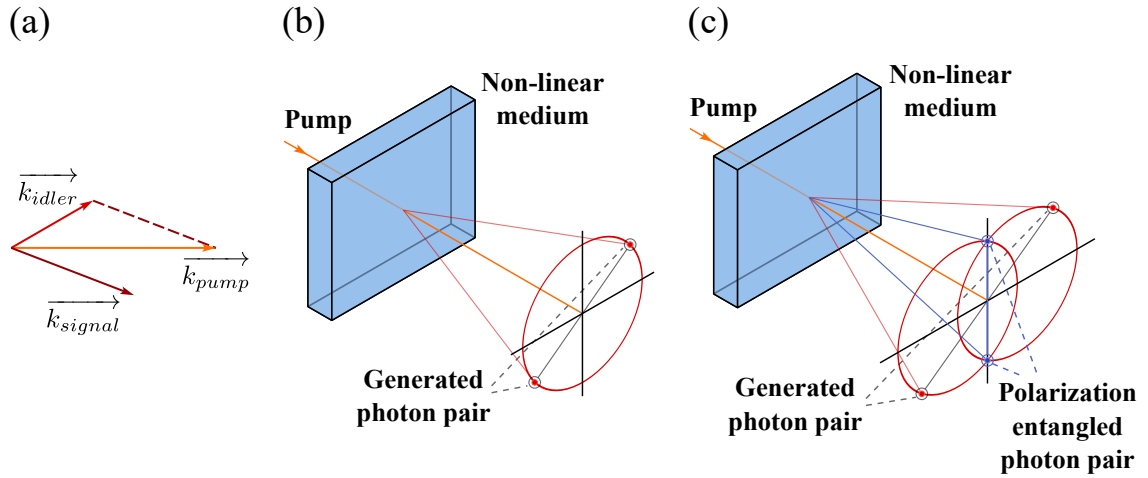


FIGURE 2.4: In order to meet the rules of energy and momentum conservation, it's possible to make use of different types of phase-matching: (b) type I and (c) type II. In both cases, photon pairs are generated on opposites sides of the pattern in order to meet the momentum conservation shown in (a).

In order for equation 2.6 to be true, we need to have $k_{pump} \leq k_{idler} + k_{signal}$ (see figure 2.4 (a)) or equivalently $n_{pump}\omega_{pump} \leq n_{idler}\omega_{idler} + n_{signal}\omega_{signal}$. This condition is impossible to meet for most materials, which possess normal dispersion, i.e. a refractive index that increases with frequency. Therefore, it's standard to use birefringent crystals, such as BBO crystals, in order to achieve phase matching. This is done by making use of the medium's refractive index dependence on polarization and on angle between propagation direction and the crystal's optical axis. Depending on the parameters chosen, there can be different types of phase-matching: type I, when the signal and idler photons have the same polarization (orthogonal to the pump), or type II, when the signal and idler photons have perpendicular polarizations (one aligned and the other orthogonal to the pump) [5, 13, 15]. Due to the dependence of the refractive index on polarization, each type of phase matching has its own characteristic pattern emission, as shown in figure 2.4. For some applications the choice of phase-matching type can be relevant, as one can obtain a polarization entangled pair of photons on the intersection of the emission cones of type II phase-matching [13], as shown in figure 2.4 (c). Less common is the type 0 phase-matching where all polarizations are collinear, which is only possible in appropriately engineered media[5].

For the purpose of constructing a single-photon source, we have to account for the fact that SPDC is a probabilistic process, namely one that follows a Poissonian distribution [13, 14], hence that the probability of either zero or multi photon emission is non zero. This means that, to reduce multi photon probability, we have to also lower the process efficiency.

In practice, this leads to only 1 in about 10^9 or 10^{10} pump photons actually undergoing SPDC [7]. In spite of that, SPDC is still one of the most popular ways to achieve single photon sources, as it's one of the more reliable means to generate entangled photons and despite the low efficiency it still achieves rates of 2 MHz [7].

Four-wave mixing

Four-wave mixing (FWM) is a nonlinear process, similar to SPDC, except it occurs due to the third-order term of the susceptibility, $\chi^{(3)}$, instead of the second. In this case, a signal and an idler photon are generated by annihilation of two pump photons of either different (non-degenerate) or equal (degenerate) wavelengths. Like SPDC, this process relies on the fulfillment of phase matching conditions. The main advantage of FWM is its availability within optical fibers, allowing it to produce photons within a single spacial mode, thus improving the coupling to photodetectors and making it compatible with existing telecom systems. The topic of quantum photon sources based on FWM will be expanded on Chapter 3.

2.5 Conclusions

The last few decades has seen incredible developments in the application of quantum physics to new technologies in the areas of information systems and metrology. Quantum photons sources are an important asset in such emerging fields. In this chapter we reviewed some of the main applications of quantum-photon sources, with special attention to its use in QKD, we discussed the fundamental theoretical points and experimental methods to characterize them, and finally, described the main types of sources currently available, within their two principal availability-based classes: deterministic and probabilistic.

As the future of quantum photons is concerned, the flexibility provided by nano-engineering of quantum dots seem to make one the most promising types sources. On the other hand, SPDC remains the main force of quantum photon generation [2], due to its relatively simple implementation in comparison to its deterministic counterparts. Finally, efforts towards scalable and more compact devices have renewed interest in fiber and silicon waveguide FWM sources, as well as continued interest in QDs, and away from bulk based SPDC sources.

Chapter 3

Four-wave mixing for use in quantum sources

3.1 Introduction

The process of four-wave mixing (FWM) can be either useful or harmful depending on the implementation. While it can induce crosstalk in communications systems with waveguide division multiplexing (WDM), thus negatively affecting the system, it can also be employed in applications such as signal amplification, wavelength conversion, channel demultiplexing, pulse generation, among many others [16]. In this chapter, however, we are particularly interested in its use for generation of quantum-correlated photon pairs. Accordingly, we first briefly introduce and talk about some of the more important aspects of the FWM process, next we characterize a type of specialty fiber, used in many FWM quantum sources, through the use of stimulated FWM, and finally we describe the use spontaneous FWM in quantum sources of either heralded single-photons or entangled photon-pairs.

3.2 The Four-wave mixing effect

The process of four-wave mixing originates from the third-order term of an optical fiber's susceptibility ($\chi^{(3)}$). If three optical fields co-propagate inside the fiber with frequencies ω_1 , ω_2 and ω_3 , a fourth field will be generated at frequency ω_4 , following the relation $\omega_4 = \pm\omega_1 \pm \omega_2 \pm \omega_3$. While, theoretically, several combinations of plus and minus signs are possible, in practice only combinations of the form $\omega_4 = \omega_1 + \omega_2 - \omega_3$ tend to build up, due to considerations of energy and momentum conservation [17], commonly referred to

as phase-matching requirements. On a more fundamental level, FWM can be understood as the annihilation of two photons of energy $\hbar\omega_1$ and $\hbar\omega_2$, due to scattering processes, and the creation of two new photons of energies $\hbar\omega_3$ and $\hbar\omega_4$ in their place, such that the total energy and momentum is conserved. A special case of FWM occurs when we have two initial optical carriers, instead of three, and the process takes place such that $\omega_1 = \omega_2$. Although originally this process was referred to as three-wave mixing, something which ought to be taken into account when researching older literature, for example [18], this name should be reserved for processes involving $\chi^{(2)}$, and the current accepted terminology is degenerate FWM [16]. Both cases of non-degenerate and degenerate FWM are schematically represented in figures 3.1 (a) and 3.1 (b), respectively. To further add that, the conventional terminology on FWM is to refer to the annihilated photons as *pump* photons, and the created photons as the *signal* and *idler* photons, for both the non-degenerate and degenerate case.

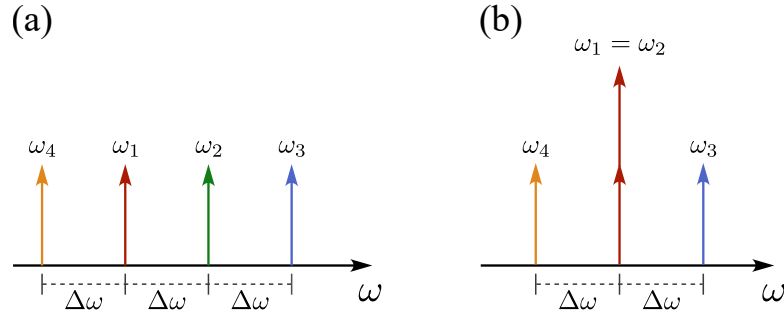


FIGURE 3.1: Schematic representation of the (a) non-degenerate and (b) degenerate FWM process.

Having in mind that the particular process of *degenerate* FWM is the one we are interested on for this study, it will be the one we will refer to, henceforth. Thus, we can now state the phase-matching requirements, in regards to energy conservation:

$$2\omega_p = \omega_s + \omega_i \quad (3.1)$$

and momentum conservation:

$$2\vec{k}_p = \vec{k}_s + \vec{k}_i \quad (3.2)$$

where the subscripts p , s and i refer to the *pump*, *signal* and *idler* photons, respectively.

In order to achieve the phase-matching requirements of equations 3.1 and 3.2 simultaneously, most studies on FWM sources take advantage of waveguide dispersion properties, namely by setting the pump wavelength near the zero-dispersion region of the

waveguide. As most common optical fibers have a zero-dispersion wavelength (ZDW) near 1300 nm, specialty devices are employed, as a way to create photons within the low-loss telecom C-band in the 1550 nm region, such as: photonic crystal fibers (PCF) [19–28], dispersion-shifted fibers (DSF) [29–38] and silicon wire waveguides (SWW) [39–41]. Other methods to achieve phase-matching, that use birefringent fiber properties, though less common, are also employed [42].

Finally we note that, based on the specific implementation, it is possible to obtain either a spontaneous or a stimulated process of FWM [43]. In the stimulated case, the signal wave is sent alongside the pump through the fiber and the FWM takes place as previously described. Conversely, in the spontaneous case, no signal beam is launched in the fiber, and both the signal and idler waves are initially created from noise at frequencies satisfying equation 3.1, and are then subsequently amplified through the regular stimulated FWM case [16]. Consequently, the spontaneous four-wave mixing process (SFWM) emits correlated signal-idler photons over a broad spectrum [16, 21, 28, 43], as represent in figure 3.2(b), and their wavelengths can be select through optical filters.

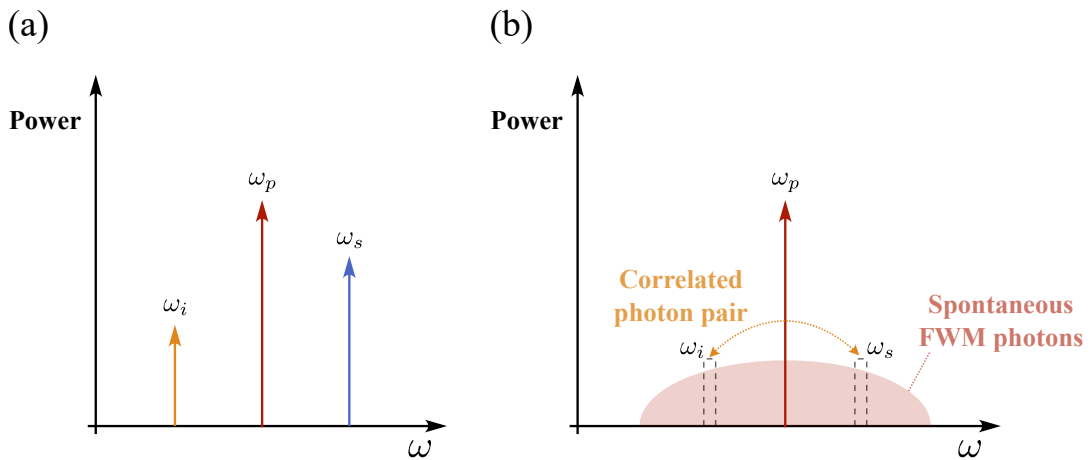


FIGURE 3.2: Schematic representation of the degenerate (a) stimulated and (b) spontaneous FWM process.

3.3 Generation of stimulated FWM using optical fibers

Before we can produce a quantum source using the FWM process, we need to verify and characterize the efficiency of said process in the intended medium, which in our case is a dispersion-shifted highly nonlinear fiber. This type of specialty fiber is produced in order to enhance nonlinear processes, such as FWM, and is dispersion-shifted so that the phase-matching conditions are met in the telecom band, as was discussed in the previous

section. In order to measure the nonlinear characteristics of such fiber, it is possible to use stimulated FWM and, by comparing experimental results with expect theoretical behavior, calculate certain values of the fiber. In this section, we discuss the theory and the experiment of how to perform such measurements, and present our obtained results.

To further note that it is also possible to implement a single-photon source using stimulated FWM [33, 36, 37, 43]. However, even though they have a near unit mean number of photons, they do not present Fock states behavior, such as photon anti-bunching, and have in fact super-Poissonian ($\Delta n^2 > \langle n \rangle$) statistics [43, 44]. Thus, they can be seen as alternatives to weak-coherent laser pulses, which although they still find use in many applications, are not a truly quantum source, as was discussed in section 2.3 of Chapter 2.

3.3.1 Theory

As is derived in appendix A, the power of the generated idler wave is dependent on such characteristics by the relation:

$$P_i(L) = \eta \gamma^2 L_{eff}^2 P_s(0) P_p(0)^2 e^{-\alpha L} \quad (3.3)$$

with

$$L_{eff} = \frac{1 - e^{-\alpha L}}{\alpha} \quad (3.4)$$

being the effective fiber length, $P_p(0)$ and $P_s(0)$ being the input pump and signal powers, respectively, and γ , α and L being the nonlinear parameter, the attenuation coefficient and the length of the fiber, respectively. η is the efficiency of the FWM process, which is given by:

$$\eta = \frac{\alpha^2}{\alpha^2 + \Delta\beta^2} \left\{ 1 + \frac{4e^{-\alpha L} \text{sen}^2(\Delta\beta L/2)}{(1 - e^{-\alpha L})^2} \right\} \quad (3.5)$$

where $\Delta\beta$ is the phase-mismatch, described by

$$\Delta\beta = -\frac{2\pi c \lambda_0^3}{\lambda_p^3 \lambda_s^2} \left. \frac{dD}{d\lambda} \right|_{\lambda_0} (\lambda_p - \lambda_0) (\lambda_s - \lambda_p)^2 \quad (3.6)$$

with λ_0 the zero-dispersion wavelength of the fiber, λ_p and λ_s the pump and signal wavelengths, respectively, and $\left. \frac{dD}{d\lambda} \right|_{\lambda_0}$ the dispersion slope at the ZDW.

Thus, measuring the power output of the idler in relation to the distance between the signal and pump wavelengths, and fitting the obtained data with equations 3.3 to 3.6, we are able to calculate the nonlinear fiber parameter γ , alongside experimental values of the ZDW (λ_0) and attenuation coefficient α .

3.3.2 Experimental Setup

In order to measure the nonlinear characteristics of the fiber utilized, we implemented the experimental setup represented in figure 3.3.

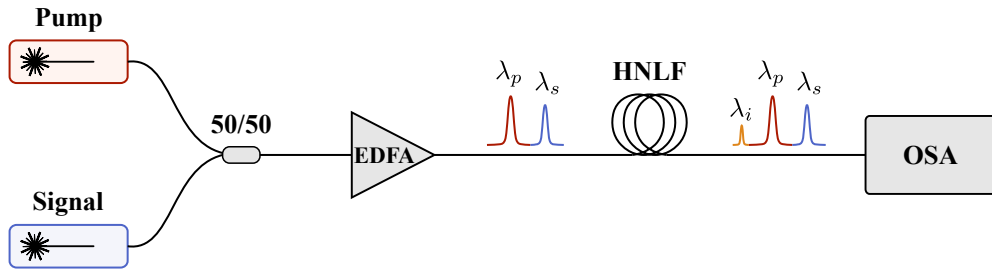


FIGURE 3.3: Experimental setup used in order to obtain stimulated FWM.

It consists of two continuous wave (CW) tunable laser sources, one that is fixed at a set wavelength, corresponding to the pump, and one that is varied, corresponding to the signal. Both waves are then coupled through a 50/50 coupler into an erbium doped fiber amplifier (EDFA). The amplified waves then reach a highly non-linear fiber (HNLF), which is dispersion-shifted as to have a ZDW in the order of ~ 1540 nm. The specifications of the HNLF, given by the manufacturer [45], are represented in table 3.1. Finally, the results are measured with an optical spectrum analyzer (OSA).

TABLE 3.1: Specifications of the HNLF used.

L km	γ (typical) $W^{-1}km^{-1}$	α (typical) km^{-1}	$\frac{dD}{d\lambda}$ $ps.nm^{-2}km^{-1}$	λ_0 nm
1	11.5	0.18	0.019 ± 0.004	~ 1540

3.3.3 Experimental Results

Some of the optical spectra obtained with the OSA are shown in figure 3.4. The slope of the noise floor that can be observed is due to the pump laser used in the experiment, something which was taken into account when analyzing the data. It can also be noted

that, in sub-figures (c) and (d) a fourth peak appears opposite the idler. This is because of a parallel FWM process that occurs, where the wave labeled as signal acts as pump, and the wave labeled as pump act as signal, a process which we disregard for the purpose of our calculations. From the obtained spectra, such as the ones represented in figure 3.4, it is possible acquire the power and wavelengths of the pump, signal and idler waves.

