Master thesis and internship[BR]- Master's thesis : Advances in free-space quantum key distribution[BR]- Integration Internship : Centre Spatial de Liège

Auteur : Chaabani, Sélim
Promoteur(s) : Habraken, Serge
Faculté : Faculté des Sciences appliquées
Diplôme : Master en ingénieur civil en aérospatiale, à finalité spécialisée en "aerospace engineering"
Année académique : 2022-2023
URI/URL : http://hdl.handle.net/2268.2/17887

University of Liège - Faculty of Applied Sciences

Advances in free-space quantum key distribution

Author:
CHAABANI Sélim

Academic advisor:
HABRAKEN Serge

Committee members:
ABSIL Olivier
CLERMONT Lionel
GEORGES Marc
HERNANDEZ Yves

Master's thesis completed in order to obtain the degree of Master of Science in Aerospace Engineering by Sélim CHAABANI

Academic year 2022-2023

Abstract

As modern societies rely on digital communications, the necessity for security becomes increasingly pressing. Nowadays, security is ensured thanks to complex mathematical operations that modern computers struggle to solve. However, the imminent emergence of quantum computers is suspected to change this situation. Among the different countermeasures, Quantum Key Distribution yields promising results. Quantum Key Distribution relies on the quantum properties of photons to distribute secured encryption keys between two parties. Many obstacles lie ahead towards global Quantum Key Distribution networks. This work introduces many of the challenges in implementing the technique widely, with a particular interest in free space operation

The present work explains the basic principles of Quantum Key Distribution and provides a presentation of its practical implementations. A review of optical fibre Quantum Key Distribution and its hurdles are introduced before considering free space as a transmission medium. Based on a thorough literature review, this study examines technical challenges and promising solutions for free-space Quantum Key Distribution from the photon source to the detectors. Afterwards, this thesis provides an analysis of the Chinese satellite Micius and the experiments conducted with it.

Following this discussion, this work presents an experimental photon source for Quantum Key Distribution. This study establishes the theoretical elements driving the design, from the non-linear optics considerations to the optics selection and including the laser source amplification. Then, this paper briefly questions the transposability of this source to space.

In light of the different aspects presented, this work discusses the current state of the technology and its feasibility on a large scale. This study concludes that provided some advances in the envisioned solutions to the current limitations, free-space Quantum Key Distribution is a promising technique that shows the potential to oppose the increased computing abilities of quantum computers and ensure global security.

Acknowledgements

I would like to thank my academic supervisor, Pr. Serge Habraken, for his support and advice throughout the production of this manuscript. This work would not be in its current state without his feedback and corrections. I would also like to thank the whole staff of CSL for their kindness and their welcome as well as their suggestions.

Next, I would like to thank the photonics team of Multitel and especially Yves Hernandez for introducing me to the team and my experimental supervisor Jean-Bernard Lecourt. I would like to thank him for his patience when introducing me to experimentation. His supervision and guidelines were essential to build the experimental setup.

Then I would like to thank my office mates Clément, Jesús and Antoine as well as Colin for their company and advice during the elaboration of this manuscript. I would also like to thank my friend Marie who also did her internship at CSL. The experience would not have been the same without them. I would like to thank my fellow intern Nolan in Mulitel for his crucial help in the development of the laser used in the experiment. It would not have progressed this fast with my hesitant hands alone.

Finally, I would like to thank my partner Elodie for her support and help with proof-reading. I would also like to thank my father, my mother and my sister for their unwavering support during the Master's thesis and my years at the university. Thank you for your patience and understanding, even in the most difficult times. I would also like to thank all the friends I already had and the ones I made during these years.

Contents

Abstract **i**

Acknowledgments **ii**

1 Introduction **1**

2 Bases of the technique **3**

2.1 Bases of cryptography 3

2.2 The BB84 protocol 5

2.3 Other protocols and methods 11

2.4 General architecture 13

3 Optical fibre QKD **15**

3.1 Technical challenges 16

3.2 Implementations 18

4 Free-Space QKD **19**

4.1 Classical satellite communication and architecture 19

4.2 Important considerations 20

4.3 Technical challenges 22

4.3.1 Sources 23

4.3.2 Losses in the optical link 23

4.3.3 Noise 27

4.3.4 Detector performances 29

4.3.5 Coupling 31

4.4 Investigated solutions 33

4.4.1 Adaptive optics 35

4.4.2 Filters 37

4.5 A proof of concept satellite: Micius 40

4.6 Future initiatives 49

5 Experimental source **50**

5.1 Introduction of non-linear optics 50

5.1.1 Sum-frequency generation 51

5.1.2 Spontaneous parametric down-conversion 54

5.2 Laser preparation 57

5.3 Laser diode characterisation 58

5.4 First amplifier pump characterisation 66

5.5 First amplifier 67

5.6 Second amplifier 76

5.7 High-power pump diodes characterisation 76

5.8 High-power amplifier 78

5.9 Optical considerations 79

5.10 Optical design 88

5.11 Lens selection 92

5.11.1 System dimensions estimation for SHG 96

5.11.2 System dimensions estimation for SPDC 97

5.11.3 Lens dimensions selection 99

5.12 Experimental layout 101

5.13 Transposability of the source to space 103

6 Conclusions **106**

7 Perspectives **107**

List of Figures

2.1 Polarisation filters. When a vertically (horizontally) polarised photon passes through a rectilinear polarisation filter, it is deflected to the right (left), as depicted in the left and middle picture respectively. When a photon that is polarised in the diagonal basis passes through a rectilinear polarisation filter, it will be deflected to the left 50% of the time and to the right 50% of the time. To be precise, it will be measured 50% of the time on the left and 50% of the time on the right. Figure from Ramona Wolf [6]. 7

2.2 The table shows an example of an implementation of the BB84 protocol using the polarisation of photons to encode qubits, assuming that no eavesdropping takes place. D: diagonal. R: rectilinear. Figure from Ramona Wolf [6]. 9

2.3 First bit sent by Alice to Bob with Eve's interaction. Figure from Wolf [6]. . . 9

2.4 Diagram of possible outcomes of the measurements of a bit in the presence of an eavesdropper when Alice and Bob's bases match. Analogously, the figure can be extended to the diagonal basis. 10

2.5 Outcomes of the measurements in a classical, non-entangled system. Figure adapted from Wilczek [12]. 11

2.6 Outcomes of the measurements in a classical yet entangled system. From Wilczek [12]. 12

2.7 General architecture of a prepare-and-measure protocol. Alice (A) and Bob have access to a quantum channel (Q) through which Alice sends quantum states to Bob (B). Eve (E) can interact with the quantum states without restrictions in this channel. Alice and Bob have also access to an authenticated classical channel (C) where they can send classical messages back and forth. Eve can listen to the messages but cannot change them. Figure from Ramona Wolf [6]. 14

2.8 General architecture of an entanglement based protocol. A source provides entangled states through quantum channels (Q) for Alice and Bob. Eve is assumed to have total control over the source to account for the worst case scenario. Alice and Bob have also access to an authenticated classical channel (C) where they can send classical messages back and forth. Eve can listen to the messages but cannot change them. Figure from Wolf [6]. 14

3.1 Multiple signals are multiplexed to be transmitted through a common medium. Afterwards, the signal in the medium is demultiplexed to retrieve several signals that can be transmitted to the right receivers. Figure from Wikimedia Commons[16]. 15

3.2 The ground stations act as the source node and destination node. The source node exchange a key K_A with the first repeater node by performing QKD. The first repeater node exchanges a second key K_C with the second repeater node. With it, the first repeater node can encrypt the first key K_A with K_C and transmit the result to the second repeater node. As the second repeater node possesses the key K_C too, it can decrypt the message and retrieve the key K_A. The process is iterated as many times as required between the different nodes. Figure from Huang et al. [18]. 17

4.1 Scattering mechanism depending on the size of the particles with respect to the wavelength. This plot considers only single scattering by spheres. Figure from John A. Dutton [27]. 21

4.2 Atmospheric transmittance with respect to the wavelength. The part of light that is not transmitted is absorbed. Figure adapted from Wikimedia Commons [28]. 22

4.3 Profile of a gaussian beam. w_0: beam waist. z_r: Rayleigh range. b: confocal parameter or depth of focus. Θ: total diffraction angle. Figure from Wikimedia Commons [31]. 24

4.4 Excess loss due to systematic pointing error for various transmitter sizes at 40° from zenith. On the left is presented the downlink and on the right the uplink. For downlink, the wavelength used is 670 nm and the receiver has a diameter of 50 cm. For uplink, the wavelength is 785 nm and the satellite receiver is 30 cm wide. The orbit altitude is 600 km and the atmosphere is rural sea level. Figure from Bourgoin et al. [35]. 26

4.5 Irradiance of the Sun at the top of the atmosphere versus spectral emitted flux of the Earth in the wavelength range 0 to 5 µm. The Earth spectrum is computed at 288 K. 27

4.6 Scattering profiles for Rayleigh and Mie scattering. Figure from Barnhart; Gunasekaran [38]. 28

4.7 Scattering profiles for Rayleigh and Mie scattering. Figure from Gruneisen et al. [40]. 28

4.8 Inside the acceptance cone, an incident light ray is refracted in the core and is then totally reflected until it reaches the other end of the fibre and is refracted out of the core. The region for which incident light rays experience total reflections and are not refracted in the cladding is defined as $\theta < \theta_{\max}$. Figure from Paschotta [50]. 31

4.9 When a collimated beam enters a thin converging lens, it is focused along a cone that corresponds to the $F\#$. The focus must be at the entrance of the fibre and the cone must be smaller than the acceptance cone. Figure from Paschotta [52]. 33

4.10 Diffraction profile of a point source through a circular aperture. Figure from Wikimedia Commons [55]. 34

4.11 General scheme of an adaptive optics system. DM: deformable mirror, BS: beam splitter, WFS: wavefront sensor, RTC: real-time controller, SMF: single mode fiber. Figure from Acosta et al. [37]. 35

4.12 Probability distribution of the detection events of the SPD for QKD operation at a clock rate of 100 MHz at night. Figure from Ko et al. [59]. 38

4.13 Performance optimisation with the temporal filtering technique in daylight. The FOV is fixed at 566 µrad. (a) QBER as a function of the valid size of the signal window. (b) Sifted and secure key rates as functions of the valid size of the window. (c) Performance of the QBER and key rates with the optimal signal window size. Figure from Ko et al. [59]. 39

4.14 Performance optimisation with the temporal filtering technique in daylight. The FOV is fixed at 283 µrad. (a) QBER as a function of the valid size of the signal window. (b) Sifted and secure key rates as functions of the valid size of the window. (c) Performance of the QBER and key rates with the optimal signal window size. Figure from Ko et al. [59]. 39

4.15 Optical link between the ground stations of Delingha and Lijiang and the satellite Micius. Figure from Yin et al. [64]. 41

4.16 Entangled photon source on board Micius. The pump laser (PL) at 405 nm is transmitted through an isolator, a Half-Wave Plate (HWP) and a Quarter-Wave Plate (QWP). The pump laser then passes through a dichroic mirror (DM) and the Polarisation Beam Splitter (PBS). When passing through the crystal (PPKTP), entangled photons are generated and follow different paths when they pass through the PBS. The two DM reflect the photon towards piezo steering mirrors (PI) that are controlled on the ground to adjust the beam pointing to maximise the collection efficiency in the single mode fibres. The long pass filter (LP) helps separating the pump photons and the signal photons. Figure from Yin et al. [64]. 41

4.17 Sagnac interferometer a) Clockwise propagation direction. b) Anticlockwise propagation direction. In both cases, orthogonally polarised photons are generated by the pump passing through the crystal. The two photons are split by the PBS to spatial modes A and B. c) Illustration of the walkoff compensation. Figure from Meraner et al. [65]. 42

4.18 The signal beam passes through the motorised wave plates to correct the polarisation shift induced by the relative motion of the satellite. It is then expanded by a beam expander (BE) and combined with a pulsed laser at 850 nm for synchronisation and a green laser at 532 nm for tracking. The Fast Steering Mirror (FSM) is used for closed-loop tracking, based on the 671 nm beacon laser images captured by camera 1 and camera 2. Figure from Yin et al. [64]. 44

4.19 Overview of the experiment setup. a) A downlink optical channel was established between the satellite Micius and the ground station of Xinglong. b) Schematic of the decoy-state QKD transmitter. Attenuated laser pulses emitted from eight laser diodes pass through a BB84 encoding module composed of two PBS, a HWP and a BS. The resulting beam is then combined through a set of mirrors to a green laser and sent through a Cassegrain telescope. A gimbal mirror (GM1) and camera (CAM1) are used in combination for the coarse tracking. c) Schematic of the receiver on ground. A 671 nm laser is used for tracking. A DM separates the incident signal from the green laser and is then analysed by the BB84 decoder which is composed of a BS and 2 PBS. The decoder ends by four detectors, one for each possible outcome. Figure from Liao et al. [67]. 45

4.20 a) Distance between the satellite and the ground station with respect to time. b) Sifted key rate with respect to time and optical link distance. c) QBER with respect to time and optical link length. Figure from Liao et al. [67]. . . . 46

4.21 Illustration of the cooperating ground stations. The distances represent the two different paths that were used for key generation. The two tables represent the achieved key lengths between the different stations. Figure from Liao et al. [68]. 46

4.22 Diagram of the exchange process. Once two secret keys are generated and one is sent to each station, the satellite performs the XOR operation. The result is sent to the station that needs to find the other's key. By performing the same operation with its own key, the shared secret key is found. Figure from Liao et al. [68]. 47

4.23 a) Illustration of the experimental setup. b) Entangled photon source on board Micius. c) Schematic of one of the receivers in the ground stations. The incident beam is composed of the signal beam and the tracking beam at 532 nm. The signal beam is separated from the tracking beam and the polarisation is compensated with the motorised HWP. The spatial filter (SF), broad-bandwidth filter and interference filter (IF) filter out the input light. The polarisation of the signal photons is then determined thanks to a decoding module composed of a BS, a HWP and two PBS. Four detectors end each branch of the analyser to detect where photons ended. Figure from Yin et al. [69]. 48

5.1 Illustration of the sum-frequency generation phenomenon in a medium exhibiting non-linearity of order 2. L is the length of the crystal. Figure from Boyd; Prato [76]. 51

5.2 Illustration of the wavenumber compensation for QPM. Λ is the length of a periodic pattern so a succession of one region of positive axis and one region of negative axis. Figure from [77]. 53

5.3 . Figure from Paschotta [78]. 54

5.4 Illustration of the spontaneous parametric down conversion of type I in the degenerated case. Figure adapted from Ghalbouni [13]. 56

5.5 Illustration of the spontaneous parametric down conversion of type II. Both photons are emitted along a cone and the overlapping region is where entangled photons are generated. Figure adapted from Ghalbouni [13]. 56

5.6 Architecture of the laser source. A laser diode at 1064 nm is amplified through three amplifiers thanks to 975 nm diodes. 58

5.7 Illustration of the stimulated emission process. An incident photon reaching an already excited atom induces an emission of another photon of the same wavelength. Figure from Wikicommons [82]. 59

5.8 Mean power of the 1064 nm laser diode with respect to the pulse repetition rate. 60

5.9 Temporal extent of the signal for the 50 ps long laser. The measurement was made for a repetition rate of 5 MHz. 62

5.10 Temporal extent of the signal for the 1000 ps long laser. The measurement was made for a repetition rate of 2 MHz. 63

5.11 Temporal extent of the signal for the 9000 ps long laser. The measurement was made for a repetition rate of 1 MHz. 64

5.12 Temporal extent of the signal for the 50 ps long laser over a longer time of measurement. The measurement was made for a repetition rate of 5 MHz. . . 65

5.13 Optical power of the 975 nm pump laser diode in function of the applied voltage. 66

5.14 Architecture of the single passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW. 67

5.15 Operating scheme of the circulator. Light generated by the laser diode enters port 1 and exits through port 2. If some back reflected light enters by port 2, it exits the circulator by port 3, isolating the laser diode. 68

5.16 Layout of a general optical circulator. The birefringent blocks help separate both polarisation components of the incident light. The Faraday rotator rotates the polarisation asymmetrically while the phase plate rotates it symmetrically. Depending on the propagation direction, this results either in a 90° rotation of the polarisation of the rays or in a 0° rotation overall. Figure from [85]. 69

5.17 Optical spectrum of the output light of the first amplifier in single passage configuration measured in the OSA. The measurement was made with a pulse duration of 50 ps and a repetition rate of 5 MHz. 70

5.18 Architecture of the double passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW. 71

5.19 Optical spectrum of the output light of the first amplifier in double passage configuration measured in the OSA. The measurement was made with a pulse duration of 50 ps and a repetition rate of 5 MHz. 72

5.20 Architecture of the quadruple passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW. . . 73

5.21 First pass of the laser pulses in the first amplifier of the pre amplifying module. 74

5.22 Second pass of the laser pulses in the first amplifier of the preamplifying module. 74

5.23 Third pass of the laser pulses in the first amplifier of the pre amplifying module. 75

5.24 Fourth pass of the laser pulses in the first amplifier of the pre amplifying module. 75

5.25 Architecture of the second amplifier in the pre amplifying module. This second amplifier is added to increase the flexibility of the system by avoiding to impose operation at the maximum power in both amplifying modules. 77

5.26 Optical power of the 975 nm pump laser diodes used in the high-power amplifier in function of the applied current. 77

5.27 Architecture of the high-power amplifier after the pre amplifying module. The high-power amplifier makes the laser reach suitable power levels for non-linear conversion. 78

5.28 Quasi-phase matching condition for the different channels of the crystal. For a specific wavelength, the QPM condition is reached in the different channels at the temperature in abscissa. Figure from Covesion [77]. 80

5.29 Oven manufactured by Covesion [77]. 80

5.30 Temperature controller manufactured by Covesion [77]. 80

5.31 Trajectory of different rays striking the converging lens with different angles with respect to the horizontal axis. The angles allow to determine the distances x_1 and x_2 if the focal length f of the lens is known. 83

5.32 Gaussian beam reaching a lens. The angle θ_0 is the maximum angle of incidence of the Gaussian beam. This angle will determine the size of the spot. Figure from Moskalev [89]. 84

5.33 Waist shift generated by the transmission of a Gaussian beam through a dielectric interface. In this case $n_1 < n_2$, and Σ is the interface. q_1 and q_2 are the complex parameters of the beam in both mediums and must remain equal. The propagation direction is from left to right. Figure from Nemoto [91] . . . 86

5.34 Waist shift that results from the modification of refractive index between the two mediums with $n_1 > n_2$. The propagation direction is from left to right. The blue dashed lines represent the trajectory of the light rays and the waist of the beam if there was no crystal from the perspective of air. The complete lines are the actual trajectory and waist of the beam. 87

5.35 Coefficients intervening in the Sellmeier equation for lithium niobate. Figure from Gayer et al. [95]. 88

5.36 Efficiency of the SHG process measured from different conditions of phase difference and focusing parameter. The phase difference is equivalent to the temperature when the crystal properties are known and the focusing parameter can be expressed as the waist of the beam in the crystal. The crystal was 2 cm long for this experiment. Figure adapted from Smirr [97]. 89

5.37 Conceptual optical design. The purpose of the setup is to focus the laser beam in the crystals at their centre. To guarantee the appropriate polarisation, a half-wave plate is used with a polariser. After each focusing, the output beams are collimated with converging lenses. The dichroic mirrors filter the output signal after the crystals. HWP: Half-wave plate. DM: Dichroic mirror 91

5.38 Disposition of a lens to collimate a beam. s is the distance from the lens to the waist of the beam. Figure from Edmund Optics [98] 93

5.39 Optimal focusing ratio of the lens with respect to the scale of the conversion crystal expressed as the ratio of the focal length on the length of the crystal. The focusing ratio is the ratio of the targeted waist size in the crystal imposed by the material on the size of the beam at the focusing lens. The focusing ratio is optimal because the waist size in the crystal is the critical limit of the material. 94

5.40 Rayleigh range of the collimated beam of adequate size as a function of the scale of the conversion module expressed as the ratio of the focal length on the length of the crystal. The waist used to compute the Rayleigh range is the optimal waist such that the focused spot size is exactly equal to the limit of the material. 95

5.41 Optimal focusing ratio as a function of the focal length of the collimating lens. The minimal focal length which corresponds to a focusing ratio of 1 is much larger for SPDC than for SHG. 97

5.42 Picture of the preamplifier. 102

5.43 Picture of the high-power pump diodes station. 102

5.44 Picture of the high-power amplifier. 102

5.45 Picture of the SHG layout. 102

List of Tables

2.1 Bit encoding in the rectilinear and diagonal bases 6

5.1 Iterations of the design. f_1 is the focal length of the focusing lens before the SHG crystal. f_2 is the focal length of the collimating lens before the focusing lens in front of the SPDC crystal. f_3 is the focal length of the focusing lens before the SPDC crystal. The spot sizes are the actual radius of the waist of the beam after passing through the real lenses. 100

Acronyms

AO Adaptive Optics.

BBO Beta Barium Borate.

BS Beam Splitter.

DCR Dark Count Rate.

DM Dichroic Mirror.

FBG Fibre Bragg Grating.

FM Faraday Mirror.

FOV Field Of View.

FSM Fast Steering Mirror.

FSO Free-Space-Optical.

FWHM Full-Width at Half-Maximum.

HWP Half-Wave Plate.

LEO Low Earth Orbit.

OSA Optical Spectrum Analyser.

PBS Polarisation Beam Splitter.

PM Polarisation-Maintaining.

QBER Quantum Bit Error Rate.

QKD Quantum Key Distribution.

QPM Quasi-Phase-Matching.

QUESS Quantum Experiment at Space Scale.

QWP Quarter-Wave Plate.

SFG Sum-Frequency Generation.

SHG Second-Harmonic Generation.

SKG Secret Key Generation.

SNSPD Superconducting Nanowire Single-Photon Detector.

SPAD Single-Photon Avalanche Diode.

SPD Single-Photon Detector.

SPDC Spontaneous Parametric Down-Conversion.

TDM Time Division Multiplexing.

WDM Wavelength Division Multiplexing.

1 Introduction

In the past decades, technologies have tremendously evolved and have allowed breakthrough innovations. From the 2000s on, computers became common; with them, the Internet has become a significant part of everyday life. They paved the way for a new world where transactions, communications and information rely on the Internet.

However, with the emerging opportunities the Internet brought came new threats for any user. Nowadays, many aspects of everyone's life rely on internet transmissions. As much information transits online, ill-intentioned people can access sensitive communications. To prevent sensitive information from being collected by unintended actors, cryptography is necessary to ensure the privacy of communications.

Cryptography is the practice and study of techniques to ensure secure communications in the presence of adversarial behaviour. The earliest known use of cryptography traces back to 1900 BC in Egypt [1]. From this time on to the modern era, several techniques have been developed with increasing complexity and efficiency. The set of rules or steps to encrypt or decrypt a message is called a cypher or key. Today, modern techniques rely on computer encryption with bits sequences. They have the advantage of requiring few resources to be used but breaking the cypher requires efforts many orders of magnitude larger. The difficulty for an eavesdropper is the algorithmic complexity of breaking the code because modern computers have limited capabilities.

However, technological evolutions predict that quantum computers will soon become a reality. Their computation capabilities are unparalleled, and the mathematical complexity of breaking a modern key will not be sufficient to ensure secure communications. Indeed, such computers are expected to be able to break most modern codes [2]. To prepare against the risk quantum computers represent, an inherently secured cryptographic technique has to be developed. The topic of this study is one of them.

Quantum Key Distribution (QKD) is a communication method that relies on the quantum properties of light to distribute an inherently secure key between parties. With a common key, information can be encrypted by the first party and then sent to the second party. Since the second party knows the key, it can decrypt the communication to retrieve the message. Its security is guaranteed because the presence of an eavesdropper can be detected, and the communication aborted should it happen. QKD is an emerging discipline and much research is currently being conducted to concretise it.

QKD is raising the interest of many instances around the world. The EU is currently building the bases of its IRIS^2 programme to deploy a new constellation of satellites. IRIS^2, which stands for Infrastructure for Resilience, Interconnection and Security by Satellites, is the EU's programme to address communication issues in the near future. The constellation is projected to be fully operational in 2027 [3]. Among the key challenges it aims to address, IRIS^2 focuses on connectivity and security. Several satellites of the constellation will be part of the European Quantum Communication Infrastructure, EuroQCI. The initiative aims to build a secure quantum communication infrastructure to serve government institutions and their data centres. However, the service is not only focused on governments as it is also

planned to provide secure communications for hospitals, energy networks, and more [4].

To prepare this initiative, the EU, in partnership with ESA and space industries around Europe, are currently developing the Eagle-1 satellite. The satellite is the first to be developed through such a partnership, and it is expected to demonstrate the feasibility of QKD within the European Union with a satellite-based system. Eagle-1 is due to launch in 2024 and will perform validation experiments supported by the European Commission for three years. The mission will be the precursor of the EuroQCI [5].

There are many constraints and considerations to make regarding the implementation of a QKD system and its integration in the current communication networks. The present work proposes to discuss the current state of the technology, its challenges and its future perspectives from two angles.

The first part of this work aims to describe the operating principles of QKD and its implementations through an extensive literature review. Section 2 starts by explaining the bases of the technique and the quantum considerations at the origin of the safety of QKD.

Then, Sec. 3 and 4 introduce the principles and technical challenges of respectively optical fibre QKD and free-space QKD. These two sections also present encouraging solutions to the problem they raise. Section 4 ends with an analysis of the Chinese satellite Micius and its operation principle before presenting the results of experiments it conducted.

Afterwards, Sec. 5 presents an experimental photon source designed and developed in the frame of this work. The section follows the design process of the photon source and introduces the different theoretical and concrete tools used to build it. It details the laser assembly, the optical considerations and the optics selection to generate photons.

Before the end of this study, Sec. 6 discusses the different results observed in this work and their limitations. Finally, Sec. 7 ends this study by arguing about the future perspectives for the technology and the experimental photon source.

2 Bases of the technique

The current section introduces the theoretical background to understand the principles behind Quantum Key Distribution. It follows the structure presented by Wolf [6].

2.1 Bases of cryptography

Before diving in the advantages of quantum key distribution, it is important to understand what is required to guarantee a secure communication. In any encryption scheme, the two parties that wish to communicate need a key to encrypt and decrypt a message. In the rest of this manuscript, the two parties are called Alice and Bob. A key is any mechanism, set of rules, artificial set of symbols or mechanical device that can encrypt a message. A renowned example is the Caesar cipher. This encryption technique consists in replacing the letters of the message we want to transmit by the letter a set number down the alphabet. This simple algorithm is considered to be a key.

Though many encryption schemes exist, QKD relies on the Vernam cipher also called one-time pad. The one-time pad is a theoretically secure scheme that is impossible to crack. It is considered "information-theoretically secure". It means that the ciphertext gives no information about the message. In the one-time pad scheme, the key is usually a string of bits i.e. a sequence of zeros and ones. The message is usually represented as a bit string too. Thanks to the key, Alice and Bob can communicate following a simple procedure.

First, Alice encrypts the message with her key. One possibility is to perform a parity addition with the key and the message. This operation is also called "exclusive or" or "exclusive disjunction". The results of the operation are given in equation 2.1.

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0 \end{aligned} \tag{2.1}$$

Each bit of the ciphertext is produced by binary adding a bit from the key to a bit from the message. The cipertext is thus the message modified thanks to the key.

Afterwards, the ciphertext is sent to Bob over a public channel. This means that an adversary has access to the ciphertext but cannot change it. This is not a problem as long as the adversary has no information about the key. Without it, the adversary is not able to decrypt the message.

Finally, Bob decodes the message by performing the same operation with the ciphertext and his key. If the keys are equal, Bob holds the exact same message as the one Alice sent after decoding. Let's consider a short example to illustrate the procedure.

Alice wants to send the message 10110 to Bob. To do this, she uses the key 01010 to encode her message :

$$\begin{array}{rccccc} & 1 & 0 & 1 & 1 & 0 \\ \oplus & 0 & 1 & 0 & 1 & 0 \\ \hline = & 1 & 1 & 1 & 0 & 0 \end{array} \tag{2.2}$$

Afterwards, Bob uses the same key to decrypt the message :

$$\begin{array}{rccccc} & 1 & 1 & 1 & 0 & 0 \\ \oplus & 0 & 1 & 0 & 1 & 0 \\ \hline = & 1 & 0 & 1 & 1 & 0 \end{array} \tag{2.3}$$

In the end, Bob has retrieved the message. This short example allows to illustrate an important feature of the key. It needs to be at least as long as the message. This encryption scheme was proven to be information-theoretically secure by Claude Shannon in 1949 [7]. However, the key has to fulfill certain properties.

1. It first needs to be at least as long as the message as the example has shown.
2. It has to be truly random which means that the individual key bits are not correlated in any way. This requirement is not easily matched as generating true randomness is a highly non-trivial task.
3. The key can never be reused in whole or partly otherwise an adversary can deduce some information on several messages if they intercepts all the ciphertexts.
4. The key must be kept completely secret by the communicating parties.

These criteria constitute the bases of one-time pad (OTP) encryption. However, they pose some drawbacks regarding implementation. Generating true randomness is a harsh task as it goes beyond statistical randomness [8]. Disposing the key after use means that in order to communicate, a new key must be generated each time a new message needs to be transmitted. The rate at which a key is generated and transmitted is thus of tremendous importance to ensure seamless communications. Furthermore, Alice and Bob need to find a way to generate exactly the same key at a distance.

What Alice and Bob need is thus a device able to manage this task. Such an ideal device should provide random identical keys to Alice and Bob. Moreover, an eavesdropper, that will be called Eve, should not be able to interact with the source. She cannot input anything to it or receive any output from it.

In practice unfortunately, it is impossible to build such an ideal device. One cannot completely prevent Eve from interacting with it. For instance, she can cut the fibres of the communication channels Alice and Bob use. Moreover, some information will probably be leaked to Eve. To account for these limitations, the requirements on the key can be weakened

in such a way that the resulting device will not be perfect anymore but its failure probability is small. The probability for the keys to differ or for the protocol to abort must remain very small.

The key that is produced by the source needs to be almost perfect. Almost perfect means that it is close to a uniformly random key. The individual key bits are also required not to have any correlation with each other. On Eve's side, a close-to-perfect key is independent of the state of Eve's system and if information leaks, it cannot be exploited. Finally, though it is impossible to prevent Eve from interacting with the device, an attack can be detected. Should it happen, the protocol needs to be interrupted. The source does not produce inherently secure keys. If a key is generated, however, it is secure.

Quantum key distribution addresses this necessity. The purpose of QKD is to create a device that generates keys that meet the weakened criteria. To do so, the quantum properties of light are exploited. In quantum mechanics, particles are described by a quantum state. A quantum state is a mathematical description that provides a probability distribution of the physical properties we can measure on a system. It associates a probability with each outcome of the measurement of a physical property. As such, quantum mechanics is inherently probabilistic in the current state of the theory. This feature is of utmost importance as it can be exploited for the development of the aforementioned device. Moreover, the no-cloning theorem states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. This guarantees that it is impossible to measure without uncertainty a property of a quantum system [9]. By using multiple copies of the quantum system, it would be possible to measure conjugated properties and violate the Heisenberg uncertainty principle.

The following section illustrates the advantages of quantum mechanics for creating a suitable key for one-time-pad encryption. It details the first example of a quantum key distribution protocol: the BB84 protocol.

2.2 The BB84 protocol

The BB84 protocol, named after its developers Charles Benett and Gilles Brassard in 1984 [10], is the pioneering method for distributing quantum keys. The BB84 protocol relies on the linear polarisation property of photons to encode qubits. The notion of qubit is explained in the next paragraph. When photons are emitted, the propagation direction and the oscillations of the electric field describe a plane. When a photon is linearly polarised, this plane does not move along the propagation. The polarisation state is usually described in three bases. A basis is a pair of two orthogonal states. In a basis, both states are either 0 or 1. Both states can be interpreted geometrically however. For instance, in the rectilinear basis, the two states 0 and 1 correspond to the horizontal and vertical polarisation respectively. In the diagonal basis, the two states correspond to 45° or 135°. In the circular basis, the two states are left handed or right handed. Any two of these three bases are conjugate to one another. The BB84 protocol uses two bases to guarantee its security since it relies on linear polarisation that is described in the rectilinear or in the diagonal basis.