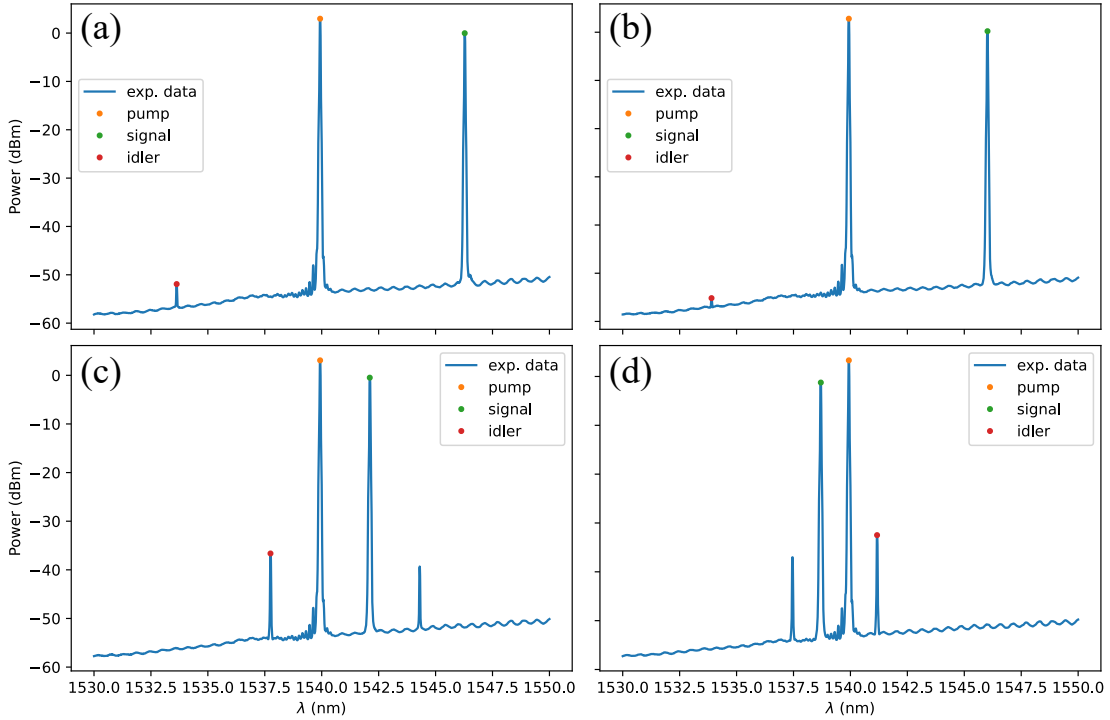


FIGURE 3.4: Some of the experimental optical spectra of stimulated FWM obtained with the OSA, for a pump wavelength of 1539.93 nm and a signal wavelength of (a) 1546.28, (b) 1546.02, (c) 1542.11 and (d) 1538.7 nm

Following, the experimental results for the idler optical power as a function of the difference between the signal and pump wavelengths is represented in figure 3.5. These results were obtained with the pump fixed at 1539.93 nm and the signal varying from ~ 1533 to ~ 1548 nm. The obtained fit of the experimental data is also shown.

To perform the fit a Python script was developed, and the least squares fitting method was utilized, with the variables $k_1 = -L \frac{2\pi c \lambda_0^3}{\lambda_p^3} (\lambda_p - \lambda_0) \frac{dD_c(\lambda_0)}{d\lambda}$, $k_2 = \alpha L$ and $k_3 = (L \gamma P_p(L))^2 P_s(L)$. The equation employed in the fit was modified from eq. 3.3, to use $P_p(L)$ and $P_s(L)$ instead of $P_p(0)$ and $P_s(0)$, using the relation $P_{\{p,s\}}(L) = P_{\{p,s\}}(0) e^{-\alpha L}$, so that we have:

$$P_i(L) = \eta \gamma^2 L_{eff}^2 P_s(L) P_p(L)^2 e^{2\alpha L} \quad (3.7)$$

This was made so the pump and signal waves were measured at the same spot as the idler, seeing that in a practical setting there will be losses, such as at pigtail connections,

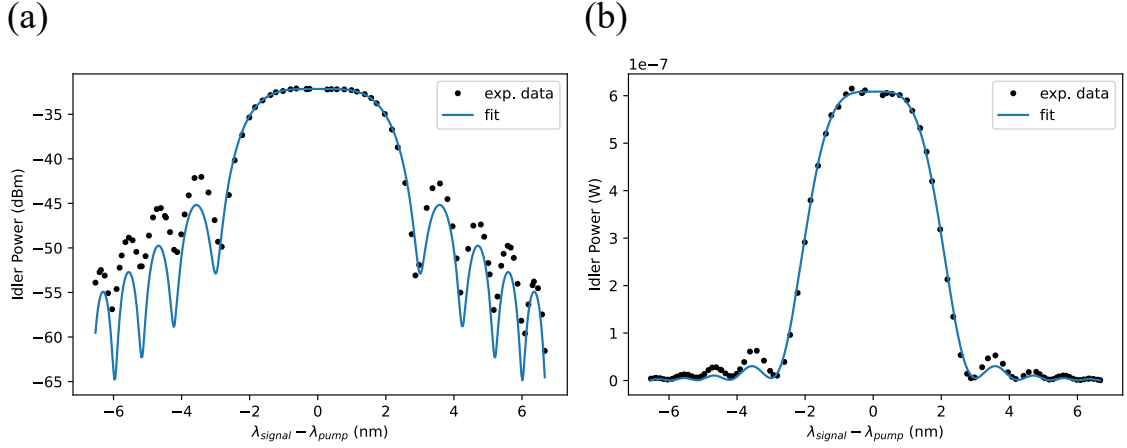


FIGURE 3.5: Experimental results and theoretical fit for the idler optical power, measured in (a) dBm and (b) W, as a function of the distance between signal and pump wavelengths.

that are not accounted by eq. 3.3. Measuring all the powers at the end of the fiber will still result in a overestimated attenuation coefficient, however, all three waves will have suffered the same connection losses and the equality in 3.7 will still be correct. If we had used equation 3.3 instead, and since the experimental measurements of $P_p(0)$ and $P_s(0)$ would have been overvalued, the difference would be absorbed by rest of the right hand factors in eq. 3.3, resulting in an underestimated γ factor. This was verified by comparing the two methods, one using the optical powers measured with, and the other without, the HNLf in figure 3.3, and calculating for the value of γ . The one using the measured values of $P_{\{p,s\}}(L)$ and eq. 3.7 resulted in $\gamma = 9.62 \text{ W}^{-1}\text{km}^{-1}$ and the one using the measured values of $P_{\{p,s\}}(0)$ and eq. 3.3 resulted in $\gamma = 1.39 \text{ W}^{-1}\text{km}^{-1}$, which is a highly significant difference.

The values obtained from the theoretical fit are represented in table 3.2. The reduced χ^2 and the graphics in figure 3.5 indicate a good correspondence between experiment and the theoretical model. The higher than expected values of α are explained, as previously mentioned, by additional sources of loss, such as pigtail connections. In addition, the lower than expected nonlinear coefficient γ , is likely due to the fact that the polarization of the pump and signal waves were not controlled as to be linearly polarized along the same axis, which negatively affects the efficiency of the FWM process [16, 18]. To note that the calculated λ_0 is very close to the pump wavelength, with less than a 5×10^{-5} nm of difference, indicating that the experimental values were obtained well within the validity of the theoretical model used in the fit.

Finally, we note that, despite the low χ^2 and relatively good fit obtained, it is clearly visible in figure 3.5 that the side bands of the measured data are above that of the expected

TABLE 3.2: Values obtained from the theoretical fit

γ $W^{-1}km^{-1}$	α km^{-1}	λ_0 nm	<i>reduced</i> χ^2
9.6 ± 1.8	0.58 ± 0.13	$1539.93005 \pm 1.0 \times 10^{-5}$	1.07×10^{-16}

value. This is quite likely due to the existence of Raman scattering photons, that act as a noise source. This phenomena as been previously reported and studied [46], with several papers having resorted to cooling the optical fiber to lower than 100 K temperatures [35, 38], among other methods [42], in order to reduce this type of noise source.

3.4 Description of FWM quantum sources

As discussed in Chapter 2, FWM can be used in order to produce heralded single photon sources, where the arrival of one photon, from the generated photon pair, is used to herald the arrival of the other, knowledge which is sufficient in some select single photon applications. Other uses of FWM come about in the generation of specific types of entangled photon states, the properties of which are the heart of many applications in quantum information processing [7, 23, 29, 32, 39, 41].

In this section we discuss the basics of how FWM heralded single-photon, and polarization-entangled photon-pair sources are constructed.

3.4.1 Heralded single-photon source

Figure 3.6 shows the basic setup of an SFWM single-photon source, which disregards most of the experimental details, in favor of emphasizing the working concept. In it, pump pulses are sent into a specialty fiber (DSF, PCF, SWW, and others) capable of producing spontaneous FWM, generating signal and idler photons. Next, a pump rejection filter and a demultiplexer, discard the pump and separate the signal and idler wavelength into two distinct paths. Both the signal and idler waves are then measured with two different photodetectors and the obtained values can then be analyzed.

To note that the pump rejection and separation of idler and signal wave are done in free space in most studies [19, 21, 22, 24, 26–28, 30, 40] (though not all [38]), due to the difficulty of finding adequate fiber-based filters/demultiplexers with the necessary sensitivity to assemble the single-photon source.

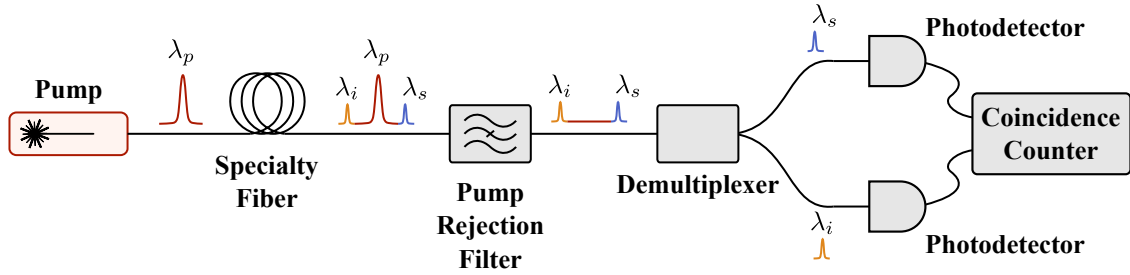


FIGURE 3.6: Basic setup of a single-photon source based on spontaneous FWM

To characterize the obtained source it is straightforward to expand the experiments described in section 2.3 of Chapter 2 to the end of the idler path in figure 3.6. To bear in mind, however, that we are dealing with a *heralded* single-photon source, and that measuring the $g^{(2)}(0)$ on the condition of detecting a signal photon, will yield different results than without any such conditioning. In fact, a study by Goldschmidt *et al.* [21] found both a $g^{(2)}(0) < 1$ and a $g^{(2)}(0) > 1$, for a heralded or unheralded version of the same source, respectively, signifying the fundamentally different nature, quantum and classical, of both versions. This classical behavior of the unheralded source is likely due to the existence of Raman scattering photons, that trigger counts in the idler photodetectors, at times when there are no idler waves reaching them, events which would have been discarded in the heralded version.

3.4.2 Polarization-entangled photon pair source

There are two main schemes for fiber-based generation of polarization entangled photon-pairs: the Sagnac-loop (SL) and the counter-propagating (CP) scheme [47]. The basic setup of the CP based source is represented in figure 3.7. In it a pump pulse, polarized at 45° , is sent to a polarization beam-splitter (PBS), in such a way that it splits into two equal powered pulses, one with horizontal polarization (H) and the other with vertical (V). The two pulses then reach the opposite ends of a specialty fiber appropriate for SFWM generation, and travel through the fiber in opposite directions. The pump pulses, along with the FWM created photons, are then recombined at the PBS, where subsequent filters are used to remove the pump photons. The polarization controller (PC) in the loop is there in order to guarantee the photons remain with their initial polarization, with no undesired rotations.

The FWM process resulting from this configuration can be written as [23]:

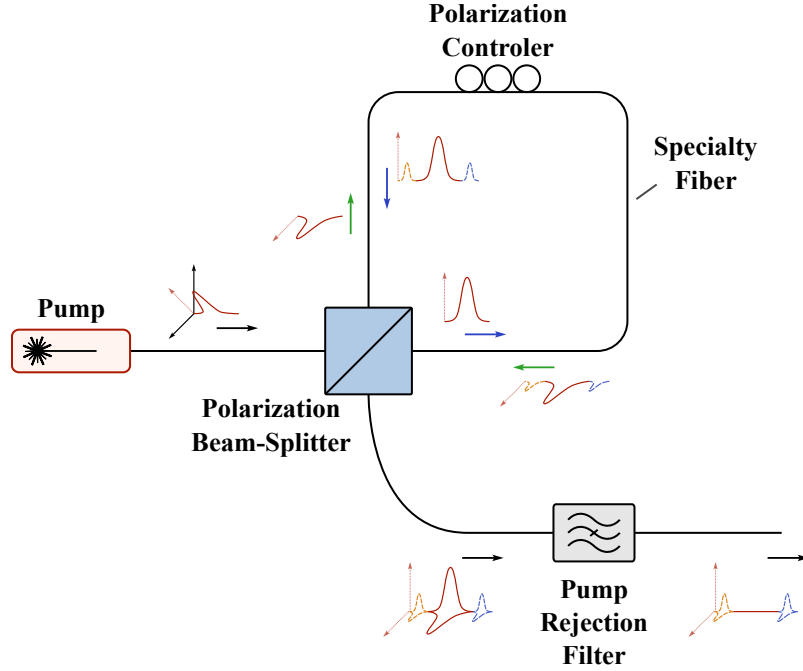


FIGURE 3.7: Basic setup of a polarization-entangled photon-pair source using the counter-propagation scheme.

$$\begin{aligned}
 |\psi\rangle \sim & \sqrt{p(0)} |0_s 0_i\rangle + \sqrt{p(1)} \{ |1_s 1_i\rangle_H |0_s 0_i\rangle_V + |0_s 0_i\rangle_H |1_s 1_i\rangle_V \} \\
 & + \sqrt{p(2)} \{ |2_s 2_i\rangle_H |0_s 0_i\rangle_V + |0_s 0_i\rangle_H |2_s 2_i\rangle_V + |1_s 1_i\rangle_H |1_s 1_i\rangle_V \} + \dots
 \end{aligned} \tag{3.8}$$

where $|n_s n_i\rangle_P$ represents a state of n number of signal-idler pairs being created with P polarization, either horizontal (H) or vertical (V). The probability of multiple photon-pair emission can be effectively suppressed with appropriately chosen small interaction strengths [23], so that the only non-vacuum order term remaining is $|1_s 1_i\rangle_H |0_s 0_i\rangle_V + |0_s 0_i\rangle_H |1_s 1_i\rangle_V$, which can be rewritten as

$$|\psi\rangle = \frac{1}{\sqrt{2}} \{ |H_s H_i\rangle + |V_s V_i\rangle \} \tag{3.9}$$

which is the desired polarization entangled state.

As previously described, other polarization entanglement generation schemes are possible and can be found at [47]. Experiments on the subject have found good agreement between expected entangled photon-pair behavior and that of measured photon-pairs obtain through SFWM [23, 29, 39, 41, 43, 47].

3.5 Conclusions

Single-photon and entangled photon-pair generation are at the center of many cutting edge technologies in the field of quantum information and metrology. The process of four-wave mixing allows for an in-fiber generation of such sources, which can have advantages over its bulk counterparts, such as compatibility with existing telecom systems and low-loss coupling to photodetectors. In this chapter we reviewed the theory of FWM, implemented a stimulated photon source and compared its behavior with the theoretical expectation, managing to obtain a fit with a reduced χ^2 of 1.07×10^{-16} , and, finally, described the working concepts of both a single-photon and an entangled photon-pair source based on spontaneous FWM.

Having proven the successful generation of idler photons, with the HNLF in the laboratory, we hope to assemble the sources described in section 3.4 during future work.

Chapter 4

Characterization and modeling of an optical receiver

4.1 Introduction

Since the introduction of the first QKD protocol by Bennett and Brassard in 1984 ([8]), various other protocols have been proposed, which can be classified in two main classes: discrete variable (DV-QKD) and continuous variable (CV-QKD). [48–51] As the name suggests, discrete variable QKD protocols encode their information on discrete variables of a quantum state, such as the polarization or the phase of a single-photon. A brief overview of such a protocol has been previously discussed on Chapter 2. For this chapter, however, we are interested in CV-QKD, which encodes information in continuous quantum variables, such as the quadrature components of coherent states [50, 52]. From an experimental point of view, a major advantage of CV-QKD, is that they require only standard telecommunication technology, employing, for example, coherent detection techniques already widely adopted in classical optics [52, 53].

In order to deploy such protocols, however, accurate descriptions of the various noise sources involved need to be developed [48, 49, 51]. It is with this in mind, that in this chapter, we focus our attention on the modeling and experimental characterization of an optical receiver.

Accordingly, in the rest of this chapter, we first briefly discuss some topics related to CV-QKD, we then establish a theoretical model of the optical receiver we want to study, next present the experimental results of that study, and finally, we present the main takeaways and conclusions of this work.

4.2 Continuous variable QKD

All CV-QKD protocols encode information in the quadratures of the quantized electromagnetic field [52]. Therefore, we first succinctly introduce the concept of field quadratures and their relation to the classical electrical field.

4.2.1 Coherent states and field quadratures

We begin by considering a plane-polarized classical monochromatic wave, enclosed within an empty cavity of dimension L , whose electric field is given by [54]

$$E_x(z, t) = E_0 \sin(kz) \sin(\omega t + \phi) \quad (4.1)$$

where E_0 is the amplitude, $k = 2\pi/\lambda$ is the wave vector, ω is the angular frequency and ϕ is a phase factor dependent on initial conditions. By using trigonometric identities we can rewrite equation 4.1 as

$$\begin{aligned} E_x(z, t) &= E_0 \sin(kz) \left[\cos(\phi) \sin(\omega t) + \sin(\phi) \cos(\omega t) \right] \\ &= E_1 \sin(\omega t) + E_2 \cos(\omega t) \end{aligned} \quad (4.2)$$

where

$$E_1 \equiv E_0 \sin(kz) \cos(\phi) \quad (4.3a)$$

$$E_2 \equiv E_0 \sin(kz) \sin(\phi) \quad (4.3b)$$

are referred to as field quadratures. These correspond to two oscillating electric field 90° out of phase with each other. The two field quadratures can be more succinctly described by using the notation of complex field amplitudes, and writing

$$\begin{aligned} E(z) &= E_0 \sin(kz) e^{i\phi} \\ &= E_1 + iE_2 \end{aligned} \quad (4.4)$$

which can be represent in the complex plane. These quadratures of the field can be rewritten, as so they are to the electromagnetic wave equations, as the position and linear momentum are to the harmonic oscillator. This connection between the quadratures of

an electric field and the position and momentum coordinates of an harmonic oscillator, provide the formalism to apply the known quantum theory of a simple harmonic oscillator to electromagnetic waves [54]. The most important result to takeaway, in our case, is that the quantum coherent states $|\alpha\rangle$, first introduced in chapter 2, can be defined as [54]

$$|\alpha\rangle = |X_1 + iX_2\rangle \quad (4.5)$$

where X_1 and X_2 are the dimensionless quadratures of the field.

4.2.2 Principle of CV-QKD with coherent states

The principle of CV-QKD can then function in similar fashion to the way already described in chapter 2. However, instead of coding information in two orthogonal polarization bases, Alice codes in the two quadratures of a coherent state, with Bob measuring randomly either of the quadratures [50]. To note, nonetheless, that other protocols of CV-QKD, with different working concepts do exist (as do other DV-QKD) [50, 52]. Adding still, that the variables that each quadrature can be encoded with are usually continuous in nature, as opposed to the vertical or horizontal polarization for the DV-QKD previously discussed.

4.3 Theoretical model of an optical receiver

The task of an optical receiver is to convert an optical signal into an electrical one, so the data transmitted along the lightwave system can be measured and processed. At the center of such device is a photodetector, whose job it is to covert light into electricity through the photoelectric effect. Ideally, photodetectors should have high sensitivity, fast response times, low noise, low cost, and its size should be compatible with that of a fiber core. Semiconductor photodetectors, most commonly referred to as photodiodes, best meet these requirements, and are therefore the most predominant type of photodetectors. [17, 55, 56]

In this section, we aim to introduce the basic theoretical concepts to model an optical receiver based on a photodiode, namely a PIN photodiode, so we can later characterize it in the laboratory. To accomplish this we first discuss the basic concepts of a photodiode, next we talk about transimpedance amplifiers, used on many photodetectors, including our own, later we examine the noise sources present when performing photodetection, and

lastly, we review two basic schemes for photodetection: direct and balanced photodetection.

4.3.1 Photodiode

PN and PIN photodiodes

The basic structure of a photodiode is a reverse-biased PN junction, as shown in figure 4.1 (a). It consists of two doped semiconductors, a *n-type* with excess of free electrons, and a *p-type* with excess of electron-vacancies or, as their more commonly referred to, “holes”. These two types, when joined together, form a depletion region at the *p-n* junction, that is devoid of charge carriers, and has a large electric field, that opposes flow of electrons from the *n-side* to the *p-side* (or equally, flow of holes from *p* to *n*). The application of a reverse-bias, as shown in figure 4.1, will increase this effect, widening the depletion region and increasing its electric field, \vec{E}_d . If a photon is absorbed in this depletion region, creating an electron-hole pair due to the photoelectric effect, then the subsequent created electron will be accelerated towards the *n-side* and the hole towards the *p-side*, because of \vec{E}_d . This resulting flow of current is proportional to the incident optical power, and thus we conclude that a reverse-biased *p-n* junction can act as photodetector. [17, 55, 56]

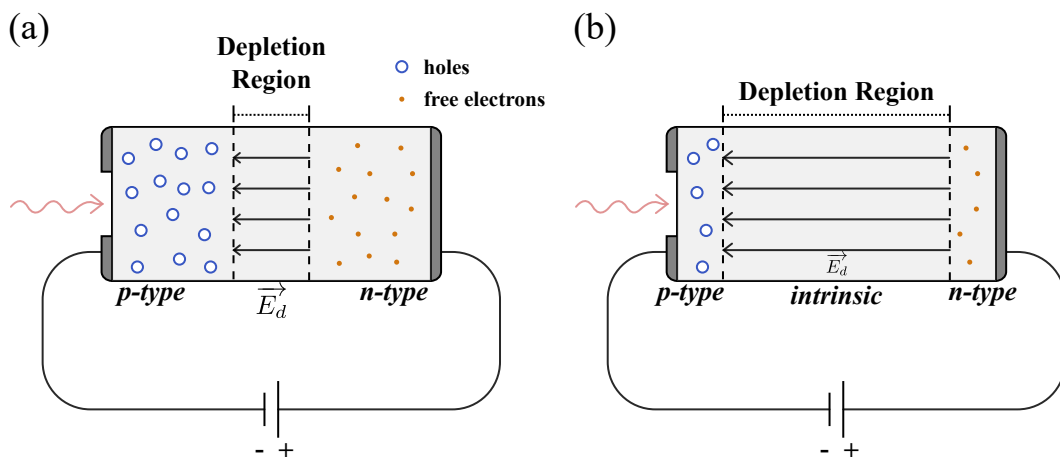


FIGURE 4.1: Schematic representation of a (a) PN and (b) PIN photodiode.

For the previously described process to work well, however, the photon needs to be absorbed in the depletion region, for if the photon is absorbed in the *p* or *n* region, it will not undergo the influence of any electric field and the desired current will not form, as the movement of the hole and electron will be random. The efficiency of the process can then be improved by decreasing the widths of the *p* and *n* side, and increasing the width of

the depletion region, insuring that the majority of photons incident on the photodiode are absorbed inside it. To achieve this, it is possible to insert an undoped, or lightly doped, semiconductor layer between the p - n junction, as represented in figure 4.1 (b). Since the middle layer is constituted by intrinsic, or nearly intrinsic, material, this structure is referred to as a p - i - n (or PIN) photodiode. [17, 55, 56]

Quantum Efficiency and Responsivity

As previously stated, the photocurrent, I_p , generated on a photodiode is directly proportional to the incident optical power, P_{in} , such as

$$I_p = RP_{in} \quad (4.6)$$

where R is the proportionality constant, measured in A/W , and referred to as the *responsivity* of the photodetector. The responsivity can also be expressed in terms of the *quantum efficiency*, η , a fundamental quantity defined as

$$\eta = \frac{\text{electron generation rate}}{\text{photon incidence rate}} = \frac{I_p/q}{P_{in}/h\nu} \quad (4.7)$$

where q is the charge of a single electron, and $h\nu$ the energy of a single photon with frequency ν . From equations 4.6 and 4.7 we can get the relation between the responsivity and the quantum efficiency as

$$R = \eta \frac{q}{h\nu} = \eta \frac{q\lambda}{hc} \quad (4.8)$$

where the relation $\nu = c/\lambda$ was used.

Bandwidth

The *bandwidth* of a photodiode is determined by the speed at which it responds to variations in the incident optical power [17]. This speed is limited by the time taken by electrons and holes to travel to the electrical contacts (the transit time) and on the response time of the electrical circuit used to process the current (the time constant of the equivalent electrical circuit) [17, 57].

To analyze the electrical properties of the photodiode, we consider the equivalent circuit of the photodiode used in the laboratory, represented in figure 4.2 (a), adapted from data given by the manufacturer [58]. It consists of a current source, I_p , in series with a

resistance R_s , and in parallel with a junction capacitance C_j , and a shunt resistance R_j . R_L represents the load resistance from the external circuit. The series resistance R_s depicts the resistance of the semiconductor material, and is usually low enough that it can be ignored. Additionally, the shunt resistance R_j represents the resistance of the photodiode junction at zero bias, and for an ideal case, is infinite. Although, for practical cases this is obviously not the case, with R_j in the order of $10\text{ M}\Omega$ for our photodiode [58], this is sufficiently high enough, compared to the load resistance ($R_L = 50\text{ M}\Omega$), that it can be ignored. Thus, we can have a simplified photodiode circuit, as is represented in figure 4.2 (b), consisting of a simple RC circuit with $R = R_L$ and $C = C_j$, where the (3 dB) cut-off frequency is [59]

$$f_{c,RC} = \frac{1}{2\pi R_L C_j} \quad (4.9)$$

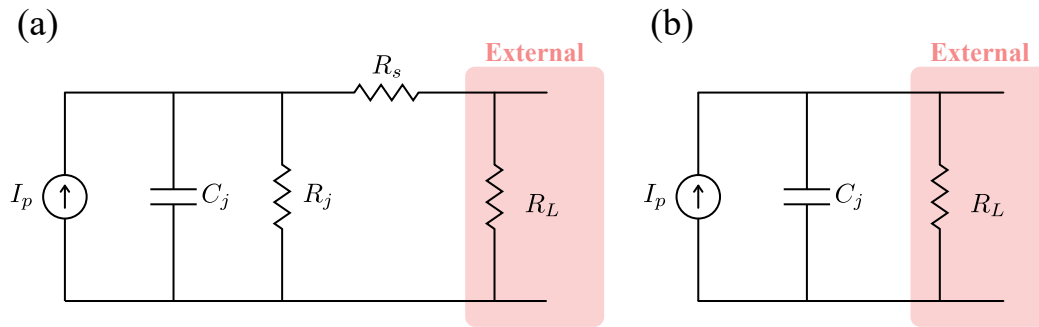


FIGURE 4.2: (a) Schematic representation of a photodiode equivalent circuit, adapted from [58], and (b) its simplified form

The bandwidth of a photodetector can then be approximated in a similar manner as that of a RC circuit, with a cut-off frequency given by [17]

$$f_c = \frac{1}{2\pi (\tau_{tr} + \tau_{RC})} \quad (4.10)$$

where τ_{tr} is the transit time and τ_{RC} is time constant of the equivalent RC circuit equal to $R_L C_j$.

4.3.2 Transimpedance Amplifier

A transimpedance amplifier (TiA) is an electronic component which converts currents to voltages, with a certain gain G , measured in V/A , such that we have

$$V_p = G I_p \quad (4.11)$$

With this in mind, we can now consider the totality of the optical receiver we propose to study, schematically represented in figure 4.3. It consists of two photodiodes and a transimpedance amplifier that generates an output voltage proportional to the difference between the current of the two photodiodes. Two additional monitors allow to separately measure the inputs of the photodiodes.

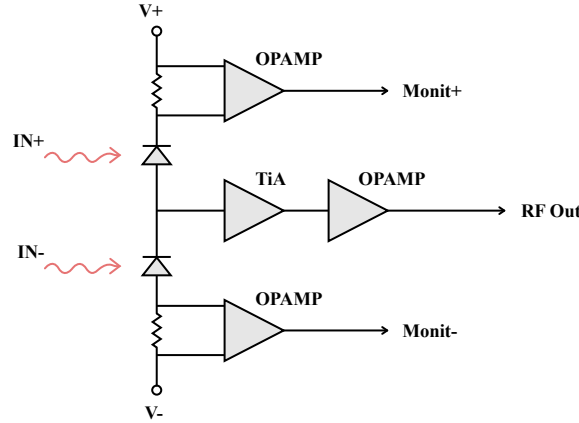


FIGURE 4.3: Schematic representation of the studied optical receiver, adapted from [60].

Considering the basic working concept of our optical receiver, we are now able to discuss the noise sources involved during the photodetection process.

4.3.3 Photodetection noise sources

Thermal noise

Even without any input signal, electrons still move around randomly inside a conductor due to their thermal energy. Mathematically, thermal motion is modeled as fluctuating current that is added to I_p , behaving as a Gaussian random process, independent of frequency, and with zero mean value. Considering the thermal noise generated at the load resistor, we have that its one-sided spectral density is given by [17, 56, 61, 62]

$$S_{th}(f) = \frac{4k_B T}{R_L} \quad (4.12)$$

where k_B is the Boltzmann constant, T is the absolute temperature (in Kelvin) and R_L is the load resistor. The mean square value of this current is thus given by:

$$\langle i_{th}^2 \rangle = \frac{4k_B T}{R_L} \Delta f \quad (4.13)$$

where Δf is the *effective noise bandwidth*. This value is defined as the bandwidth of a brick-wall filter, which would produce the same integrated noise power as that of the actual filter. The determination of the effective noise bandwidth will be discussed later in this section.

Shot noise

Shot noise, also known as quantum noise, is a consequence of the fact that an electric current consists of a discrete stream of electrons generated at random times. This manifests itself as a fluctuation of the electrical current, with Poissonian statistical properties, which can be approximated by Gaussian statistics, whenever the number of electrons is not too small. For a photodiode, its power spectral density can be shown to be given by [17, 56, 59, 61, 62]

$$S_{sh}(f) = 2qRP_{in} \quad (4.14)$$

where q is the charge of one electron. Since, like thermal noise, shot noise is independent of frequency, it is straightforward to calculate its mean square current, thus obtaining:

$$\langle i_{sh}^2 \rangle = 2qRP_{in}\Delta f \quad (4.15)$$

Relative intensity noise (RIN) of the laser

The noise analysis done so far has assumed that the incident optical power on the photodiode does not fluctuate. However, this is not the case, as light emitted by any transmitter exhibits power fluctuations. The effects of these fluctuations can be approximated by [17]

$$\langle i_{RIN}^2 \rangle = 2(RIN)R^2P_{in}^2\Delta f \quad (4.16)$$

where the RIN is the *relative intensity noise* of the transmitter, measured in Hz^{-1} , and is a parameter usually provided by the manufacturer.

TiA noise

Up until now, we have considered the effects of the noise on the photocurrent (I_p) coming out of the photodiode. To consider the effects of noise on the voltage, V_p , we consider the

noise sources to be *independent* random variables, and their contributions to the voltage can be accounted by [63]:

$$\langle v_{noise,1}^2 \rangle + \langle v_{noise,2}^2 \rangle = G^2 \left(\langle i_{noise,1}^2 \rangle + \langle i_{noise,2}^2 \rangle \right) \quad (4.17)$$

given that $v_{noise,x} = G \times i_{noise,x}$.

Furthermore, the transimpedance amplifier will also add its own noise, on top of altering the photodiode's noise sources as described in equation 4.17. The one that is most relevant to consider, is the TiA's thermal noise, and thus, we describe the total thermal mean square voltage, as

$$\langle v_{th}^2 \rangle = G^2 \langle i_{th}^2 \rangle + \langle v_{th,TiA}^2 \rangle \quad (4.18)$$

where $\langle v_{th,TiA}^2 \rangle$ is the TiA contribution. The total effect of thermal noise can be difficult to describe by an neat equation like 4.13, and can, instead, usually be quantified through the *noise-equivalent power* (NEP) [17, 62], a parameter often provided by the manufacturer. To do this, we first consider that the only relevant noise contribution is that of thermal noise, writing the signal-to-noise ratio (SNR), as

$$SNR = \frac{V_p^2}{\langle v_{th}^2 \rangle} = \frac{(GRP_{in})^2}{\langle v_{th}^2 \rangle} \quad (4.19)$$

Considering the definition of NEP as the minimum input optical power necessary to produce a signal-to-noise ratio equal to 1, in 1 Hz of output bandwidth [17, 62, 64], we can write

$$NEP = \frac{P_{in,SNR=1}}{\sqrt{\Delta f}} = \frac{\sqrt{\langle v_{th}^2 \rangle}}{GR\sqrt{\Delta f}} \quad (4.20)$$

From equation 4.20 it is straightforward to get

$$\langle v_{th}^2 \rangle = [(NEP) GR]^2 \Delta f \quad (4.21)$$

Effective noise bandwidth

Although the effective noise bandwidth often used in calculations is approximated by the conventional 3-dB bandwidth, this is technically not correct, and may lead to incongruous results [59]. Consulting the manual for the optical receiver in study [60], its frequency response resembles that of a third-order low-pass Butterworth filter. For this type of filter,

the relation between the effective noise bandwidth and the conventional 3-dB bandwidth, is given by [59]:

$$\Delta f = 1.15f_{BW,3dB} \quad (4.22)$$

4.3.4 Detection scheme

Direct detection

In the direct detection scheme only one PIN photodiode of the optical receiver (see figure 4.3) is used, with the signal being measured in the difference channel (*RF Out*). It is then simple to obtain the formulas for the output average power, and noise variance, as

$$V_p = GRP_{in} \quad (4.23)$$

$$\begin{aligned} \sigma^2 &= \langle v_{th}^2 \rangle + G^2 \left(\langle i_{sh}^2 \rangle + \langle i_{RIN}^2 \rangle \right) \\ &= \Delta f G^2 \left[(NEP)^2 R^2 + 2qRP_{in} + 2(RIN)R^2P_{in}^2 \right] \end{aligned} \quad (4.24)$$

To note that, even though only one PIN is receiving a signal, the term $\langle v_{th}^2 \rangle$ still includes the thermal noise of both PINs, as well as of the TiA. This happens as we are measuring the signal on RF OUTPUT, which evaluates the input difference between both PINs.

Balanced detection

In the balanced detection scheme, a signal is sent to a 50/50 beam-splitter, and the two resulting branches are sent, one each, to the two PINs of the optical receiver. The measurements are once again performed on the difference output channel, *RF Out*.

The advantage of this scheme, is that it allows to distinguish between quantum noise (shot noise) and classical optical noise [65]. Since the classical noise sent to both inputs through the beam-splitter is *correlated* and equal in power, when they are subtracted at the optical receiver, they end up canceling each other out. For quantum noise, however, the two photocurrents are *not correlated*, and the respective noise variances are added to each other, even if the signals themselves are subtracted. [65]

Therefore, we have that the expected average power and noise variance, in this scheme, are

$$V_p = 0 \quad (4.25)$$

$$\sigma^2 = \langle v_{th}^2 \rangle + G^2 \left(\langle i_{sh,+}^2 \rangle + \langle i_{sh,-}^2 \rangle \right) \quad (4.26)$$

where $\langle i_{sh,+}^2 \rangle$ and $\langle i_{sh,-}^2 \rangle$ represents the shot noise corresponding to PIN+ and PIN-, respectively. Since the photocurrents need to be properly balanced to achieve $V_p = 0$, i.e $R_+ P_{in,+} = R_- P_{in,-}$, equation 4.26 can be reduced to

$$\begin{aligned} \sigma^2 &= \langle v_{th}^2 \rangle + 2G^2 \langle i_{sh,+}^2 \rangle \\ &= \Delta f G^2 \left[(NEP)^2 R^2 + 4q R_+ P_{in,+} \right] \end{aligned} \quad (4.27)$$

4.4 Experimental characterization of an optical receiver

4.4.1 Experimental Setup

The setup used in the laboratory is represented in figure 4.4. It consists mainly of a continuous wave laser at 1550.92 nm, a variable optical attenuator (VOA), a spectral filter to remove the laser's side-band frequencies, a 50/50 beam-splitter, the optical receiver we want to characterize, and an oscilloscope to read the receiver's outputs. The optical receiver possesses two inputs: *IN+* and *IN-*, and three outputs: two monitors, *Monit+* and *Monit-*, showing the average measured voltage of their respective input, and *RF Out*, showing a voltage proportional to the difference between the *IN+* and *IN-* photocurrents. Depending on whether we were measuring in the direct or balanced scheme, only one or both inputs of the receiver was used, respectively. Furthermore, in the balanced scheme, in order to ensure both outputs were properly balanced, with the two measured average powers canceling each other, an additional optical attenuator was introduced in the highest powered path (shown in figure 4.4 in dashed lines). Although, it was not used for the average voltage measurements, a DC Block (8535 Inmet RF DC Block) after *RF Out* was employed for noise variance measurements (also shown in dashed lines in figure 4.4). All measurements were performed using *RF Out*, as it the best suited output to do so [60], with the monitors only being used to ensure that both input photocurrents were equal during the balanced detection scheme. The VOA was used to change the incident power

in the beam-splitter and an optical power meter was used to calibrate the power in the photodiode input in relation to the power measured in the VOA.