The measurement of the polarisation state allows to leverage one of the most significant aspects of quantum mechanics. The polarisation of photons allows to encode qubits. A qubit represents a two-state quantum system. The polarisation of a photon can be represented by a qubit in the appropriate basis. A qubit has the particularity to be in the superposition of two coherent states that are represented as $|0\rangle$ and $|1\rangle$. A classical bit i.e. a value of 0 or 1 can be encoded in the polarisation of a photon in a given basis. While the classical bit can only take one value at a time, a qubit is not bound by this restriction. For example in the case of photons, the state of polarisation of a linearly polarised photon at 45° can be represented in the rectilinear basis as the superposition of the two fundamental states, vertical and horizontal:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{2.4}$$

The diagonal polarisation can thus be represented by a qubit in the rectilinear basis. On the other hand, Tab. 2.1 gives the correspondence between the linear polarisation of a photon and the value of the encoded classical bit in the different bases.

Bit value	0	1
Rectilinear basis	↔	↕
Diagonal basis	↙↗	↖↘

Table 2.1: Bit encoding in the rectilinear and diagonal bases

To distinguish the different polarisation states, a measurement needs to be made. To do so, a possibility is to use a filter to perform the measurement in a basis. According to the indeterminacy in quantum mechanics, no measurement distinguishes between the four polarisation states as they are not all orthogonal. The only possible measurement is between two orthogonal states. There exist filters that allow to distinguish between horizontally and vertically polarised photons and analogously between +45° and -45°. Some filter mechanisms are explained in the later sections.

When a vertically polarised photon passes through the rectilinear filter, it is deflected according to its vertical polarisation and can be measured afterwards by a detector. A horizontally polarised photon passing through the filter will be deflected in the other direction and thus a properly placed detector will measure it. Hence two detectors are required, one for each orientation. Depending on its polarisation, the photon will end up reaching one detector or the other. If a diagonally polarised photon reaches the rectilinear filter, however, the photon will be randomly deflected in one of the two directions.

As presented in Eq. 2.4, a diagonal polarisation is described as a superposition of the horizontal and the vertical polarisation state. Measuring in the rectilinear basis will yield one of the two possible measurements with the corresponding probability. The polarisation state is thus modified by the filter as after passing through, it is either in the vertical state or the horizontal state. Since the polarisation state is changed after the filter, it is impossible to determine its orientation before it passed through. Furthermore, since the result is random, no information is gained after the measurement. The same applies in the case where the

measurement is performed in the diagonal basis except the rectilinearly polarised photons will be the ones deflected and changed randomly. The two bases are qualified as mutually unbiased. The process is represented in Fig. 2.1.

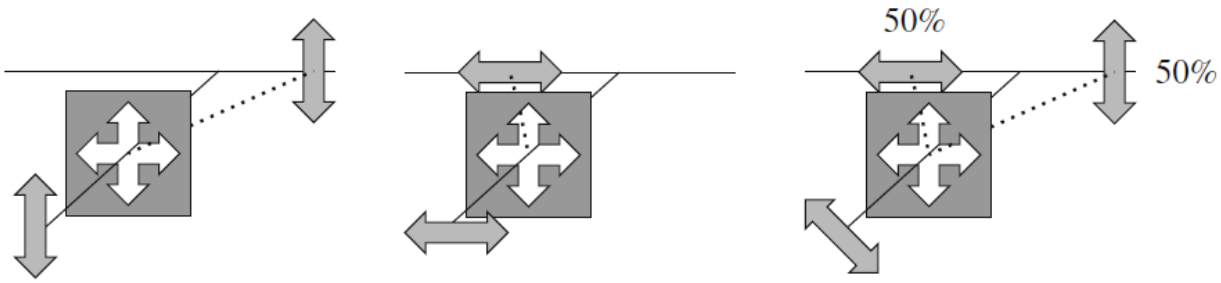

Figure 2.1: Polarisation filters. When a vertically (horizontally) polarised photon passes through a rectilinear polarisation filter, it is deflected to the right (left), as depicted in the left and middle picture respectively. When a photon that is polarised in the diagonal basis passes through a rectilinear polarisation filter, it will be deflected to the left 50% of the time and to the right 50% of the time. To be precise, it will be measured 50% of the time on the left and 50% of the time on the right. Figure from Ramona Wolf [6].

Figure 2.1 illustrates the fundamental property of quantum mechanics that ensures secure communications. When a measurement is made, the system state is modified. The state of the system after the measurement corresponds to the outcome of the measurement. In Figure 2.1, the state of a photon that was diagonally polarised before the filter becomes either horizontal or vertical according to the side the photon is measured at. This property will be exploited to detect the presence of Eve, an adversary, as explained further.

Now that the essential principle of the measurement has been explained, it is possible to describe the procedure of the BB84 protocol. Two authorised parties, Alice and Bob, want to establish a secret key over a distance to communicate. To do this, they have access to two different channels. The first channel is a quantum communication channel that allows quantum states to be transmitted. In the case of photons, this channel can be a series of optical fibres or simply free-space. The quantum channel is completely insecure as it is accessible by Eve. She can perform any operation allowed by quantum mechanics. Alice and Bob also communicate through a second public classical channel which can be broadcast radio or the internet for instance. The public channel is also accessible by Eve but she cannot change the message that is sent.

The first phase is called quantum transmission. It includes all the operations that are performed on quantum states. The classical bits are encoded and decoded into quantum states and communication is made over a quantum channel.

Alice starts by choosing a string of N random bits. For each bit, she chooses randomly the value and the basis. According to the two, she encodes the bit following Table 2.1 by preparing a photon in the corresponding state. She records the value of the bit, the polarisation basis and the time she sent the photon. She repeats the process for the N bits that she wants to send.

Bob then receives the photons sent by Alice. For each photon, Bob randomly and independently of Alice chooses the basis in which he will measure the polarisation of the incoming photons. He obtains a bit for each photon. Similarly to Alice, Bob records the basis he used and the bit value he obtained after his measurement for each photon. After this step, Alice and Bob both hold a classical bit string called the raw key pair. The quantum part of the process ends here.

The following steps are purely classical. Bob publicly announces the bases he chose to measure the polarisation of the photons Alice has sent him. Alice can thus compare Bob's bases to the ones she selected to send the photons. She then announces which bases Bob chose correctly i.e. when their bases were the same. With this information, Alice and Bob can discard all the bits for which their choice of bases did not match. This is called the sifting process.

Now that they possess bits that were measured in the same basis, Alice and Bob want to estimate the error rate in their shared key. To do so, Bob reveals at random some of the bits in his key. In the absence of perturbation or eavesdropper, the bits should coincide as a prepared photon remains in its prepared state in the absence of said perturbation. A world without perturbations does not exist however and some errors might appear even in the absence of an eavesdropper. The nature of these perturbations is detailed later. If the error rate is superior to a statistical threshold accounting for those perturbations, it indicates that there has been some eavesdropping and the protocol is aborted. The discrepancies the eavesdropper generates will be detailed in the next section. After Alice and Bob conclude that no eavesdropper was spying on them, they discard the bits Bob revealed as they are now public. Alice and Bob now possess two strings of equal length but some errors might still be present. Alice and Bob need to ensure their keys are the same. They will thus perform certain steps to correct errors and increase the secrecy of their keys.

The first step is called error correction where Alice and Bob erase all errors in their bit strings and thus possess identical keys afterwards. Many error correction protocols exist as it was a well-studied research area even before quantum cryptography was imagined. The first error correction code was invented in 1950 by the American mathematician Richard Hamming [11]. He pioneered this research field and several error correction protocols or error correction codes were invented afterwards.

After the error correction, Alice and Bob proceed to privacy amplification in order to minimise Eve's knowledge of the key. This is achieved by using randomness extractors. These are functions that take as input a source of randomness and together with a small uniformly random string called the seed yields as output a uniformly random output that is longer than the seed. The seed is common and communicated via the public channel. This procedure is important to make sure Eve has no information on the actual key by generating a random key with respect to Eve's information. At the end of these two processes, Alice and Bob possess identical keys or bit strings that are close to being uniformly random and Eve has almost no knowledge of the key. It is interesting to notice that although the protocol can be aborted if the presence of Eve is detected, these steps are still applied to minimise any information she could have gathered on the key. As there are also errors that are not linked to Eve, the protocol is aborted only if the number of error bits is larger than a threshold. The threshold is determined such that if Eve knows fewer bits than this value, privacy amplification can be

used to reduce Eve's knowledge to an arbitrarily small amount at the expense of the length of the key. To illustrate the protocol, a short example is developed in Fig. 2.2 and the influence of Eve will be shown right after.

Quantum transmission													
Alice's random bits	0	1	1	1	0	1	0	1	1	0	0	1	1
Random sending bases	D	R	D	D	R	D	R	R	D	D	D	R	D
Photons Alice sends	↗	↕	↘	↗	↔	↘	↔	↕	↘	↗	↗	↕	↘
Random receiving bases	D	R	R	D	R	D	D	D	R	D	R	R	D
Bits as received by Bob	0	1	0	1	0	1	1	1	0	0	0	1	1
Classical post-processing													
Bob reports bases of received bits	D	R	R	D	R	D	D	D	R	D	R	R	D
Alice says which bases are correct	OK	OK		OK	OK	OK				OK		OK	OK
Presumably shared information (without eavesdropper)	0	1		1	0	1				0		1	1
Bob reveals some key bits		1				1						1	
Alice confirms them		OK				OK						OK	
Outcome													
Remaining shared secret bits	0			1	0					0			1

Figure 2.2: The table shows an example of an implementation of the BB84 protocol using the polarisation of photons to encode qubits, assuming that no eavesdropping takes place. D: diagonal. R: rectilinear. Figure from Ramona Wolf [6].

Let's investigate what happens if the eavesdropper Eve tries to gather information on the polarisation state of a photon. This will illustrate why the protocol is theoretically secure. The key idea as explained earlier is that in quantum mechanics it is impossible to gain information on a system without disturbing it. Every interaction with a quantum system and so every measurement will alter the said system. This can be exploited to detect the presence of Eve. Let's consider the first column of Figure 2.2 but Eve interacts by trying to measure the first bit while it is being sent to Bob. The interaction is summarised in Fig. 2.3.

Alice's bit:	0
Alice's basis:	D
State that is sent:	↗
Eve's measurement basis:	R
State after the measurement:	↔
Bob's measurement basis:	D
Bob's bit:	1

Figure 2.3: First bit sent by Alice to Bob with Eve's interaction. Figure from Wolf [6].

Since Eve does not know the basis Alice chose to prepare her photon, she is obliged to choose one randomly. In this case, she chose the wrong basis and performed a measurement. She measured a value of the bit of 0 which means the photon is in a horizontal polarisation state after measurement. Afterwards, Bob made a measurement in the correct basis and obtained the value 1. When comparing their results, if this bit is part of the ones used to estimate the error rate, Alice will be able to spot the mismatching despite the fact that Bob chose the same basis as her. They will then be able to attribute this error to the presence of an eavesdropper if there is no other perturbation.

However, it is worth noticing that the described case is not the most probable to happen. Eve has a 50% chance to choose each basis. This means that in half of the cases on average she cannot induce modifications because she measures the photon in the same basis as Alice and Bob. In the other half of the cases, she chooses the wrong basis. Afterwards, the photon has a 50% chance to be in each polarisation state of this basis. Bob will then measure the photon polarised in the wrong basis in the same basis as Alice, having again a 50% chance to find the photon in each state of the basis. This is represented in Fig. 2.4.

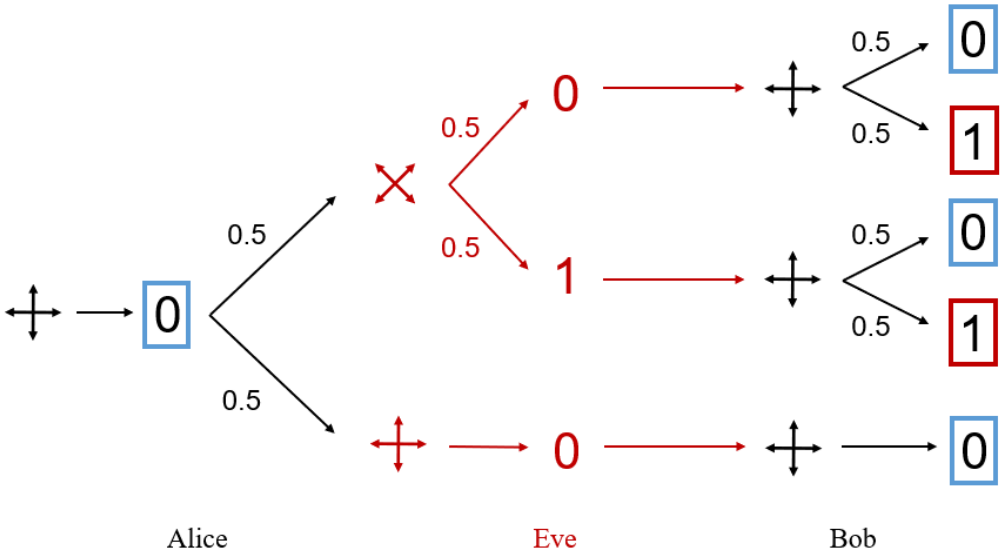

Figure 2.4: Diagram of possible outcomes of the measurements of a bit in the presence of an eavesdropper when Alice and Bob's bases match. Analogously, the figure can be extended to the diagonal basis.

At the end of the process, only two outcomes can jeopardise the presence of Eve. Both have a 12.5% chance to occur which leads to a 25% chance in total for each bit for which Alice and Bob chose the same basis. At first, this result seems surprising as it indicates that Eve has a larger probability of not being detected at the end of the comparison of a bit. However, the probability that Eve will induce at least one error over a total of n bits grows larger as n increases according to

$$P(\text{Detecting Eve}) = 1 - \left(\frac{3}{4}\right)^n. \tag{2.5}$$

This relation determines the number of bits n that Alice and Bob are ready to sacrifice to detect the presence of the eavesdropper. In practice, the protocol is not aborted for a single error but error rates have to be estimated to guarantee the security of the protocol.

2.3 Other protocols and methods

The BB84 protocol is the first QKD protocol that was imagined. Over the years, many others were designed. There are two categories of protocols. The first category is the one the BB84 protocol belongs to. It is part of the prepare-and-measure protocols. The second category of protocols is those based on entanglement. In order to understand them, it is important to explain the notion of entanglement.

Entanglement is a quantum property that several particles can exhibit in which they are spatially separated and yet their individual states are correlated. Two particles that are entangled cannot be described individually. In the case of photons, it corresponds to states for which the individual state of one of the two photons is impossible to describe independently of the state of the other whatever the distance between the particles. Let's consider a simple example to grasp the essence of entanglement. The objective is to measure the shape of two objects in a system. They can either have a circular shape or a square shape. In a classical system, each object can have any of the two shapes with even probabilities. In the end all the combinations are equally likely as shown in Fig. 2.5.

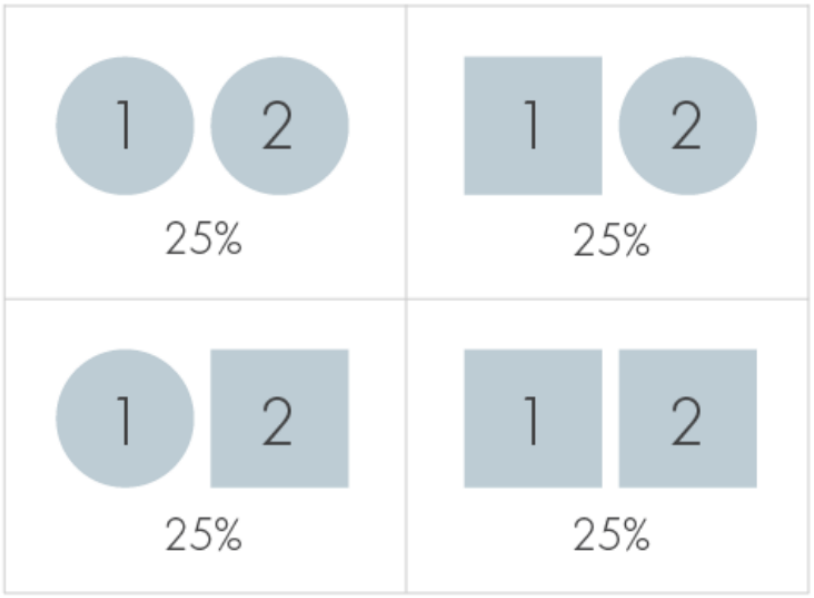

Figure 2.5: Outcomes of the measurements in a classical, non-entangled system. Figure adapted from Wilczek [12].

In the classical case, measuring the shape of the first object gives no information about the second. They are not correlated. In the case of entangled objects or systems, there will be some correlation. One possibility is for both shapes to match. This is represented in Fig. 2.6.

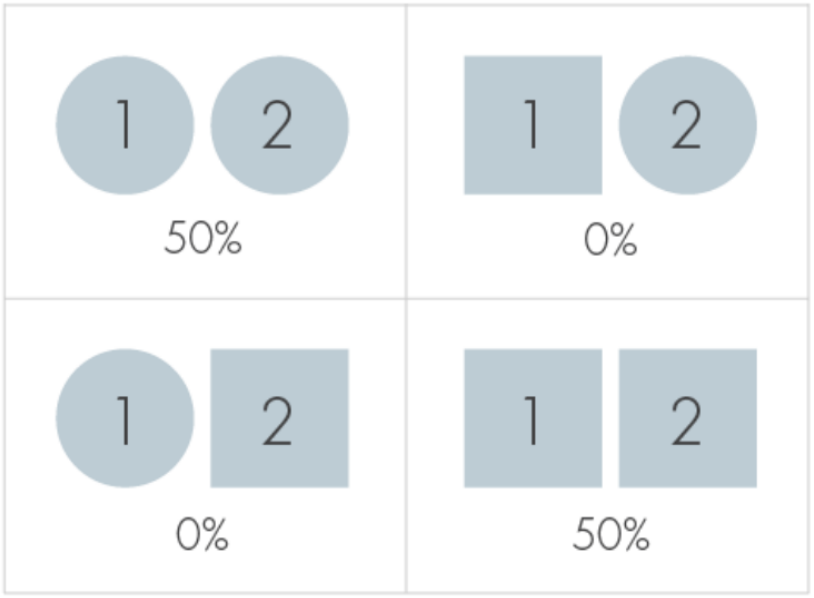

Figure 2.6: Outcomes of the measurements in a classical yet entangled system. From Wilczek [12].

This representation of classical entanglement illustrates the principle of correlation of entanglement. When a measurement is performed to determine the shape of the first object, the result allows to infer the shape of the second object with certainty since both share the same shape. However, correlation is not sufficient to explain quantum entanglement. In quantum systems, entanglement is also heavily dependent on the measurement that is made.

From a practical point of view, the correlation of entangled photons can be used to generate secret keys between the two parties Alice and Bob. When the same property is measured along the same axis by Alice and Bob on their respective photon of the pair, Alice can infer what Bob measured as long as the photons are entangled. It is thus required to verify the entanglement of the photons. To do so, they can use the CHSH inequality. This inequality is a bound on the expectation values of certain classical correlations. The formalism of the inequality presented in this work is the one developed by Ghalbouni [13]. Let's consider four classical random variables that can take the values -1 or $+1$. The variables are ϵ_A, ϵ'_A, ϵ_B and ϵ'_B. Bell's parameter is defined as:

$$S = \epsilon_A\,\epsilon_B + \epsilon'_A\,\epsilon_B - \epsilon_A\,\epsilon'_B + \epsilon'_A\,\epsilon'_B. \tag{2.6}$$

Bell's parameter is comprised between -2 and 2. This can be verified by replacing the random variables by all the combinations of -1 and $+1$. The expression can be rewritten to obtain the inequality by taking the expectation of Bell's parameter:

$$\langle S\rangle = \langle\epsilon_A\,\epsilon_B\rangle + \langle\epsilon'_A\,\epsilon_B\rangle - \langle\epsilon_A\,\epsilon'_B\rangle + \langle\epsilon'_A\,\epsilon'_B\rangle \leq 2. \tag{2.7}$$

In the case of polarisation entanglement, Clausert, Horne, Shimony and Holt [14] defined the parameter S as:

$$S(a, a', b, b') = E(I_a, II_b) - E(I_a, II_{b'} + E(I_{a'}, II_b) + E(I_{a'}, II_{b'}). \quad (2.8)$$

$E(I_a, II_b)$ is the quantum correlation between measurements on the first particle with a polariser at an angle of a and measurements on the second particle with a polariser at an angle of b. Finally, in order to demonstrate the entanglement of the photons, Alice and bob need to chose appropriately the angles at which they perform the measurements of the polarisation to find a value superior to 2 and thus violate the CHSH inequality. The maximum value that is achievable is equal to $S = 2\sqrt{2}$. In that case, this means that both photons are in a maximally entangled state. Maximally entangled biparties state cannot be entangled with a third party and so Eve has no information about the key. In practice, the value of S is lower than the maximum value but can still violate the CHSH inequality. In that case, Eve can have some knowledge about the key yet a secret key can still be extracted. This criterion helps detecting the presence of an eavesdropper as Eve will reduce the correlation between the photons.

The two categories of protocols consist of three different families. The first family, known as discrete variable protocols, relies on encoding bits in discrete variables of photons. The polarisation based protocols belong to this category. They were the first to be invented and are the most widely implemented. The two other categories are called continuous variable and distributed phase reference coding aim to overcome practical limitations. Continuous variable QKD protocols encode the key information on squeezed states and coherent states of light. Light is treated as a wave and the properties that are studied are the amplitude, the phase and quadratures. Finally in the distributed phase reference coding, information is encoded thanks to phase relationships between pulses. This latter family however is rarely encountered.

2.4 General architecture

The main components are the same for each system even though their nature might differ. A general QKD system is composed of a source of photons that are transmitted through a transmitter. The photons are sent through a quantum channel to a receiver or two depending on the type of protocol.

In a prepare-and-measure protocol, Alice prepares the photons and sends them to Bob who intercepts them and measures some properties. Eve has access to the quantum channel and the classical channel but she can only modify the communication in the quantum channel as discussed in section 2.2. The architecture is represented in Fig. 2.7.

In an entanglement based protocol, entangled pairs of photons are sent by an external source. The source sends one photon to Alice and the other one to Bob. The source is supposed to be untrustworthy as neither Alice nor Bob have access to it. It is supposed that Eve can access the source but this does not compromise the security of the protocol as any attempt at modifying the photons will result in a loss of entanglement and thus of correlation. The presence of Eve can be spotted by studying the CHSH inequality with some measurements. The general architecture is represented in Fig. 2.8.

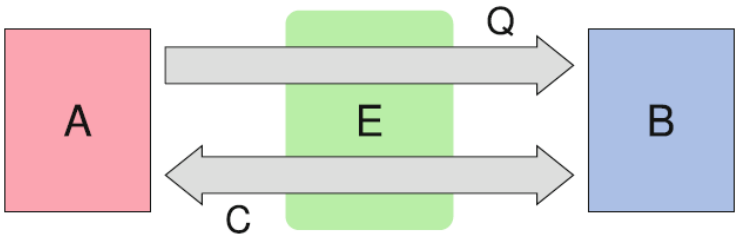

Figure 2.7: General architecture of a prepare-and-measure protocol. Alice (A) and Bob have access to a quantum channel (Q) through which Alice sends quantum states to Bob (B). Eve (E) can interact with the quantum states without restrictions in this channel. Alice and Bob have also access to an authenticated classical channel (C) where they can send classical messages back and forth. Eve can listen to the messages but cannot change them. Figure from Ramona Wolf [6].

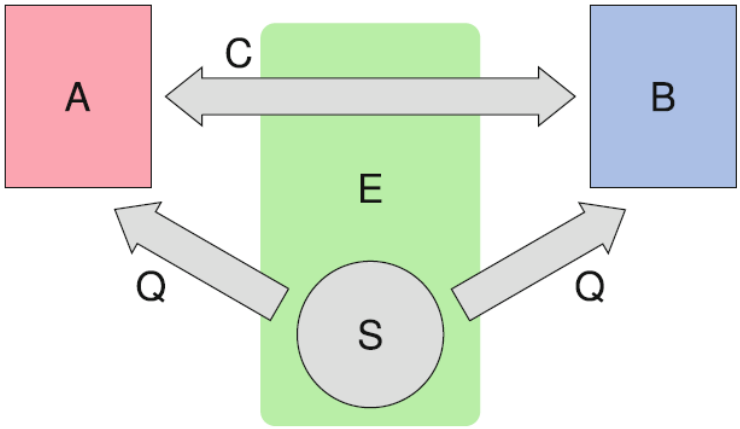

Figure 2.8: General architecture of an entanglement based protocol. A source provides entangled states through quantum channels (Q) for Alice and Bob. Eve is assumed to have total control over the source to account for the worst case scenario. Alice and Bob have also access to an authenticated classical channel (C) where they can send classical messages back and forth. Eve can listen to the messages but cannot change them. Figure from Wolf [6].

Having comprehensively addressed the theoretical aspects of quantum key distribution (QKD), it is now opportune to shift our focus towards its practical implementation. The following two sections provide a detailed presentation and discussion of the primary practical implementations of QKD, with a particular emphasis on free-space QKD. Each implementation's specific aspects are introduced, followed by an analysis of their respective advantages and drawbacks. Subsequently, the challenges involved in achieving a global implementation are explained, and potential solutions are presented. Lastly, a concise overview of several proof-of-principle experiments is provided.

3 Optical fibre QKD

One approach to implement QKD is to use optical fibres. It is historically the first method that was developed to implement QKD. As the name suggests, optical fibres are used to transmit photons from one place to another.

There are several advantages to using optical fibres for quantum key distribution. Optical fibres are mature channels that are already being used around the world. It is a well-known technology that allows one to have deep control over the transmission environment. Besides, optical fibre networks are already in use in many cities. These pre-existing networks provide a basis for further expansions. The existing networks could be adapted such that they could be used for QKD without compromising their current function which is to provide data links between parties [15].

In order to integrate QKD in existing optical networks, it is required to resort to multiplexing techniques. Multiplexing is a method through which multiple signals are combined in a single signal in a shared channel. The opposite operation is called demultiplexing. The intent of multiplexing is to mix quantum and classical signals together to allow the existing networks to be used. Multiplexing and demultiplexing are represented in Fig. 3.1.

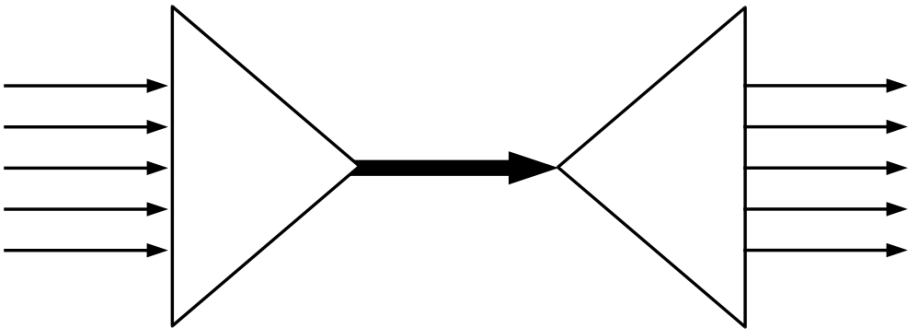

Figure 3.1: Multiple signals are multiplexed to be transmitted through a common medium. Afterwards, the signal in the medium is demultiplexed to retrieve several signals that can be transmitted to the right receivers. Figure from Wikimedia Commons[16].

There are two types of multiplexing: Time Division Multiplexing (TDM) and Wavelength Division Multiplexing (WDM). TDM is used to transmit multiple data streams over a communication channel by separating them into multiple segments as explained by Sharma et al. [15]. Each data stream is demultiplexed at the receiving end in the time domain. TDM can

also be seen as sequencing groups of bits or bytes from each input stream one after another to the appropriate receiver.

Wavelength Division Multiplexing (WDM) uses the wavelength of light to separate the different signals to be transmitted. It permits the transmission of multiple optical signals onto a single fibre using multiple wavelengths. WDM is of interest since the wavelengths of quantum signals and classical ones could be selected such that multiplexing technologies allow the dissociation of the signals.

The global usage of optical fibres was achieved thanks to thorough research and development. As such, optical fibres are already a well-developed technology which could shorten the adoption procedure to implement QKD in optical networks. Nevertheless, adapting existing networks for QKD brings many challenges to the table that are explained in the next section.

3.1 Technical challenges

One of the main challenges towards global QKD integration is due to the nature of the transmission channels. Optical fibres exhibit losses of signal that are proportional to the distance travelled by the signal [17]. Moreover, optical networks transmit weak quantum signals poorly. As the length of the transmission channel increases, the signal becomes so faint that it is not usable anymore. To avoid this problem for long-distance transmission, it is necessary to use trusted repeater nodes. A repeater node is the analogous of an amplifier in a conventional communication system. Its role is to repeat the signal such that it remains usable for communication. It is worth stressing that because of the no-cloning theorem, the way a repeater functions is different than an amplifier. It is impossible to amplify a quantum signal because this would imply that the quantum state is completely known in order to copy it. This is impossible because of Heisenberg's uncertainty principle. What a repeater can do however is to perform quantum key distribution with its adjacent nodes. This means that the nodes are required to know the key to function and are required to be trusted as a consequence [15]. Precisely, the key that needs to be transmitted is encrypted with intermediate keys between adjacent nodes. This key is transmitted through a sequence of QKD protocols where the key is encrypted by intermediate keys of same length between the nodes. The operational principle of trusted repeaters is illustrated in Fig. 3.2 with satellites.

The longer the transmission distance has to be, the more repeaters are needed along the channel. Moreover, the low transmission reach of quantum signals in classical optical fibres constraints the number of repeater nodes which must be larger than conventional nodes. With a large number of repeater nodes arises an increasingly high risk of failure and increasing costs. In case of a failure, the secret key rate and transmission distance can get drastically reduced. This risk requires new strategies and survivability schemes to be developed. To avoid the reliance on repeater nodes, detailed research on alternative QKD schemes are performed.

In the future, QKD is envisaged to coexist with the global classical networks. As such, most of the works regarding QKD integration in optical networks have been conducted with the current wavelength division multiplexing networks. However, the bandwidth demands continue increasing exponentially. As such, little space would be left for QKD applications in

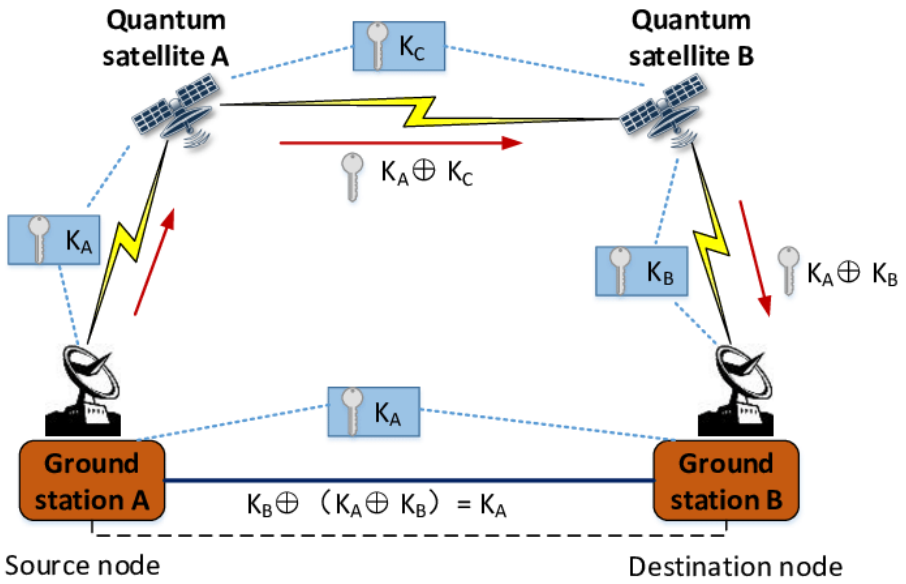

Figure 3.2: The ground stations act as the source node and destination node. The source node exchange a key K_A with the first repeater node by performing QKD. The first repeater node exchanges a second key K_C with the second repeater node. With it, the first repeater node can encrypt the first key K_A with K_C and transmit the result to the second repeater node. As the second repeater node possesses the key K_C too, it can decrypt the message and retrieve the key K_A. The process is iterated as many times as required between the different nodes. Figure from Huang et al. [18].

the near future. As an alternative to WDM, a new approach was proposed to accommodate the increasing bandwidth requirements. In a classical WDM, the frequency (or wavelength) band allocated to each channel is determined at once. In elastic optical networks (EON); the bandwidth allocated to each user is allocated dynamically. The bit rate is thus adapted to the needs of the different users, providing flexibility [15].