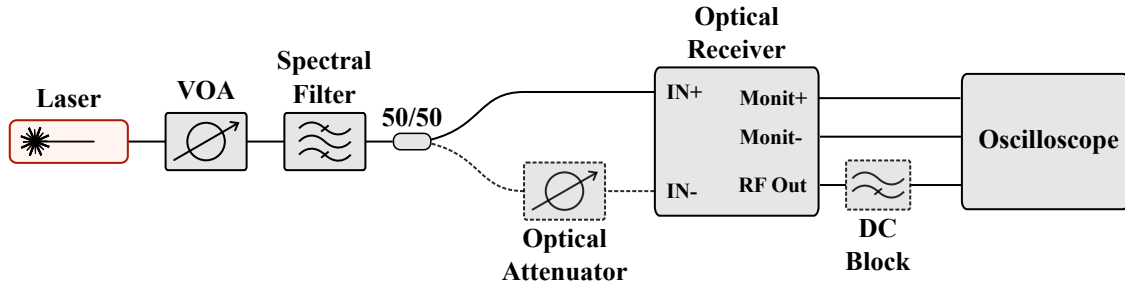


FIGURE 4.4: Experimental setup used to characterize a PIN photodetector.

The optical receiver characterized was a *Thorlabs* PDB450C balanced amplified photodetector, whose main specifications are represented in table 4.1 ([60]). The oscilloscope utilized was a PicoScope 6403D, that digitized the signals and allowed them to be processed on the computer. For each power level incident on the optical receiver, 100 waveforms were obtained using the PicoScope. A Matlab script subsequently joined all samples in a continuous wave, with caution to correct the small shift observed in each average power. This was done by calculating the global average and centering all the waveforms accordingly. Finally, we add that the oscilloscope measurements were made in the $50\ \Omega$ DC mode, and that the RIN of the laser used was $-145\ \text{dB/Hz}$ [66].

TABLE 4.1: Specifications of the optical receiver used.

Max. R (typical)	G (for $R_L = 50\Omega$)	f_{BW} (-3 dB)	Min. NEP
A/W	V/A	MHz	$\text{pW}/\sqrt{\text{Hz}}$
1.0	0.5×10^4	45	14.9

4.4.2 Experimental Results

The results obtained for the measurements of average power and noise variance in the direct detection scheme, and of the noise variance in the balanced detection scheme, are represented in figure 4.5. A linear fit to the average power in the direct detection scheme and to the noise variance in the balanced scheme, was calculated, as well as, a quadratic fit to the noise variance in the direct detection scheme. The expected behavior, showed in dashed green lines in figure 4.5, was obtained from the theoretical formulas specified in section 4.3, and the values from the equipment's data-sheets, shown in subsection 4.4.1. The calculated values for the fit and theoretical curves are shown in Appendix B.

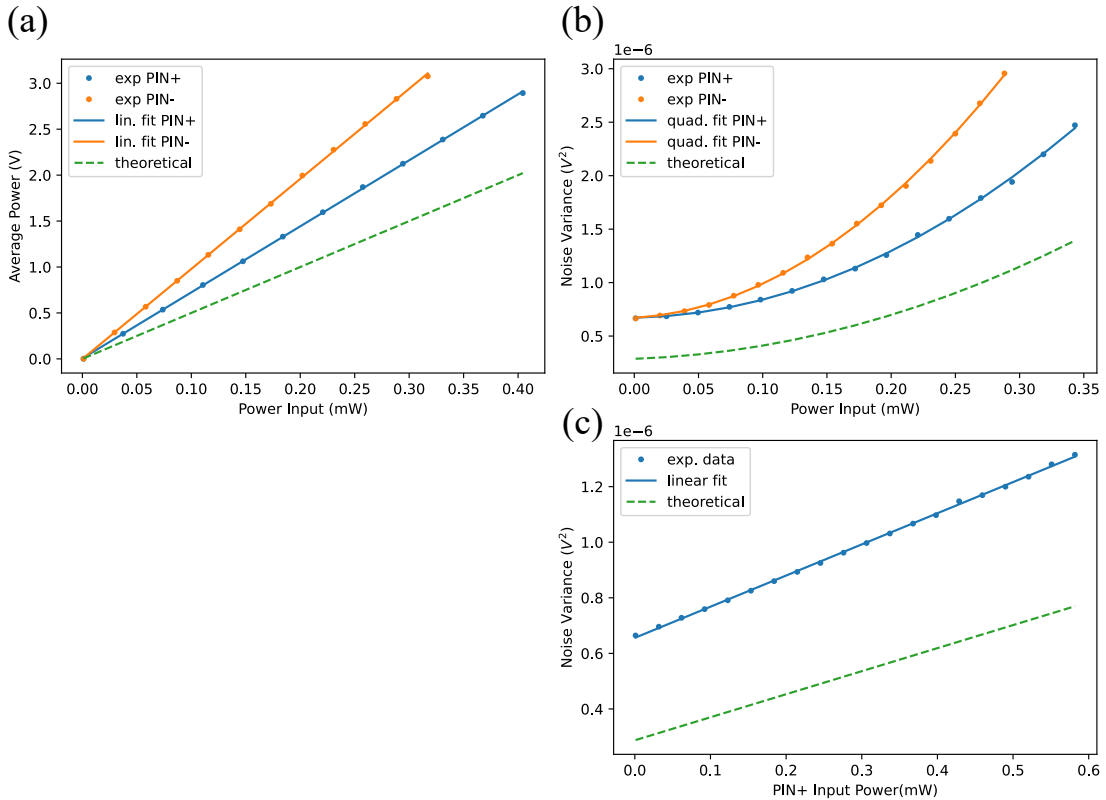


FIGURE 4.5: Experimental results for the (a) average power and (b) noise variance in the direct detection scheme, and the (c) noise variance in the balanced detection scheme. The linear fits, for (a) and (c), and quadratic fit, for (b), of the obtained data are also shown. The theoretical predictions, using the formulas specified in section 4.3 and the values from the equipment data-sheets, are shown in a dashed green line.

As it can be observed, although the qualitative behavior measured was similar to expected, i.e. linear in figures 4.5 (a) and (c), and quadratic for 4.5 (b), the actual quantitative values are noticeably off.

The first observation is that the thermal noise (the y-intersect in fig. 4.5 (b) and (c)) is underestimated. This is not surprising considering that the NEP value supplied by the manufacturer, from which the thermal noise was calculated, was only meant as a minimum possible value [60].

The second noticeable observation, is that, despite the PINs being reported to be similar in order to achieve balanced detection [60], this is clearly not found in the results. To note as well, that throughout this work, the conversion gains obtained, especially for *PIN+*, were not consistent. This is explained, in large part, because the photodiodes of the optical receiver are mounted in such a way that the gap between the protective diode glass and the fiber tip is as small as possible [60]. This led, on one occasion, to the protective glass of one of the detectors breaking due to the pressure of the pigtail connector's tip, and subsequently, the corresponding PIN becoming unable to read any signal. Although

the results shown here were obtained with a different optical receiver, the protective glass was found to be highly sensitive to pressure, and small abrasions and scratches to the glass are likely to have occurred, quite possibly originating a source of loss to the input signal. As a precaution the pigtailed connectors were not screwed all the way in, possibly causing another source of coupling loss between the fiber and the photodiode.

Lastly, we note that, although the slopes in figure 4.5 (c) are relatively similar, showing a reasonably good prediction of the shot noise behavior, the fit's slope was still obtained with a 35% error in relation to the expected theoretical value.

Despite the quantitative values obtained being far from those expected, the behavior obtained shows good qualitative agreement between experimental data and theoretical model. This implies that the theoretical model is correct, but the values used to calculate it are off. Note, for example, that even if, as previously discussed, there is a coupling loss between the optical fiber and the detector, this can be accounted in the model by considering an *effective* responsivity, which would change only the value of R , but nothing else. In this manner, during the remainder of this section, we assume the theoretical model correct, and calculate the set of parameters that best explains the obtained experimental results.

Improving characterization

Instead of trying to anticipate the value of the thermal noise from the given NEP, this was instead estimated by experimentally averaging several measurements of the noise variance, obtained without any input optical power in both PINs. The acquired value was of $6.581 \times 10^{-7} V^2$.

To further improve characterization of the optical receiver, a new set of parameters, to plug into the theoretical model, were calculated from the obtained experimental fit coefficients. Following, the new gain was calculated as

$$G_{new} = \frac{m_{Bal}}{4q\Delta f m_{Dir+}} \quad (4.28)$$

where m_{Bal} and m_{Dir+} are the slopes obtained in the fits for the noise variance of the balanced detection, and the average power of PIN+ in the direct detection, respectively. The responsivity of each PIN was assumed to be different, and calculated as

$$R_+ = \frac{m_{Dir+}}{G_{new}} \quad (4.29a)$$

$$R_- = \frac{m_{Dir-}}{G_{new}} \quad (4.29b)$$

To obtain the RIN of the laser, its value was calculated for each PIN, and the average between both was taken, such as

$$RIN_+ = \frac{a_{Dir+}}{2\Delta f m_{Dir+}^2} \quad (4.30a)$$

$$RIN_- = \frac{a_{Dir-}}{2\Delta f m_{Dir-}^2} \quad (4.30b)$$

$$RIN = \frac{RIN_+ + RIN_-}{2} \quad (4.30c)$$

where a_{Dir+} and a_{Dir-} are the quadratic coefficients obtain for the fits of the noise variance of the direct detection, in $PIN+$ and $PIN-$, respectively. Of importance to note that, equations 4.28 to 4.30c are all dependent on the effective noise bandwidth Δf in such a way, that changing this value would alter all calculated parameters, but would not affect the resulting curve obtained from the theoretical model. In fact, if we calculate the parameters as is, with a theoretical noise bandwidth of $\Delta f = 1.15 \times 45 \text{ MHz}$, it would result in a quantum efficiency of 1.2 and 1.7 for $PIN+$ and $PIN-$. This result is obviously absurd, as it is not possible to have a quantum efficiency higher than 1. If we consult the data sheet of the optical receiver [60], we can see that the maximum responsivity of $RF \text{ Out}$ is 1 A/W , corresponding to a quantum efficiency of 0.8. Therefore, it was decided that the value of Δf employed would be such that the highest responsivity would equal the value of 1 A/W , so neither photodiode's responsivity would cross this maximum specified value.

The new theoretical curves obtained with this model, alongside the original experimental data, are represented in figure 4.6, with the corresponding values calculated from equations 4.28 to 4.30c, represented in table 4.2.

TABLE 4.2: Parameters calculated from the experimental fits, for $\Delta f=24.824 \text{ MHz}$.

Δf	G	R_+	R_-	RIN
MHz	V/A	A/W	A/W	dB/Hz
24.824	9804 ± 61	0.7330 ± 0.0050	1.0	-142.67 ± 0.15

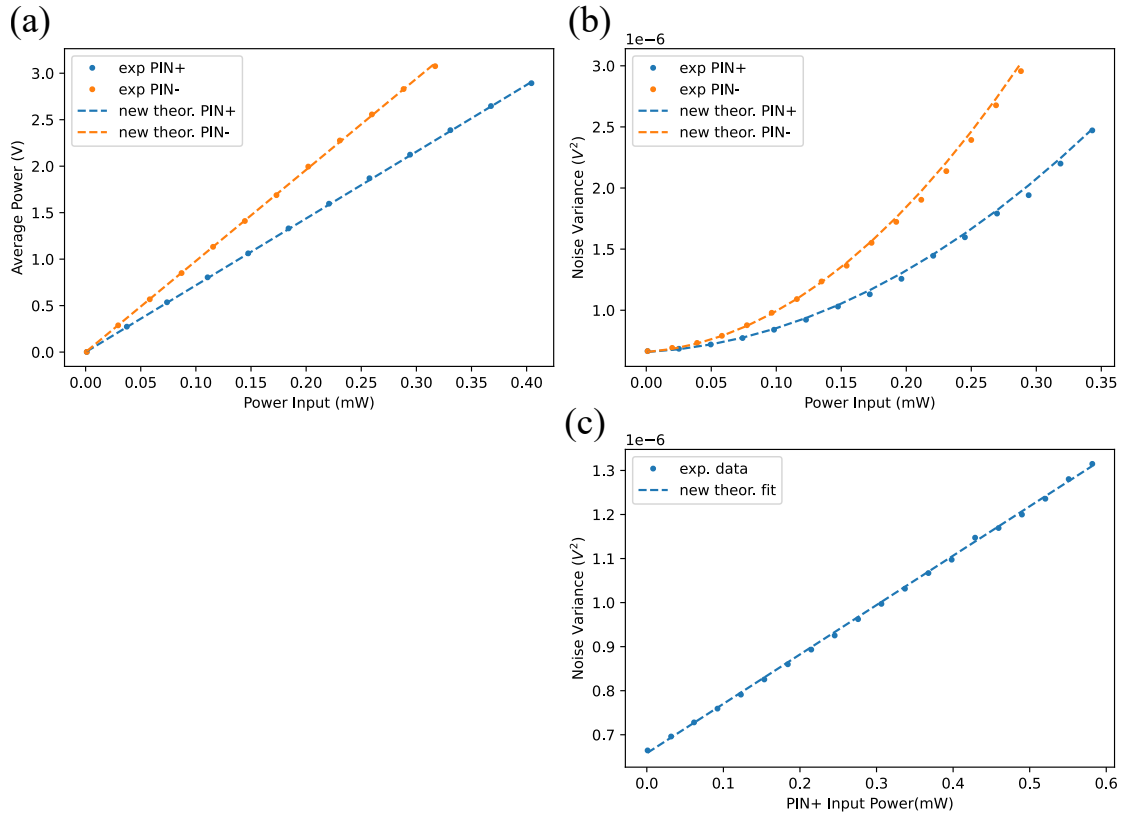


FIGURE 4.6: Experimental results for the (a) average power and (b) noise variance in the direct detection scheme, and the (c) noise variance in the balanced detection scheme. A new theoretical line, using the formulas specified in section 4.3 and the values calculated from the fits, is shown in dashed lines.

As it would be obviously expected, the new theoretical curves better follow the experimental measurements. Interesting to note that, the lowest value of Δf for the responsivity to behave as described in the data-sheet is 24.824 MHz, 48% of the initially expected value of 51.7 MHz. Even relaxing the conditions, as so the quantum efficiency of *PIN-* equals 1, the highest physically allowed value, one obtains a bandwidth of 31.1 MHz. Thus, it is reasonably to conclude that either the theoretical model for the effective noise bandwidth was overestimated, or that its relation to the other values wrongly deduced.

4.5 Conclusions

The introduction of CV-QKD protocols provide a useful alternative approach to the field of quantum cryptography. The proper study and characterization of optical receivers for use in such protocols proves to be a necessary first step for its implementation. In this chapter, we discussed some basic notions related to CV-QKD, developed a theoretical model for an optical receiver and its noise sources, and lastly, presented and analyzed the experimental results of the characterization of such an optical receiver. While we managed to provide

a good qualitative description and an *experimental* model for its behavior, the theoretical predictions were somewhat different from the observed.

For future work, we hope to implement a CV-QKD protocol, using the optical receiver characterized in the laboratory.

Chapter 5

Secure key distribution using a ultra-long fiber laser

5.1 Introduction

Many encryption protocols require the transmission of a secret key between two parties before communication between them can take place. The distribution of this key constitutes one of the weakest links in this type of communication system, and is the driving force for the development of unconditionally secure key distribution schemes based on fundamental properties of quantum mechanics. Although quantum key distribution (QKD) provides theoretically unconditional security, its practical implementation remains technologically challenging and the search for classically based alternatives continues to be relevant.

With this in mind, a system based on a ultra-long fiber laser (UFL) that utilizes standard fiber optic components was proposed by Scheuer *et al.*[67]. This scheme, unlike the ideal implementation of QKD, is not unconditionally secure, relying instead on the technological difficulty of an eavesdropper to get access to the shared key. Such unconditional security has not, however, been a necessary pre-requisite for many encryption schemes, such as public key encoding schemes, which rely on the computational difficulty on part of the eavesdropper, rather than an absolute security proof.

In this chapter we first discuss the principle of operation of the UFL key distribution system, we then expand on the security principles of said system, next we present and analyze the results obtained for our own experimental implementation of the system, and finally, we discuss possible improvements, as well as possible lines of attack, to the protocol, both in general and to our setup in particular.

5.2 Principle of operation

The basic setup for a UFL key distribution system (KDS) is shown in figure 5.1. The scheme consists of a long erbium doped fiber laser that connects two users, Alice and Bob, positioned at opposing sides of the laser. Each user possesses an identical mirror which can be selected to have its peak reflectivity at two different frequencies, which we will call f_0 and f_1 . For the exchange of a single key bit, Alice and Bob choose, randomly and independently, one of these mirror states to reflect at. If both of them make the same choice of mirror state, there will be enough gain in the cavity to surpass the lasing threshold and a clear signal at either f_0 or f_1 will form, thus giving a potential eavesdropper (Eve) an easy access to the arrangement of both mirrors. However, if Alice and Bob choose different mirrors states, only a small signal at $f_c = \frac{1}{2}(f_0 + f_1)$ will develop, and Eve will not be able to easily determine the exact configuration of mirror states used, only that Alice's and Bob's differ from one another. Thus, we can assign, for example, a bit value of '0' to the configuration of $(Alice : f_0; Bob : f_1)$ and a bit value of '1' to the configuration of $(Alice : f_1; Bob : f_0)$, which will allow Alice and Bob, knowing their own mirror state, to deduce the others choice, while preventing Eve getting access to the exchanged key bit. This protocol for key distribution using UFL is summed up in table 5.1.