Another solution is to improve directly the capacity of the networks. For this purpose, multiband transmission is being explored. In the long-term, a promising solution is to use multi core fibres. Spatial and spectral separation as well as flexibility will tremendously increase the capacity of optical networks. A convenient solution to avoid splitting the optical band for QKD is to assign one core to quantum communications in a multi core channel. However, the presence of several cores in the fibre can lead to intercore crosstalk. The weak quantum signals will thus be deteriorated by the strong classical signals in the other cores because of interferences. This issue needs to be addressed before relying on multi-core fibres. Methods to solve the problem are being investigated by researchers [19] [20].

Architectural considerations need to be investigated towards a global usage of QKD in optical networks. Before reaching a global QKD network, it is expected that quantum services will be provided through the Internet according to Sharma et al. [15]. Therefore, QKD will have to be integrated into a cloud infrastructure. The heterogeneity of services represents networking challenges that still need to be explored and addressed. Moreover, as quantum computing facilities are expected to share the same networks as classical communications,

trust models need to be developed. Besides, the topology of QKD secured optical networks remains to be studied to reach a global integration. Finally, migration strategies need to be thought out to articulate the transition from classical to quantum communication systems. Some lines of thought include traffic forecasting to account for the gradual migration and the variability of the QKD services in time and cost. To help tackle these issues, artificial intelligence, machine learning and deep learning represent promising options.

3.2 Implementations

Many experiments achieved QKD in optical fibres. In fact, many efforts are devoted to increasing the key rates and the distance at which the process is viable. In 2008, a secret key rate of 1 Mbit/s was achieved by Dixon et al. in a 20 km optical fibre [21]. The team also managed to get a key rate of 10.1 kbit/s over a fibre distance of 100 km.

Since then, separate research teams performed various experiments trying to increase the key rate or the distance. Moreover, several strategies have been explored with their advantages and drawbacks. Twin-field quantum key distribution experiments are yielding promising results. For instance, Wang et al. managed to perform QKD over 830 km fibre [22].

Finally, it is worth noting that commercial systems are already on the market. One of the world's first exchange of information with QKD in a private sector was a bank transfer carried out in 2004 in Vienna, Austria [23]. Since then, several companies have developed to offer quantum key distribution systems around the world. They remain rare however and those services are not widespread.

4 Free-Space QKD

Although optical fibres offer many advantages to develop QKD protocols, the intrinsic losses make them a costly approach. Moreover, the lack of flexibility makes them difficult to implement [24]. The main alternative to optical fibres QKD is free-space QKD. In Free-Space-Optical (FSO) QKD, optical signals are transmitted directly through the atmosphere to a receiver in the line of sight. FSO QKD can be performed with terrestrial or satellite-based infrastructures. Free-space QKD is particularly interesting because the transmission channel can be much longer than for fibre QKD. As the medium through which information is sent is less controlled than an optical fibre, some effects exclusive to free space need to be considered.

This section introduces the different factors that need to be considered to implement free-space QKD. Afterwards, the specific challenges of FSO QKD are explained as well as the promising solutions to these problems. Finally, some interesting existing experiments are presented.

4.1 Classical satellite communication and architecture

Before diving into the specifics of free-space quantum key distribution, it is important to understand the fundamental architecture and functioning of conventional communication satellites as well as FSO QKD predecessor, laser communication satellites.

Most communication satellites rely on micro or radio waves to transmit information. Radio waves are artificially produced by transmitters which produce alternating electric currents at the desired radio frequency. Those electric currents are applied to the antenna that radiates corresponding radio waves when it is excited by the currents. After travelling through free space, the radio waves reach another antenna linked to a receiver. Similarly, the antenna is excited by the radio wave and produces an electric current at its terminals which is applied to the receiver. Then, the receiver extracts the information from the alternating currents it is subjected to.

The first communication satellites were designed in the 1960s to develop and improve communication networks across oceans. Satellites were of extreme interest to enable long-distance communication. At that time, the first attempts were performed with passive and active satellites, the two major classes of communication satellites. Passive satellites reflect an incident radio wave emitted from the source towards the receiver. As such, passive satellites do not amplify the signal, they only redirect it. This posed a major challenge in the early days of satellite communication because only a very small amount of the emitted signal energy could reach the receiver. The atmosphere of the Earth induces losses that make only a fraction of the emitted power reach the target. On the other hand, active satellites amplify the signal by re-emitting it in the direction of the receiver. This approach minimises the problems due to atmospheric losses [25].

Nowadays, radio communication satellites are an essential component of most information transfer technologies. They are crucial for telephony. As mentioned, satellites allow

two parties separated by long distances to communicate. Although satellites have been supplanted by submarine cables for the most part, they were particularly useful in the earlier days of intercontinental communication. Nevertheless, they are still used for telephony in some remote areas of the world. Another application is television. Satellites are used to provide direct-to-home television in many countries around the world. They are used for radio broadcasting as well. The advantage is that satellite radio broadcasting allows users to listen to their program on a much larger scale than terrestrial radio broadcasting. For example, some services are available on a whole continental scale. Radio satellites are helpful to people that want to access the Internet from remote areas where a broadband connection is not accessible. Finally, radio satellites are also used in military applications [26].

Among the different types of communication satellites, radio statellites were the first to appear. Nevertheless, substantial advances have been made and research is being performed towards new types of communication satellites. A promising solution is laser communication thanks to satellites. Lasers offer the advantage over radio waves to have much shorter wavelengths and thus much larger frequencies. Larger frequencies mean that information is much more tightly packed than radio frequencies. This difference leads to data rates being orders of magnitude larger. The lasers transmitted by such systems are collected by telescopes and directed towards the receiver. Laser satellites are currently being deployed and used in commercial applications with Starlink as an example. The constellation has been active since 2021. Laser satellites represent an intermediate step towards quantum key distribution because of the range of wavelengths they are designed to use. The privileged wavelength in QKD systems is still being debated but it is much closer to the wavelengths of laser communication satellites than radio satellites. A more detailed discussion about the wavelength is presented later.

QKD shares several characteristics with both previously mentioned techniques. The fundamental difference lies in the nature of the measured signal. In radio and laser communication, the information is coded by modulating the signal and using light as a carrier wave. The signal is composed of many photons and the important information is carried by the combination of photons. In QKD on the contrary, the signal is composed of much fewer photons. Depending on the scheme the signal can even be composed of single photons. Since the information is carried by so few carriers, the powers are much smaller and losses are much more detrimental. The limitations induced by this difference are explained later.

4.2 Important considerations

One of the most important parameters in free space propagation of light is the wavelength of the signal λ. The wavelength or equivalently the frequency of an electromagnetic wave is determinant to describe the effects the atmosphere will induce on the propagation for instance. The magnitude of some perturbations and deteriorating effects will vary depending on the wavelength.

Moreover, in optical fibre, the wavelength is fixed by the properties of fibres, which have the best performances at telecommunications wavelengths namely 850, 1300 and 1550 nm. The properties of the atmosphere make choosing a working wavelength non-trivial since it

conditions the response and design of the complete system.

In FSO QKD, the transmission medium is the atmosphere. Electromagnetic wave propagation is heavily influenced by the atmosphere. The different constituents of the atmosphere exhibit varying properties with light. These properties induce three behaviours of light while it travels the atmosphere. Light can either be absorbed, scattered or transmitted.

Absorption is the process through which a photon is converted to another energy form. The most common case is photons being absorbed and turned into heat. Different molecules and particles absorb different wavelengths. Moreover, the extent to which light is absorbed depends heavily on the optical depth that is considered. To perform FSO QKD, the optical depth at the surface of the Earth is relevant.

Scattering is the process through which a photon propagation direction is modified by the particles in suspension in the atmosphere. There are predominantly two mechanisms at play in the atmosphere, the Rayleigh scattering and the Mie scattering. The type of scattering depends on the size of the molecules compared to the wavelength of the incident light. The different types of scattering applicable as a function of particle size and wavelength are represented in Fig. 4.1.

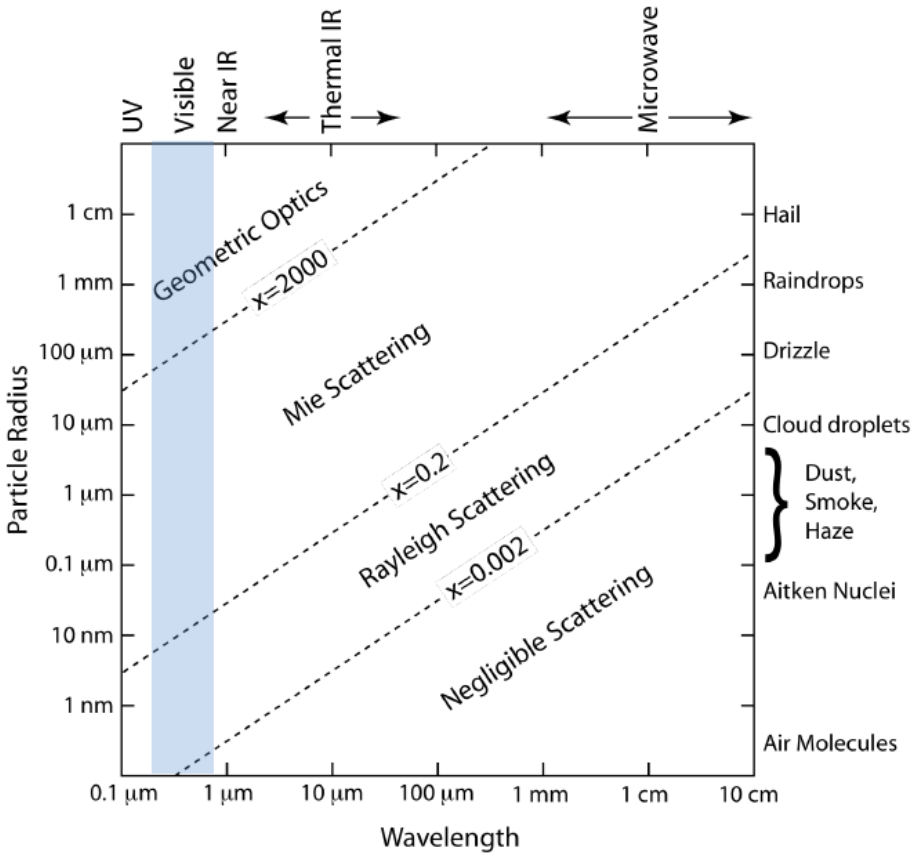

Figure 4.1: Scattering mechanism depending on the size of the particles with respect to the wavelength. This plot considers only single scattering by spheres. Figure from John A. Dutton [27].

Rayleigh scattering is proportional to $1/\lambda^4$ and occurs when the size of the particles is smaller than the wavelength of the light. Mie scattering occurs when the size of the particles is comparable to the wavelength of the incident radiation. Finally, when the particle size is much smaller than the wavelength, light is transmitted unhindered.

While the three mechanisms seem distinct, in practice they combine altogether and result in the observed properties of the atmosphere. The atmosphere is usually described in terms of transmission and absorption although the exact behaviour is more complex. The transmission and absorption of the atmosphere depending on the wavelength is usually represented on a transmittance or absorptance plot. It is represented in Fig. 4.2.

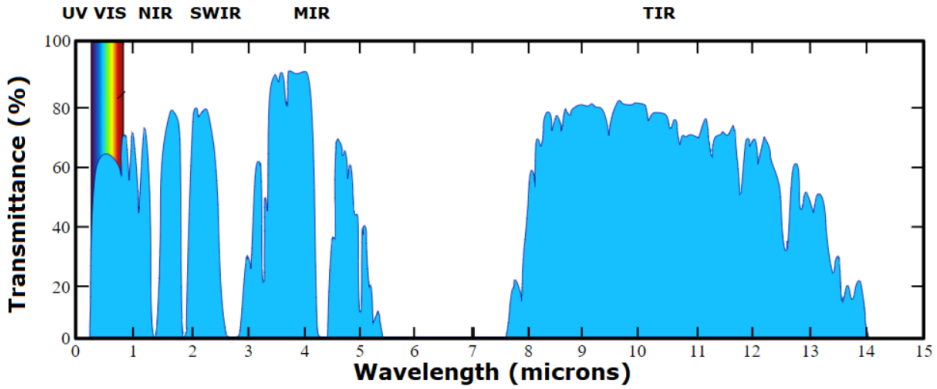

Figure 4.2: Atmospheric transmittance with respect to the wavelength. The part of light that is not transmitted is absorbed. Figure adapted from Wikimedia Commons [28].

It appears clear that some wavelengths should be avoided as the transmission of the atmosphere is low. It is worth noting that the atmosphere has several windows in the range 0 to 2.8 μm. Particularly, telecommunication wavelengths can transit through the atmosphere. Larger wavelengths are not appropriate for QKD because they require larger infrastructures to detect and are less energetic. As some wavelengths do not travel through the atmosphere, they are excluded from discussions. To determine the exact operating wavelength, further considerations are necessary.

4.3 Technical challenges

This section will explore the current limitations towards global FSO QKD. It is worth noting that research with both discrete variable QKD and continuous variable QKD is being conducted because each family of QKD has interesting properties. Moreover, for satellite FSO QKD, two configurations are being investigated to determine the best architecture of such systems.

The first configuration is called uplink or ground to satellite. The quantum information is transmitted from the ground to the satellite. Conversely, in the downlink or satellite to ground configuration, the satellite transmits the quantum information to one or several ground stations. Both present advantages and drawbacks that this section explores. Nevertheless, from a practical perspective, the uplink scenario makes implementing the source

much more convenient since it is accessible on the ground. This solution also presents fewer risks since replacing or repairing the photon source is much simpler.

To quantify the feasibility of quantum key distribution, an equivalent to the signal-to-noise ratio is helpful. The Quantum Bit Error Rate (QBER) is the percentage of the sifted raw key that is erroneous. In the example of Section 2.2, the quantum bit errors correspond to bits where Alice and Bob chose the same basis but their result differed. The QBER is influenced by multiple phenomena that mainly revolve around losses and noise. Different sources of losses and noise are detailed hereafter.

4.3.1 Sources

Before detailing the origin of losses and noise, the first step is to generate photons. For QKD, the information is encoded at the single photon level. The ideal scenario would be to produce strings of single photons to encode strings of bits to encrypt information. Single photons are ideal to detect eavesdroppers. If several photons are generated simultaneously, all these photons are prepared in a similar state. This means that Eve could catch one of the photons and hold it without consequences for the other photons. On the other hand, Bob will measure the other photons that Eve did not retain. If Eve stores the photon she stole until Alice reveals the encoding basis, she can gain information on the key without being detected. This type of attack is called photon-number splitting attack. This compromises the safety of the protocols which are not secured against these attacks.

In practice, however, building single photon sources is difficult. In many implementations, the basis of the photon source is a pulsed laser whose pulses are composed of many photons which are attenuated to single photon levels. The number of photons contained in an attenuated pulse follows a Poisson distribution. The targeted number of photons per pulse is usually 0.1 to 0.2 on average [29] [30]. Researchers are still trying to determine the optimal mean photon number [29]. Since the number of photons follows a Poisson distribution, most pulses are composed of no photons. Some are made of one photon, the ideal case, but very few are composed of 2 photons or more. The multiphoton pulses pose security issues. Many QKD protocols would benefit from true single photon sources. Nowadays, however, the limitations imposed by the attenuated pulses need to be taken into account for protocols that are not immune to photon-number splitting attacks.

4.3.2 Losses in the optical link

As stated in Sec. 4.1, losses are especially detrimental in QKD. In addition to reducing the intensity of the signal, the propagation can also modify the characteristics of the photons and render them unsuitable to transmit information. Thus, losses encompass photons that are lost and not detected as well as photons whose characteristics were modified such that they cannot be used to generate a shared key. The different sources of loss limit the Secret Key Generation (SKG) and contribute to the QBER.

The first source of losses addressed in this work is a consequence of the nature of light

beams. A light beam is subjected to broadening also known as diffraction. The rate at which a Gaussian beam broadens can be expressed thanks to the Rayleigh length. The Rayleigh length determines the length from the minimal waist of the beam after which the beam radius has increased by $\sqrt{2}$ and thus its area by 2. Figure 4.3 represents the geometry of a Gaussian beam.

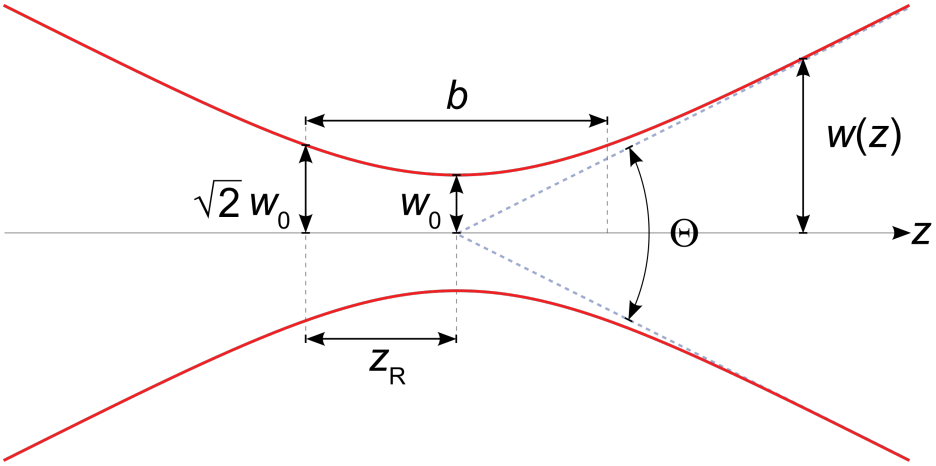

Figure 4.3: Profile of a gaussian beam. w_0: beam waist. z_r: Rayleigh range. b: confocal parameter or depth of focus. Θ: total diffraction angle. Figure from Wikimedia Commons [31].

As the information is contained in the surface of the beam, the diffraction process reduces the signal density as the same number of photons are spread on a larger surface. It also means that a fixed-size telescope cannot retrieve the complete signal if the radius of the beam becomes too large. Diffraction increases as the square of the link length [32]. Diffraction effects are conjugated to some atmospheric phenomena that determine their harm. A detailed discussion of the effects of the atmosphere is presented hereafter.

Diffraction losses are predominant in a downlink configuration in which the beam broadens before reaching the atmosphere. Once the beam reaches the atmosphere, its dimensions are already larger than turbulence inhomogeneities and thus the effects of the atmosphere are much less detrimental according to Liorni et al. [33].

Apart from the losses inherent to beam diffraction, The major contributor to losses is the Earth's atmosphere. Most of the detrimental effects of the atmosphere are due to the fluctuations of the air masses inside it. These air masses that can exhibit very different properties like temperature, speed and composition possess different refractive indexes. The variations of refractive index along the optical link are responsible for several phenomena.

One of these effects is to make the beam wander. As the beam travels through the atmosphere, the fluctuations of refractive index in the propagation direction make the beam experience deflections. As a result, the beam wanders or oscillates randomly in the transverse plane to the propagation direction [34]. In itself, this effect induces significant fluctuations of the measured signal which might induce an excessive deterioration of the key rates in QKD. The wandering can also make the beam broaden due to atmospheric properties and not electromagnetic beam properties. The first type of broadening will be referred to as

diffraction to distinguish it from the broadening due to the atmosphere.

The magnitude of the effect depends on the configuration the system lies in. The atmospheric turbulence is most significant in the 20 km directly above the surface of the Earth. This distance is much shorter than the distance from the ground to the satellite which ranges from a few hundred kilometres to thousands of kilometres. As a consequence, a light beam travels much longer through near-vacuum than through the atmosphere. As such, downlink configurations are much less affected since the most critical case is having turbulence near the source of the photons as detailed in the next paragraph with simulated performances.

For a low Earth orbit satellite with a 30 cm wide receiver, atmospheric wandering is responsible for more than 20 dB of loss for a 1 m ground transmitter. For a geostationary satellite, more than 60 dB of losses are solely due to atmospheric turbulence. These results were computed by Bedington et al. [32]. In the case of a downlink scheme, the losses in the same scenarios are respectively 6.4 dB for LEO to ground and 43.6 dB for GEO to ground links.

This difference is explained for several reasons. For the uplink scheme, wandering causes the beam that is emitted on the ground to broaden because of the atmosphere before reaching an almost vacuum where diffraction causes the beam to broaden even more for several km before being detected. As the effects of wandering are angular, their magnitude on the final losses is proportional to the distance travelled after deflection. In the uplink configuration, the distance travelled after deflection in the atmosphere is much longer than for the downlink scheme. Consequently, losses are much more important. In the downlink configuration, the beam broadens because of diffraction and then reaches the top of the atmosphere where the wandering effects are already less pronounced because of the dimension of the beam as explained earlier. Moreover, since the beam travels much less after deflection in the atmosphere, the angular effects are less pronounced.

The last geometrical effect linked to the beam divergence consists in pointing errors. As satellites transmit light beams, the necessity to accurately point the receiver to the satellite arises especially when considering low powers like expected in QKD and focused beams. Bourgoin et al. performed an analysis of the effects of pointing inaccuracies on losses [35]. Figure 4.4 presents their results.

The transmitter size determines the extension of the Full-Width at Half-Maximum (FWHM) which is equal to half of its diameter. Two features are worth pointing out. The first is that in the downlink scenario, the size of the transmitter and thus the waist of the beam has a direct influence on the excess losses but not in the uplink case. The excess loss designates the losses due to pointing inaccuracies. For the uplink, the four curves for the different transmitter sizes are confused. This suggests that the pointing error losses are similar for all the beam waists. The origin of this phenomenon is that for an uplink configuration, the atmosphere broadening is much more important than the diffraction broadening, which becomes negligible. This reduces the advantage to use a larger transmitting telescope. As a consequence, the diameter of the beam has less influence on the final overall beam broadening. As such, losses due to pointing inaccuracies are similar since diffraction is negligible. For the downlink scenario, the four curves are easily distinguishable because the diameter of the beam influences the final broadening of the beam over the receiver.

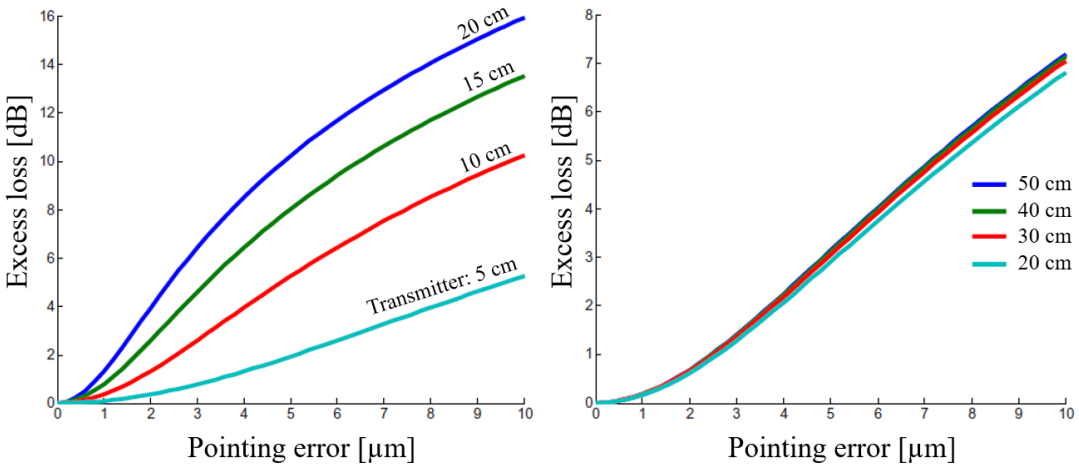

Figure 4.4: Excess loss due to systematic pointing error for various transmitter sizes at 40° from zenith. On the left is presented the downlink and on the right the uplink. For downlink, the wavelength used is 670 nm and the receiver has a diameter of 50 cm. For uplink, the wavelength is 785 nm and the satellite receiver is 30 cm wide. The orbit altitude is 600 km and the atmosphere is rural sea level. Figure from Bourgoin et al. [35].

The second observation is that the excess losses due to pointing errors are up to two times lower for the uplink scenario. Indeed, as the beam is already much broader because of atmospheric turbulence, the size of the beam at the level of the receiver is so important that pointing errors hardly matter. At first glance, this observation seems counter-intuitive. It is worth insisting that Fig. 4.4 presents the excess loss that adds to turbulence losses.

For these reasons, the relative influence of the different losses mechanisms for both configurations can be summarised. In an uplink scenario, diffraction losses are considered negligible in front of wandering and atmospheric broadening losses. Reducing pointing errors below the influence of atmospheric turbulence should be the priority. For the downlink, on the other hand, diffraction losses are dominant as the atmosphere plays a much lesser role in making the beam diverge. To make losses as small as possible, reducing pointing errors such that diffraction becomes the dominant source of broadening is enough [35].

Although much more practical, the significant losses due to turbulence in the uplink scenario dampen the many technical advantages perceived in implementing the transmitter on the ground. Nevertheless, both uplink and downlink configurations are studied as it is possible to still operate an uplink configuration as increasing the power of the source is easier to do on the ground.

The effects of atmospheric turbulence on the light beam can also be described by quantum aspects over geometrical ones. The phenomena remain the same. Through the fluctuations of the local refractive index in the atmosphere, a plane wavefront is distorted and deviated. If the distortion induces an angle of arrival at the receiver, it is called wavefront tilt [36]. Wavefront tilt induces a phase difference as the optical path is different for several points on the wavefront. The amplitude of the light beam is also modified by the atmosphere depending on the wavelength. As discussed in section 4.2, each wavelength is absorbed

differently. The overall light beam is consequently attenuated. Thus, turbulence modifies the phase and the amplitude of the quantum signal. These perturbations result in aberrations which render detection more complicated according to Acosta et al. [37]. Some photons are likely not detected or modified such that their information cannot be exploited anymore. The combination of both phenomena results in photon loss.

4.3.3 Noise

Noise designates all sources of errors that are not linked to losses. It can be interpreted as any detection that is not due to a useful photon. Those spurious detections introduce additional bits in the keys that are not shared by Alice and Bob and increase the QBER.

One of the main sources of noise in FSO systems is stray light. Stray light designates any light that is not intended to enter the optical system. Stray light comes from a source and is transmitted to the detector through either reflections, scattering, diffraction or straight shots. Although several wavelengths are still being explored in FSO QKD, the privileged wavelengths span from the end of the visible spectrum to a few microns. Figure 4.5 presents the irradiance spectrum of the Sun and the emitted flux of the Earth in the range of 0 to 5 µm. In this range, the only source of light that can interfere is the Sun as the Earth's radiation is much smaller and also further in the infrared range.

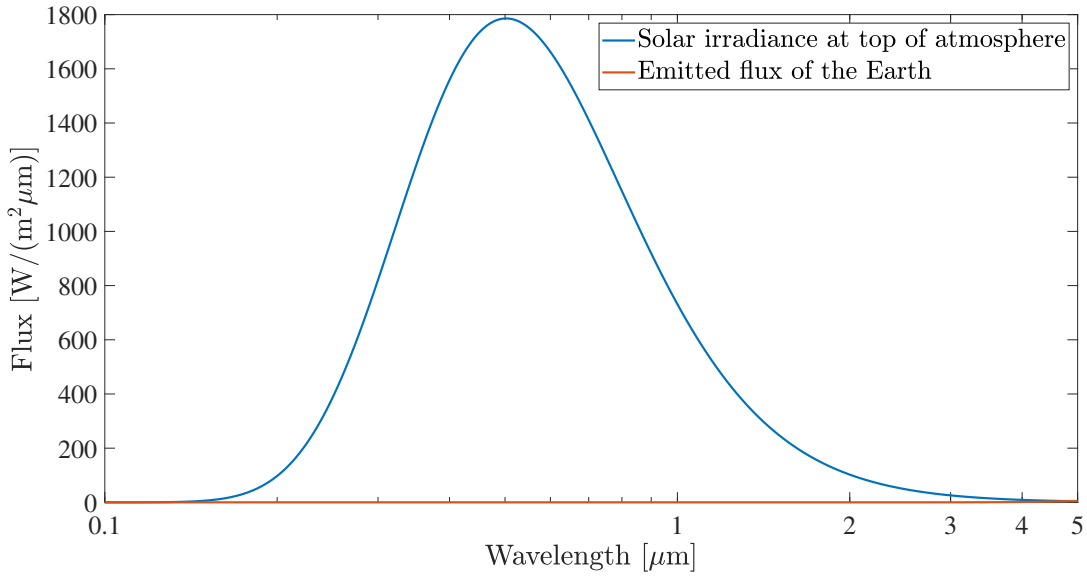

Figure 4.5: Irradiance of the Sun at the top of the atmosphere versus spectral emitted flux of the Earth in the wavelength range 0 to 5 µm. The Earth spectrum is computed at 288 K.

The light coming from the Sun is not directly sent to the optical system. The main mechanism through which stray light enters the system is scattering. As discussed in section 4.2, scattering is a phenomenon through which light is deviated from its initial path because of elements in the propagation channel. The deviation direction depends on the particle

size and wavelength of the incident light. Mie scattering tends to conserve better the initial propagation direction while Rayleigh scattering can deflect in all directions more easily. When sunlight is scattered into the quantum channel, some spurious detection events happen and contribute to the quantum bit error rate. Figure 4.6 presents the different profiles of scattering.

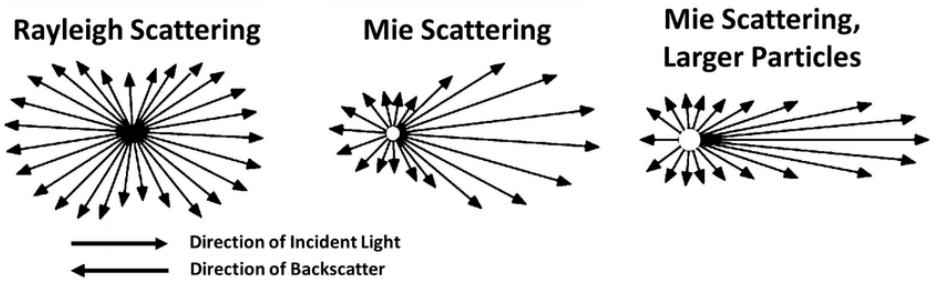

Figure 4.6: Scattering profiles for Rayleigh and Mie scattering. Figure from Barnhart; Gunasekaran [38].

The amount of stray photons that enter the system depends directly on the size of its field stop. Atmospheric turbulence has an indirect influence on the amount of stray light that is captured by the system. Turbulence increases the size of the signal distribution at the receiver field stop. The field stop size needs thus to be increased to capture the signal which increases the levels of transmitted sky noise [39]. This is represented in Fig. 4.7.

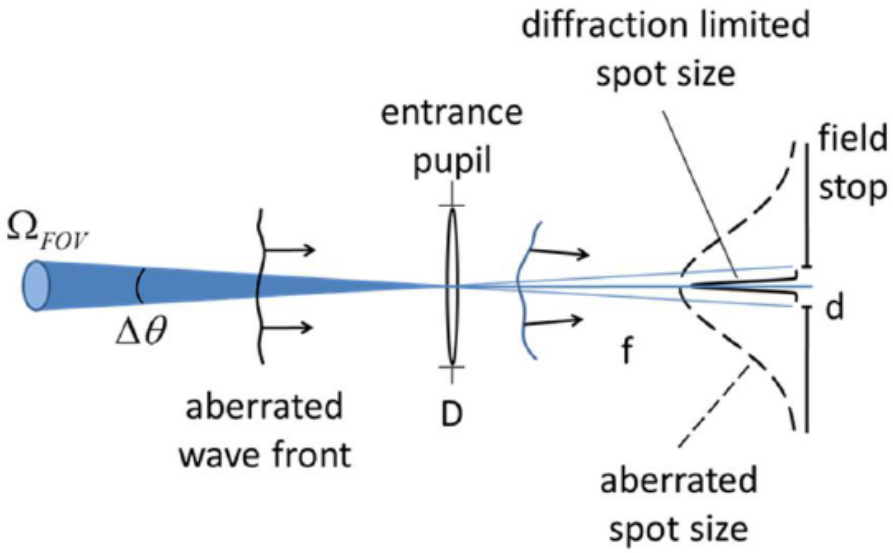

Figure 4.7: Scattering profiles for Rayleigh and Mie scattering. Figure from Gruneisen et al. [40].

It is clear that stray light is especially concerning for daylight operations. During the night, nearly no direct light from the Sun can enter the quantum channel through scattering.

Nighttime operations is thus easier although the light reflected by the moon can still bother systems.

Human activities are also a source of stray light. Human activities and cities require light that can end up in the telescope. Although the investigated wavelengths for QKD are in the infrared range and the human eye is sensitive to the visible range, some light is generated nevertheless in these wavelengths. To prevent this light from inducing problems in the detection, ground stations dedicated to QKD should be built far from important poles of activities such as cities.

4.3.4 Detector performances

Signal detection is especially challenging in QKD. As the signal powers are particularly low in quantum key distribution, the need for ultra-sensitive detectors arises. For discrete variable QKD, single-photon detectors (SPD) are required. Several designs exist for SPD depending on the wavelength range of interest and the conditions of operation. Before exploring the types of single-photon detectors, the following paragraphs recall how detectors function.

When photons hit the electrons in a material, they can dislodge the electrons from their atom depending on their energy and the material. These electrons, which are called photoelectrons, have a larger energy than their binding energy. This process is called the photoelectric effect. In semiconductor materials, the electrons that are transmitted enough energy can travel to the conduction band, where they can move in the material. Semiconductors are the basis of detector technologies thanks to this property.

Detectors are fundamental to any optical system and are one of the most critical parts of QKD systems. Their intrinsic properties are often the bottleneck of whole systems. Several limiting aspects of detectors influence the performance of the system. Among them is the dark-count rates. Because of thermal effects, a detector can measure a signal even without incident light. Indeed, electrons can be excited randomly above the detection threshold due to temperature in perfect darkness. As a consequence, the detector measures an electron that did not appear because of an incident electromagnetic radiation. This average number of counts per second is called the dark count rate.

The reciprocal of the dark count rate is a mean time during which a count is more likely attributed to a true detection event rather than a thermal detection. Dark counts introduce random errors in the quantum protocol. Since there is a threshold on the error above which the communication is aborted, the dark count rate needs to be kept under a certain level that depends on the rate of detection of signal photons and the registration scheme [41]. Moreover, because of the dependence on temperature of the dark count rate, detectors need to be cooled down to a certain extent that depends on the targeted performance and the design. The dark count rate determines the noise level of the detector.

Another important constraint of SPD is that after each detection, a recovery time is required to clear the detector from the freed electrons and be able to detect a new photon. This time interval is called the dead time. If a photon arrives during this time interval, it is not counted. This dead time directly constrains the maximum attainable number of photon

counts, which directly limits the Secret Key Generation (SKG). The dead time should be the shortest as possible to guarantee a maximum SKG. The dead time of SPD is particularly limiting in current system performances.

In addition, detectors are also subjected to jitter. Detection jitter is the deviation or variance introduced by the detector in the measurement of the arrival time of a photon [42]. This measurement time variability can introduce mismatching between different measurements that result in more errors that increase the QBER. A small jitter means that the variability in the measurement times is low and is beneficial to QKD.

These three issues are common to all detectors and limit system performances. The different designs of SPD perform differently regarding these three problems. Nowadays, two types of SPD are investigated to suit QKD applications.

The most advanced technology is called single-photon avalanche diode (SPAD). In SPAD, when charge carriers are liberated by the photoelectric effect, they are accelerated such that they possess enough kinetic energy to ionise the material and knock more electrons out of the atoms. Subsequent carriers are knocked out of other atoms by the first generations in cascade. A single carrier is able thanks to the electric field in the detector to initiate the avalanche such that a single photon is detected.

The performances of these detectors are poorer than the next design, but they are more flexible to use since they need to be cooled only to 250 K. SPADs suffer from high dark count rates and large dead times at telecommunication wavelengths [43]. This is especially problematic for low-distance links with high clock rates [44]. Another specific problem to SPADs is called afterpulsing. After an avalanche has started, some carriers can remain trapped between the valence band and the conduction band. After the detector has been cleaned from its carriers, there is a probability that a trapped carrier from the previous avalanche receives enough energy to initiate a new avalanche. One detection event, intended or not, can thereby generate several avalanches. These afterpulses are noise counts that increase the DCR after each count for a short time.

The other type of single-photon detectors are called Superconducting Nanowire Single-Photon Detectors (SNSPD). SNSPDs were first developed in 2001 at Moscow State Pedagogical University [45] and at the University of Rochester [46]. SNSPD performances are significantly better than SPAD. Their detection efficiencies can reach up to 93% [47]. Moreover, their dark count rates can be made as small as one count per second. In addition, their temporal resolution can reach less than 3 ps [48] due to very small timing jitter. These characteristics result in count rates of the order of GHz [49]. Due to their performances and as they are the fastest single-photon detectors, SNSPD are a key technology for quantum optics. However, they require to be operated at very low temperatures, from 1 to 4 K. It is possible to reach those temperatures with cryocoolers and liquid helium. However, this constraining requirement is a major concern regarding the integration of SNSPD for space applications.

4.3.5 Coupling

As QKD systems consist of three parts, namely the source, the channel and the detector, technical challenges appear at the junction of the different parts. To assemble the system, it is necessary to couple the different parts together. The two different links are between the source and the quantum channel and between the channel and the detector. Before discussing properly the coupling, a few considerations regarding optical fibres are essential.

There are mainly two types of optical fibres, the multimode fibres and the single-mode fibres. As their names suggest, the difference lies in the electromagnetic modes that the fibre can transfer. In some QKD protocols, the polarisation of the photons is used to encode information. Therefore, the polarisation needs to be maintained throughout the system. For this reason, Polarisation-Maintaining (PM) optical fibres are employed. PM fibres are single-mode fibres in which the linearly polarised light propagates and maintains its linear polarisation. In other protocols that do not rely on polarisation, single-mode fibres are also used as they filter out some of the incoming light. For this reason, the following discussion focuses mainly on single-mode fibres. Filtering is detailed in the next section.

When light exits an optical fibre, it is emitted in a cone that depends on the refractive indices of the fibre. This is due to the manner fibres transmit light. An optical fibre is composed of a core that transmits the light and a cladding whose purpose is to ensure total reflections in the core. To be transmitted, an incident light ray should enter the core and reach the end of the fibre after a set of total reflections. Otherwise, some part of the light is transmitted at the interface between the core and the cladding and consequently lost.

To achieve total reflections at the interface between the core and the cladding, the angle of incidence of a light ray should remain smaller than a limit angle $\theta_{\max}$. All the light rays whose angle of incidence is smaller than $\theta_{\max}$ will be transmitted. As a consequence, $\theta_{\max}$ determines a cone in which all light rays are transmitted, called the acceptance cone. Figure 4.8 represents the propagation of a light ray inside the fibre.

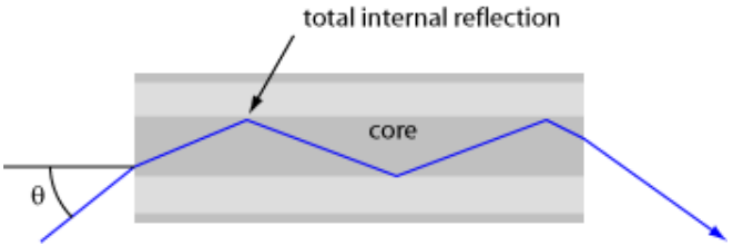

Figure 4.8: Inside the acceptance cone, an incident light ray is refracted in the core and is then totally reflected until it reaches the other end of the fibre and is refracted out of the core. The region for which incident light rays experience total reflections and are not refracted in the cladding is defined as $\theta < \theta_{\max}$. Figure from Paschotta [50].

The maximum angle for incident light to experience total reflection defines the limit of the acceptance cone. This angle allows to define the numerical aperture of an optical fibre

$$NA = n_0 \sin\theta_{\max}, \tag{4.1}$$

where n_0 is the refractive index of the medium through which light propagates before entering the fibre. The maximum angle and thus the numerical aperture depend directly on the refractive indices of the core and the cladding of the fibre. The numerical aperture can be expressed thanks to the refractive indices as

$$NA = \sqrt{n_{\text{core}}^2 - n_{\text{cladding}}^2}, \tag{4.2}$$

where n_{core} and n_{cladding} are the refractive indices of the core and the cladding. The numerical aperture is linked to the acceptance cone of the optical fibre. The larger the NA is, the larger the acceptance cone is. In the case of single-mode fibres, the numerical aperture is significantly smaller than that of multimode fibres. It is usually comprised between 0.05 and 0.4 [51]. The exiting cone is due to the same phenomenon as the acceptance cone but confines the output light instead of the input light. The numerical aperture is important to understand to couple light in and out of an optical fibre.

At first, coupling the source to the optical channel is necessary to transmit the quantum signal. In the case of fibre-based photon sources, the source needs to be coupled to the sending telescope of the FSO QKD system. To do so, it is possible to collimate the beam that goes out of the fibre. A collimator is a device that serves that purpose. It consists of one or several lenses to collimate the beam exiting the optical fibre. A collimator usually comprises mechanical elements to adjust the collimated beam exiting it. Some models include screws to control the beam direction or the longitudinal positioning of the lens to change the focusing distance. Once the light beam is collimated, it can be directed towards mirrors and sent to the telescope.

To finely adjust the position of the light beam entering the telescope, there are several possibilities. Fast Steering Mirror (FSM) or turning mirrors can be used. The other possibility is to use mechanical systems to control the position of the collimator. In the case of the Micius satellite, collimated output beams are adjusted thanks to moving mirrors and sent through a telescope. The details of the mission are provided in a later section.

Upon reaching the receiver, light must reach detectors to be analysed. To do so, it is often necessary to inject the incident light into fibres that transmit the light to the detectors. In the case of multimode fibres, it is sufficient for the telescope to guide the light towards the fibre in a smaller cone than the previously mentioned acceptance cone. For a simple telescope, the guiding cone is directly given by the $F\#$ of the instrument

$$F\# = \frac{f}{D}. \tag{4.3}$$

f is the focal length of the telescope and D is the diameter of the entrance pupil. The case of a simple lens is represented in Fig. 4.9.

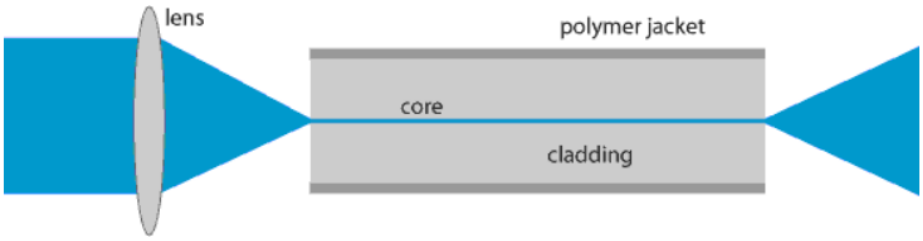

Figure 4.9: When a collimated beam enters a thin converging lens, it is focused along a cone that corresponds to the $F\#$. The focus must be at the entrance of the fibre and the cone must be smaller than the acceptance cone. Figure from Paschotta [52].

For single-mode fibres, launching light is more complicated. The numerical aperture of a single-mode fibre is much smaller than the one of a multimode fibre. Launching light in a single-mode fibre is also dependent on the intensity profile of light in the focusing plane. To achieve this, the focus needs to be produced at the fibre end and the transverse intensity profile of the injected light must be similar to the transverse intensity profile of the fibre mode [53][1].

The focusing process requires precise positioning of the fibres. To tune finely the position of the optical fibre, positioning platforms can be used. Such devices rely on piezoelectric systems or screws to position precisely the fibre. It is also worth mentioning that focusing a light beam in a PM fibre requires aligning the linear polarisation of the beam with the axis of the fibre. The process is not different than for conventional single-mode fibres, but it might be required to rotate the fibre. For that purpose, some fibre launch systems can make the fibres or fibre connectors rotate.

4.4 Investigated solutions

A few considerations can help mitigate the previously mentioned problems without implementing proper technical solutions. The losses originating from atmospheric turbulence decrease slightly by increasing the wavelength [32]. As such, investigating longer wavelengths is interesting. Moreover, losses are proportional to the travel path in the atmosphere and thus depend on the zenith angle of the optical link. Minimising the optical path through the atmosphere helps to reduce the problems induced by turbulence.

In particular, diffraction losses depend on the telescope design. The size and configuration of a telescope influence these losses. This can be understood by considering the relation that links the diffraction pattern of a light beam through an aperture. Because of diffraction, an ideal telescope cannot focus light on a single point. Instead, the best-focused spot of light follows a specific pattern. For a circular aperture, the diffraction-limited pattern is described by the airy disk. A typical airy disk is represented in Fig. 4.10.

[1]The coupling efficiency is computed as the overlap integral of the electric field of the input light and the electric field of the mode of the single-mode fibre. The highest efficiency possible is 81% and is dictated by the maximum overlap it is possible to achieve between a Bessel function (the intensity profile of the input light) and the Gaussian intensity profile of the single mode of the fibre [54].

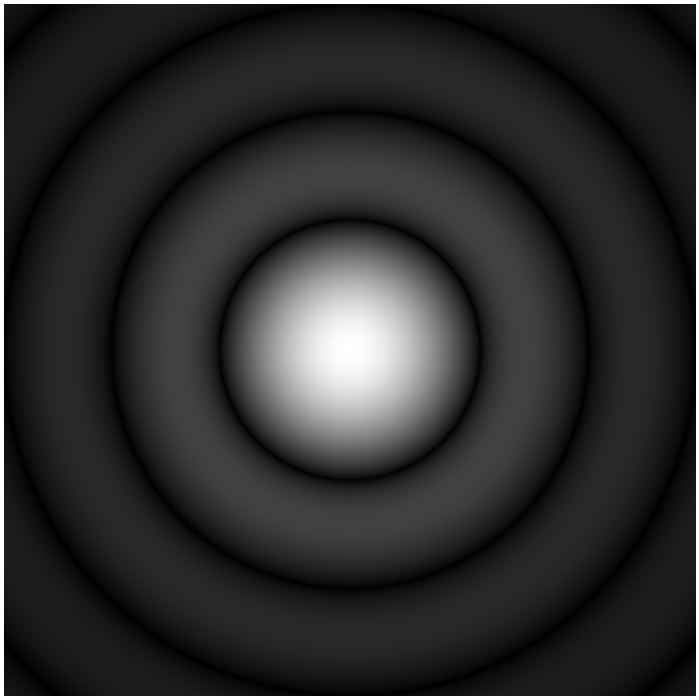

Figure 4.10: Diffraction profile of a point source through a circular aperture. Figure from Wikimedia Commons [55].

The airy pattern shows how information from a single point source is spread on a larger geometrical surface. The angular size of the central circle is described by the equation

$$\sin\theta = 1.22\,\frac{\lambda}{d}, \tag{4.4}$$

where λ is the wavelength of the incident light and d is the diameter of the aperture. The size of the airy disk increases as λ increases and decreases as d increases. Increasing the wavelength is thus harmful regarding the diffraction aspects. The diameter of the receiving telescope can be increased to mitigate the diffraction at the telescope, but it also increases the amount of stray light that enters the instrument.

The losses induced by errors in the tracking system can be reduced by minimising the said errors. However, no tracking system is perfect, and it is impossible to reduce errors to an arbitrarily small value. Moreover, tracking systems are also subjected to jitters which limit the performance of the tracking systems. Since the overall losses due to the errors of the tracking system are minor, tracking systems imperfections should be minimised to the point where the losses they induce are inferior to losses caused by diffraction and atmospheric turbulence.

While helpful, these passive adjustments might not be sufficient to reduce the losses to an acceptable value. Moreover, the benefits of passive adjustments are sometimes accompanied by drawbacks. For instance, increasing the diameter of the aperture is beneficial to reduce the size of the airy disk, but it increases the amount of stray light collected by the instrument. As a consequence, the overall benefit for the system might be marginal. Depending on

the configuration, it is thus important to compare the benefits and drawbacks of passive adjustments to select the modification that diminishes overall losses at best. Nevertheless, active techniques can become necessary in certain scenarios.

4.4.1 Adaptive optics

Adaptive Optics (AO) is a technology that aims at improving the quality of the light wavefront that enters inside the receiver. The technique consists in using a deformable mirror to intercept the light wavefront. The shape of the mirror is adapted continuously to reflect the incoming light. The first stammering of adaptive optics was initially envisioned by Babcock [56] to correct the seeing phenomenon in the 1950s. Astronomical seeing designates the degradation of the image of an astronomical object due to atmospheric turbulence. The images of a single point result in speckle patterns that degrade their quality.

Babcock proposed to apply electric charges on an oil film on a mirror such that the oil film would distort due to the electrostatic forces. Because of the difference in refractive indexes, the wavefront would be corrected. Nowadays, mirrors are directly deformed thanks to microelectromechanical systems (MEMS). The main role of the AO system is to couple the free space wave into the core of a single-mode optical fibre. Fibres are the best way to couple the incoming signal into the SPD.

Figure 4.11 presents the architecture of a modern AO system.

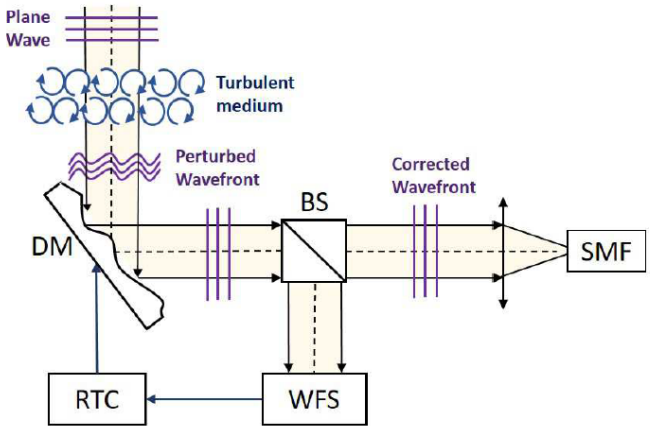

Figure 4.11: General scheme of an adaptive optics system. DM: deformable mirror, BS: beam splitter, WFS: wavefront sensor, RTC: real-time controller, SMF: single mode fiber. Figure from Acosta et al. [37].

The perturbed wavefront is first reflected by the deformable mirror and reaches a beam splitter that transmits a part of the incoming signal to the single-mode fibre and reflects the rest to the wavefront sensor. The wavefront sensor measures the aberrations in the signal due to turbulence and transmits the information to the real-time controller. The RTC allows deforming the mirror according to the aberrations that were measured such that they are

corrected upon reflection. This closed loop is continuously enabled to correct in real time the perturbations.

To estimate the wavefront perturbations, a beacon at a different wavelength is used as a probe to measure the phase aberrations of the wavefront. This is possible due to the nearly perfectly achromatic nature of the atmospheric turbulence [37]. Since the signal is composed of low or single photons, another light ray that is more easily detectable is best suited to model the aberrations. The beacon ray allows to model the optical aberrations by decomposing them in the basis of Zernike polynomials. The most basic ones correspond to low-order polynomials and are thus referred to as low-order aberrations. The more complex the aberration, the higher its order. Once the optical aberrations are modelled, the RTC sends instructions to the mechanisms driving the DM. However, Dichroic Mirror cannot correct all aberrations because they are only able to compensate for a few orders of aberrations. Moreover, they are limited by practical constraints such as their response time and the sampling frequency of the aberrations. For these reasons, some aberrations will remain in the wavefront after correction.

Many experiments and simulations have been performed to assess the usefulness of AO for QKD. They highlighted several interesting aspects of AO focusing on the key contributions it could have for the implementation of a complete system. One of the main advantages of AO is its capacity to help with daytime operations.

The first reason for this is atmospheric physics. Turbulence levels are much more important during the day than during the night because solar radiation heats the air at the surface of the Earth [57]. The hot air then moves because of buoyancy, and denser air falls. These processes are especially important in the lower layers of the atmosphere where turbulent effects are the most important. Since atmospheric turbulence modifies the phase of the signal, it is particularly detrimental for QKD schemes that rely on the phase of the photons [58]. As AO is a technique that aims at correcting the wavefront perturbations due to turbulence, its usefulness is especially apparent during the day.

There is another reason AO is especially useful during the day. As explained later, one way to mitigate stray light problems in daylight is to reduce the Field Of View (FOV) of the receiver telescope. As stated in Sec. 4.3.3, atmospheric turbulence enlarges the signal spot. To capture the same amount of light as in a diffraction-limited system, the field stop needs to be enlarged. Thus, more stray light enters the system. AO can significantly limit this disadvantage by restoring the aberrated wavefront to a near diffraction-limited quality. This, in turn, reduces significantly the errors in the channel, and so the secret key rate.

Gruneisen et al. [39] simulated that appropriate AO systems could help to optimise the trade-off between noise, losses and receiver FOV. They concluded that high-order AO systems can considerably increase SKG rates and even enable it in strong turbulence where it would be prohibited without. AO is more beneficial for small FOVs where turbulence losses are more pronounced. Nevertheless, AO systems help stabilise SKG rates even with a lower level of losses induced by turbulence.

The team of Acosta et al. [37] investigated, in particular, the coupling efficiency of light in single-mode fibres that would be required to transmit light from free space to the detector

station. They studied the role of AO in optimising the said coupling of light. They investigated the advantages of using an AO system in different turbulence levels for both DV-QKD and CV-QKD for two receiver apertures, one of 1.5 m and one of 0.8 cm. Their model suggested that an advanced AO system leads to an overall improvement of the coupling efficiency, especially in the daytime when turbulence levels are the highest. The improvement is not equivalent for both receiver diameters, however. The simulations highlighted that the improvement was less important for the smaller aperture. Zhao et al. demonstrated experimentally that AO can also significantly help in scenarios of phase encoding although higher orders of correction are necessary [58].

4.4.2 Filters

As stated previously, one of the concerns of FSO QKD is the difficulty to carry out the process during the day because of stray light and turbulence. Experiments are conducted to quantify the usefulness of filtering techniques in addressing the problem. They are separated into three categories: spatial, temporal and spectral filters.

Spatial filtering consists in reducing the FOV of the optical receiver to diminish the number of noise photons the system captures. Section 4.4.1 mentioned this technique. Reducing the FOV can be performed in several ways. The most evident is to reduce the extension of the field stop. This can be achieved by using several lenses and a pinhole to limit the bundle of rays that can enter the system.

Temporal filtering is a technique that consists in optimising the signal windows. Some detections are considered irrelevant and discarded if they occur in a specific period. Specifying detection windows avoids mistaking a noise photon for a signal photon. The technique is also helpful in mitigating the effects of dark counts since they are automatically discarded if they occur at an inappropriate time.

Spectral filtering designates all techniques to eliminate all photons that do not belong to the wavelength of interest. For that purpose, spectral filters are used in series to filter out the irrelevant spectrum parts. The combination of several spectral filters enables the selection of a specific wavelength within a specified spectral band. This technique is the most straightforward to eliminate stray light photons.

The combination of these techniques can significantly benefit the efficiency of a QKD system. Nevertheless, their use must be thoroughly investigated and optimised to maximise the SKG rate. Ko et al. studied the effects of filtering techniques and how to combine them by implementing a free-space BB84 QKD system over 275 m [59]. Their study focused on spatial and temporal filtering, since spectral filtering is the easiest to combine with the others. They eventually drew several interesting conclusions. Night operation does not require high-performance filters to be possible but higher performances are required for daytime operation.

Ko et al. observed that reducing the FOV of the receiver reduces greatly the QBER and the noise counts. They also observed that the SKG rate increased so much that daytime operation became possible while it was not without spatial filtering. However, although they observed that the SKG rate increased, they also observed that the standard deviation of the

sifted key rate increased considerably. This increase comes from the fact that as the FOV becomes smaller, signal photons are filtered out more frequently due to the vibration of the beam propagation path. Their results suggest that decreasing the FOV is an efficient way to enable daytime operation at the cost of losing signal photons and increasing fluctuations of the key rate. However, it is worth noting that for such a short link, turbulence effects were negligible. Therefore, spatial filtering is helpful but might not be sufficient to allow daytime QKD for space links alone. As explained earlier, an AO system combined with a beam tracking system can help correct the effects of beam fluctuations in real time even at low FOVs.

Ko et al. also studied the effects of temporal filtering on the system performance. Jitter effects in the SPD and delays in the electronic devices broaden the detection distribution in time of signal photons. This adds a level of unpredictability to the exact time to expect the detection of the pulse. As a consequence, the detection of the laser pulses occurs at an instant inside a time window. The probability for the detection event to happen at a certain time is represented in Fig. 4.12.

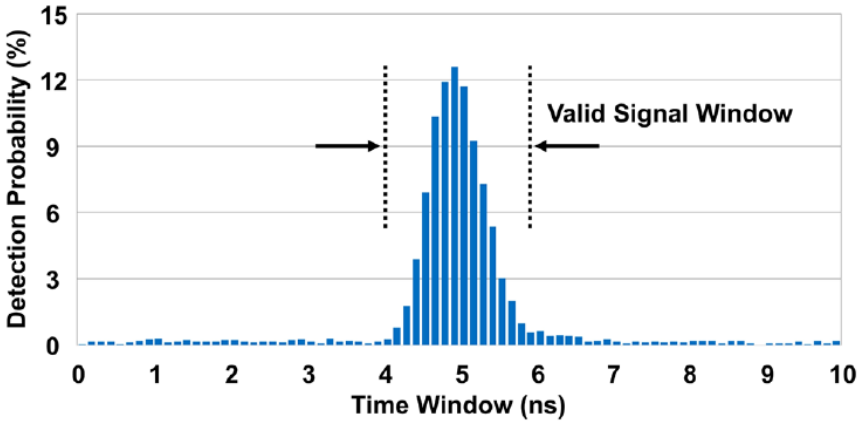

Figure 4.12: Probability distribution of the detection events of the SPD for QKD operation at a clock rate of 100 MHz at night. Figure from Ko et al. [59].

The consistency of the detection event is a constraining bottleneck for temporal filtering. The technique is more effective when the detection distribution is sharp. A sharp distribution is achieved by minimising the jitters and time delays in the system. The efficiency of temporal filtering depends heavily on the characteristics of the system in which the technique is applied. Figure 4.13 represents the results of the experiment with only temporal filtering.

Reducing the signal window duration diminished the QBER as well as the sifted key rate. Since the bases of encryption are supposed random, the sifted key rate is a measurement of the amount of signal and noise photons that are captured. The QBER is a measurement of the relative proportion of errors. As explained earlier, noise is the main contributor to quantum errors. Ko et al. found that reducing the signal window with a medium FOV helps to diminish the QBER because noise photons are equally distributed in all temporal regions contrary to signal photons. Besides the relative decrease of noise photons, they also observed that the amount of signal and noise photons decreased as the signal window decreased,

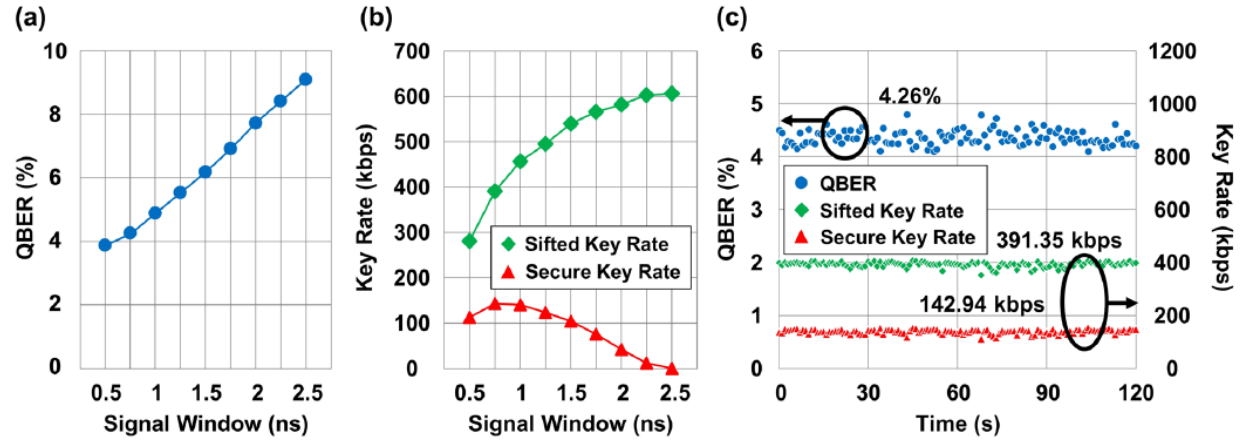

Figure 4.13: Performance optimisation with the temporal filtering technique in daylight. The FOV is fixed at 566 µrad. (a) QBER as a function of the valid size of the signal window. (b) Sifted and secure key rates as functions of the valid size of the window. (c) Performance of the QBER and key rates with the optimal signal window size. Figure from Ko et al. [59].

manifested by the sifted key rate. Nevertheless, this increased the secure key rate. It is also worth mentioning that decreasing the signal window too much is detrimental to the secure key rate since the number of photons lost outclasses the reduction of the QBER.

Ko et al. finally examined the combination of spatial filtering and temporal filtering. They reduced the FOV of the receiver and studied the influence of the signal window length. They compared the performance of the combined filtering techniques with the performance of temporal filtering alone. Figure 4.14 presents their observations.

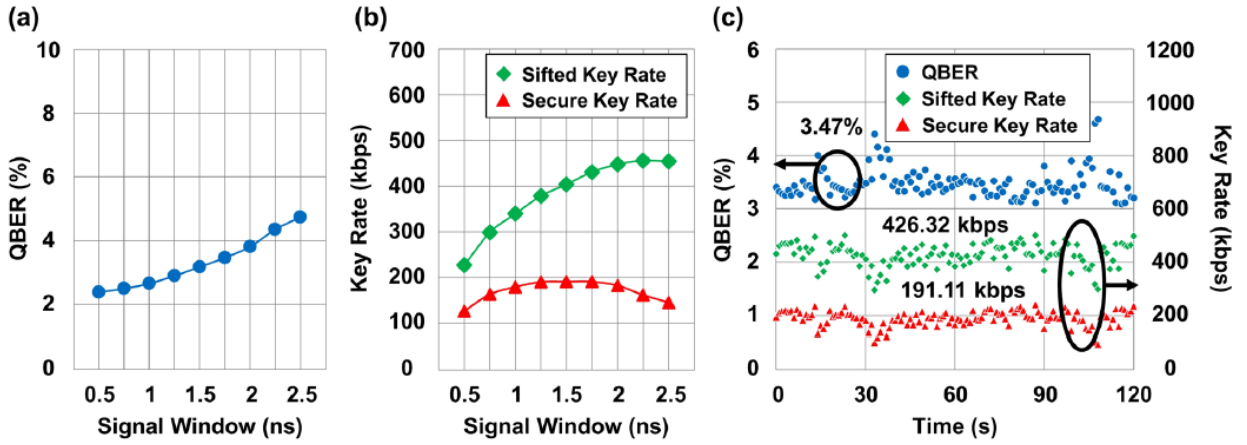

Figure 4.14: Performance optimisation with the temporal filtering technique in daylight. The FOV is fixed at 283 µrad. (a) QBER as a function of the valid size of the signal window. (b) Sifted and secure key rates as functions of the valid size of the window. (c) Performance of the QBER and key rates with the optimal signal window size. Figure from Ko et al. [59].