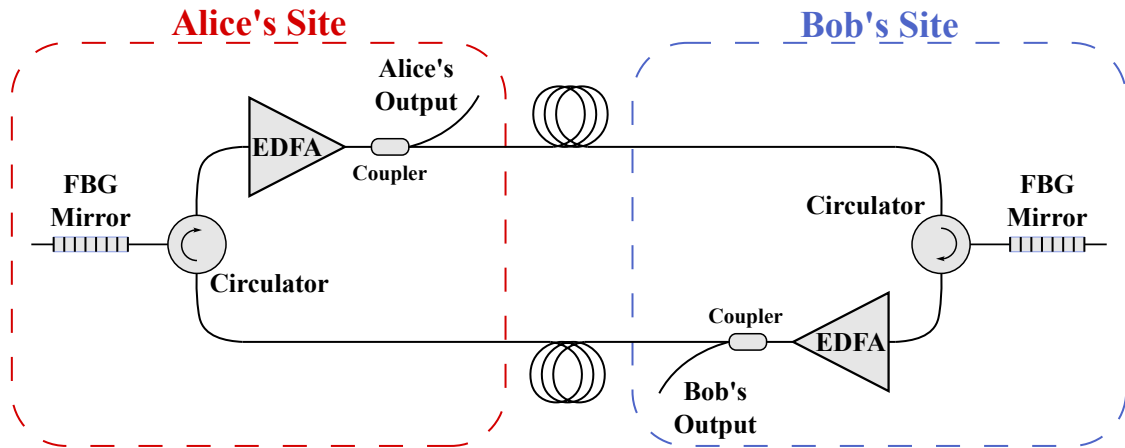









FIGURE 5.1: Schematic setup for secure key distribution using a ultra-long fiber laser.

Different configurations using non-lasing secure states [68] and cavity length variations [69], have been proposed.

TABLE 5.1: Protocol for a key distribution system using a ultra-long fiber laser. Only when Alice and Bob choose different mirror states are the bits kept in order to obtain the sift-key.

Alice's mirror choice	0	0	1	1	1	0	0
Bob's mirror choice	0	1	1	0	1	1	0
System's signal							
Sift-key		0		1		0	

5.3 Security of the system

The security of this system depends on the capacity of Eve to obtain information beyond the correlation of the mirror choices, for which purpose she can deploy either *passive* or *active* attacks [67, 70–72]. *Active* attacks are characterized by the tampering of the cavity by injection of light into it, while *passive* attacks require only the tapping of the optical signal on part of the eavesdropper [71, 72]. In classical based systems *passive* attacks are usually preferred, as they are harder to detect, thus being the focus of most studies on UFL-KDS [67, 68, 70–72]. However, *active* attacks, as well as solutions to them, that exploit the noise levels of the EDFA have been proposed (see [73]). As *passive* attacks are easier to implement experimentally they will, nevertheless, be the focus of this study. *Passive* attacks on UFL systems can further be divided into spectral, temporal or combined attacks [68, 71, 72]. Spectral attacks rely on the analysis of the spectrum of the optical signal at its steady state. This type of attack, with an appropriate choice of filters at the middle frequency f_c , was proven to be largely ineffective, first computationally [67] and then experimentally [70]. Further improvements were made by Kotlicki *et al.* [68] with the introduction of dark-states based UFL, by modifying the setup so that the secure states are below the lasing threshold thus ensuring the spectrum of the secure states to be mostly noise and harder to distinguish between each other. Temporal attacks, on the other hand, rely on monitoring the evolution of the optical field in the cavity over time. Since the secure bits are characterized by the absence of signal built up, it might seem that this type of attack is useless, however, the transition between secure and non-secure states is capable of relaying information on the secure state's mirror choice [68, 71, 72]. As studied in [68], this can be prevented by adding switches to both Alice's and Bob's site that disconnect each user from the main cavity before choosing their respective mirror states. The third class of attacks, a combination of spectral and temporal attacks, is the most difficult to

defend against, relying on the spectral analysis of the residual signal coming from each user's terminal while on a secure state. When this residual signal arrives at the other end of the cavity it is reflected by a mirror at a different frequency thus not allowing the built up of such signature. Nonetheless, it is theoretically possible, following the switch on, for an eavesdropper to get access to the mirror states. To defend against this attack requires lowering the power of the residual signal below the detection capabilities of the adversary. Studies on such attacks [71, 72] obtained a success rate on part of the eavesdropper of $\sim 55\%$ with a signal power of -73 dBm. This result is only marginally better than the ideal case of a 50% success rate, where Eve would randomly guess the secure state's mirror choice.

5.4 Experimental Implementation of a UFL-KDS

5.4.1 Experimental Setup

The experimental setup utilized in the laboratory is shown in figure 5.2 (a). It consists of two separate users, Alice and Bob, each with a fiber Bragg grating (FBG) mounted on a translation stage, allowing for the manual tuning of their peak reflectivity wavelengths by application of mechanical tension. Each user was further equipped with a 99:1 coupler in order to perform measurements on the cavity's signal. The gain of the system was provided by a bidirectional EDFA from *MWTechnologies*, whose internal schematic is depicted in figure 5.2 (b). It consists of two circulators and two conventional EDFAs, i.e. an erbium-doped fiber and a co-directional pump, with each pump being able to be independently controlled by separate voltage sources.

To perform the measurements required for the experiment, an optical spectrum analyzer (OSA) model "AQ6370D" with wavelength range of 600 nm to 1700 nm from *Yokogawa* was used. Time domain measurements were performed with a InGaAs photodetector (model "PDA10CS-EC" from *Thorlabs*) and an oscilloscope (model "TDS1002C-EDU" from *Tektronix*).

5.4.2 Experimental Results

The obtained spectrum of the four possible states of the UFL (read in Alice's output) are depicted in figure 5.3. The pump powers to the EDFA were chosen so the non-secure states were obtained near the lasing threshold. While the spectra for the non-secure

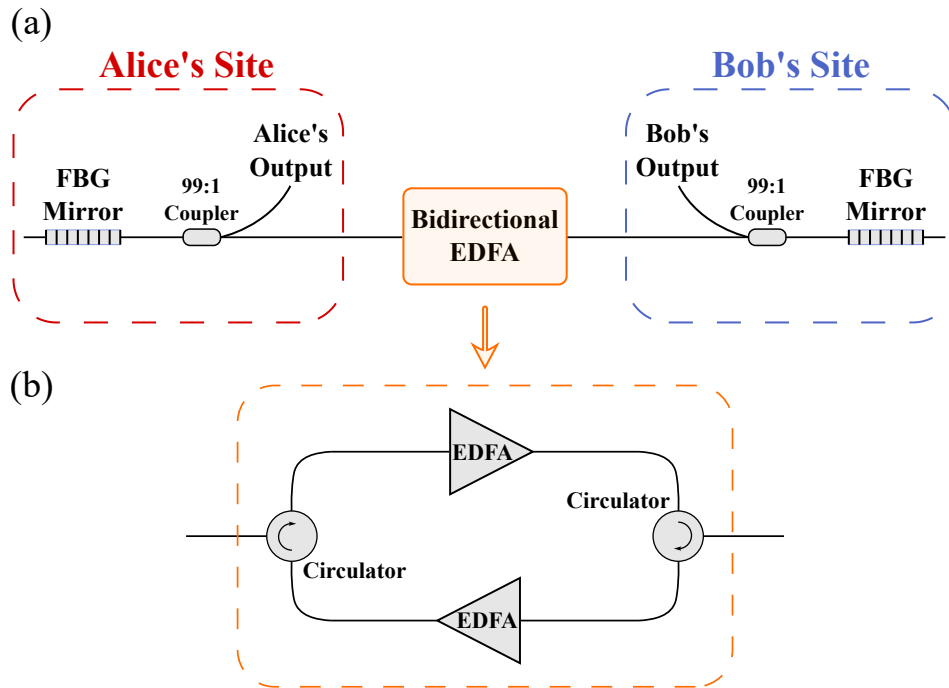


FIGURE 5.2: (a) Lab setup and (b) internal schematic of the bidirectional EDFA utilized.

states presents distinct well defined lasing peaks ($\lambda_{0,0}=1561.098$ nm at -17.703 dBm and $\lambda_{1,1}=1561.484$ nm at -18.280 dBm), the spectra for the secure states, (1,0) and (0,1), resemble optical noise and are thus difficult to distinguish. As expected, Eve would not find it technologically easy to access Alice's and Bob's mirror choice.

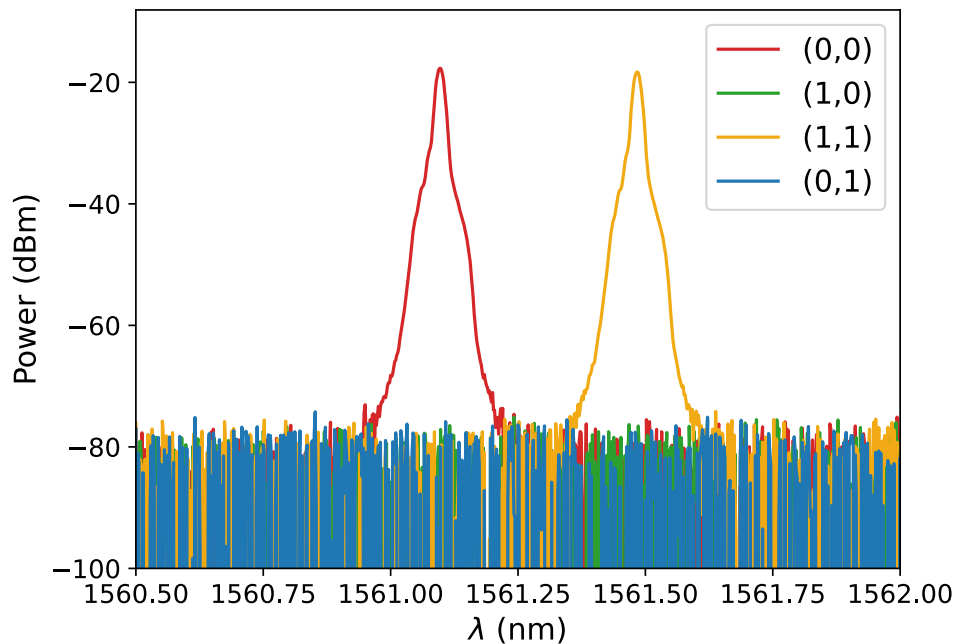


FIGURE 5.3: Optical spectrum of the four states of the UFL-KDS

To study the temporal response of the system, transitions from secure to non-secure states and vice-versa were effectuated and measured with a photodetector and oscilloscope. To counteract the transmission of useful information to Eve that may occur between transitions of mirror state, both pumps of the EDFA were switched off between such transitions. Since no signal travels the fiber when Alice and Bob are choosing their mirror state, a signature of a secure state is less likely to occur on a build-up or a downfall of the cavity's signal. Figure 5.4 shows the transitions between the non-secure state (1,1) and both possible secure states, and vice-versa. As it is possible to observe there is no significant difference between each secure state, thus no useful information is gained by Eve. Similar results were obtained using the (0,0) non-secure state instead of (1,1).

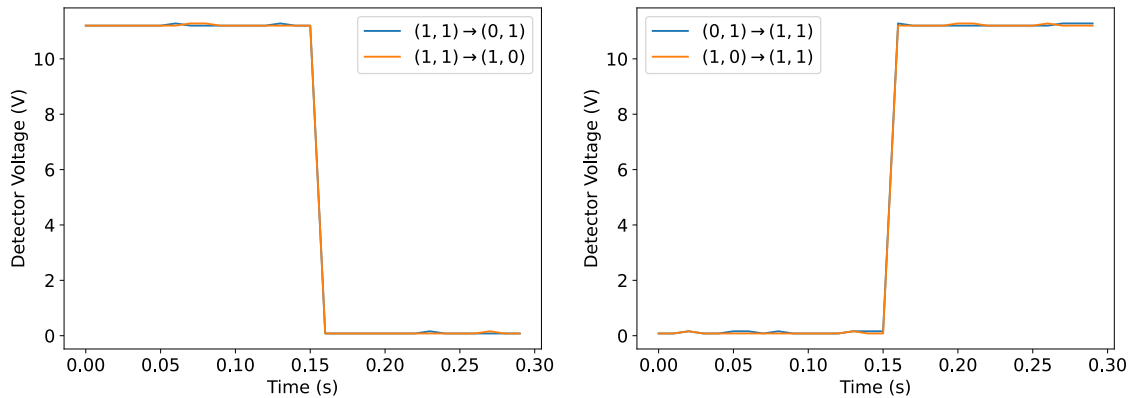


FIGURE 5.4: Cavity signal when transitioning from non-secure to secure states (left) and vice-versa (right)

The study of the spectral temporal response was made by taking advantage of the 0 nm span measurements allowed by the OSA. The results were taken from Alice's output for the signal at $\lambda_{0,0}$ and $\lambda_{1,1}$ between several transitions of UFL states and are represented in figure 5.5. As mentioned before the pumps of the EDFA were switched off between transitions and the graphics of figure 5.5 were obtained as follows: between 0 and ~ 200 time units the UFL was in a non-secure state, between ~ 200 and ~ 400 the pumps were switched off and the peak reflectivity of one of the FBG mirrors was switched, between ~ 400 and ~ 600 the pumps were turned on and thus the UFL is in a secure state, between ~ 600 and ~ 800 the pumps were again switched off and the relevant FBG mirror was switched back to its initial state and finally, from ~ 800 to ~ 1000 , the pumps were switched on and the UFL is back to its original non-secure state.

Seeing that the results of figure 5.5 were taken at Alice's terminal, it would be necessary to read the residual signal filtered through her FBG for these measurements to be useful to Eve. In other words, the signal measured at λ_A needs to be greater than at λ_B for the

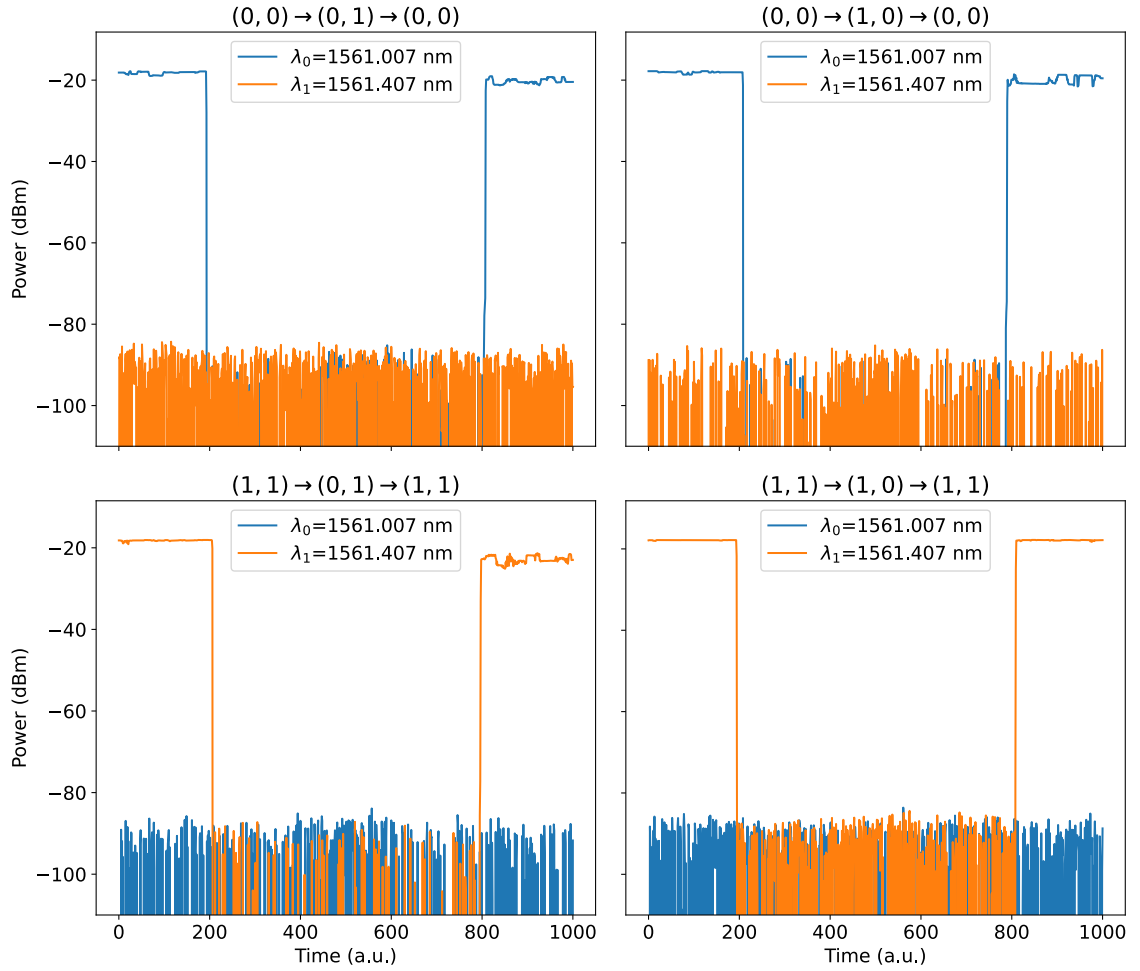


FIGURE 5.5: Cavity signal filtered at λ_0 and λ_1 for the transitions: $(0,0) \rightarrow (0,1) \rightarrow (0,0)$ (top left), $(0,0) \rightarrow (1,0) \rightarrow (0,0)$ (top right), $(1,1) \rightarrow (0,1) \rightarrow (1,1)$ (bottom left) and $(1,1) \rightarrow (1,0) \rightarrow (1,1)$ (bottom right).

system in a state (A, B) , with $A, B \in \{0,1\}$. As it can be observed the power level of the secure states is similar to the optical noise of the system and therefore hard to differentiate.

5.5 Discussion

5.5.1 Improvements to the system

The setup tested was reliant on a manually tuned translation staged, thus severely limited on the achievable bit-rates. In order to make a practical KDS system it is necessary to automate the system by, for example, mounting the FBGs on piezoelectric controlled stages. This type of setup allowed to achieve bit-rates of 500 bps (0.002 s per bit) by Kotlicki *et al.* [68] and of 100 bps (0.01 s per bit) by El-Taher *et al.* [71]. As desirable as increasing bit-rates is, both to generally speed up the process and to give Eve less time to measure the cavity signal, they are limited by the time required by Alice and Bob to identify the

UFL state. That means the signal has to have enough time to pass through both mirrors, and build up to a level capable of distinguishing a lasing from a non-lasing state. This translates to approximately 1.5 round trips [68], which results in a maximum frequency of

$$f = \frac{c}{3dn} \text{ bps} \quad (5.1)$$

where d is the length of the link and n the refractive index of the fiber. This gives a maximum frequency in the order of 10^2 bps for a 100 km long link. Furthermore, the efficiency of a basic UFL protocol is only half of the total rate, as on average the number of secure bits sent will only be half of the total number. To address this relatively low effective bit-rate, modifications to the basic protocol have been proposed and numerically tested by Bar-Lev *et al.* [74]. The simplest one, in terms of implementation, is to use wavelength division multiplexing (WDM) to run multiple UFL channels each with a distinct central frequency f_c . This way, it is possible to use the same cavity infrastructure, as long as, Alice and Bob both have an assigned mirror for each distinct channel. This scheme is straightforward to expand and provides a linearly scalable way to increase the effective bit-rate. Other proposed protocols involve improving the actual efficiency of secure bit transmission, by changing the number of possible states a single UFL channel is allowed to be in (see [74]).