Although reducing the signal window is always beneficial to reduce the QBER, the optimal signal window in Fig. 4.14 is not as small as in the case where only temporal filtering was performed. In both cases, the objective is to reduce the QBER without sacrificing too many

signal photons to increase the secure key rate. When the FOV is not reduced, it is particularly important to reduce the QBER by solely reducing the signal window. For this reason, the optimal signal window is smaller, about 0.75 ns.

For a smaller FOV, a large amount of noise photons are already eliminated by spatial filtering. Reducing the signal window too much is detrimental as the negative effect of cutting signal photons out becomes dominant over the QBER reduction [59]. The optimal signal window is longer, about 1.75 ns. One can finally observe that Ko et al. obtained the maximum SKG for the combination of spatial and temporal filtering. As their experiment was performed for a short link, the absolute values they obtained are not directly transposable to a space link.

4.5 A proof of concept satellite: Micius

Significant progress was made in the past two decades in FSO QKD since its first implementation. The team of Bennett and Brassard, the authors of the BB84 protocol demonstrated free space QKD in 1992 for the first time, following their protocol theorisation [60]. The optical channel was 32 cm long and composed of free air.

Four years later, the first free-space QKD experiment outdoors was performed by Jacobs; Franson [61]. Since then, many experiments managed to enlarge further and further the optical path. One interesting experiment is the work of Ursin et al. [62]. The European team generated entangled photons and transmitted them over 144 km in free space. They managed to communicate thanks to their entangled states between two of the Canary Islands during the night. This experiment was particularly important because the travel path of the photons was entirely comprised below 10 km from the surface of the Earth. This corresponds to the layer of the atmosphere where turbulence effects are especially prominent. Moreover, the distance travelled in the atmosphere by the photons was much larger than the distance photons would travel through it with a satellite link. This experiment was thus a promising step towards satellite QKD.

Other research and experiments were conducted in the wake of this achievement towards a globalisation of satellite QKD. The most important project of this research field is arguably the Quantum Experiment at Space Scale (QUESS). QUESS is a Chinese research project revolving around quantum optics experiments. The mission comprised the launch of two satellites. The first is Tiangong-2, China's second space laboratory module to perform quantum experiments in space. The second satellite is the most important of the two. This satellite, nicknamed Micius, is the world's first quantum communication satellite [63]. QUESS is a proof-of-concept mission whose satellite was built to facilitate quantum communication experiments. Micius was launched on 16 August 2016. The satellite weighs 635 kg and is in a sun-synchronous orbit, 500 km above the surface of the Earth.

The first experiment performed with the satellite was entanglement distribution over 1200 km of free space. Yin et al. [64] used the Micius satellite to distribute entangled photons to two Chinese ground stations separated by a distance on the ground of 1203 km. The satellite simultaneously established two satellite-to-ground optical links for an expanded time when

both ground stations were visible. The links between the ground stations and the satellite are represented in Figure 4.15.

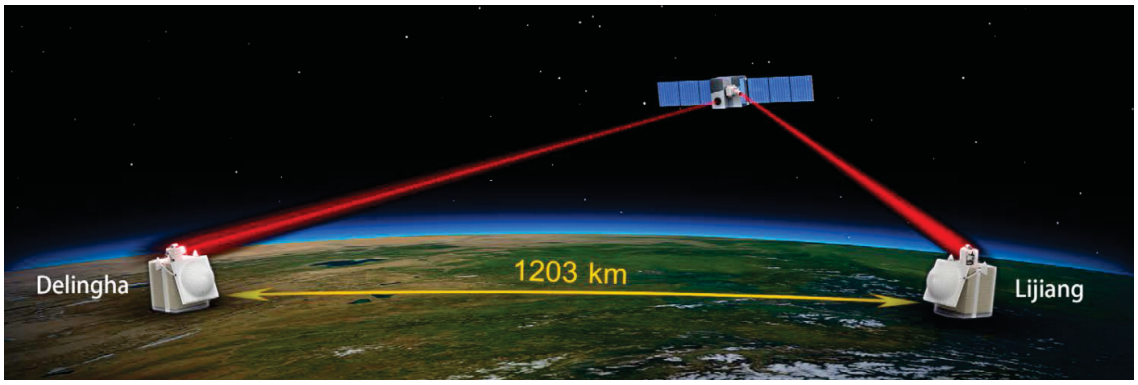

Figure 4.15: Optical link between the ground stations of Delingha and Lijiang and the satellite Micius. Figure from Yin et al. [64].

The satellite distributed photons to the ground stations and Bell's inequality tests were performed, which lead to the conclusion that the distributed photons were entangled. This experiment allowed to verify expected behaviours and solutions intrinsic to the architecture of a satellite-to-ground communication channel. The entangled photons source of Micius is represented in Fig. 4.16.

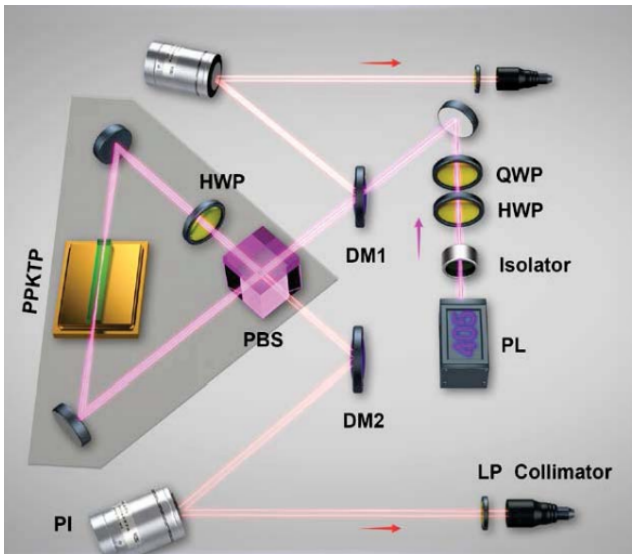

Figure 4.16: Entangled photon source on board Micius. The pump laser (PL) at 405 nm is transmitted through an isolator, a Half-Wave Plate (HWP) and a Quarter-Wave Plate (QWP). The pump laser then passes through a dichroic mirror (DM) and the Polarisation Beam Splitter (PBS). When passing through the crystal (PPKTP), entangled photons are generated and follow different paths when they pass through the PBS. The two DM reflect the photon towards piezo steering mirrors (PI) that are controlled on the ground to adjust the beam pointing to maximise the collection efficiency in the single mode fibres. The long pass filter (LP) helps separating the pump photons and the signal photons. Figure from Yin et al. [64].

The configuration of the source of Micius is called a Sagnac interferometer. The pump is a continuous-wave laser diode that is separated by the PBS. The appropriate way to describe the propagation of electromagnetic waves in the interferometer relies on quantum physics notions. The laser photons' wave functions are split in both directions. The signal photons are generated according to the propagation direction. However, no matter the propagation direction (clockwise or anti-clockwise), the signal photons have opposite polarisations. Consequently, upon reaching the PBS, they will be split towards both channels starting by DM1 and DM2 and ending in each collimator that will inject the photons in single-mode optical fibres. Figure 4.17 presents a similar interferometer to understand the propagation of photons.

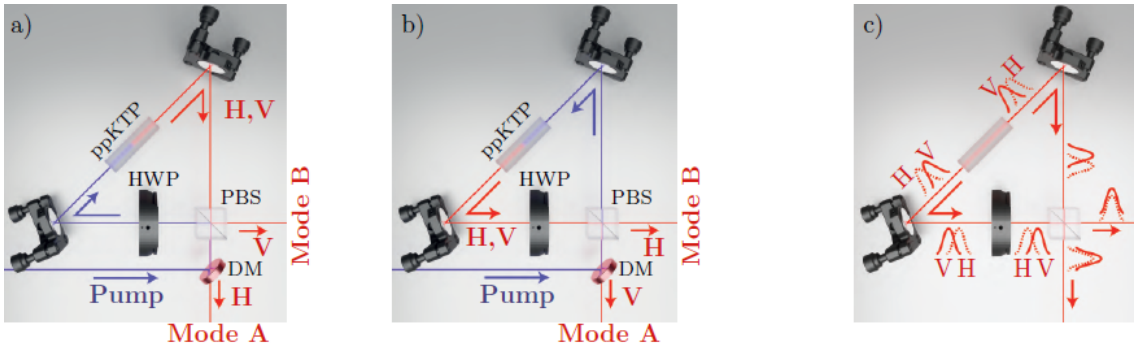

Figure 4.17: Sagnac interferometer a) Clockwise propagation direction. b) Anticlockwise propagation direction. In both cases, orthogonally polarised photons are generated by the pump passing through the crystal. The two photons are split by the PBS to spatial modes A and B. c) Illustration of the walkoff compensation. Figure from Meraner et al. [65].

Figure 4.17 depicts the two propagation directions in the interferometer. If a photon propagates along either direction, the vertically or horizontally polarised signal photons are sent to mode A or mode B. As the PBS splits horizontal photons on one side and vertical photons on the other side, the propagation direction of a photon in either configuration is predictable. Considering a diagonally polarised photon highlights different behaviours. A diagonal photon is described in the rectilinear basis as the combination of the horizontal and vertical states. Upon reaching a PBS, both components have to be considered simultaneously since it is impossible without measurement of the polarisation to collapse the wave function in only one of the states and know where the photon lies. As a consequence, the probability to measure the photon out of both propagation directions is equal to 50%.

Due to its inherent birefringence, the crystal induces a temporal walk-off between the horizontally and vertically polarised photons. If the walk-off is not compensated, it is thus a way to know a posteriori the path the photons took, therefore, their respective polarisation without directly measuring it. Indeed, by supposing Eve has access to the moment the pump fired and one of the output modes, the time after which she measures the passage of a photon is smaller for the horizontal polarisation than for the vertical one. Figure 4.17 c) shows that the horizontal photon escapes the system first for both propagation paths in the absence of the HWP. In reality, the detection probability is distributed over time and thus only the part of the time when both detection probabilities do not overlap allows to confidently determine the polarisation. The same applies if Eve has access to both quantum channels. The moment

Eve detects both photons in their channels gives information on their polarisation. Once it is known, Eve can for instance prepare and send another photon in the same state to remain undetected.

This would compromise the security of the quantum channel since Eve could gain information about the key without being detected because she would not need to risk modifying the polarisation to know it. The HWP is there to avoid this problem by switching polarisations and thus the walk-off is identical for both propagation directions after the PBS. The HWP guarantees the indistinguishability of the propagation paths, and thus a true entangled state is generated. In the end, even if a single photon pair is produced at a time and since it is impossible to know which path it took, the result of measuring the polarisation of the photon of one of the spatial modes cannot be known a priori [65]. The photon pairs can thus be used to distribute a key. In the case of the Micius satellite, the photons are in the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_1 |V\rangle_2 + |V\rangle_1 , |H\rangle_2 \right), \tag{4.5}$$

where H and V denote the horizontal and vertical polarisation states as explained by Lu et al. [66]. The subscripts 1 and 2 designate the two spatial modes.

Since the satellite possesses a relative motion to the ground, the polarisation seen by the receivers is rotated from the perspective of the reference frame. The relative motion of the satellite also induces a drift of arrival time that needs to be corrected. To correct the polarisation, a motorised wave-plates combination rotates the photons' polarisation such that the polarisation measured in the satellite frame corresponds to the one measured in the ground station frame. The polarisation shift was monitored with a pulsed beacon laser co-aligned with the signal beam [64]. The transmitter architecture is presented in Figure 4.18.

The 671 nm cameras detect the beacon laser sent from the ground to the satellite. This experiment demonstrated that entangled photons can be distributed thanks to satellites and remain entangled. It is a fundamental step towards QKD since as long as entangled photons are transmitted, it is possible to generate a secret key.

Following this first experiment that demonstrated entanglement distribution, another one was conducted with Micius too. In September 2017, Liao et al. [67] employed the satellite to carry on QKD with a ground station. The station is located in Xinglong, China. The team conducted a variant of the BB84 protocol, the decoy-state BB84 protocol. The complete set-up of the experiment is presented in Fig. 4.19.

The BB84 encoding module functions as follows. One of the four diode couples emits an attenuated laser pulse that is polarised right before entering the PBS to be guided towards the BS. Depending on the diode couple that fires the laser pulse, the pulse enters the BS with either a vertical, horizontal, diagonal or anti-diagonal polarisation. The diode couple that fired determines the polarisation entering the beam splitter. To obtain a diagonal polarisation, a HWP is used to modify the polarisation of the incident pulses, which can be horizontal or vertical. The polarisation reference laser diode (RLD) serves to keep track of the relative motion of the satellite to the ground. The following part of the transmitter

Figure 4.18: The signal beam passes through the motorised wave plates to correct the polarisation shift induced by the relative motion of the satellite. It is then expanded by a beam expander (BE) and combined with a pulsed laser at 850 nm for synchronisation and a green laser at 532 nm for tracking. The Fast Steering Mirror (FSM) is used for closed-loop tracking, based on the 671 nm beacon laser images captured by camera 1 and camera 2. Figure from Yin et al. [64].

accomplishes the same tasks as the transmitter presented in Fig. 4.18. The signal beam is combined with a green laser to track the satellite. The cameras are used for tracking the ground and time synchronisation by decomposing the laser at 671 nm from the ground. The difference with the previous transmitter is that the compensation process is conducted on the ground.

In the receiver, the signal beam and the tracking beam are collected by a 1000 mm aperture telescope. Similarly to the transmitter, the incident laser at 532 nm is decomposed in two paths for tracking and synchronisation. Then, the signal beam is directed to the BB84 decoding module, which consists of the BS and the two PBS. Right before the decoder, the motorised HWP compensates for the polarisation base shift due to the motion of the satellite. The basis and bit value depend on the detector that captured the photon. The side of the beam splitter the detector is positioned at determines the measurement basis. The exact detector determines the bit value.

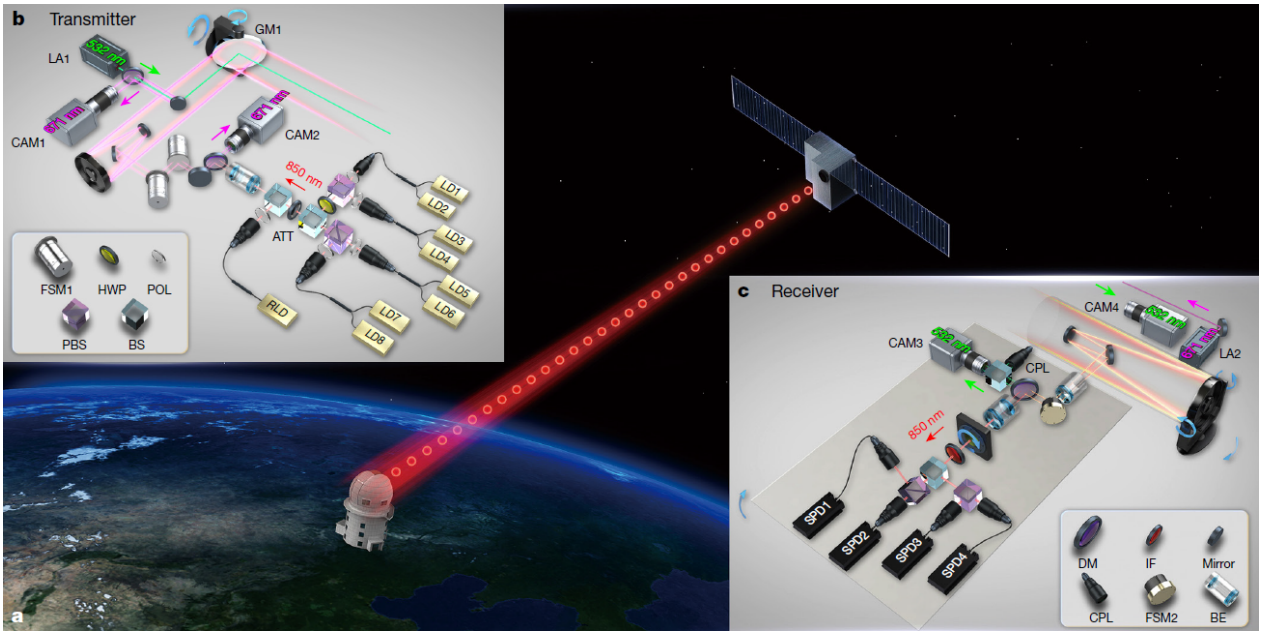

Figure 4.19: Overview of the experiment setup. a) A downlink optical channel was established between the satellite Micius and the ground station of Xinglong. b) Schematic of the decoy-state QKD transmitter. Attenuated laser pulses emitted from eight laser diodes pass through a BB84 encoding module composed of two PBS, a HWP and a BS. The resulting beam is then combined through a set of mirrors to a green laser and sent through a Cassegrain telescope. A gimbal mirror (GM1) and camera (CAM1) are used in combination for the coarse tracking. c) Schematic of the receiver on ground. A 671 nm laser is used for tracking. A DM separates the incident signal from the green laser and is then analysed by the BB84 decoder which is composed of a BS and 2 PBS. The decoder ends by four detectors, one for each possible outcome. Figure from Liao et al. [67].

The experiment was conducted at night and illustrated the impact of the atmosphere and the zenith angle. Figure 4.20 presents the evolution of the distance from the ground station, the sifted key rate and the QBER along time. The time window for the data collection was 273 seconds long.

One can observe that the shorter the distance and thus the straighter through the atmosphere photons travel, the more photons are detected and transmitted. This is indicated by the larger sifted key rate. Moreover, when the angle between the beam and the ground becomes large and thus when the path through the lower layer of the atmosphere increases, the QBER becomes larger too. This experiment demonstrated that QKD protocols are viable in space and paved the way for the one that is detailed next.

After experimenting with a single ground station, Liao et al. [68] conducted an intercontinental communication thanks to QKD with the help of the Micius satellite. To do so, the satellite established a link between itself and three different ground stations. The first is the Xinglong ground station, near Beijing. This is the same station in the previously described experiment. The two other stations in Nanshan in China and Graz in Austria. They are respectively 2500 km and 7600 km away from Xinglong. The optical link is presented in Figure 4.21.

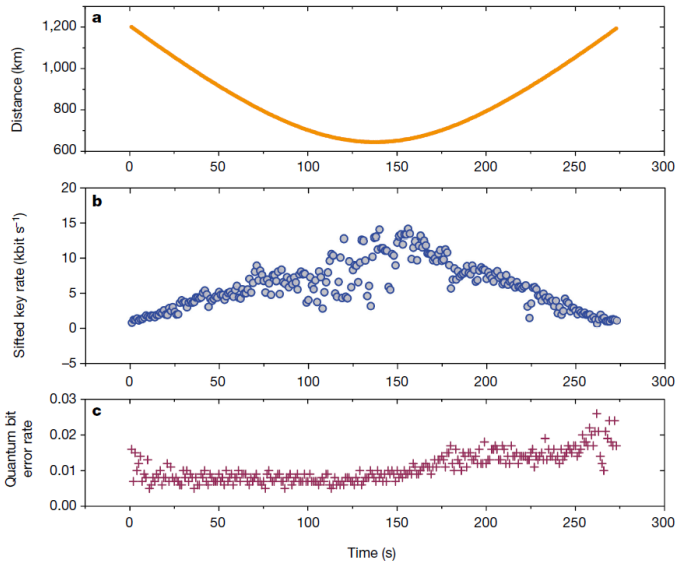

Figure 4.20: a) Distance between the satellite and the ground station with respect to time. b) Sifted key rate with respect to time and optical link distance. c) QBER with respect to time and optical link length. Figure from Liao et al. [67].

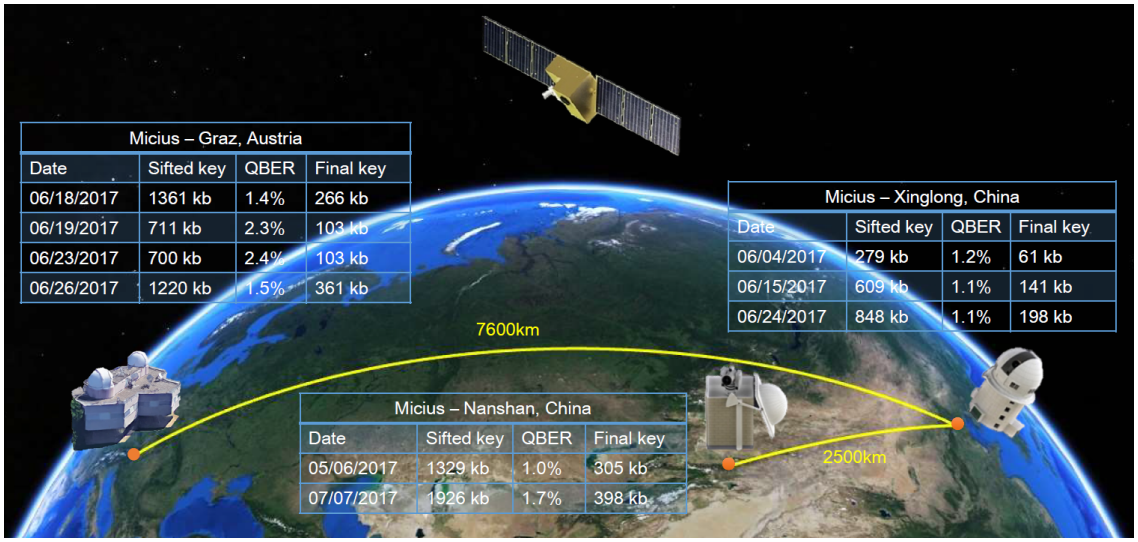

Figure 4.21: Illustration of the cooperating ground stations. The distances represent the two different paths that were used for key generation. The two tables represent the achieved key lengths between the different stations. Figure from Liao et al. [68].

To exchange a key between the two parties, the team relied on the same protocol as in the previous experiment. The BB84 protocol requires a direct channel between two parties. However, only the satellite can see all the ground stations. This happens at different times through the orbit though and thus a delay naturally occurs for the exchange. The procedure starts by establishing a link between the satellite and the first ground station. A secret key is distributed to the station by the satellite by conducting the BB84 protocol. The satellite needs then to store the secret key. Upon reaching the next ground station later in its orbit,

the satellite generates a new key and transmits it to this second ground station with the BB84 protocol. The satellite also stores the key and acts as a trusted relay.

To be able to encrypt and decrypt data and then communicate safely, the two parties need to share a secret key. Each ground station needs to know the other station's key. For one of the stations to retrieve the key, the satellite acts as an intermediary that knows both keys. The satellite performs the bitwise exclusive OR operation between the two keys. This operation was presented in equation 2.1 in section 2.1. The advantage is that by performing the XOR operation between the result and one of the two terms, the other term is retrieved. The satellite can thus send the result of the operation to the station of interest and let it retrieve the other key. For example, if the station of Xinglong which possesses the key MX wants to retrieve the key of the station of Graz MG, it needs to perform another XOR operation. Mathematically, we have $MG = (MX \oplus MG) \oplus MX$. The satellite can send the string $MX \oplus MG$ through a classical communication channel. This method is analogous to the trusted node method depicted in Fig. 3.2 in Sec. 3.1. Figure 4.22 illustrates the exchange.

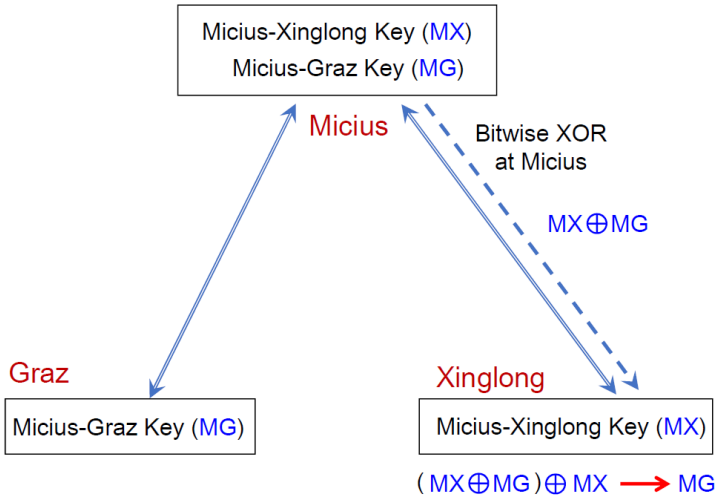

Figure 4.22: Diagram of the exchange process. Once two secret keys are generated and one is sent to each station, the satellite performs the XOR operation. The result is sent to the station that needs to find the other's key. By performing the same operation with its own key, the shared secret key is found. Figure from Liao et al. [68].

With the shared secret key, files can be transferred securely. They are on the first hand encrypted, sent through a classical communication channel and then decrypted with the key. To ensure the feasibility of a real-world application, the team of the station Xinglong transmitted a picture to the team of Graz in Austria and vice versa. On 29 September 2017, an intercontinental video conference was held between the Chinese Academy of Sciences and the Austria Academy of Sciences. To conduct the conference, the satellite link was aided by optical fibres. The ground station of Xinglong is connected to the city of Beijing by an optical fibre link of 280 km. Inside the city, an optical fibre network is used to connect many users within 100 km. The satellite link was combined with this network to carry on the call. This experiment managed to perform a secret key distribution by exploiting the inherent

advantages of satellite orbits. The distance between parties was much larger than what conventional optical fibre links could offer. Moreover, as expected, a collaboration between satellite QKD links and fibres networks poles was proved efficient [68].

One of the most recent experiments with Micius was conducted by Yin et al. They managed to perform QKD by using entangled photons. The experimental setup is presented in Fig. 4.23.

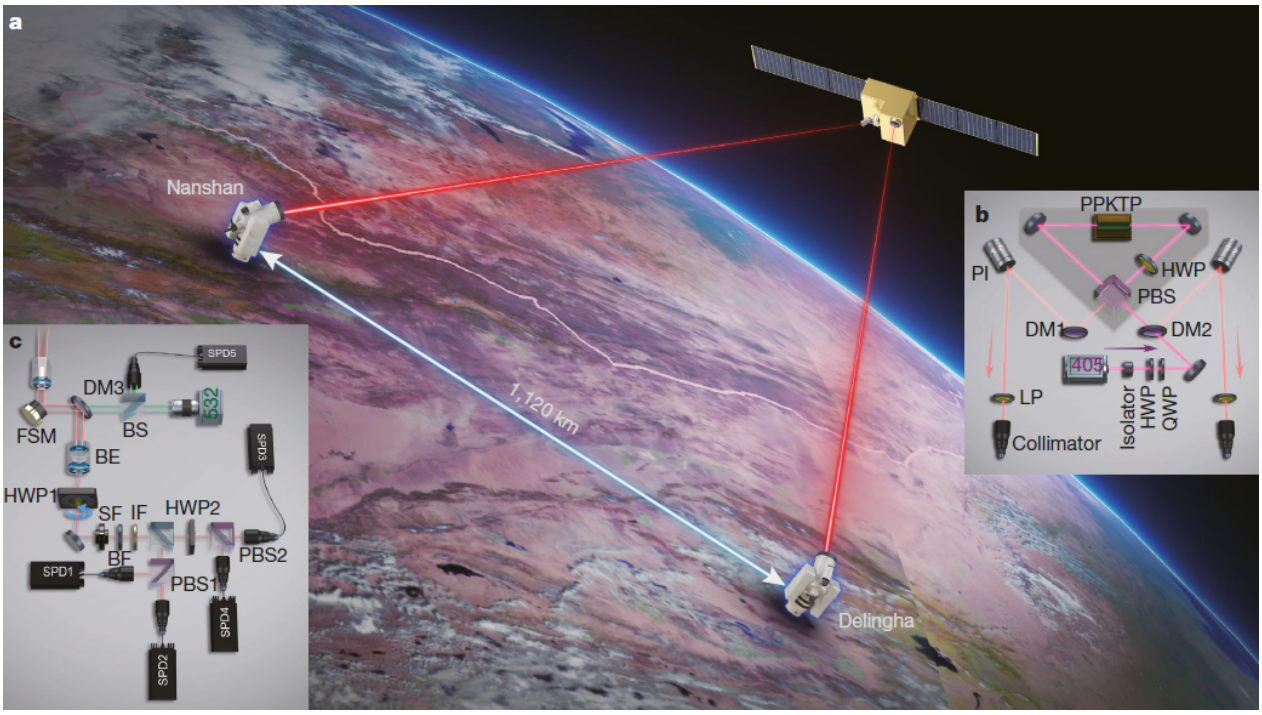

Figure 4.23: a) Illustration of the experimental setup. b) Entangled photon source on board Micius. c) Schematic of one of the receivers in the ground stations. The incident beam is composed of the signal beam and the tracking beam at 532 nm. The signal beam is separated from the tracking beam and the polarisation is compensated with the motorised HWP. The spatial filter (SF), broad-bandwidth filter and interference filter (IF) filter out the input light. The polarisation of the signal photons is then determined thanks to a decoding module composed of a BS, a HWP and two PBS. Four detectors end each branch of the analyser to detect where photons ended. Figure from Yin et al. [69].

The source used in this experiment is the source that was previously used to distribute the entangled photons. It was previously explained following Fig. 4.16. The design of the receiver is similar to the receiver used in the previous experiments. When photons arrive on the BS, they can be found with a probability of 50% on either side of it. The part of the optical path without HWP corresponds to the horizontal and vertical basis, while the part with the wave plate corresponds to the diagonal basis.

The key was established between two ground stations separated by 1120 km at a rate of 0.12 bits per second without trusted repeaters. Compared to transmitting the quantum states with optical fibres, they estimated that the effective link efficiency and thus the secret key rate is eleven orders of magnitude higher. Although 0.12 bits per second is very low, Yin

et al. predict that by increasing the source brightness by two orders of magnitude, the key rate could be increased to tens of bits per second or tens of kilobits per orbit [69].

The experiments conducted with the help of Micius are extremely encouraging towards the global implementation of QKD with satellite-to-ground links. For example, it confirmed that the atmospheric turbulence does not have a detrimental effect on the polarisation of the photons. However, some important limitations need to be taken into account. All the experiments described in this section were performed during the night. Thus, the detrimental effects of daylight did not pose a problem. Atmospheric turbulence was less of an issue too. The secret key rates remain small compared to what is required to achieve quantum communications on a global scale. Nevertheless, the bit rate is expected to be improvable by developing brighter sources and minimising the losses in the optical channel.

4.6 Future initiatives

Satellite QKD is considered to be a promising solution to tackle the pressing matter of global communication security. As the previous sections have detailed, many aspects of the system need to be improved and some problems are still requiring solutions. Nevertheless, many initiatives of researchers are contributing to making the technology a reality. Besides all the already mentioned potential solutions to some of the problems, some other initiatives are also interesting to consider.

In the wake of the Micius success, much interest arose for QKD satellites. Currently, ESA is working with a consortium of over 20 companies led by the Luxembourger company SES to develop a QKD experimentation satellite named Eagle-1 [70]. The satellite is meant to provide first access to long-distance QKD for EU governments, critical sectors and institutions. The Italian company SITAEL is in charge of developing the satellite platform [71]. The German company Tesat Spacecom is in charge of developing the quantum-key payload on board the satellite [72]. The satellite will be operated by SES in Luxembourg [73]. It is due to launch in 2024 and will complete three years of in-orbit validation.

In terms of technology, a team of researchers suggested an interesting approach to solving some of the problems that were mentioned in the previous sections. There is no consensus about the ideal wavelength to use for free-space QKD yet. When searching for the appropriate wavelengths to perform free-space QKD, scientists naturally explored the wavelength range of optical fibres. The range between 1300 nm and 1600 nm is the range of wavelength for which optical fibres exhibit low transmission losses [74]. Apart from around 1400 nm, the atmospheric transmittance is satisfying in this range. Although some focused on the fibre range at first, many experiments were performed at different wavelengths between 700 and 1550 nm because most entangled sources were developed at these wavelengths [75].

However, for several reasons mentioned earlier, longer wavelengths are advantageous. Rayleigh scattering is much less effective for longer wavelengths. Moreover, the Sun irradiance at 2 microns is three times smaller than at 1.5 µm [75]. This would reduce significantly the amount of stray light and enable QKD in daylight more easily. However, sources and detectors at that range of wavelengths need to be developed.

5 Experimental source

Following the theoretical developments presented in the previous sections, a proper experiment was implemented to illustrate several concepts described in this work.