5.5.2 Vulnerabilities

As previously discussed, even in its theoretical ideal case, the UFL protocol is still susceptible to attacks, relying instead on the technological difficulty of an eavesdropper to distinguish between different secure states. The biggest threat, in terms of passive attacks, is the spontaneous emission noise from the EDFA that is filtered by the user's mirror, and subsequently emerges from the user's site. This results in slightly different spectra during secure states between both users output, which can be exploited by Eve by tapping at least one of those outputs, filtering the signal at f_0 and f_1 and comparing intensities. As discussed in section 5.3, to defend against this type of attack requires lowering the power of the filtered EDFA noise below the detection capabilities of Eve. This can be done by either lowering the gain of the EDFA or placing an inline filter at the center wavelength. There is a trade-off, however, with both these methods, as the residual signal on secure states needs to be lowered enough to not be measured by Eve, but the power of the non-secure states needs to be high enough to be distinguishable from the secure states by Alice

and Bob. A way to counteract this would be to lower the lasing threshold by, for example, optimizing the length of the active medium on the EDFAs.

Other types of vulnerabilities are those posed by *active* attacks. Although they have been dismissed by most studies on the subject [67, 68, 70–72], the paper by Garcia-Escartin *et al.* [73] suggests they need to be considered as important threats. The proposed attack is reliant on the ability of Eve to introduce a probing signal on the cavity, below the noise floor. She achieves this by spectrally broadening the signal using modulation, so that the total power is stretched out over the bandwidth of interest. While possible countermeasures were also proposed, to our knowledge, they have yet to be tested, and correspond to important future work in the study of the reliability of the UFL protocol.

5.6 Conclusions

Practical limitations of QKD have motivated searches for alternative, classically based solutions to key distribution. Accordingly, a system based on an ultra-long fiber laser was proposed on [67] and expanded upon by subsequent studies [68–72, 74]. In this chapter we discussed the basic operation principle of the UFL protocol, reviewed the main security principles the system relies on, implemented our own UFL setup and analyzed its results, and lastly, discussed some possible improvements to our system and some possible vulnerabilities of the UFL protocol as a whole.

As the future of the UFL protocol goes, and seeing most studies have been focused on passive attacks, it is important that the susceptibility to active attacks, in particular those proposed in [73], be fully tested, in order to evaluate the feasibility of the protocol.

Chapter 6

Final conclusions and future work

The research topic of this thesis focused on the applicability of optics for use in quantum information fields, such as quantum cryptography. The work present in it can be divided into three major sections: (i) the study of FWM for use in quantum sources, (ii) the characterization and modeling of an optical receiver, capable of being used in CV-QKD, and (iii) the study of a classically based alternative to QKD: UFL-KDS protocol. In this chapter we summarize the work developed and present some suggestions for future work.

In Chapter 2 we presented an overview of single photon sources, some of their applications, their theoretical behavior and to characterize it, and a basic description of some of the most common types of single photon sources in use.

In Chapter 3 the process of FWM and its use for generation of single-photons and entangled photon-pairs was described. We presented the experimental implementation of a stimulated FWM photon source, and used it to characterize the highly non-linear fiber utilized. Having proven the successful generation of idler photons, a fully single-photon source is hoped to be implemented in the future.

In Chapter 4 the concept of CV-QKD was briefly discussed, as well as, the importance of proper characterization of the utilized optical receiver. A theoretical model for an optical receiver and its noise sources was established, and its experimental characterization was presented. The differences between theoretical model and obtained results were discussed, and an improved experimental characterization was developed. The ultimate objective of this work is to develop a fully functional CV-QKD protocol.

In Chapter 5 a classically based alternative to QKD, the UFL key distribution system,

was presented and studied. Its main security principles were discussed and an experimental implementation of the protocol was performed and analyzed. Some possible improvements to the implemented setup were presented, and the vulnerabilities of the protocol as a whole were expanded upon. For future studies on the subject, the susceptibility to active attacks, which have mainly been ignored in research thus far, should be fully tested, in order to evaluate the feasibility of the protocol.

Bibliography

- [1] M. A. Nielsen, I. Chuang, and L. K. Grover, *Quantum Computation and Quantum Information*, 2002, vol. 70, no. 5. [Cited on page 1.]
- [2] B. Lounis and M. Orrit, “Single-photon sources,” *Reports on Progress in Physics*, vol. 68, no. 5, pp. 1129–1179, 2005. [Online]. Available: <https://doi.org/10.1088/0034-4885/68/5/R04> [Cited on pages 1, 4, 5, 10, 11, and 13.]
- [3] National Academies of Sciences Engineering and Medicine, *Quantum Computing: Progress and Prospects*, E. Grumbling and M. Horowitz, Eds. Washington, DC: The National Academies Press, 2019. [Online]. Available: <https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects> [Cited on page 1.]
- [4] S. Scheel, “Single-photon sources-an introduction,” *Journal of Modern Optics*, vol. 56, no. 2-3, pp. 141–160, jan 2009. [Cited on pages 1, 3, 4, 5, 9, and 10.]
- [5] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, “Invited Review Article: Single-photon sources and detectors,” *The Review of scientific instruments*, vol. 82, no. 7, p. 71101, 2011. [Cited on pages 3, 4, 5, 10, 11, and 12.]
- [6] M. Oxborrow and A. G. Sinclair, “Single-photon sources,” *Contemporary Physics*, vol. 46, no. 3, pp. 173–206, 2005. [Cited on page 1.]
- [7] U. Sinha, S. N. Sahoo, A. Singh, K. Joarder, R. Chatterjee, and S. Chakraborti, “Single-Photon Sources,” *Opt. Photon. News*, vol. 30, no. 9, pp. 32–39, 2019. [Online]. Available: <http://www.osa-opn.org/abstract.cfm?URI=opn-30-9-32> [Cited on pages 1, 3, 5, 10, 11, 13, and 21.]
- [8] C. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, jan 1984, vol. 560. [Cited on pages 4 and 25.]

- [9] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, no. 6816, pp. 46–52, 2001. [Online]. Available: <https://doi.org/10.1038/35051009> [Cited on page 5.]
- [10] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Rev. Mod. Phys.*, vol. 79, no. 1, pp. 135–174, jan 2007. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.79.135> [Cited on page 5.]
- [11] A. Kuhn, M. Hennrich, and G. Rempe, "Deterministic Single-Photon Source for Distributed Quantum Networking," *Physical Review Letters*, vol. 89, no. 6, pp. 4–7, 2002. [Cited on page 10.]
- [12] G. C. Shan, Z. Q. Yin, C. H. Shek, and W. Huang, "Single photon sources with single semiconductor quantum dots," *Frontiers of Physics*, vol. 9, no. 2, pp. 170–193, 2014. [Cited on page 10.]
- [13] C. Couteau, "Spontaneous parametric down-conversion," *Contemporary Physics*, vol. 59, no. 3, pp. 291–304, 2018. [Cited on pages 11 and 12.]
- [14] V. Camus, "Quantum technology: Single-photon source," *arXiv*, no. September 2012, pp. 1–18, 2017. [Cited on pages 11 and 12.]
- [15] P. J. Mosley, "Generation of Heralded Single Photons in Pure Quantum States," *Thesis*, pp. 1–246, 2008. [Online]. Available: <papers2://publication/uuid/0EB99429-34BB-434F-B059-6F187F847C42> [Cited on page 12.]
- [16] G. P. Agrawal, *Nonlinear Fiber Optics Fifth Edition Nonlinear Fiber Optics*, 2007. [Cited on pages 14, 15, 16, 20, 62, 65, 66, 67, 68, and 71.]
- [17] —, *Fiber-Optic Communications Systems, Third Edition.*, 2002, vol. 6. [Cited on pages 14, 27, 28, 29, 30, 31, 32, and 33.]
- [18] K. O. Hill, D. C. Johnson, B. S. Kawasaki, and R. I. MacDonald, "Cw three-wave mixing in single-mode optical fibers," *Journal of Applied Physics*, vol. 49, no. 10, 1978. [Cited on pages 15, 20, 62, and 68.]
- [19] J. Fan, A. Dogariu, and L. J. Wang, "Generation of correlated photon pairs in a microstructure fiber," *Optics Letters*, vol. 30, no. 12, p. 1530, 2005. [Cited on pages 16 and 21.]

- [20] J. Fan, A. Migdall, and L. J. Wang, "Efficient generation of correlated photon pairs in a microstructure fiber," *Optics Letters*, vol. 30, no. 24, p. 3368, 2005.
- [21] E. A. Goldschmidt, M. D. Eisaman, J. Fan, S. V. Polyakov, and A. Migdall, "Spectrally bright and broad fiber-based heralded single-photon source," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 78, no. 1, pp. 1–4, 2008. [Cited on pages [16](#), [21](#), and [22](#).]
- [22] O. Alibart, J. Fulconis, G. K. Wong, S. G. Murdoch, W. J. Wadsworth, and J. G. Rarity, "Photon pair generation using four-wave mixing in a microstructured fibre: Theory versus experiment," *New Journal of Physics*, vol. 8, 2006. [Cited on page [21](#).]
- [23] J. Fan, A. Migdall, J. Chen, and E. A. Goldschmidt, "Microstructure-fiber-based source of photonic entanglement," *IEEE Journal on Selected Topics in Quantum Electronics*, vol. 15, no. 6, pp. 1724–1732, 2009. [Cited on pages [21](#), [22](#), and [23](#).]
- [24] J. G. Rarity, J. Fulconis, J. Duligall, W. J. Wadsworth, and P. S. J. Russell, "Photonic crystal fiber source of correlated photon pairs," *Optics Express*, vol. 13, no. 2, p. 534, 2005. [Cited on page [21](#).]
- [25] J. Fan and A. Migdall, "Phase-sensitive four-wave mixing and Raman suppression in a microstructure fiber with dual laser pumps," *Optics Letters*, vol. 31, no. 18, 2006.
- [26] J. Fulconis, O. Alibart, W. J. Wadsworth, P. S. Russell, and J. G. Rarity, "High brightness single mode source of correlated photon pairs using a photonic crystal fiber," *Optics Express*, vol. 13, no. 19, p. 7572, 2005. [Cited on page [21](#).]
- [27] A. Ling, J. Chen, J. Fan, and A. Migdall, "Mode expansion and Bragg filtering for a high-fidelity fiber-based photon-pair Source," *Optics Express*, vol. 17, no. 23, p. 21302, 2009.
- [28] J. Fan and A. Migdall, "A broadband high spectral brightness fiber-based two-photon source," *Optics Express*, vol. 15, no. 6, p. 2915, 2007. [Cited on pages [16](#) and [21](#).]
- [29] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, "Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band," *Physical Review Letters*, vol. 94, no. 5, pp. 534–544, 2005. [Cited on pages [16](#), [21](#), and [23](#).]

- [30] M. Fiorentino, P. L. Voss, J. E. Sharping, and P. Kumar, "All-fiber photon-pair source for quantum communications," *IEEE Photonics Technology Letters*, vol. 14, no. 7, pp. 983–985, 2002. [Cited on page 21.]
- [31] J. E. Sharping, M. Fiorentino, and P. Kumar, "Observation of twin-beam-type quantum correlation in optical fiber," *Optics Letters*, vol. 26, no. 6, p. 367, 2001.
- [32] M. Medic, J. B. Altepeter, M. A. Hall, M. Patel, and P. Kumar, "Fiber-based telecommunication-band source of degenerate entangled photons," *Optics Letters*, vol. 35, no. 6, p. 802, 2010. [Cited on page 21.]
- [33] Á. Almeida, N. Silva, N. Muga, and A. Pinto, "Single-Photon Source Based on FWM With Adjustable Linear SOP," *Electrónica e Telecomunicações*, vol. 5, no. 2, pp. 151–155, 2010. [Cited on page 17.]
- [34] N. A. Awang, M. Z. Zulkifli, A. A. Latif, S. W. Harun, and H. Ahmad, "Stable power multi-wavelength fibre laser based on four-wave mixing in a short length of highly non-linear fibre," *Journal of Optics*, vol. 13, no. 7, 2011.
- [35] S. D. Dyer, M. J. Stevens, B. Baek, and S. W. Nam, "High-efficiency, ultra low-noise all-fiber photon-pair source," *Optics Express*, vol. 16, no. 13, p. 9966, 2008. [Cited on page 21.]
- [36] P. Antunes and P. S. André, "A Simple and Inexpensive Single-Photon Source by Means of Four-Wave-Mixing and Attenuation A Simple and Inexpensive Single-Photon Source by Means of Four-Wave-Mixing and Attenuation and Armando Nolasco Pinto," no. March, 2014. [Cited on page 17.]
- [37] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Single-photon source using stimulated FWM in optical fibers for quantum communication," *International Conference on Applications of Optics and Photonics*, vol. 8001, p. 80013W, 2011. [Cited on page 17.]
- [38] H. Takesue and K. Inoue, "1.5- μm band quantum-correlated photon pair generation in dispersion-shifted fiber: suppression of noise photons by cooling fiber," *Optics Express*, vol. 13, no. 20, p. 7832, 2005. [Cited on pages 16 and 21.]

- [39] H. Takesue, Y. Tokura, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S. I. Itabashi, "Entanglement generation using silicon wire waveguide," *Applied Physics Letters*, vol. 91, no. 20, pp. 10–13, 2007. [Cited on pages 16, 21, and 23.]
- [40] J. E. Sharping, K. F. Lee, M. A. Foster, A. C. Turner, B. S. Schmidt, M. Lipson, A. L. Gaeta, and P. Kumar, "Generation of correlated photons in nanoscale silicon waveguides," *Optics Express*, vol. 14, no. 25, p. 12388, 2006. [Cited on page 21.]
- [41] K.-i. Harada, H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, and S.-i. Itabashi, "Generation of high-purity entangled photon pairs using silicon wire waveguide," *Optics Express*, vol. 16, no. 25, 2008. [Cited on pages 16, 21, and 23.]
- [42] B. J. Smith, P. Mahou, O. Cohen, J. S. Lundeen, and I. A. Walmsley, "Photon pair generation via spontaneous four-wave mixing in birefringent optical fibers," *Optics InfoBase Conference Papers*, vol. 17, no. 26, pp. 1288–1293, 2009. [Cited on pages 16 and 21.]
- [43] Á. J. Almeida, "Quantum Communications in Optical Fibers," PhD, Universidade de Aveiro, 2016. [Online]. Available: <http://hdl.handle.net/10773/16306https://ria.ua.pt/bitstream/10773/16306/1/tese.pdf> [Cited on pages 16, 17, and 23.]
- [44] N. A. Silva, A. J. Almeida, and A. N. Pinto, "Statistical characterization of a single-photon source based on stimulated FWM in optical fibers," *EUROCON 2011 - International Conference on Computer as a Tool - Joint with Conftele 2011*, no. 4, 2011. [Cited on page 17.]
- [45] OFSoptics, "HNLF Standard." [Online]. Available: <https://fiber-optic-catalog.ofsoptics.com/HNLF-Standard-1157> [Cited on page 18.]
- [46] Q. Lin, F. Yaman, and G. P. Agrawal, "Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 75, no. 2, pp. 1–20, 2007. [Cited on page 21.]
- [47] J. Chen, K. F. Lee, X. Li, P. L. Voss, and P. Kumar, "Schemes for fibre-based entanglement generation in the telecom band," *New Journal of Physics*, vol. 9, 2007. [Cited on pages 22 and 23.]

- [48] X. Tang, R. Kumar, S. Ren, A. Wonfor, R. V. Penty, and I. H. White, "Performance of continuous variable quantum key distribution system at different detector bandwidth," *Optics Communications*, vol. 471, no. December 2019, p. 126034, 2020. [Online]. Available: <https://doi.org/10.1016/j.optcom.2020.126034> [Cited on page 25.]
- [49] M. Navascués and A. Acín, "Security bounds for continuous variables quantum key distribution," *Physical Review Letters*, vol. 94, no. 2, pp. 1–4, 2005. [Cited on page 25.]
- [50] Y. M. Li, X. Y. Wang, Z. L. Bai, W. Y. Liu, S. S. Yang, and K. C. Peng, "Continuous variable quantum key distribution," *Chinese Physics B*, vol. 26, no. 4, 2017. [Cited on pages 25 and 27.]
- [51] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations," 2018. [Cited on page 25.]
- [52] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015. [Cited on pages 25, 26, and 27.]
- [53] J. Li, L. O’Faolain, I. H. Rey, and T. F. Krauss, "Four-wave mixing in photonic crystal waveguides: slow light enhancement and limitations," *Optics Express*, vol. 19, no. 5, p. 4458, 2011. [Cited on page 25.]
- [54] M. Fox, *Quantum Optics: An Introduction*, ser. Oxford Master Series in Physics. OUP Oxford, 2006. [Online]. Available: <https://books.google.pt/books?id=2{ }ZP-LDF9jkC> [Cited on pages 26 and 27.]
- [55] Rongqing Hui, *Introduction to Fiber-Optic Communications*. [Cited on pages 27, 28, and 29.]
- [56] R. Khare, "Fiber Optics and Optoelectronics," 2004. [Cited on pages 27, 28, 29, 31, and 32.]
- [57] S. M. Sze and K. K. Ng, *Physics of semiconductor devices*. Wiley-Interscience, 2006, vol. 10. [Cited on page 29.]