As the previous sections have detailed, a complete QKD channel is composed of three main architectural modules: a photon source, a quantum channel and a detection module. Each of these modules is composed of several components, and the technical limitations associated with the three modules have also been explored theoretically earlier.

Considering the complexity associated with the development of any of the three modules, it was decided to restrict the scope of the experimental part of this study to the first module of a system: the source. In the frame of the thesis, a photon source was conceptualised and assembled. The photon source is the basis of any QKD system and permits a variety of experiments. Precisely, this work focuses on the production of entangled photons with non-linear optical phenomena. Before detailing the experimental setup, it is necessary to understand some concepts of non-linear optics.

5.1 Introduction of non-linear optics

This section presents the fundamental concepts for the elaboration of the photon source. It does not dive into all the details of the equations and mainly focuses on the principles that allow the creation of photons. When an electromagnetic wave reaches a medium containing charges, a dipolar-type interaction occurs between the dipoles in the medium (the charges) and the incoming wave at the frequency ω. When the energy of the incoming field becomes large, the system starts to respond non-linearly. Particularly, the induced polarisation of the medium is no more proportional to the inner fields. The next equations are the ones developed by Boyd; Prato in the book "Nonlinear optics: Third edition" [76]. The interaction can be highlighted by developing the Maxwell equations to obtain the general wave equation

$$\nabla \times \nabla \times \tilde{E} + \frac{1}{c^2}\frac{\partial^2 \tilde{E}}{\partial t^2} = \frac{-1}{\varepsilon_0 c^2}\frac{\partial^2 \tilde{P}}{\partial t^2}. \tag{5.1}$$

$\tilde{E}$ is the electric field, $\tilde{P}$ is the polarisation, c is the speed of light and ε_0 is the vacuum permittivity. The "tilde" ($\tilde{}$) designates quantities that vary rapidly in time.

By developing the first term on the left as $\nabla \times \nabla \times \tilde{E} = \nabla(\nabla \tilde{E}) - \nabla^2 \tilde{E}$, the term $\nabla(\nabla \tilde{E})$ can be omitted for its negligible contribution. As the electric field is that of a plane wave, the gradient of the electric field is zero [13]. Equation 5.1 becomes

$$\nabla^2 \tilde{E} - \frac{1}{c^2}\frac{\partial^2 \tilde{E}}{\partial t^2} = \frac{1}{\varepsilon_0 c^2}\frac{\partial^2 \tilde{P}}{\partial t^2}. \tag{5.2}$$

The polarisation can be developed as a sum of increasing powers of the field following equation

$$\tilde{P} = \varepsilon_0 \left[\chi^{(1)} \tilde{E} + \chi^{(2)} \tilde{E}^2 + \chi^{(3)} \tilde{E}^3 + ... + \chi^{(n)} \tilde{E}^n \right] \tag{5.3}$$

$$= \tilde{P}^{(1)} + \tilde{P}^{(2)} + \tilde{P}^{(3)} + ... + \tilde{P}^{(n)}. \tag{5.4}$$

$\chi^{(l)}$ represents the nonlinear susceptibility of the medium of order l. In order for a material to exhibit non-linear properties, one of the susceptibility coefficients of order 2 or more should be nonzero. It is thus possible to express the polarisation as the sum of a linear part and a non-linear part

$$\tilde{P} = \tilde{P}^{(1)} + \tilde{P}^{(NL)} = \varepsilon_0 \left[\chi^{(1)} \tilde{E} \right] + \tilde{P}^{(NL)}. \tag{5.5}$$

This decomposition allows to rewrite Equation 5.2 as

$$\nabla^2 \tilde{E} - \frac{\varepsilon}{\varepsilon_0 c^2} \frac{\partial^2 \tilde{E}}{\partial t^2} = \frac{1}{\varepsilon_0 c^2} \frac{\partial^2 \tilde{P}^{(NL)}}{\partial t^2}, \tag{5.6}$$

with $\varepsilon = \varepsilon_0 (1 + \chi^{(1)})$. The electric field and the polarisation can be expressed as sums for all the different frequencies interacting. The equation is thus valid for all the frequencies and by solving it for all of them, the different non-linear phenomena can be derived. The next part of the chapter will focus on a qualitative description of the phenomena that will be helpful to build the source of the entangled photons.

5.1.1 Sum-frequency generation

In the case where two incident electric fields of frequencies ω_1 and ω_2 interact in a non-linear medium, a third field of frequency ω_3 is created provided the power of the incident waves is sufficiently large. This third electric field must respect the condition $\omega_1 + \omega_2 = \omega_3$ for energy conservation. This process is called Sum-Frequency Generation (SFG). Figure 5.1 illustrates Sum-Frequency Generation.

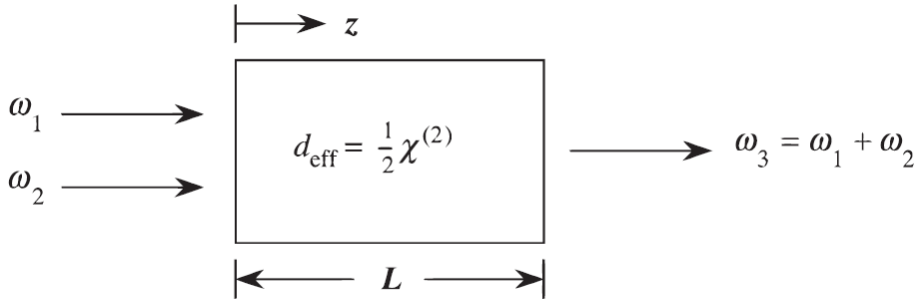

Figure 5.1: Illustration of the sum-frequency generation phenomenon in a medium exhibiting non-linearity of order 2. L is the length of the crystal. Figure from Boyd; Prato [76].

The efficiency of the process is expressed through the intensity of the generated wave as follows by Ghalbouni

$$I_3 = \frac{2d_{eff}^2\omega_3^2 I_1 I_2}{n_1 n_2 n_3 \varepsilon_0 c^3} L^2 \operatorname{sinc}^2\left(\frac{\Delta k L}{2}\right) = I_3^{(\max)} \left[\frac{\sin(\Delta k L/2)}{(\Delta k L/2)}\right]^2, \tag{5.7}$$

where d_{eff} is the effective nonlinear coefficient of the material, I_1 is the intensity of the wave of frequency ω_1, I_2 is the intensity of the second wave, n_i are the refractive indices of the corresponding waves and L is the length of the non-linear material. The process efficiency decreases as $|\Delta k|L$ increases. This occurs because if the length L is superior to $\frac{\pi}{\Delta k}$, the resulting wave is out of phase with the non-linear polarisation [13]. It is thus possible to define the coherence length $L_{\text{coh}} = \pi/\Delta k$.

To maximise the efficiency of this process, it is necessary to reach the phase matching condition i.e. $\Delta k = 0$. Phase matching ensures that when photons are created inside the material, they interact constructively with other photons of the same frequency which maximises the efficiency of the process. If the condition is not fulfilled, the generated photons interact destructively with each other and the final amount of generated photons remains small [77]. This condition can be expressed in terms of the angular frequency of the three waves

$$\begin{aligned} \Delta k &= 0 \\ k_3 - k_2 - k_1 &= 0 \\ n_3\,\omega_3 - n_2\,\omega_2 - n_1\,\omega_1 &= 0 \\ n_3\,\omega_3 &= n_2\,\omega_2 + n_1\,\omega_1, \end{aligned} \tag{5.8}$$

where k_i is the wavenumber of the electric field. It can be expressed as

$$k_i = \frac{n_i\,\omega_i}{c} = \frac{\omega_i}{v_p}, \tag{5.9}$$

where v_p is the phase velocity of the electric field.

To guarantee the phase matching condition, the medium through which the process occurs should be selected such that the different refractive indices satisfy the condition. One way to ensure phase matching is to use birefringent crystals. In a birefringent crystal, the refractive index depends on the polarisation of the incident wave. Uniaxial crystals possess an optical axis that depends on the crystal structure. An incident wave whose polarisation is parallel to the optical axis is called extraordinary, while a wave with a perpendicular polarisation is called ordinary wave. The refractive index for the same wavelength is different if the polarisation is either parallel or perpendicular to the optical axis. Ghalbouni defines the different refractive indices as follows. The light ray whose polarisation is perpendicular to the plane that contains the propagation vector $\overrightarrow{k}$ and the optical axis of the crystal travels with a refractive index n_o. The light ray whose polarisation lies in the plane containing the

propagation vector $\overrightarrow{k}$ and the optical axis of the crystal undergoes an refractive index $n_e(\theta)$ that depends on θ, the angle between the optical axis and the wave vector $\overrightarrow{k}$ [13].

There are two types of phase matching conditions. In type I phase matching, both waves at frequency ω_1 and ω_2 have the same polarisation. For type II phase matching, their polarisations are orthogonal.

In the case where the material is not birefringent, the phase matching cannot be guaranteed thanks to the dependence of the refractive index on the polarisation. Nevertheless, if quasi-phase matching is achieved, it is possible to generate photons that will interfere constructively with each other, resulting in a significant amount of generated photons.

If achieving phase matching is not possible for the selected wavelengths, an alternate technique called Quasi-Phase-Matching (QPM) can still increase the amount of generated photons. QPM is achieved inside a material by manufacturing it such that it is divided into domains where the optical axis of the material is periodically inverted. By creating a periodic inversion of the optical axis, the generation of photons is efficient even though the phase matching condition is not reached. It is a way to compensate for the mismatch between the different wavenumbers. The QPM condition requires the phase difference to be equal to 0. The phase associated to a periodic pattern of length Λ is $k_{QPM} = \frac{2\pi}{\Lambda}$. The quasi-phase matching condition is thus

$$\Delta k_Q = k_1 + k_2 - k_3 + k_{QPM} = k_1 + k_2 - k_3 + \frac{2\pi}{\Lambda} = 0. \tag{5.10}$$

By isolating the length of the periodic pattern, it becomes

$$\Lambda = \frac{2\pi}{k_3 - k_1 - k_2} = 2\,L_{\text{coh}}, \tag{5.11}$$

by recalling that $L_{\text{coh}} = \pi/\Delta k$. The QPM is illustrated geometrically in Fig. 5.2:

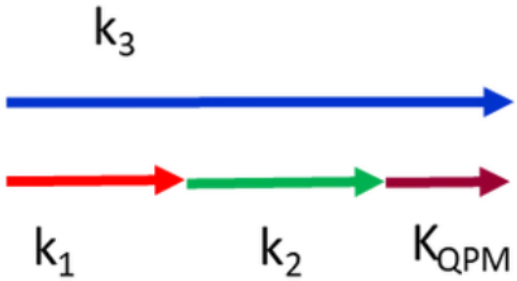

Figure 5.2: Illustration of the wavenumber compensation for QPM. Λ is the length of a periodic pattern so a succession of one region of positive axis and one region of negative axis. Figure from [77].

The non-linear materials layout is presented in Fig. 5.3. With the appropriate periodicity

or domain length, the photons interact constructively and the amount of generated photons increases along the propagation.

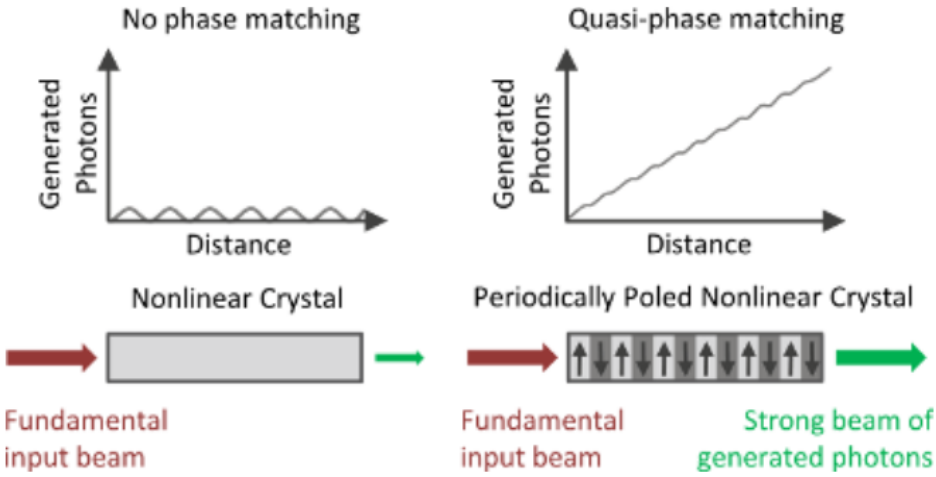

Figure 5.3: . Figure from Paschotta [78].

In the scope of the experiment, a specific case of SFG is performed. The Second-Harmonic Generation (SHG) also known as frequency doubling is the particular case of SFG where the two incident waves have the same frequency. According to energy conservation, the resulting wave's frequency is twice the incident one.

5.1.2 Spontaneous parametric down-conversion

Spontaneous Parametric Down-Conversion (SPDC) is a nonlinear process where a photon splits into two other photons of lower energies. This process is also known as parametric fluorescence, parametric noise or parametric scattering [79]. The incident photon is usually called the pump photon and the two generated ones are called signal and idler photons. SPDC is the opposite phenomenon of SFG. It also satisfies the energy conservation:

$$\omega_p = \omega_s + \omega_i, \tag{5.12}$$

and the phase matching condition

$$\overrightarrow{k_p} \approx \overrightarrow{k_s} + \overrightarrow{k_i}. \tag{5.13}$$

The main difference lies in the fact that for the momentum conservation i.e. eq. 5.13, uncertainty remains as several solutions can satisfy the momentum conservation. For this reason, the possible trajectories that satisfy the momentum conservation are constrained along the sides of two cones. Nevertheless, when a photon pair is emitted, both photons lie in their cone symmetrically from the pump beam.

The energy conservation (eq. 5.12) implies that the signal and idler photons have symmetrical frequencies with respect to the half pump frequency. Before detailing the three different types of SPDC, it is important to consider the way the photons will come out of the non-linear material. In the process of SPDC, three waves propagate simultaneously through the material, the pump wave, the signal wave and the idler wave. Since they all possess a certain polarisation and wavelength, they do not travel at the same velocity which leads to a temporal and spatial walk-off. Temporal walk-off, also known as longitudinal walk-off, is due directly to the difference in velocity between the photons. Depending on their polarisation and wavelength, the refractive index is different. This results in a time difference between the moment the first photon comes out of the crystal and the moment the second does. This temporal difference is directly proportional to the length of the crystal and depends on the different refractive indices

$$\Delta t = \left| L_c \left(\frac{1}{n_e} - \frac{1}{n_o} \right) \right|. \tag{5.14}$$

n_e and n_o are the extraordinary and ordinary refractive indices and L_c is the length of the crystal. Besides the temporal walk-off, there is also a spatial walk-off. The spatial or transverse walk-off comes from the fact that in a birefringent material, the energy propagation or Poynting vector direction is not necessarily the same as the wavevector of the down-converted photons [79]. It is the case for the ordinary wave but not for the extraordinary wave. As a result, the cone for the ordinary wave is not centred around the same point as the cone for the extraordinary wave. This is illustrated later in Fig. 5.5.

Now that some important concepts have been explained, the different types of phase matching can be discussed. For SPDC, there are three types of phase matching conditions. The three types are explained hereafter.

In SPDC of type I, the signal and idler photons share the same polarisation which is orthogonal to the pump polarisation. The way photons exit the non-linear material depends on the type of the phase matching. For type I SPDC, both photons exit in a cone shape that depends on the frequency of the generated photons. Both cones are concentric since type I SPDC converts an incident polarised wave into two waves that share the same polarisation. As such, the cones of emission are centred around the pump beam. The radius of the cone depends on the wavelength of the photon. The case of an SPDC of type I with degenerated signal and idler photons $\omega_s = \omega_i$ is shown in Fig. 5.4.

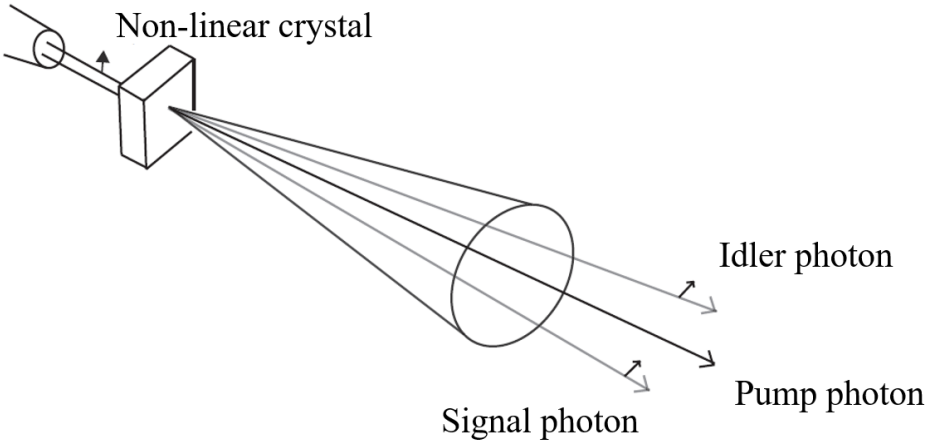

Figure 5.4: Illustration of the spontaneous parametric down conversion of type I in the degenerated case. Figure adapted from Ghalbouni [13].

In the case of type II SPDC, the signal and idler photons have orthogonal polarisations. Each photon is emitted along a cone that depends on the frequency of the photon. The cones are centred around different points since the generated waves have opposite polarisations from one another. In a birefringent Beta Barium Borate (BBO) crystal, this is because one of the generated waves is polarised along the ordinary axis and the other along the extraordinary one. This is illustrated in Fig. 5.5.

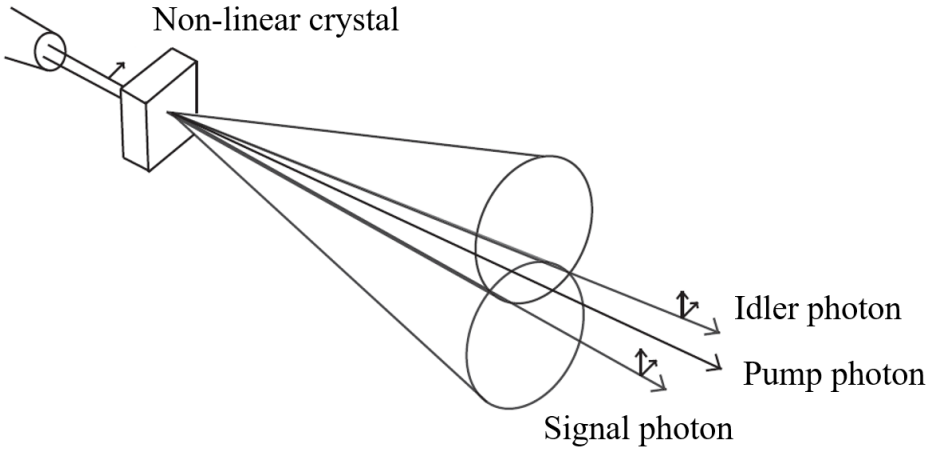

Figure 5.5: Illustration of the spontaneous parametric down conversion of type II. Both photons are emitted along a cone and the overlapping region is where entangled photons are generated. Figure adapted from Ghalbouni [13].

In the end, there is an overlap region where entangled photons are found. Indeed, photon pairs are emitted symmetrically around the pump beam position. If a photon is found in a position corresponding to a part of only one of the cones, its polarisation is known since each cone corresponds to one polarisation. If a photon is found at one of the intersections of the cones, it is impossible to determine which cone it belongs to and thus its polarisation. Moreover, if one photon is found at the first intersection, the second is necessarily at the

other intersection. As a result, entangled photon states are generated at the intersections of the cones. To only select the photons emitted along the intersections of the cones, it is possible to use a combination of a narrow-band filter to select spectrally the photon pairs, a spatial filter to select only the photons in this region and a temporal filter that select the relevant photon detections [79].

Finally, in the case of type 0 SPDC, the pump, signal and idle photons share the same polarisation. As all the polarisations are identical, the refractive indices do not differ because of the polarisations but differ because the wavelengths are different. As the difference in the refractive index only depends on the wavelength, the differences in the index are much less important which limits walk-off issues.

The efficiency of the process in bulk crystals is expressed in the following equation using the definition of Leverrier et al. [80] and Yariv [81]. SPDC is a special case of three-wave mixing. The three-wave mixing coefficient is defined as

$$k = d_{\text{eff}}\,\varepsilon_0 \sqrt{\frac{\mu_0}{\varepsilon_0}\frac{\omega_s \omega_i \omega_p}{n_s n_i n_p}}, \tag{5.15}$$

where d_{eff} is the effective non-linear coefficient of the material, $\omega_{s,i,p}$ and $n_{s,i,p}$ are respectively the angular frequencies and the refractive indices of the signal, the idler and the pump photons in the material. The effective non-linear coefficient depends on the material that is used to produce non-linear effects. It depends on the polarisation of the incident light and the molecular structure of the crystal. The coefficient allows to define the rate of photon pair generation for perfect phase-matching

$$Rate = \frac{1}{4\pi}\left(\frac{\mu_0}{\varepsilon_0}\right)^{1/2} (kL)^2 \frac{\delta\omega}{\omega_p} I_{\text{pump}}, \tag{5.16}$$

where L is the length of the crystal, $\delta\omega$ is the bandwidth of the SPDC and I_{pump} is the pump intensity. The bandwidth of SPDC is defined as

$$\delta\omega = \frac{2\pi c}{|n_i - n_s| L}. \tag{5.17}$$

It is the natural bandwidth defined by the phase patching condition. The photon pair generation is directly proportional to the intensity of the pump. Increasing the power of the pump is thus helpful to increase the efficiency of the process [80].

5.2 Laser preparation

The previously detailed non-linear effects can be exploited to create a single photon pair source. A source using both principles of SHG and SPDC was developed in the frame of this work. The purpose of the source is to convert at first a 1064 nm laser beam in a 532 nm

beam thanks to SHG. Once done, this 532 nm beam is converted to a combination of two beams at 800 nm and 1588 nm through SPDC. In a complete FSO QKD system, the photons at 800 and 1588 nm could be used to conduct a quantum protocol.

To prepare this experiment, several modules were assembled to obtain the right conditions. The main purpose of the modules is to obtain a laser beam at the appropriate power. The architecture of the complete system to obtain the laser is depicted in Fig. 5.6.

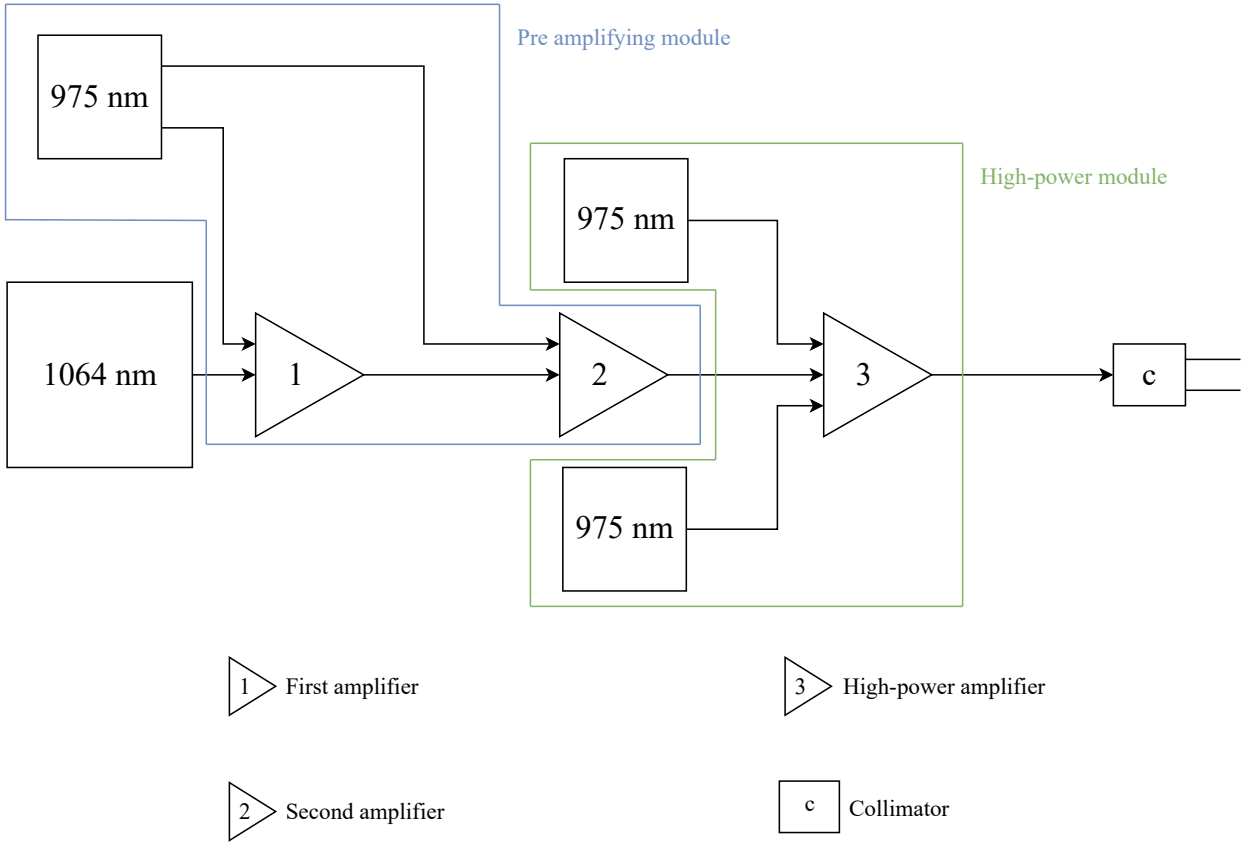

Figure 5.6: Architecture of the laser source. A laser diode at 1064 nm is amplified through three amplifiers thanks to 975 nm diodes.

At first, the pump lasers used in the experiment were characterised. The next objective was to obtain suitable power levels to inject in the non-linear crystals. Afterwards, an optical setup was designed to inject the laser into the first crystal and subsequently into the second crystal. The subsequent sections detail the different steps of the whole experiment.

5.3 Laser diode characterisation

The laser that needs to be amplified comes out of a 1064 nm pulsed laser diode and are vertically polarised. A laser diode is a device built with semiconductors that can reach lasing conditions when subjected to an electrical current. In order to understand how they operate, it is worth explaining in few words how lasers function.

The acronym laser stands for Light Amplification by Stimulated Emission of Radiation. It is made of three components: a gain medium, an energy source and an optical cavity. The gain medium is the material actively emitting light. Lasers exploit the properties of electrons to emit said light. When electrons absorb energy, they travel to higher energy levels around the atoms they are bound to. The energy levels electrons can have are discrete. As such, the amount of energy that an electron needs to travel to a higher level, also called layer, is determined by the energy difference between the original energy level and the level after absorption. When an electron remains in an excited state above the fundamental one, it loses spontaneously its energy and returns to its original layer. To release this excess energy, a photon of a specific wavelength is emitted since the energy of a photon depends on its wavelength or equivalently, on its frequency. This process is called spontaneous emission.

An energy source must be used to excite the electrons inside the gain medium. This energy source can adopt different forms, the process can be optical or electrical. This is the pumping process. However, a gain medium and an energy source are not sufficient to create a laser. Indeed, when an electron is excited, it loses its energy by emitting a photon. If this photon does not meet another particle, it does not induce other effects. However, if another electron is hit by this spontaneously emitted photon, another process called stimulated emission takes place. When an electron that is excited above its fundamental level is struck by a photon of appropriate energy, it will emit another photon of the same energy. This process allows to amplify light waves. It is illustrated in Fig. 5.7.

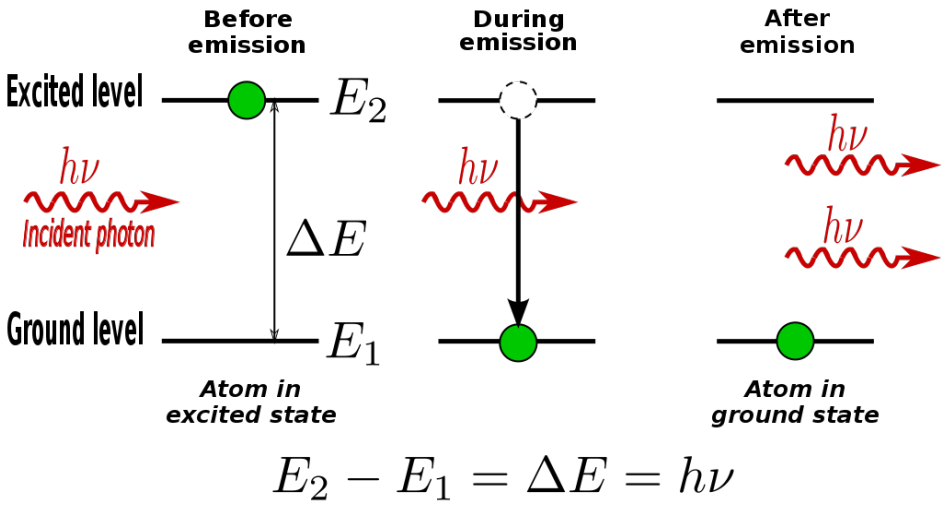

Figure 5.7: Illustration of the stimulated emission process. An incident photon reaching an already excited atom induces an emission of another photon of the same wavelength. Figure from Wikicommons [82].

To build a laser, the gain medium is thus placed in an optical cavity that confines light such that it travels back and forth through the gain medium. Lasers exploit these processes to emit concentrated light beams of a given wavelength. When an electron excited by the energy source spontaneously emits light in the cavity, the other excited electrons emit light in a cascade stimulated by the different photons travelling back and forth. The cavity allows a small fraction of the emitted light to escape and this light has interesting properties for many applications.

In the case of a laser diode, the gain medium is a semiconductor material in which electrons at higher energy levels coexist with holes. Spontaneously, electrons and holes can recombine and release photons. Over a certain voltage, recombinations between electrons and holes are stimulated. Similarly, when an incident photon reaches an electron, it stimulates the emission of a photon of the same wavelength by recombination and the output power increases significantly.

The laser diode used in this experiment is made of an InGAs substrate. The larger the indium composition, the larger the wavelength [83]. The model used in the experiment is tuned to emit pulses at 1064 nm. Although the characteristics of the laser are set in the driver provided with the laser, the diode spectrum and the duration of the pulses were measured. The laser allows the selection of the pulse duration and repetition rate among the pre-implemented values. The pulse durations range from 50 ps to 9000 ps and the repetition rate from 100 kHz to 5 MHz. It was decided to study the combination between three values of pulse duration and five values of repetition rate to characterise the diode. The pulse durations are 50 ps, 1000 ps and 9000 ps. The repetition rates are 100 kHz, 500 kHz, 1 MHz, 2 MHz and 5 MHz. By performing measurements for this restricted set of combinations that are spread on the possible parameters, the laser diode characteristics are evaluated without studying each and every possible combination.

In the source developed in the experiment of this work, it is desirable to use the laser with a pulse repetition rate of 5 MHz and a pulse duration of 50 ps to obtain the largest peak power as frequently as possible to maximise the non-linear effects. This specific combination was thus investigated more thoroughly than the others.

The different combinations of pulse durations and repetition rates lead to different values of mean power. The different values of the measured mean power are represented in Figure 5.8.