- [58] Thorlabs, "Photodiodes and Photoconductors Tutorials." [Online]. Available: <https://www.thorlabs.com/newgrouppage9.cfm?objectgroup{id}=9020> [Cited on pages 29 and 30.]
- [59] J. M. Palmer and B. G. Grant, *The art of radiometry*, 2009, vol. 148. [Cited on pages 30, 32, 33, and 34.]
- [60] Thorlabs, "PDB450C-Manual." [Online]. Available: <https://www.thorlabs.com/thorproduct.cfm?partnumber=PDB450C> [Cited on pages 31, 33, 35, 36, 37, and 39.]
- [61] R. Hui, "Photodetectors," *Introduction to Fiber-Optic Communications*, pp. 125–154, 2020. [Cited on pages 31 and 32.]
- [62] G. P. Agrawal, *Lightwave Technology: Telecommunication Systems*, 2005. [Cited on pages 31, 32, and 33.]
- [63] M. Taboga, *Lectures on Probability Theory and Mathematical Statistics Second Edition*, 2012. [Cited on page 33.]
- [64] Thorlabs, V. Mackowiak, J. Peupelmann, Y. Ma, and A. Gorges, "NEP - Noise Equivalent Power." [Online]. Available: <https://www.thorlabs.com/images/TabImages/Noise{ }Equivalent{ }Power{ }White{ }Paper.pdf> [Cited on page 33.]
- [65] H.-A. Bachor and T. C. Ralph, "A Guide to Experiments in Quantum Optics," 2004. [Online]. Available: <http://dnb.ddb.de> [Cited on page 34.]
- [66] Yenista Optics, "OSICS TLS-AG Low Linewidth WDM Tunable Laser Source." [Online]. Available: <http://www.sun-ins.com/lineup2/yenista/OSCISTLS-AG.pdf> [Cited on page 36.]
- [67] J. Scheuer and A. Yariv, "Giant fiber lasers: A new paradigm for secure key distribution," *Physical Review Letters*, vol. 97, no. 14, pp. 1–4, 2006. [Cited on pages 42, 44, and 50.]
- [68] O. Kotlicki and J. Scheuer, "Dark states ultra-long fiber laser for practically secure key distribution," *Quantum Information Processing*, vol. 13, no. 10, pp. 2293–2311, 2014. [Cited on pages 43, 44, 48, 49, and 50.]
- [69] A. Tonello, A. Barthélémy, K. Krupa, V. Kermène, A. Desfarges-Berthelemot, B. M. Shalaby, S. Boscolo, S. K. Turitsyn, and J. D. Ania-Castañón, "Secret key exchange in

- ultralong lasers by radiofrequency spectrum coding,” *Light: Science and Applications*, vol. 4, no. 4, 2015. [Cited on page 43.]
- [70] A. Zadok, J. Scheuer, J. Sendowski, and A. Yariv, “Secure key generation using an ultra-long fiber laser: transient analysis and experiment,” *Optics Express*, vol. 16, no. 21, p. 16680, 2008. [Cited on pages 44 and 50.]
- [71] A. El-Taher, O. Kotlicki, P. Harper, S. Turitsyn, and J. Scheuer, “Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser,” *Laser and Photonics Reviews*, vol. 8, no. 3, pp. 436–442, 2014. [Cited on pages 44, 45, and 48.]
- [72] J. Scheuer, “Secure long-range and high bit-rate distribution of shared key using dark states ultra-long fiber laser (UFL),” vol. 1055902, no. January 2018, p. 1, 2018. [Cited on pages 44, 45, and 50.]
- [73] J. C. Garcia-Escartin and P. Chamorro-Posada, “Hidden probe attacks on ultralong fiber laser key distribution systems,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 24, no. 3, pp. 1–9, 2018. [Cited on pages 44 and 50.]
- [74] D. Bar-Lev and J. Scheuer, “Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 373, no. 46, pp. 4287–4296, 2009. [Online]. Available: <http://dx.doi.org/10.1016/j.physleta.2009.09.035> [Cited on pages 49 and 50.]
- [75] N. Shibata, R. P. Braun, and R. G. Waarts, “Phase-Mismatch Dependence of Efficiency of Wave Generation Through Four-Wave Mixing in a Single-Mode Optical Fiber,” *IEEE Journal of Quantum Electronics*, vol. 23, no. 7, pp. 1205–1210, 1987. [Cited on pages 62, 68, 70, and 71.]
- [76] R. W. Tkach, A. R. Chraplyvy, F. Forghieri, A. H. Gnauck, and R. M. Derosier, “Four-Photon Mixing and High-Speed WDM Systems,” *Journal of Lightwave Technology*, vol. 13, no. 5, pp. 841–849, 1995. [Cited on pages 62 and 71.]
- [77] R. W. Boyd, *Nonlinear Optics, Third Edition*, 3rd ed. USA: Academic Press, Inc., 2008. [Cited on pages 62 and 65.]
- [78] P. N. Butcher and D. Cotter, *The Elements of Nonlinear Optics*. Cambridge: Cambridge University Press, 1990. [Online]. Available: <http://ebooks.cambridge.org/ref/id/CBO9781139167994> [Cited on pages 62, 64, 65, and 68.]

- [79] K. Inoue, "Phase-mismatching characteristic of four-wave mixing in fiber lines with multistage optical amplifiers," *Optics Letters*, vol. 17, no. 11, p. 801, 1992. [Cited on page 71.]
- [80] —, "Four-Wave Mixing in an Optical Fiber in the Zero-Dispersion Wavelength Region," *Journal of Lightwave Technology*, vol. 10, no. 11, pp. 1553–1561, 1992. [Cited on page 71.]
- [81] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *IEEE Journal of Quantum Electronics*, vol. 46, no. 3, pp. 285–291, 2010.
- [82] P. S. André and J. L. Pinto, "Simultaneous measurement of the nonlinear refractive index and chromatic dispersion of optical fibers by four-wave mixing," *Microwave and Optical Technology Letters*, vol. 34, no. 4, pp. 305–307, 2002.
- [83] S. J. Jung, J. Y. Lee, and D. Y. Kim, "Novel phase-matching condition for a four wave mixing experiment in an optical fiber," *Optics Express*, vol. 14, no. 1, p. 35, 2006.
- [84] W. Chen, Z. Meng, H. J. Zhou, and H. Luo, "Numerical simulation of four-wave mixing efficiency and its induced relative intensity noise," *Chinese Physics B*, vol. 21, no. 6, pp. 1–5, 2012.
- [85] K. Kikuchi and C. Lorattanasane, "Design of Highly Efficient Four-Wave Mixing Devices Using Optical Fibers," *IEEE Photonics Technology Letters*, vol. 6, no. 8, pp. 992–994, 1994. [Cited on page 71.]

Appendix A

Efficiency of the FWM process in optical fibers

When searching the literature for the efficiency of the FWM process in optical fibers, most articles cite [18, 75] as their sources. However, these articles present different formulas for the same concepts, as some books on the subject, namely *Nonlinear Fiber Optics* by Agrawal [16]. This remains true, even when taking into account that these articles, along most older articles, use gaussian units instead of SI units. These differences arise from the different approximations taken to solve the equations for the idler power within optical fibers. To add that, even among several articles, different formulas are also sometimes presented ([75, 76], for example, show different efficiencies).

Therefore, we present in this appendix, the deduction of the equations used in this work, as well as, explanations for the specific approximations used. This appendix follows mainly the process described in *Nonlinear Fiber Optics* by Agrawal [16], among others.

We begin with the general wave equation used in nonlinear fiber optics [16, 77, 78]

$$\nabla \times \nabla \times \mathbf{E} = -\frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} - \mu_0 \frac{\partial^2 \mathbf{P}}{\partial t^2} \quad (\text{A.1})$$

where it was assumed that the material in which the wave travels is nonmagnetic ($\mathbf{M} = 0$) and contains no free charges ($\rho_f = 0$) or currents ($\mathbf{J} = 0$), such is the case for optical fibers. This equation can be simplified by using the vector calculus's identity $\nabla \times \nabla \times \mathbf{E} = \nabla (\nabla \cdot \mathbf{E}) - \nabla^2 \mathbf{E}$ and the approximation that $\nabla \cdot \mathbf{E} \sim 0$ and can be dropped for most cases of interest [16, 77, 78]. Thus, equation A.1 takes the form

$$\nabla^2 \mathbf{E} - \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} = \mu_0 \frac{\partial^2 \mathbf{P}}{\partial t^2} \quad (\text{A.2})$$

Due to its complexity, several approximations have to be made, in order to solve the wave equation for the nonlinear case. A major one is to treat the nonlinear polarization as a small perturbation to the total polarization \mathbf{P} . This approximation is justified as the nonlinear effects of silica fibers are relatively weak.

To do this, we first separate the polarization \mathbf{P} , in its linear (\mathbf{P}^L) and nonlinear parts (\mathbf{P}^{NL}), such that

$$\mathbf{P} = \mathbf{P}^L + \mathbf{P}^{NL} \quad (\text{A.3})$$

where the linear part is given by

$$\mathbf{P}^L = \varepsilon_0 \chi^{(1)} \cdot \mathbf{E} \quad (\text{A.4})$$

with ε_0 being the vacuum permeability and $\chi^{(1)}$ the first order susceptibility of the medium. This allows to write equation A.2 as

$$\nabla^2 \mathbf{E} - \frac{\varepsilon^{(1)}}{c^2} \cdot \frac{\partial^2 \mathbf{E}}{\partial t^2} = \mu_0 \frac{\partial^2 \mathbf{P}^{NL}}{\partial t^2} \quad (\text{A.5})$$

where $\varepsilon^{(1)} \equiv 1 + \chi^{(1)}$ is the dielectric tensor. As it can be observed, equation A.5 has the form of an inhomogeneous wave equation with the nonlinear response of the medium acting as a source term.

Since we are dealing with a dispersive medium, as is the case for fiber optics, we must treat each frequency component separately, and thus represent the electric and nonlinear polarization fields as:

$$\mathbf{E}(\mathbf{r}, t) = \sum_n \mathbf{E}_n(\mathbf{r}, t) \quad (\text{A.6a})$$

$$\mathbf{P}^{NL}(\mathbf{r}, t) = \sum_n \mathbf{P}_n^{NL}(\mathbf{r}, t) \quad (\text{A.6b})$$

where the sum is performed over positive frequencies only. Now we consider, for each frequency component, equation A.5 for the most straightforward case of a wave propagating in the $+z$ direction in a isotropic medium with zero nonlinearities ($\mathbf{P}^{NL} = 0$) and fiber attenuation ($\alpha = 0 \rightarrow \varepsilon^{(1)} \in \mathbb{R}$), i.e.

$$\frac{\partial^2 \mathbf{E}_n(z, t)}{\partial z^2} - \frac{\varepsilon^{(1)}}{c^2} \frac{\partial^2 \mathbf{E}_n(z, t)}{\partial t^2} = 0 \quad (\text{A.7})$$

This has solutions of the form:

$$\mathbf{E}_n(z, t) = \hat{e} \left[\frac{1}{2} A_n e^{i(\beta_n z - \omega_n t)} + c.c. \right] \quad (\text{A.8})$$

where

$$\beta_n = \frac{n\omega_n}{c} \quad (\text{A.9a})$$

$$n^2 = \varepsilon^{(1)} \quad (\text{A.9b})$$

\hat{e} is the polarization unit vector and A_n is a *constant*. As previously stated, it is expected, on physical grounds, that the nonlinear source term will act as a small perturbation on total field. In mathematical terms this means that solutions to equation A.5 will be the same as of equation A.7, except that the amplitude of the wave A_n will become a slowly varying function of z ($A_n \rightarrow A_n(z)$ in eq. A.8). Additionally, we also need to consider the effects of absorption of optical power by the medium ($\alpha \neq 0 \rightarrow \varepsilon^{(1)} \in \mathbb{C}$). For the vast majority of media used in optics, the effects of attenuation are rather small over distances to the scale of a optical wavelength, and can, therefore, be treated as small perturbation [78], or in mathematical terms:

$$\varepsilon^{(1)} = \left(n + i \frac{\alpha c}{2\omega} \right)^2 \simeq n^2 + i \frac{n\alpha c}{\omega} \quad (\text{A.10})$$

Finally, it is convenient to explicitly separate the time varying part of each component of the nonlinear polarization field, by writing it in the form:

$$\mathbf{P}_n^{NL}(\mathbf{r}, t) = \mathbf{P}_n^{NL}(\mathbf{r}) e^{-i\omega_n t} + c.c. \quad (\text{A.11})$$

Now, using equations A.10 and A.11, we can solve equation A.5, for each frequency component and wave propagating in the $+z$ direction, if we use the *ansatz* solution in equation A.8 with an amplitude varying in z :

$$\frac{\partial^2 \mathbf{E}_n(z, t)}{\partial z^2} - \frac{\varepsilon^{(1)}}{c^2} \frac{\partial^2 \mathbf{E}_n(z, t)}{\partial t^2} = \mu_0 \frac{\partial^2 \mathbf{P}_n^{NL}(z, t)}{\partial t^2} \Leftrightarrow \quad (\text{A.12a})$$

$$\begin{aligned} \Leftrightarrow \frac{1}{2} \left[\frac{\partial^2 A_n(z)}{\partial z^2} + 2i\beta_n \frac{\partial A_n(z)}{\partial z} - \beta_n^2 A_n(z) + \frac{\omega_n^2}{c^2} \left(n^2 + i \frac{n\alpha c}{\omega_n} \right) A_n(z) \right] e^{i(\beta_n z - \omega_n t)} \\ = -\mu_0 \omega_n^2 P_n^{NL}(z) e^{-i\omega_n t} \end{aligned} \quad (\text{A.12b})$$

As stated before, the amplitude of the electric field is a slowly varying function of z . Consequently, we have that

$$\left| \frac{\partial^2 A_n(z)}{\partial z^2} \right| \ll \left| \beta_n \frac{\partial A_n(z)}{\partial z} \right| \quad (\text{A.13})$$

and can thus neglect the second order derivative of A_n when solving eq. A.12b, resulting in

$$i\beta_n \left(\frac{\partial A_n(z)}{\partial z} + \frac{\alpha}{2} A_n(z) \right) = -\mu_0 \omega_n^2 P_n^{NL}(z) e^{-i\beta_n z} \quad (\text{A.14})$$

Now, in order to proceed, the nonlinear polarization for the particular case in study, that of degenerate FWM, needs to be found. FWM is an effect that arises due to the third-order susceptibility, thus we can write:

$$\mathbf{P}^{NL} = \varepsilon_0 \chi^{(3)} \mathbf{E} \cdot \mathbf{E} \cdot \mathbf{E} \quad (\text{A.15})$$

Usually FWM is polarization dependent and requires the tensor form of $\chi^{(3)}$ to be considered. However, for simplicity sake and following the treatment presented in the literature [16, 77, 78], we consider the scalar case, in which all fields are linearly polarized along a main axis.

Calculations on FWM commonly consider the electric field to be the sum of four continuous waves (CW) at four different frequencies. However, as we are interested in the degenerate instance of FWM, where both pump photons have equal frequencies, we will only consider three CW, and write the total electric field as:

$$E(z, t) = \sum_{n=1}^3 \frac{1}{2} A_n(z) e^{i\psi_n} + c.c. \quad (\text{A.16})$$

where we define $\psi_n \equiv \beta_n z - \omega_n t$, in order to simplify notation. Substituting equation A.16 in equation A.15, we obtain

$$P^{NL} = \varepsilon_0 \chi^{(3)} E(z, t)^3 \quad (\text{A.17a})$$

$$= \frac{\varepsilon_0 \chi^{(3)}}{8} \sum_{i,j,k \in \{1,2,3\}} A_i^\square A_j^\square A_k^\square e^{i(\pm\psi_i \pm \psi_j \pm \psi_k)} \quad (\text{A.17b})$$

where A_n^\square is an abuse of notation and it can either represent the function A_n or its conjugate A_n^* , if the corresponding phase is either positive ($+\psi_n$) or negative ($-\psi_n$), respectively. To obtain the nonlinear polarization term to plug into equation A.14, we need to find all terms of the sum in equation A.17b that occur at a certain frequency. Lets take ψ_1 , for example. If we were to merely simplify equation A.17b and separate the terms that happen at frequency ω_1 , we would obtain

$$P_1^{NL} = \frac{\varepsilon_0 \chi^{(3)}}{8} 3 \left(|A_1|^2 + 2|A_2|^2 + 2|A_3|^2 \right) A_1 e^{i\psi_1} \quad (\text{A.18})$$

However, we are interested in studying FWM, where we have a process that coherently builds up along the fiber, if the phase match conditions are met. The energy conservation phase-matching requirement has, in the degenerate case, that $2\omega_1 = \omega_2 + \omega_3$, if we assign ω_1 to be the pump frequency. Thus, we need to add to equation A.18, the terms in equation A.17b that correspond to $\omega_2 + \omega_3 - \omega_1 (= \omega_1)$. Accordingly, we get:

$$P_1^{NL}(z, t) = e^{-i\omega_1 t} \varepsilon_0 \chi^{(3)} \frac{3}{8} \left\{ \left(|A_1|^2 + \sum_{n=2,3} 2|A_n|^2 \right) A_1 e^{i\beta_1 z} + 2A_2 A_3 A_1^* e^{i(\beta_2 + \beta_3 - \beta_1)z} \right\} \quad (\text{A.19})$$

Now, we can make the appropriate substitutions into equation A.14, obtaining:

$$i\beta_1 \left(\frac{\partial A_1}{\partial z} + \frac{\alpha}{2} A_1 \right) = -\mu_0 \omega_1^2 \varepsilon_0 \chi^{(3)} \frac{3}{8} \left\{ \left(|A_1|^2 + \sum_{n=2,3} 2|A_n|^2 \right) A_1 + 2A_2 A_3 A_1^* e^{i(\beta_2 + \beta_3 - 2\beta_1)z} \right\} \quad (\text{A.20})$$

Defining $\Delta\beta \equiv \beta_2 + \beta_3 - 2\beta_1$, and simplifying equation A.20, we have:

$$\frac{\partial A_1}{\partial z} = i \frac{\omega_1}{cn} \chi^{(3)} \frac{3}{8} \left\{ \left(|A_1|^2 + \sum_{n=2,3} 2|A_n|^2 \right) A_1 + 2A_2 A_3 A_1^* e^{i\Delta\beta z} \right\} - \frac{\alpha}{2} A_1 \quad (\text{A.21})$$