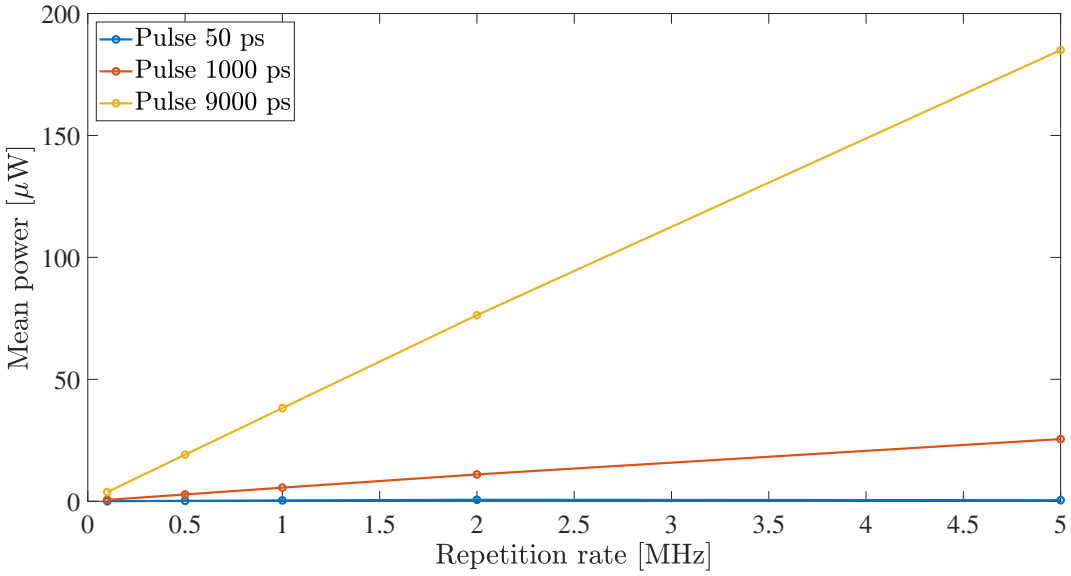

Figure 5.8: Mean power of the 1064 nm laser diode with respect to the pulse repetition rate.

The measured power corresponds to the total amount of energy the power meter received throughout a second. Figure 5.8 shows that the power increases linearly with the repetition rate. This suggests that the energy per pulse is constant and increasing the amount of pulses increases linearly the amount of energy per second. This measured power will be referred to as mean power. Moreover, increasing the pulse width or duration increases directly the mean power for the same pulse repetition rate. This is coherent because each pulse contains more energy. From the mean power and the repetition rate, it is possible to compute the amount of energy per pulse as follows

$$E = \frac{P}{f}, \tag{5.18}$$

where E is the energy per pulse, P is the mean power and f is the repetition rate. As the energy is distributed in time because of the pulsed nature of the diode, a more relevant measurement of the power is the peak power. The peak power is a measurement of the physically accurate power that any irradiated object experiences. This quantity determines how detectors and other devices withstand the irradiation by the laser. The peak power is expressed as

$$P_{\text{peak}} = \frac{E}{PW}. \tag{5.19}$$

PW is the pulse width of the laser and P_{peak} is the peak power. It is important to stress that in this definition, the hypothesis of a constant power over the duration of the laser pulse is made. However, in reality, this is not correct as highlighted later.

After studying the power characteristics of the laser, it is interesting to study the spectrum and the temporal extension of the pulses. The laser is injected in an Optical Spectrum Analyser (OSA) to measure the frequency bandwidth. The OSA displays the spectral extension of the signal. Before injecting the laser in the instrument, it was necessary to measure its mean power as the OSA can withstand no more than 200 mW. The pulse spectrum is centred around 1063.36 nm and the bandwidth does not exceed 1 nm for all the different combinations of repetition rates and pulse durations. This comes in adequacy with the specifications of the supplier of the laser and the requirements of the source that was built. The spectrum is illustrated later in this work.

The final step was to measure the temporal extent of the laser signal. A precise oscilloscope was used to measure the shape of the laser pulses i.e. the distribution of energy in time. To inject light into the oscilloscope, a photodiode converts incident photons in an electric current that the oscilloscope can characterise. The photodiode is particularly sensitive and can only withstand a power of up to 1 mW to avoid saturation that could deteriorate its performance. The different pulse widths were characterised at the different repetition rates. This confirmed that the repetition rate has little influence on the pulse durations as expected. The different pulse durations are shown hereafter. As the repetition rate did not influence the pulse durations, the most precise measurements are shown even though they correspond to different repetition rates. Figures 5.9, 5.10 and 5.11 represent the temporal extent of the pulses of 50 ps, 1000 ps and 9000 ps respectively.

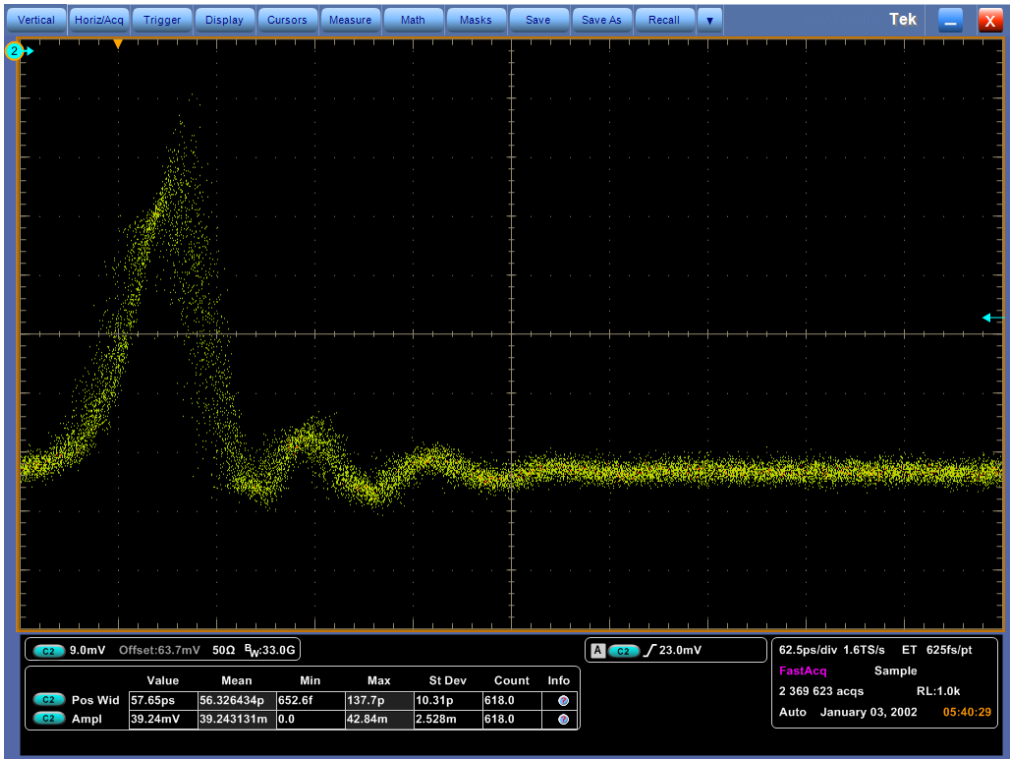

Figure 5.9: Temporal extent of the signal for the 50 ps long laser. The measurement was made for a repetition rate of 5 MHz.

The horizontal scale in Figure 5.9 represents 62.5 ps per division. As can be seen, the signal is not contained within one graduation only. One can observe right after the peak relaxation oscillations. When the photodiode is excited abruptly, it starts emitting electrons and when the excitation stops, the return to steady state is not immediate. Instead, oscillations are observed. The same phenomenon occurs when the power provided to the diode decreases abruptly to a non-zero value. The change between a steady state at a large power to a steady state at a low power is also characterised by relaxation oscillations. These oscillations blur the measurement at the beginning of the pulse. Moreover, since the time scale is extremely small, the curve is blurred since a smaller time interval means that the sampling is coarser.

Nevertheless, the main peak width is comparable to the divisions. Still, the duration of the pulses is measured to be longer than the one expected. In the following discussions, the pulse duration is still considered to be equal to 50 ps. The discrepancy between the actual pulse duration and the theoretical one needs to be recalled as it might explain some effects observed in the rest of the experiment. Moreover, Fig. 5.9 illustrates the inhomogeneity in the energy distribution along the pulse duration. The peak power defined in Equation 5.19 makes the assumption the energy is distributed uniformly or in other words, that the pulse is a step. The measurement of the power shows that this hypothesis is not physically correct. This difference needs to be taken into account when dimensioning the optical elements that are required.

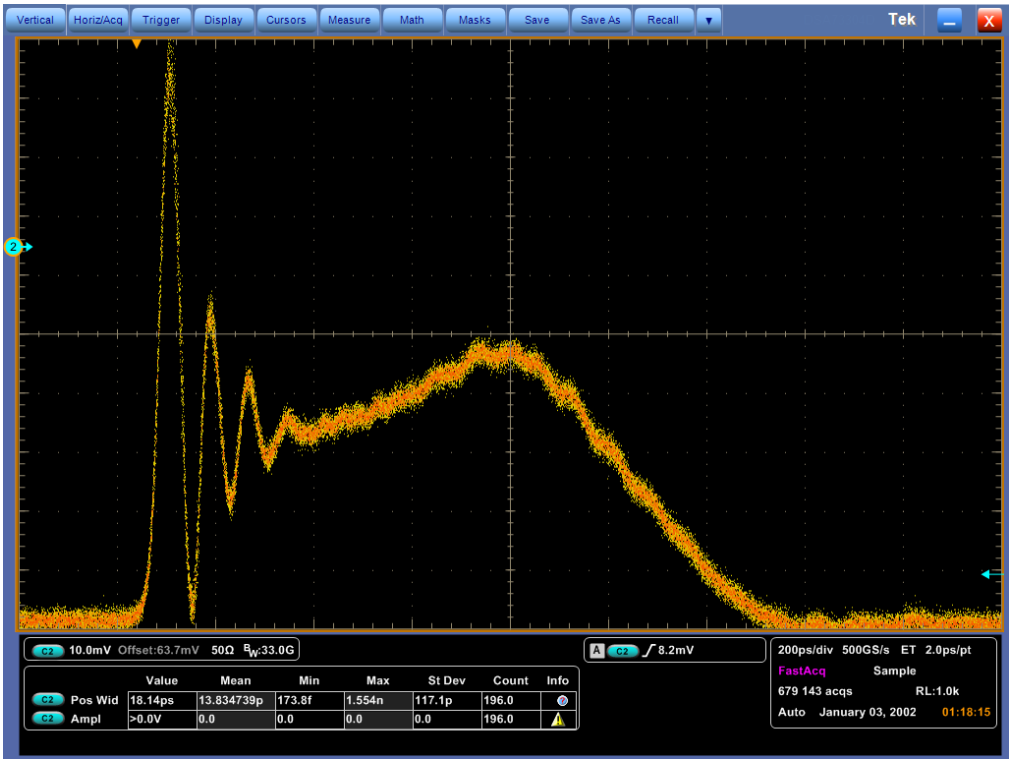

Figure 5.10: Temporal extent of the signal for the 1000 ps long laser. The measurement was made for a repetition rate of 2 MHz.

In Fig. 5.10, one division represents 200 ps. The pulse is spread over six horizontal divisions and lasts thus for less than 1200 ps. This is slightly longer than the expected 1000 ps. Concerning the distribution of energy along the pulse, Fig. 5.10 depicts another behaviour. The same relaxation oscillations are observed at the beginning of the pulses similarly to the case where the pulse duration was set to 50 ps. Specifically, one can observe in Fig. 5.10 a broader maximum before the signal ends. The hypothesis of a constant power throughout the pulse is more accurate in this case. This broader peak is characteristic of modulated laser diodes which produce a peak of power followed by a step when producing long pulses. Figure 5.11 presents the case of 9000 ps pulses where this behaviour is particularly observable.

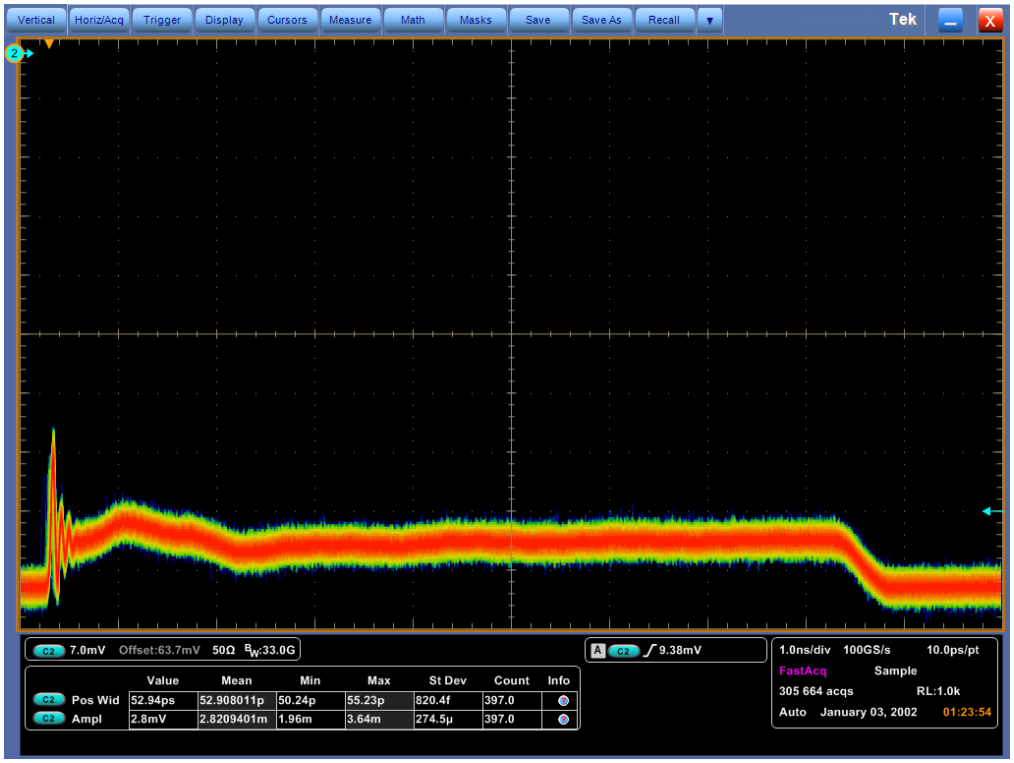

Figure 5.11: Temporal extent of the signal for the 9000 ps long laser. The measurement was made for a repetition rate of 1 MHz.

In the case of a pulse of 9000 ps, each division represents 1 ns. The pulse culminates in a duration of about 8500 ps over slightly less than nine divisions. One can observe the oscillations highlighted thanks to the 50 ps pulse and the broad maximum highlighted by the pulse at 1000 ps. Afterwards, a plateau of the power can be observed for more or less 6000 ps. This profile is similar to an actual step function that was expected and used to compute the peak power of each pulse. One can see that the step follows the broad maximum.

With the oscilloscope, it is also possible to measure the signal over longer periods of time. Figure 5.12 represents the measurement over a duration of 1 µs.

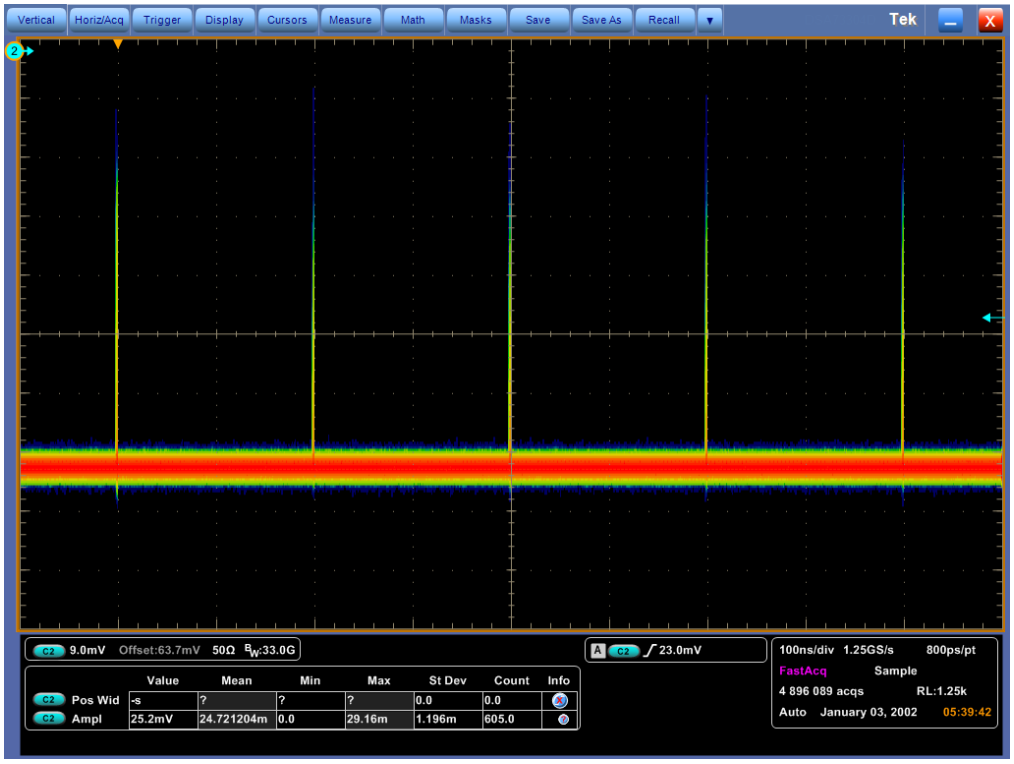

Figure 5.12: Temporal extent of the signal for the 50 ps long laser over a longer time of measurement. The measurement was made for a repetition rate of 5 MHz.

One can observe in Fig. 5.12 that peaks corresponding to different pulses are measured by the oscilloscope. The different pulses are separated by 200 ns. This corresponds exactly to a pulse repetition rate of 5 MHz.

The different measurements highlight several behaviours. The assumption of a step makes the most sense for longer pulses. This appears because when current is injected into the diode to generate a pulse, the diode needs to initiate its lasing conditions. This occurs with a sudden start of the laser until it stabilises. Stable lasing conditions were only achieved with the 9000 ps pulses duration. It is thus important to keep in mind the shape of the power distribution for short pulses for the later steps of the source development. The measured pulse repetition rate corresponds to the specified one.

In the source that was built for this work, it was decided to use the shortest pulses at 50 ps and a pulse repetition rate of 5 MHz because it corresponds to the maximum peak power. This combination of parameters yields a mean power of 1 µW at maximum. With the assumption of a step pulse of 50 ps, this corresponds to a peak power $P_{\text{peak}} = 0.04\text{W}$ according to Equation 5.19. However, to generate non-linear effects, the power should be increased to reach a satisfying efficiency. It was decided that a peak power of about 4 kW was adequate to measure sufficiently easily the generated photons. This amount of peak power corresponds to a mean power of 1 W with the pulse duration set at 50 ps and the repetition rate at 5 MHz. This corresponds to a value of energy per pulse of 200 nJ. An amplification of a 1 µW laser to a 1 W laser corresponds to an increase of 60 decibels. It is difficult to achieve a gain of 60 dB with only one amplifier hence the combination of the two

amplifying modules.

The next sections follow step by step the assembly process of the amplifiers. As mentioned, each amplifier requires another pump laser to increase the power of the 1064 nm laser. The first step was thus to characterise the pump laser diode for the first amplifier.

5.4 First amplifier pump characterisation

The pump laser used to amplify the 1064 nm laser is a 975 nm continuous laser generated by a semiconductor diode, similar to the first one. This was verified thanks to an oscilloscope and the power was constant over time as expected. The spectrum of the diode was also measured thanks to the OSA, and a well-defined peak centred at 975.75 nm was observed. The width of the peak is smaller than 0.5 nm.

Characterising the power of the laser diode is different than for the 1064 nm one. There are no pre-implemented settings and instead, the laser diode can be mechanically tuned by increasing or decreasing the voltage applied to the diode. The optical power was measured in function of the voltage applied to the diode. It is represented in Fig. 5.13.

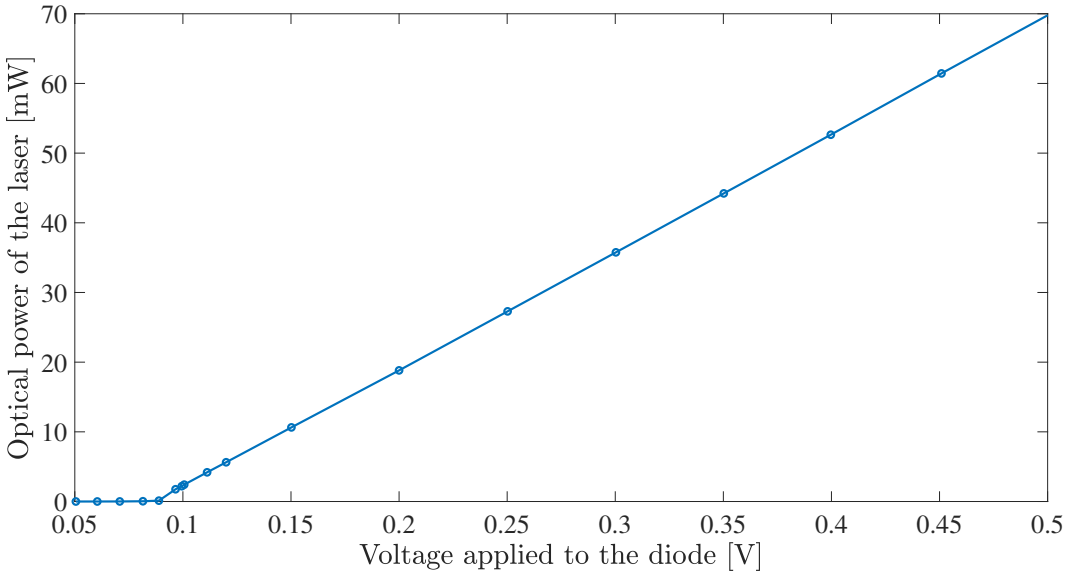

Figure 5.13: Optical power of the 975 nm pump laser diode in function of the applied voltage.

At low voltage values, the optical power remains negligible. This is due to the fact that laser diodes enter lasing conditions after a certain threshold current is reached. Under the lasing threshold, the output of the diode is dominated by spontaneous emission rather than stimulated emission. The output power increases slowly as the excitation of the diode increases. Above the threshold however, the slope of the output power with the excitation is constant and much larger than the increase of power under the threshold. This behaviour is illustrated in Fig. 5.13. One can see at first that the output power barely increases with

the voltage until the threshold is reached and the power increases linearly with the current or equivalently the voltage [84].

5.5 First amplifier

The previously characterised diode is used to amplify the 1064 nm pulsed laser. In the end, the laser that comes out of the diode should be amplified by 60 dB. This was achieved by using two amplifying modules of about 30 dB. Both modules developed in this work rely on ytterbium (YB) fibres. Doped fibres act as an active medium identically to any medium in a laser. The core of the optical fibre is sprinkled with rare-earth elements. Depending on the material with which the fibre is doped, the wavelength of the light that is emitted is different.

To amplify the 1064 nm laser, ytterbium fibres are the best suited. Doped fibres emit light when they are excited. One way to excite the fibre is to inject some optical power inside resulting in the emission of energy. The energy the pump photons brought is evacuated through two mechanisms, the release of heat and the emission of a photon. There is thus an inherent loss of energy that cannot be exploited. When a photon at 975 nm is absorbed by the ytterbium fibre, a part of the energy is released as heat and the rest as a photon at 1064 nm. Ytterbium fibres have the advantage that the energy loss is proportionally lower than for other doped fibres. It corresponds to the energy difference between photons at 975 nm and photons at 1064 nm.

For the first amplifier, three different configurations were tested. The different configurations of amplifiers rely on different micro-optical elements. The first configuration is depicted in Fig. 5.14.

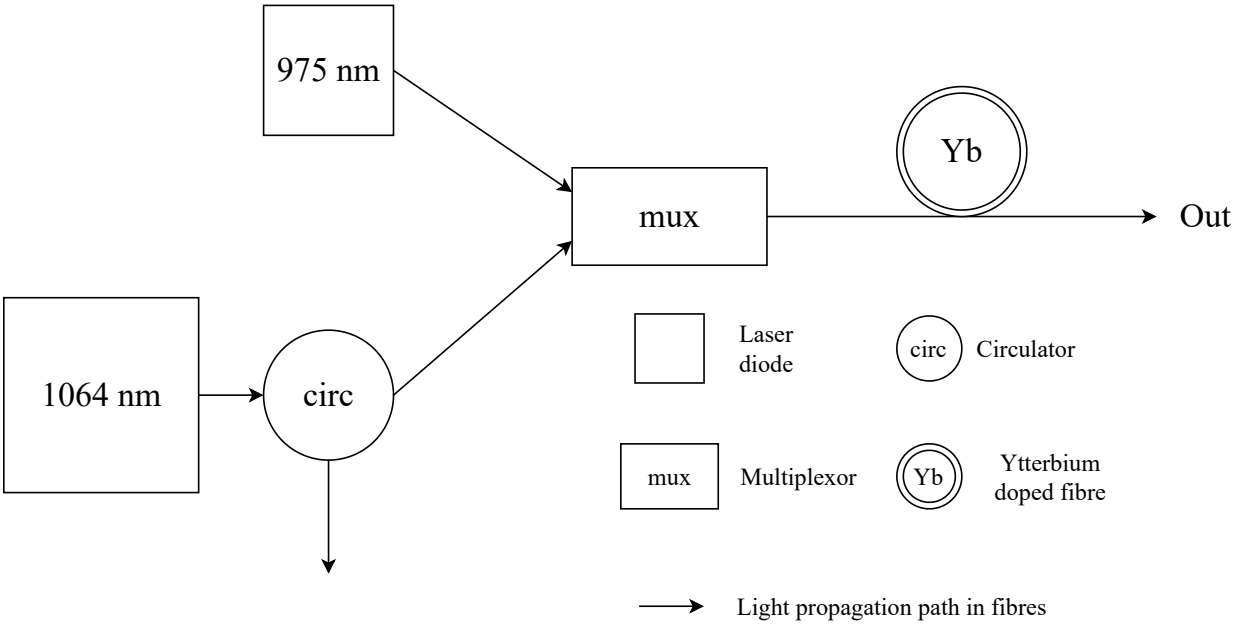

Figure 5.14: Architecture of the single passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW.

The laser diode at 1064 nm produces the pulses that have to be amplified. After a pulse is emitted by the diode, the first component it reaches is a circulator. An optical circulator is a micro-optical device with a set number of ports such that depending on which port the signal enters the circulator, the output port is predictable. In the amplifier, a three ports circulator is used. Circulators are frequently used to control the propagation of light in the system. In a three ports circulator, light entering port 1 is then transmitted to port 2. When light enters by port 2, it exits the circulator by port 3. Optical circulators function the same way electronic circulators work.

In the presented amplifier, the circulator acts as an isolator. The laser diode at 1064 nm is attached to port 1 such that the light it emits enters the circulator by this port. The intended output port is thus port 2. Should some light be reflected down the circuit and reenter the circulator by port 2, the diode will be preserved of these reflections since light will be redirected towards port 3. This principle is illustrated in Fig 5.15.

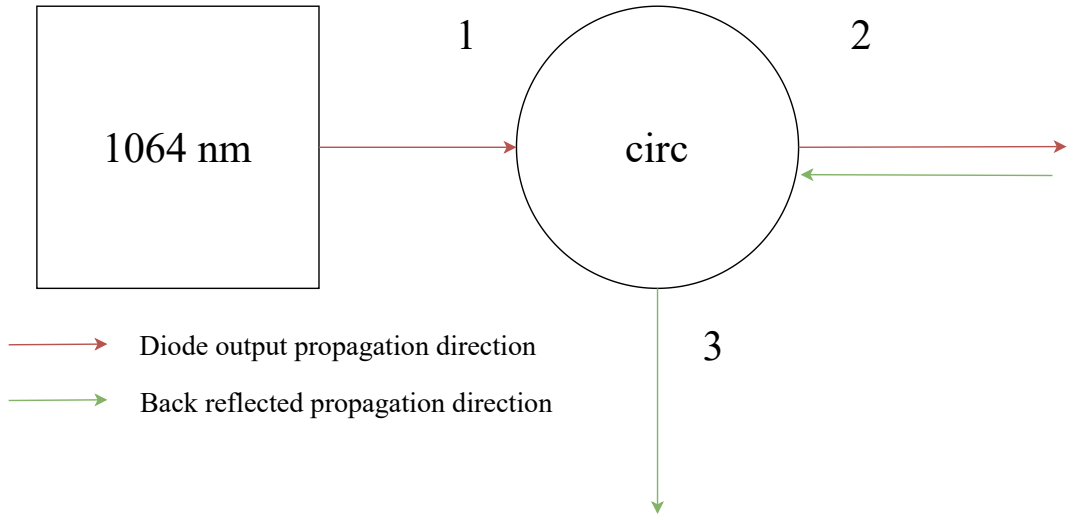

Figure 5.15: Operating scheme of the circulator. Light generated by the laser diode enters port 1 and exits through port 2. If some back reflected light enters by port 2, it exits the circulator by port 3, isolating the laser diode.

In practice, a circulator is made of several optical elements and there are different schemes to create one. An example of optical circulator is shown in Fig. 5.16.

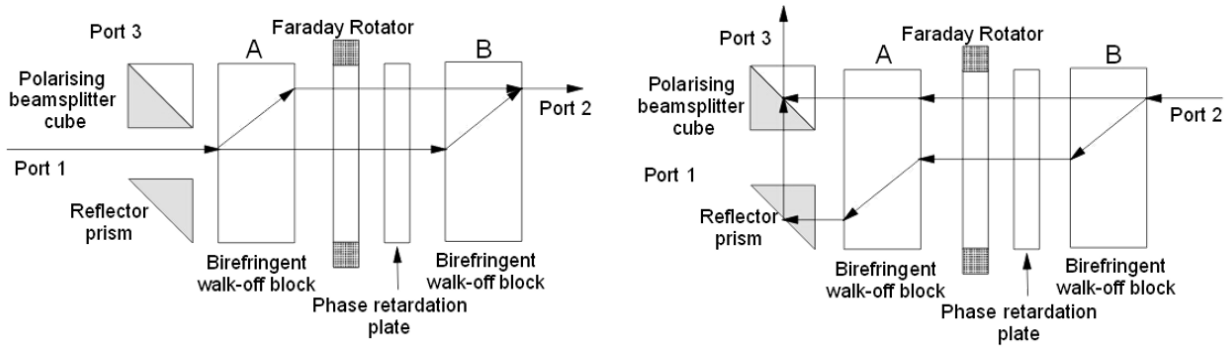

Figure 5.16: Layout of a general optical circulator. The birefringent blocks help separate both polarisation components of the incident light. The Faraday rotator rotates the polarisation asymmetrically while the phase plate rotates it symmetrically. Depending on the propagation direction, this results either in a 90° rotation of the polarisation of the rays or in a 0° rotation overall. Figure from [85].

When a linearly polarised light ray enters the birefringent blocks, it is separated into two components: an ordinary and an extraordinary wave. The ordinary wave passes straight through the crystal while the extraordinary wave is refracted. By rotating the polarisation by 90° through the combination of the Faraday rotator and phase plate in the left-to-right propagation direction, the polarisation of the previously refracted component becomes ordinary from the perspective of the second crystal, passing unrefracted. In the right-to-left propagation direction, the Faraday rotator and the phase plate counter each other. Faraday rotators are known for their asymmetrical behaviour. If a light ray enters the Faraday rotor and has its polarisation rotated in a certain direction, being reflected through the rotator does not undo the polarisation change, the effects are doubled. However, for phase plates, a double passage through the plate undoes the polarisation shift. Because of this, a ray propagating from right to left experiences no net polarisation shift after the combination of rotator and plate. An extraordinary wave entering the circulator from port 2 remains extraordinary for both birefringent blocks. Consequently, it is refracted twice. This asymmetry allows to guide the light rays towards polarisation beam splitters that will direct the light towards port 3.

Back to Fig. 5.14, after the circulator, the multiplexor separates the light wavelengths in different channels. For the single passage amplifier, the two input channels are a 1064 nm channel, a 975 nm channel and the output channel is a common channel in which both wavelengths propagate. The multiplexor acts as a beam combiner that injects the laser pulses at 1064 nm and the pump laser at 975 nm in the channel leading to the ytterbium fibre. The ytterbium fibre amplifies the laser pulses at 1064 nm and the resulting laser exits the optical fibres afterwards. It is worth mentioning that the laser diode at 975 nm is protected from back reflections thanks to an isolator. The optical isolator only allows light to travel in one direction. In this case, the isolator allows light from the 975 nm diode to be injected in the multiplexor but prevents back reflections from propagating back to the laser diode. If some power travels back to the laser diode, this can damage the component because laser diodes are not made to receive power back from the emitted light. When this happens, the mirrors composing the optical cavity can be damaged and their reflectivity diminished. Moreover,

the excess power can heat the diode above its limits and the components can be damaged or even destroyed.