Equation can further be straightforwardly simplified by using the definition of the nonlinear-index coefficient, given by [16]:

$$\bar{n}_2 \equiv \frac{3}{8} \frac{\chi^{(3)}}{n} \quad (\text{A.22})$$

Up until now we have disregarded the transverse distribution of the electric field, however, it is necessary to take it into account for a proper description of a wave traveling inside an optical fiber. In this manner, we write the electric field as:

$$E_n(\mathbf{r}, t) = \frac{1}{2} A_n(z) F_n(x, y) e^{i\psi_n} + c.c. \quad (\text{A.23})$$

where $F_n(x, y)$ is the modal distribution of the wave. Following the description in chapter 2 of Agrawal's *Nonlinear Fiber Optics* [16], and assuming $F_n(x, y)$ does not vary significantly over the pulse bandwidth, we can evaluate the impact of the modal distribution by making the substitution

$$\frac{\omega_1 \bar{n}_2}{c} \rightarrow \frac{\omega_1 \bar{n}_2}{c} \frac{\iint |F(x, y)|^4 dx dy}{\iint |F(x, y)|^2 dx dy} \quad (\text{A.24})$$

on the equations we have obtained so far. For practical reasons, it is also common to normalize A_n such that $|A_n|^2$ equals the optical power. Following [16], we can do this by redefining the parameters in equation A.24 as

$$\frac{\omega_1 \bar{n}_2}{c} \frac{\iint |F(x, y)|^4 dx dy}{\iint |F(x, y)|^2 dx dy} \rightarrow \frac{\omega_1 n_2}{c A_{eff}} \quad (\text{A.25})$$

where

$$n_2 \equiv \frac{2\bar{n}_2}{\epsilon_0 n c} \quad (\text{A.26})$$

is called the nonlinear Kerr parameter, with units m^2/W . A_{eff} is the effective area which depends on the parameters of the fiber, and is usually given by the manufacturer. Finally, we define the nonlinear parameter as

$$\gamma(\omega) = \frac{\omega n_2}{c A_{eff}} \quad (\text{A.27})$$

and make the approximation that $\gamma(\omega)$ is roughly similar for all four frequencies involved. Taking into consideration equations A.22 to A.27, we can rewrite equation A.21 as

$$\frac{\partial A_1}{\partial z} = i\gamma \left\{ \left(|A_1|^2 + \sum_{n=2,3} 2|A_n|^2 \right) A_1 + 2A_2A_3A_1^* e^{i\Delta\beta z} \right\} - \frac{\alpha}{2} A_1 \quad (\text{A.28})$$

From a similar manner, we can also obtain the equations for A_2 and A_3

$$\frac{\partial A_2}{\partial z} = i\gamma \left\{ \left(|A_2|^2 + \sum_{n \neq 2} 2|A_n|^2 \right) A_2 + 2A_1A_3A_2^* e^{-i\Delta\beta z} \right\} - \frac{\alpha}{2} A_2 \quad (\text{A.29})$$

$$\frac{\partial A_3}{\partial z} = i\gamma \left\{ \left(|A_3|^2 + \sum_{n \neq 3} 2|A_n|^2 \right) A_3 + 2A_1A_2A_3^* e^{-i\Delta\beta z} \right\} - \frac{\alpha}{2} A_3 \quad (\text{A.30})$$

The terms in equations A.28 to A.30 represent the effects of self-phase modulation (SPM), cross-phase modulation (XPM), FWM and fiber attenuation on the traveling waves, and require numerical approaches to solve [16]. To find analytical solutions we need to make some simplifications. Researching the literature we find that most studies on the efficiency of FWM cite article [75] and [18] for the theoretical formula of the idler power, which do not take into account the effects of SPM and XPM on their calculations. However, books on the subject of nonlinear optics, such as [16] and [78], use these effects when solving their equations on FWM. Furthermore, we have that study [18] uses the approximation $A_{pump}, A_{signal} \gg A_{idler}$ and that $\alpha \neq 0$, while book [16] disregards the effects of fiber attenuation and uses the approximation $A_{pump} \gg A_{signal}, A_{idler}$. Having in mind that we are only interest in the stimulated case of FWM, we will use [18] approximations ($A_{pump}, A_{signal} \gg A_{idler}$), taking, nevertheless, into account the SPM and XPM terms.

Renaming waves 1,2 and 3 as the *pump*, *signal* and *idler* waves, respectively, and rewriting equation A.28 with the simplifications mentioned above, we have:

$$\frac{\partial A_p}{\partial z} \simeq i\gamma \left(|A_p|^2 + 2|A_s|^2 \right) A_p - \frac{\alpha}{2} A_p \quad (\text{A.31})$$

In order to solve this equation, we introduce

$$B_x = A_x e^{\frac{\alpha}{2}z}, \quad x = \{p, s\} \quad (\text{A.32})$$

Thus, we are able to obtain

$$\frac{\partial B_p}{\partial z} = i\gamma \left(|A_p(0)|^2 + 2|A_s(0)|^2 \right) e^{-\alpha z} B_p \quad (\text{A.33})$$

which has the straightforward solution

$$B_p = C_p \exp \left(\frac{i\gamma \left(|A_p(0)|^2 + 2|A_s(0)|^2 \right) e^{-\alpha z}}{-\alpha} \right) \quad (\text{A.34})$$

where C_p is a constant dependent on the initial conditions. Defining $W_p \equiv |A_p(0)|^2 + 2|A_s(0)|^2$ in order to simplify notation, and writing explicitly in terms of the pump's amplitude initial value, $A_p(0)$, we have that the solution to eq. A.31 is then:

$$A_p = A_p(0) \exp \left(\frac{i\gamma W_p}{\alpha} \left(1 - e^{-\alpha z} \right) - \frac{\alpha}{2} z \right) \quad (\text{A.35})$$

From a similar manner, we can obtain the amplitude of the signal wave as:

$$A_s = A_s(0) \exp \left(\frac{i\gamma W_s}{\alpha} \left(1 - e^{-\alpha z} \right) - \frac{\alpha}{2} z \right) \quad (\text{A.36})$$

where again we have defined $W_s \equiv |A_s(0)|^2 + 2|A_p(0)|^2$, in order to simplify notation.

Using the solutions of eqs. A.35 and A.36, we can write eq. A.30, regarding the idler,

as

$$\begin{aligned} \frac{\partial A_i}{\partial z} = & i\gamma \left\{ \left(|A_i|^2 + \sum_{n=p,s} 2|A_n|^2 \right) A_i + \right. \\ & \left. A_p(0)^2 A_s^*(0) \exp \left[\frac{i\gamma}{\alpha} \left(2W_p - W_s \right) \left(1 - e^{-\alpha z} \right) - \frac{3}{2}\alpha z - i\Delta\beta z \right] \right\} - \frac{\alpha}{2} A_i \end{aligned} \quad (\text{A.37})$$

Simplifying eq. A.37, employing the previously discussed approximations, we have

$$\frac{\partial A_i}{\partial z} \simeq i\gamma A_p(0)^2 A_s^*(0) \exp \left[\frac{i\gamma}{\alpha} 3|A_s(0)|^2 \left(1 - e^{-\alpha z} \right) - \frac{3}{2}\alpha z - i\Delta\beta z \right] - \frac{\alpha}{2} A_i \quad (\text{A.38})$$

where we have used the fact that $2W_p - W_s = 3|A_s(0)|^2$. Defining $B_i \equiv A_i e^{\frac{\alpha}{2}z}$, in a similar way as was done for pump and signal, we can obtain

$$\frac{\partial B_i}{\partial z} = i\gamma A_p(0)^2 A_s^*(0) \exp \left[\frac{i\gamma}{\alpha} 3|A_s(0)|^2 \left(1 - e^{-\alpha z} \right) - \alpha z - i\Delta\beta z \right] - \frac{\alpha}{2} A_i \quad (\text{A.39})$$

In order to solve eq. A.39, it is necessary to make some approximations, namely we used

$$\frac{(1 - e^{-\alpha z})}{\alpha} \simeq z \quad (\text{A.40})$$

valid for small αz . If we plug in the values of the fiber utilized, $\alpha \sim 0.2 \text{ km}^{-1}$ and $z = 1 \text{ km}$, into eq. A.40, we obtain an error of 10%. In this manner, we have that equation A.39 becomes

$$\frac{\partial B_i}{\partial z} = i\gamma A_p(0)^2 A_s^*(0) \exp \left[iz \left(3\gamma |A_s(0)|^2 - \Delta\beta \right) - \alpha z \right] \quad (\text{A.41})$$

Solving equation A.41, with the initial condition that there is no idler propagating in the beginning of the fiber, i.e. $A_i(0) = 0 \rightarrow B_i(0) = 0$, gives

$$B_i(z) = \frac{i\gamma A_p(0)^2 A_s^*(0)}{i \left(3\gamma |A_s(0)|^2 - \Delta\beta \right) - \alpha} \left(1 - \exp \left[iz \left(3\gamma |A_s(0)|^2 - \Delta\beta \right) - \alpha z \right] \right) \quad (\text{A.42})$$

Defining the value $\Delta\beta_{eff} \equiv \Delta\beta - 3\gamma |A_s(0)|^2$, in order to simplify notation, we have that the amplitude of the idler wave is given by

$$A_i(z) = \frac{i\gamma A_p(0)^2 A_s^*(0)}{\alpha + i\Delta\beta_{eff}} e^{-\frac{\alpha}{2}z} \left\{ 1 - e^{-(\alpha + i\Delta\beta_{eff})z} \right\} \quad (\text{A.43})$$

From here, and having defined the amplitudes, A_n , in such a way that $|A_n|^2$ equals the optical power, we then have that the idler optical power is given by

$$\begin{aligned} P_i(z) &= |A_i(z)|^2 \\ &= \gamma^2 P_p(0)^2 P_s(0) e^{-\alpha z} \left| \frac{1 - e^{-(\alpha + i\Delta\beta_{eff})z}}{\alpha + i\Delta\beta_{eff}} \right|^2 \end{aligned} \quad (\text{A.44})$$

Following the definitions used in the paper by Shibata *et al.* [75], we introduced the efficiency of the FWM process as

$$\begin{aligned} \eta &\equiv \frac{P_i(z, \Delta\beta_{eff})}{P_i(z, \Delta\beta_{eff} = 0)} \\ &= \frac{\alpha^2}{\alpha^2 + \Delta\beta_{eff}^2} \frac{\left| 1 - e^{-(\alpha + i\Delta\beta_{eff})z} \right|^2}{\left| 1 - e^{-\alpha z} \right|^2} \end{aligned} \quad (\text{A.45})$$

Simplifying equation A.45, we are able to obtain

$$\eta = \frac{\alpha^2}{\alpha^2 + \Delta\beta_{eff}^2} \left\{ 1 + \frac{4e^{-\alpha z} \text{sen}^2(\Delta\beta_{eff}z/2)}{(1 - e^{-\alpha z})^2} \right\} \quad (\text{A.46})$$

Thus, the idler power through the length of the fiber, is able to be written as

$$\begin{aligned} P_i(z) &= \eta P_i(z, \Delta\beta_{eff} = 0) \\ &= \eta \gamma^2 P_p(0)^2 P_s(0) e^{-\alpha z} \left(\frac{1 - e^{-\alpha z}}{\alpha} \right)^2 \end{aligned} \quad (\text{A.47})$$

The results obtained in equations A.46 and A.47 are similar to those obtained in most papers about FWM efficiency [75, 76, 79–85], with the exception that instead of $\Delta\beta$, we have a phase-mismatch that accounts for the SPM and XPM effects, such that $\Delta\beta_{eff} = \Delta\beta - 3\gamma |A_s(0)|^2$. Agrawal's *Nonlinear Fiber Optics* [16] also takes into account an *effective* phase-mismatch, though they arrive at a different value, since their initial approximations were also different.

To calculate the value of $\Delta\beta$, we follow the reasoning set forth in article [80] by Inoue. Thus, we expand the propagation constant, β , around the frequency of zero-dispersion, f_0 , as

$$\beta(f) = \beta(f_0) + (f - f_0) \left. \frac{d\beta}{df} \right|_{f_0} + \frac{1}{2} (f - f_0)^2 \left. \frac{d^2\beta}{df^2} \right|_{f_0} + \frac{1}{6} (f - f_0)^3 \left. \frac{d^3\beta}{df^3} \right|_{f_0} + \dots \quad (\text{A.48})$$

Considering the definition of the dispersion parameter, D , we can write the second derivative of β as

$$\frac{d^2\beta}{df^2} = -D\lambda^2 \frac{2\pi}{c} \quad (\text{A.49})$$

and the third derivative as

$$\begin{aligned} \frac{d^3\beta}{df^3} &= \frac{d}{df} \left(-D\lambda^2 \frac{2\pi}{c} \right) \\ &= \frac{d\lambda}{df} \frac{d}{d\lambda} \left(-D\lambda^2 \frac{2\pi}{c} \right) \\ &= \frac{c}{f^2} \frac{2\pi}{c} \left(\frac{dD}{d\lambda} \lambda^2 + 2\lambda D \right) \\ &= \frac{2\pi\lambda^2}{c^2} \left(\frac{dD}{d\lambda} \lambda^2 + 2\lambda D \right) \end{aligned} \quad (\text{A.50})$$

Since $D(\lambda_0) = 0$, and discarding terms higher than third order, equation A.48 can be rewritten, with help from equations A.49 and A.50, as

$$\beta(f) \simeq \beta(f_0) + (f - f_0) \left. \frac{d\beta}{df} \right|_{f_0} + \frac{(f - f_0)^3}{6} \frac{2\pi\lambda_0^4}{c^2} \left. \frac{dD}{d\lambda} \right|_{\lambda_0} \quad (\text{A.51})$$

Calculating the phase-mismatch, $\Delta\beta$, using equation A.51, we have

$$\begin{aligned} \Delta\beta &= \beta(f_s) + \beta(f_i) - 2\beta(f_p) \\ &= \left. \frac{d\beta}{df} \right|_{f_0} \left(\cancel{f_s + f_i} - 2f_s \right) + \frac{\pi\lambda_0^4}{3c^2} \left. \frac{dD}{d\lambda} \right|_{\lambda_0} \left\{ (f_i - f_0)^3 + (f_s - f_0)^3 - 2(f_p - f_0)^3 \right\} \end{aligned} \quad (\text{A.52})$$

Using the help from the property $2f_p = f_i - f_s$, and after some arithmetic manipulation, equation A.52 can be rewritten as

$$\begin{aligned} \Delta\beta &= \frac{\pi\lambda_0^4}{3c^2} \left. \frac{dD}{d\lambda} \right|_{\lambda_0} 6(f_p - f_0)(f_s - f_p)^2 \\ &= -\frac{2\pi c\lambda_0^3}{\lambda_p^3 \lambda_s^2} \left. \frac{dD}{d\lambda} \right|_{\lambda_0} (\lambda_p - \lambda_0)(\lambda_s - \lambda_p)^2 \end{aligned} \quad (\text{A.53})$$

With equation A.53, alongside equations A.47 and A.46, we can properly describe the evolution of the idler power along an optical fiber, due to the process of stimulated FWM.

Impact of the SPM and XPM effects on FWM efficiency

As previously stated, the results obtained for the FWM efficiency are similar to those found on several articles, with the exception of the phase-mismatch

$$\Delta\beta_{eff} = \Delta\beta - 3\gamma P_s(0) \quad (\text{A.54})$$

that includes a term $-3\gamma P_s(0)$, resulting from the effects of SPM and XPM. To study the impact of this term on the efficiency of FWM, a constant $C_1 \equiv -3\gamma P_s(0)L$ was defined, and the outcomes of several different values of C_1 on the parameter $\Delta\beta_{eff}L$ and the idler power $P_i(L)$, were studied. The results thus obtained, with the help of a Python script, are plotted in figure A.1. As can be observed the effect of C_1 only starts to become relevant for absolute values higher than ~ 0.5 . If we calculate the value of C_1 we expect to obtain with our data, we get ~ -0.05 . However, at this order of magnitude, variations on the value of

C_1 are largely irrelevant. For this reason, the fit obtained in Python was done by fixing the value of C_1 , such that $C_1 = 0$.

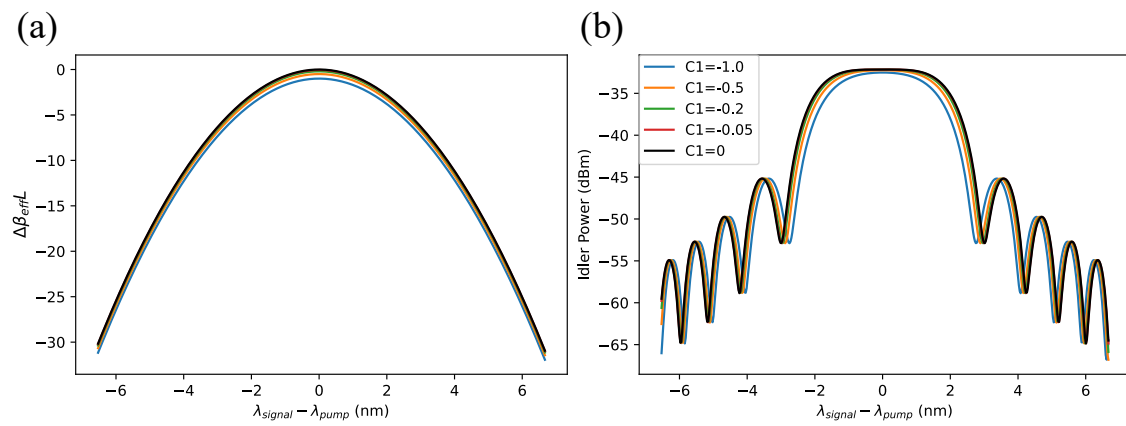


FIGURE A.1: Impact of different values of the parameter C_1 on (a) $\Delta\beta_{eff}L$ and (b) the idler power

Appendix B

Coefficients of the fits in Chapter 4

The values calculated for the fit to the experimental data, and the expected theoretical behavior, shown in figures 4.5 (a), (b) and (c), of chapter 4, are shown in tables B.1, B.2 and B.3, respectively.

TABLE B.1: Calculated fit and theoretical values for the *average power* measured in the *direct detection* scheme

$mx + b$	Fit		Theoretical
	PIN+	PIN-	
$m (V/W)$	7186 ± 20	9804 ± 40	5×10^3
$b (V)$	$(5.4 \pm 4.8) \times 10^{-3}$	$(-1.6 \pm 7.5) \times 10^{-3}$	0
r^2	0.99992	0.9998	-

TABLE B.2: Calculated fit and theoretical values for the *noise variance* measured in the *direct detection* scheme

$ax^2 + bx + c$	Fit		Theoretical
	PIN+	PIN-	
$a (V^2/W^2)$	14.32 ± 0.46	24.94 ± 0.50	8.182
$b (V^2/W)$	$(2.5 \pm 1.6) \times 10^{-4}$	$(6.9 \pm 1.5) \times 10^{-4}$	4.146×10^{-4}
$c (V^2)$	$(6.71 \pm 0.12) \times 10^{-7}$	$(6.703 \pm 0.093) \times 10^{-7}$	2.8723×10^{-7}
r^2	0.9992	0.9997	-

TABLE B.3: Calculated fit and theoretical values for the *noise variance* measured in the *balanced detection* scheme

$mx + b$	Fit	Theoretical
$m (V/W)$	$(1.1210 \pm 0.0063) \times 10^{-3}$	8.2913×10^{-4}
$b (V)$	$(6.559 \pm 0.021) \times 10^{-7}$	2.8723×10^{-7}
r^2	0.9994	-