The optical spectrum of the output light is measured thanks to the OSA. The spectrum of the output light does not depend on the pulse duration. For this reason, only the most interesting measurements of the spectrum among all the ones that were performed are shown hereafter. In the case of a single-pass amplifier, the optical spectrum is represented in Fig. 5.17.

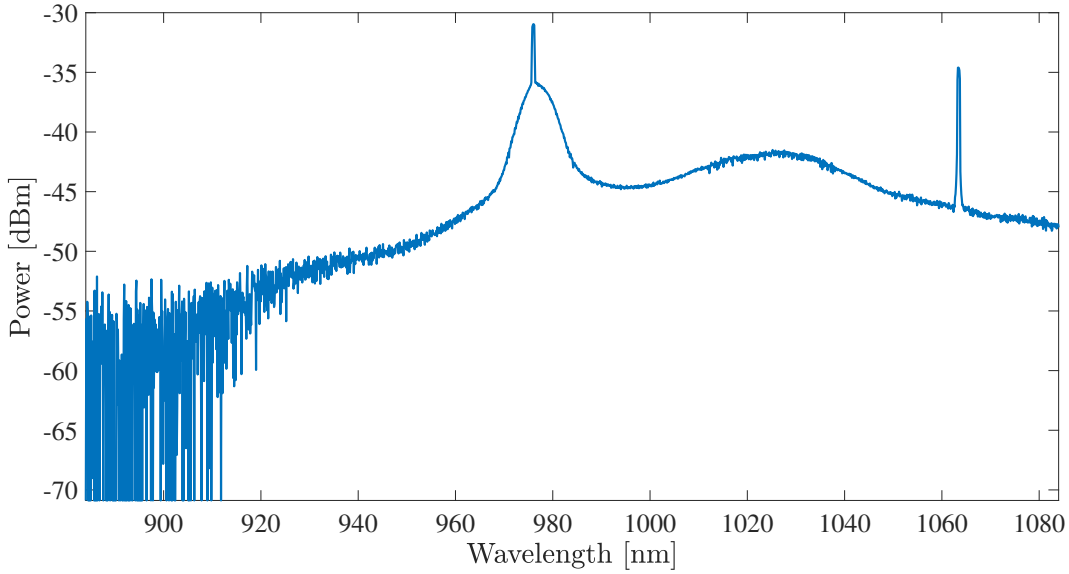

Figure 5.17: Optical spectrum of the output light of the first amplifier in single passage configuration measured in the OSA. The measurement was made with a pulse duration of 50 ps and a repetition rate of 5 MHz.

One can observe in Figure 5.17 two peaks located at 975 nm and 1064 nm. The peaks correspond respectively to the pump laser and the pulsed laser. The power corresponding to the 975 nm laser is larger than that at 1064 nm. This suggests that a major part of the pulse laser is transmitted through the ytterbium fibre without being absorbed. Although filters are used in the final source design to discard the 975 nm light, this peak indicates that in the current state, the amplifier is not efficient. Indeed, the single-pass amplifier output power that was measured corresponds to an increase of about 20 dB with the maximum voltage injected in the pump diode. This is lower than the amplification of 30 dB sought for the experiment. One of the reasons could be that the ytterbium fibre is too short and thus the laser is not amplified enough. Moreover, the junctions of different components are responsible for some losses even though their magnitude is small.

In the end, the single-pass amplifier does not reach the required performances and comes with the disadvantage of letting a significant part of the pump laser go through. Even with filters used later in the source, minimising the output power at other wavelengths is of interest to avoid unexpected absorption behaviours. It is also worth pointing out that this single-pass amplifier does not exclude any wavelength from the output. This means that the noise is not attenuated. To solve these problems, the second configuration that was studied is a double

passage amplifier. The architecture of the double passage amplifier is represented in Fig. 5.18.

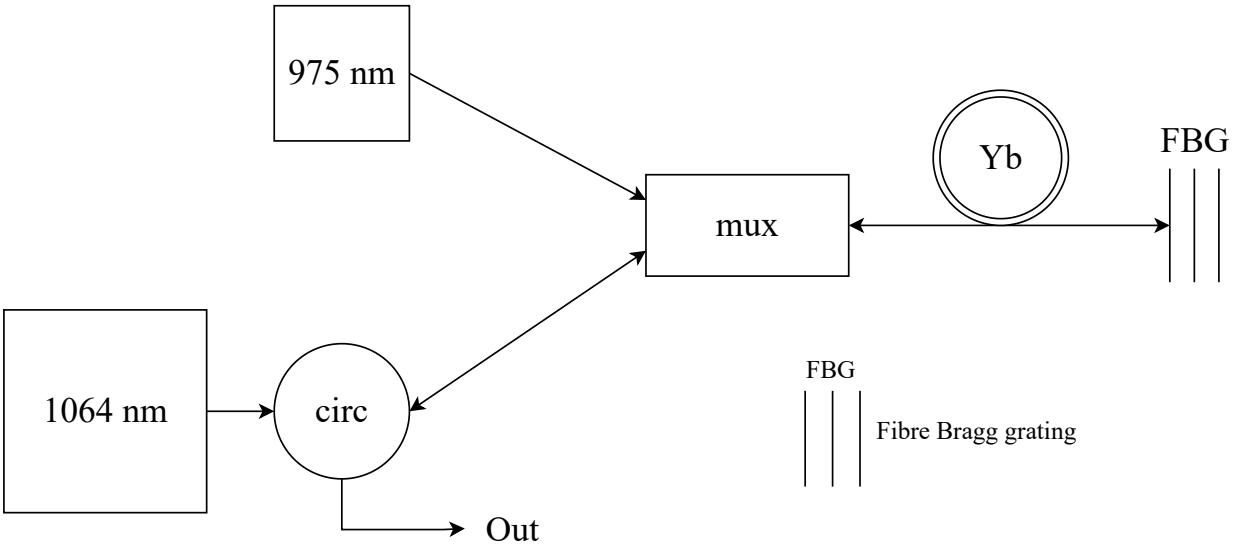

Figure 5.18: Architecture of the double passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW.

The new component is a Fibre Bragg Grating (FBG). Fibre Bragg gratings are fibre components that reflect some wavelengths and transmit the others. This behaviour is achieved by creating a periodic variation of the refractive index in the fibre core. This creates a dielectric mirror for a specific wavelength. The wavelength that will be reflected obeys the following relation

$$\lambda = 2n_e\Lambda, \tag{5.20}$$

where n_e is the effective refractive index of the fibre core and Λ is the period of the grating. In the double passage amplifier, the grating reflects the 1064 nm laser and transmits the other wavelengths. When a laser pulse is emitted by the 1064 nm laser diode, it enters the circulator by port 1 and is directed towards port 2, which leads to the multiplexor. The multiplexor combines the pulsed laser and the continuous pump laser in the ytterbium fibre. The 1064 nm laser is amplified once until it reaches the Bragg grating. Upon reaching the grating, the 1064 nm laser is reflected back to the Yb fibre while the 975 nm pump laser is transmitted and exits the circuit. The previously reflected pulse propagates once more in the Yb fibre and is thus amplified a second time. When it reaches the multiplexor, it is sent towards the 1064 nm channel that links the circulator and the multiplexor. When the reflected pulse reaches the circulator, it is sent towards port 3 to preserve the laser diode. The pulse then exits the circuit and can be collected.

The spectrum of the output light is measured thanks to the OSA and is represented in Fig. 5.19.

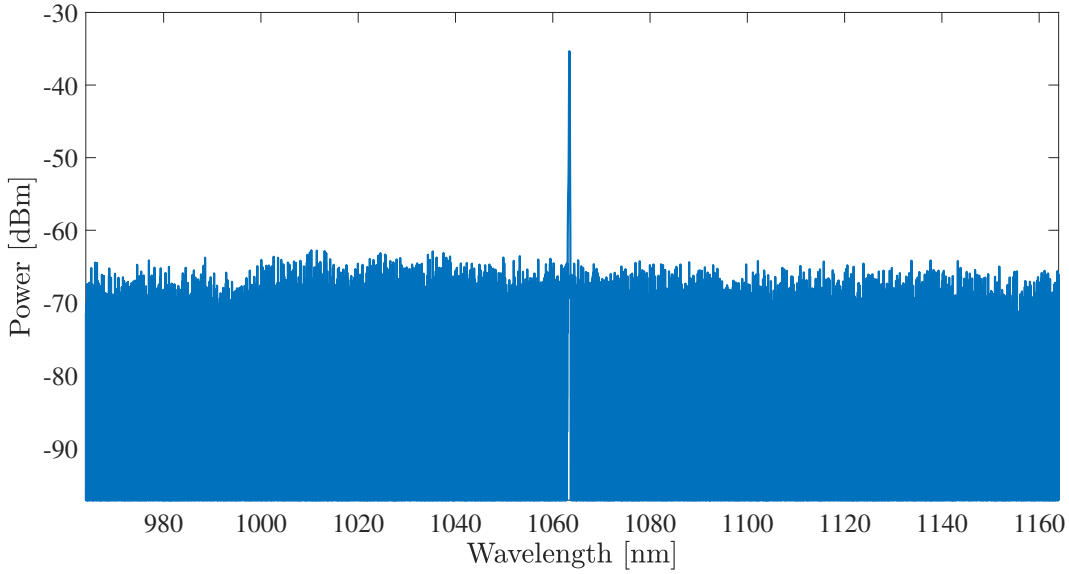

Figure 5.19: Optical spectrum of the output light of the first amplifier in double passage configuration measured in the OSA. The measurement was made with a pulse duration of 50 ps and a repetition rate of 5 MHz.

Figure 5.19 confirms that the double passage is a better configuration to mitigate the problems the simple amplifier exhibited. One can observe that at 975 nm, the previously important peak has disappeared. This is because the 975 nm laser is sent out of the pump diode towards the Bragg grating which only reflects the 1064 nm laser and the multiplexor that separates the signal and pump laser before sending them towards the output. Thus, the continuous laser at 975 nm does not reach the output of the system. Moreover, the magnitude of the peak at 1064 nm compared to the rest of the measured spectrum is much larger than before. This reinforces the point that the double passage amplifier selects the appropriate wavelength and does not transmit the other wavelengths and noise. In terms of performance, the double passage amplifier does not reach the requirement of 30 dB even at a voltage close to the limit of the pump diode.

The double passage amplifier is not suitable for the experiment. Its performances are better than those of the single passage amplifier and it prevents the pump laser light from exiting the circuit with the pulsed laser but they are still insufficient. The pump laser at 975 nm is not completely absorbed by the Yb fibre. This is verified by measuring the optical spectrum of the light that is transmitted by the Bragg grating. To increase the performance, it would be advantageous to increase the amount of pump light that is absorbed by the Yb fibre and increase the amplification of the system for lower power values. The solution to both problems is to increase the number of passages in the fibre for the pulsed laser and the pump laser, leading to the final amplification design: the quadruple passage amplifier. Figure 5.20 represents the schematic of the quadruple passages amplifier.

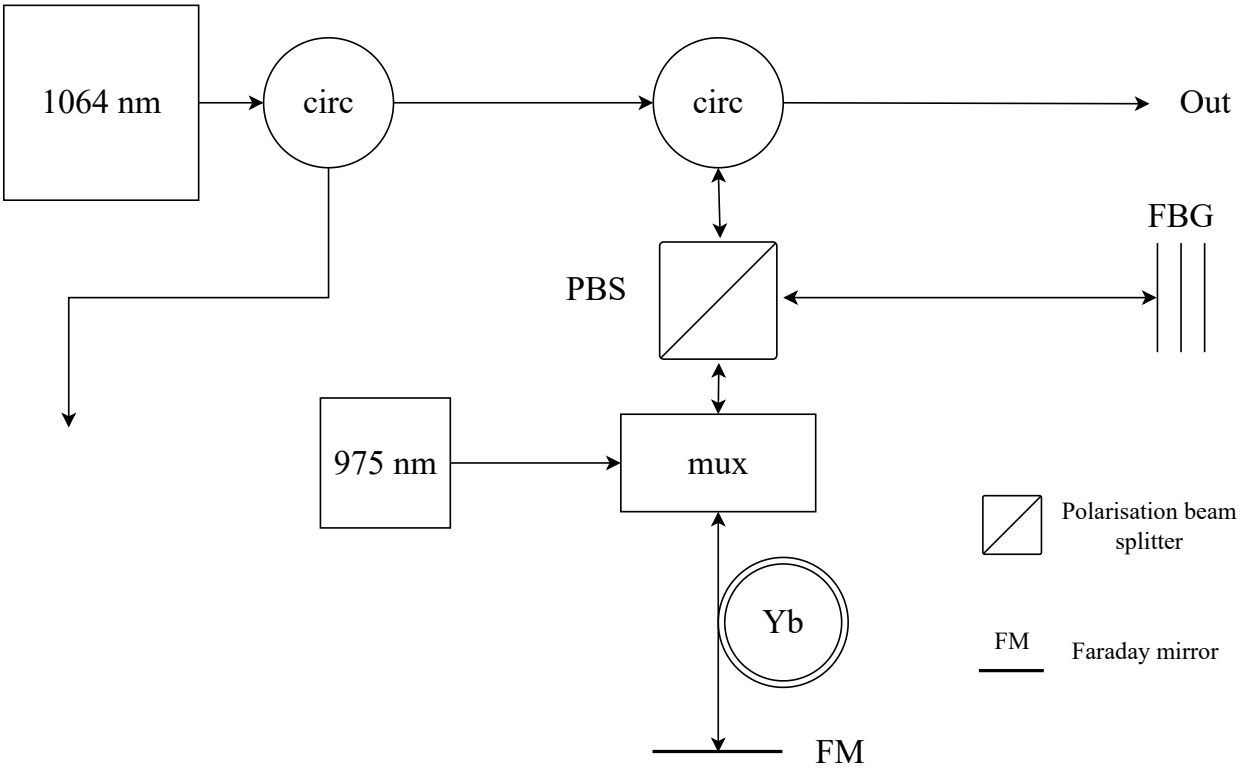

Figure 5.20: Architecture of the quadruple passage amplifier. First part of the pre amplifying module to increase the power of the laser to a target value of 1 mW.

The new components of the system are the Polarisation Beam Splitter (PBS) and the Faraday Mirror (FM). The PBS transmits the vertical polarisation and reflects the horizontal one. This property is exploited as explained later. A FM is a device made of a Faraday rotator and a mirror. It relies on the cumulative effect of Faraday rotators after reflection to rotate the polarisation of an incident wave by 90°. A light beam entering with a vertical polarisation will come back from the device with a horizontal polarisation. Another circulator was also added to isolate the laser diode from any back reflection. Although not necessary, the combined action of both circulators ensures the laser diode is protected.

When a laser pulse is emitted by the laser diode at 1064 nm, it propagates in the fibres through the first and second circulators. The second circulator sends the laser pulse to the PBS since it is connected to its port 2. The laser pulses are vertically polarised. They are thus transmitted by the PBS to the multiplexor. Afterwards, the laser pulses get amplified for the first time in the ytterbium fibre thanks to the pump diode at 975 nm. They finally reach the Faraday Mirror. This path is represented in Fig. 5.21.

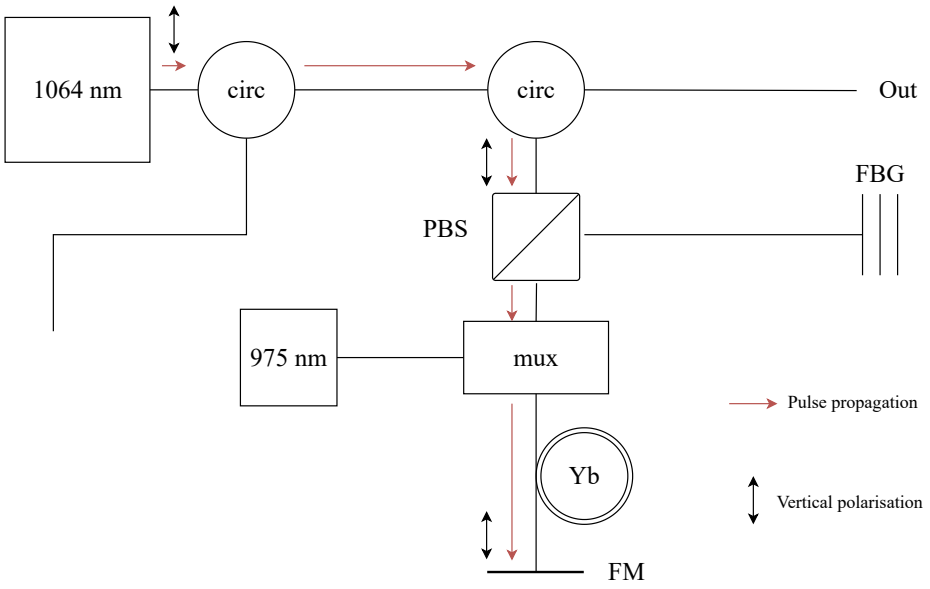

Figure 5.21: First pass of the laser pulses in the first amplifier of the pre amplifying module.

After the laser pulses are reflected by the FM, the polarisation is rotated by 90° and is thus horizontal. The pulses pass once more through the ytterbium fibre to the multiplexor. The pulses are sent back to the channel linking the PBS and the multiplexor. It is worth mentioning that the PBS is linked to the output of the multiplexor at 1064 nm. Now that the pulses are polarised horizontally, they are reflected by the beam splitter towards the fibre Bragg grating. The grating reflects the 1064 nm pulses afterwards. This is represented in Fig. 5.22.

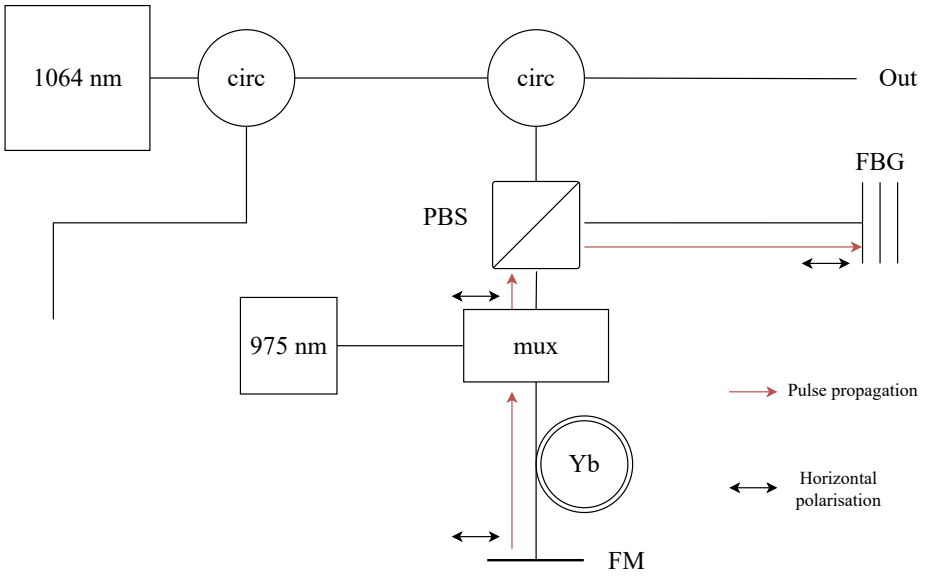

Figure 5.22: Second pass of the laser pulses in the first amplifier of the preamplifying module.

Once the pulses are reflected by the Bragg grating, they are reflected again by the PBS

towards the multiplexor. The pulses then go through the ytterbium fibre for the third time. This is represented in Fig. 5.23.

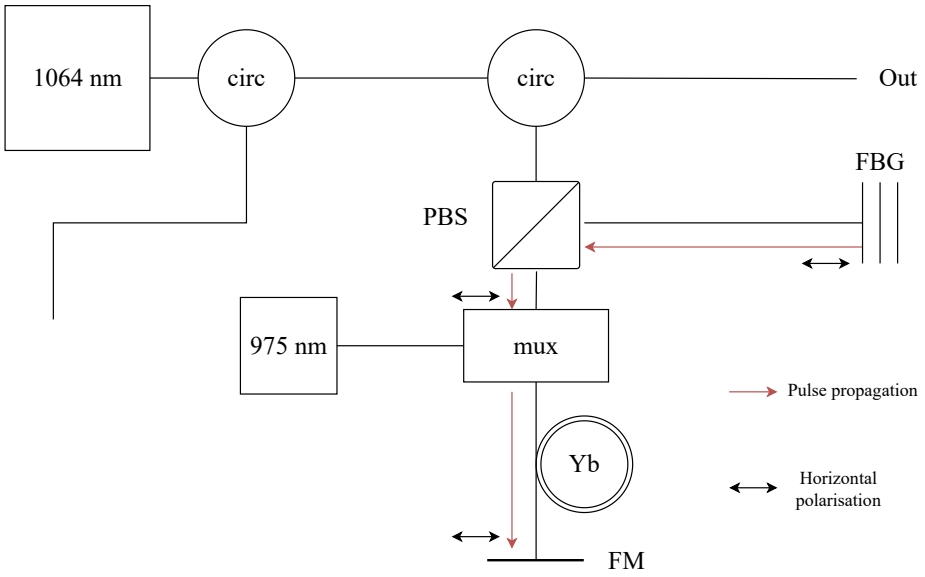

Figure 5.23: Third pass of the laser pulses in the first amplifier of the pre amplifying module.

Finally, the polarisation of the pulses is rotated once more and becomes vertical again. The laser pulses propagate through the ytterbium fibre a fourth time and through the multiplexor. Upon reaching the PBS, the polarisation being vertical, the pulses are transmitted and reach the circulator. Since the pulses come from port 2, they are finally sent towards port 3 and out of the fibres. This is represented in Figure 5.24.

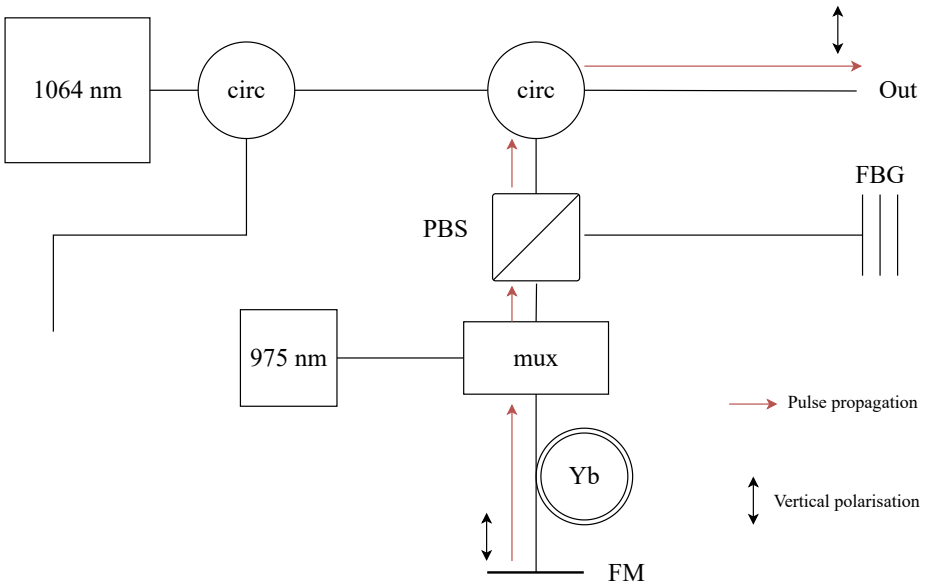

Figure 5.24: Fourth pass of the laser pulses in the first amplifier of the pre amplifying module.

As expected, the four-pass amplifier exhibits better performance than the double-pass

amplifier. The amplification ratio for the same voltage in the pump laser is larger. The optical spectrum of the output light is similar to the double-pass amplifier since the signal is only cleaned once by the FBG and passes through the multiplexor too.

Nevertheless, the superior amplification ratio of the four-pass amplifier is not sufficient alone as it barely reaches the requirements of 30 dB even with the max current intensity the pump diode can withstand. This restricts the flexibility of the system as larger amplification ratios are not achievable with this amplifier. Although the objective of the whole set of amplifications whose next steps are detailed hereafter is to reach a power of 1 W for the laser diode, the possibility of increasing the power would open opportunities to test different configurations. Thus, it was estimated that the four-pass amplifier was insufficient on its own in the pre amplifying module.

5.6 Second amplifier

A second amplifier was built to be part of the pre amplification module to address these problems. This second preamplifier is a double-pass amplifier whose architecture is very similar to the one presented in Fig. 5.18. Both amplifiers are connected by welding the output fibre of the first one to the input fibre of the second such that the amplified light that comes out of the four-pass amplifier is sent directly to the second amplifier. The same pump diode is used to supply the ytterbium fibre in the second amplifier with power. By splitting the light that comes out of the diode, both amplifiers can be powered at the same time with one diode. This also comes with the advantage of reducing the amount of pump light that is not absorbed by the ytterbium-doped fibre. Figure 5.25 depicts the layout of this second amplifier.

Although the pump power going out of the quadruple pass amplifier is low, a bandpass filter centred at 1064 nm was added right at the output of this first amplifier to ensure robustness. Overall, this reduces the noise in the circuit. The combination of both amplifiers allows to amplify the laser at 1064 nm above the 1 mW. As expected, this amplification ratio is achieved with an input current in the pump diode at 975 nm which is below the maximum the diode can withstand. To avoid spreading the degrees of freedom on the power over both amplifying modules, the power inside the pump diode is fixed slightly below the maximum such that the output power of the pre amplifying module is larger than 1 W. One only needs to play on the input power of the pump diodes inside the high-power amplifier to select the output power of the system. This will be helpful to fine-tune the power of the laser.

5.7 High-power pump diodes characterisation

As the target is to amplify the laser to a power of 1 W, it is necessary to amplify the laser once more. To do so, a high-power amplifier is built in a single-pass scheme. This single-pass amplifier is pumped by a combination of two pump diodes at 975 nm that can withstand larger input currents. The optical power of the diodes is displayed in Fig. 5.26.

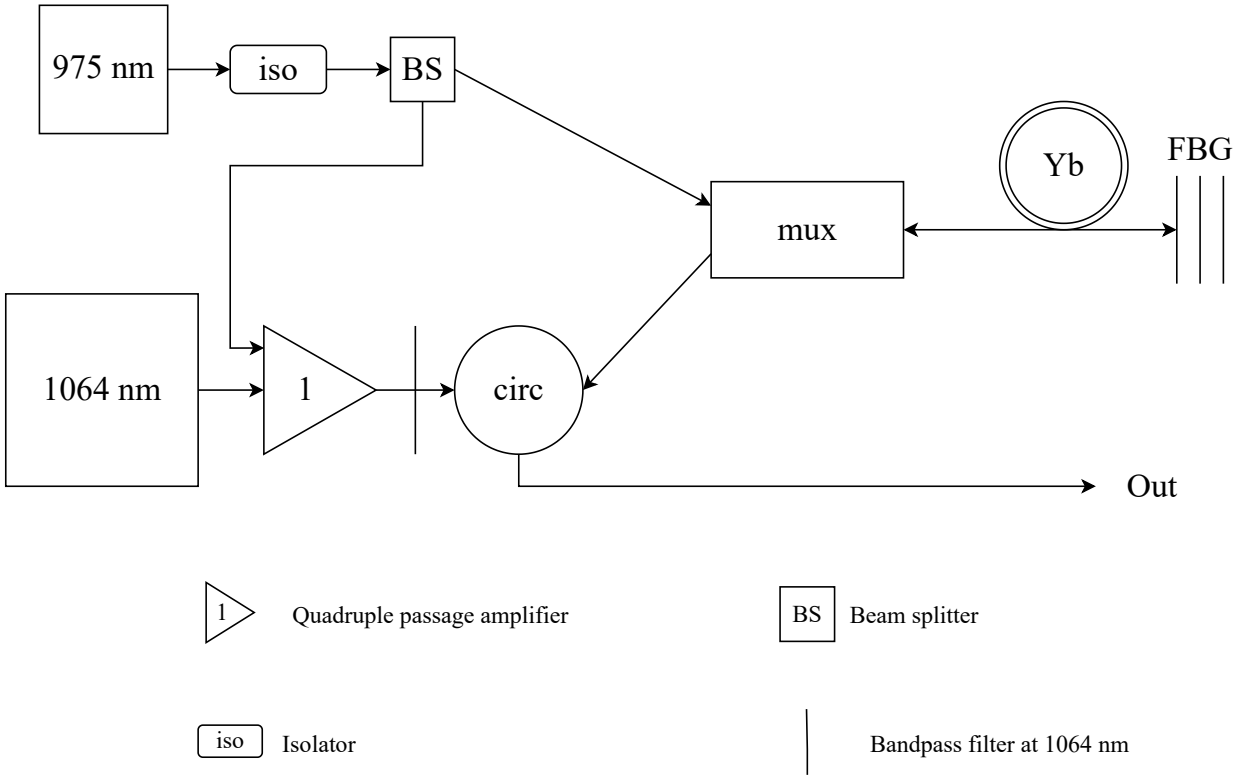

Figure 5.25: Architecture of the second amplifier in the pre amplifying module. This second amplifier is added to increase the flexibility of the system by avoiding to impose operation at the maximum power in both amplifying modules.

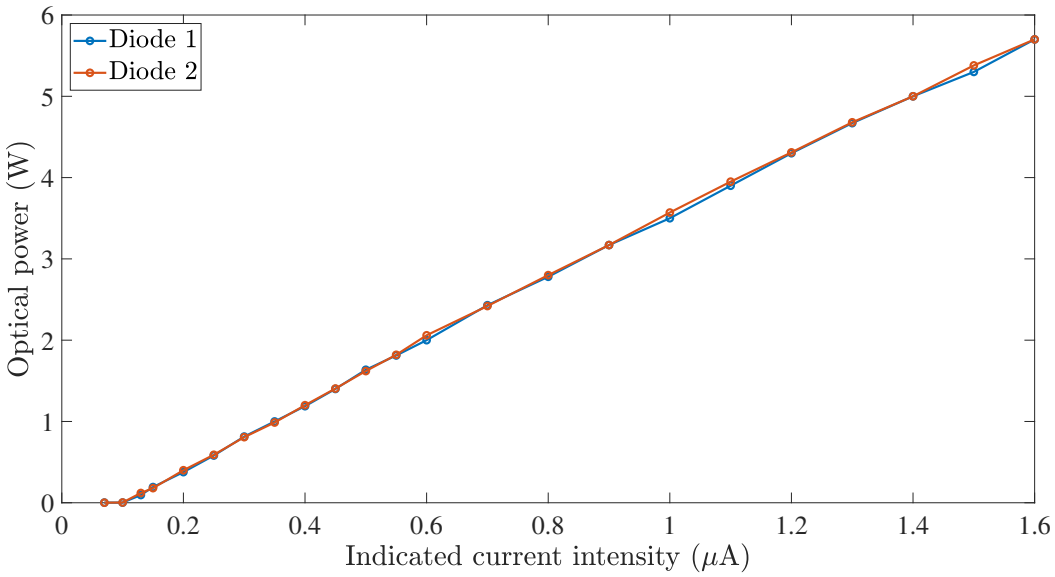

Figure 5.26: Optical power of the 975 nm pump laser diodes used in the high-power amplifier in function of the applied current.

The output power of both high-power diodes follows a steady linear profile after the lasing

current intensity is reached. The same behaviour was observed for the laser diode at 975 nm that was used in the pre amplifying module. The optical spectrum of the laser diodes was also monitored to verify it was centred around suitable values. As power is much larger, the diodes are also regulated in temperature thanks to a Peltier module. By injecting a specific current in the Peltier module, the temperature of the laser diodes can be controlled. It is worth mentioning that depending on the temperature of the diode, the peak of the spectrum is located at a different wavelength. For temperatures from 20°C to 30°C, the centre wavelength of the peak shifts from 969 nm to 965 nm. Although the diodes' spectrum was expected to be centred around 975 nm, the difference is not a concern for the amplification as the energy difference between photons at 975 nm and photons at 969 nm is tenuous. With the two diodes, it is thus possible to amplify the signal a last time to reach suitable powers for the experiment.

5.8 High-power amplifier

The final step of the amplification process is to make the laser reach suitable powers for the experiment. A value of 1 W and above is targeted to conduct the conversion. To do so, another single pass amplifier is built. This high power amplifier architecture is depicted in Figure 5.27.

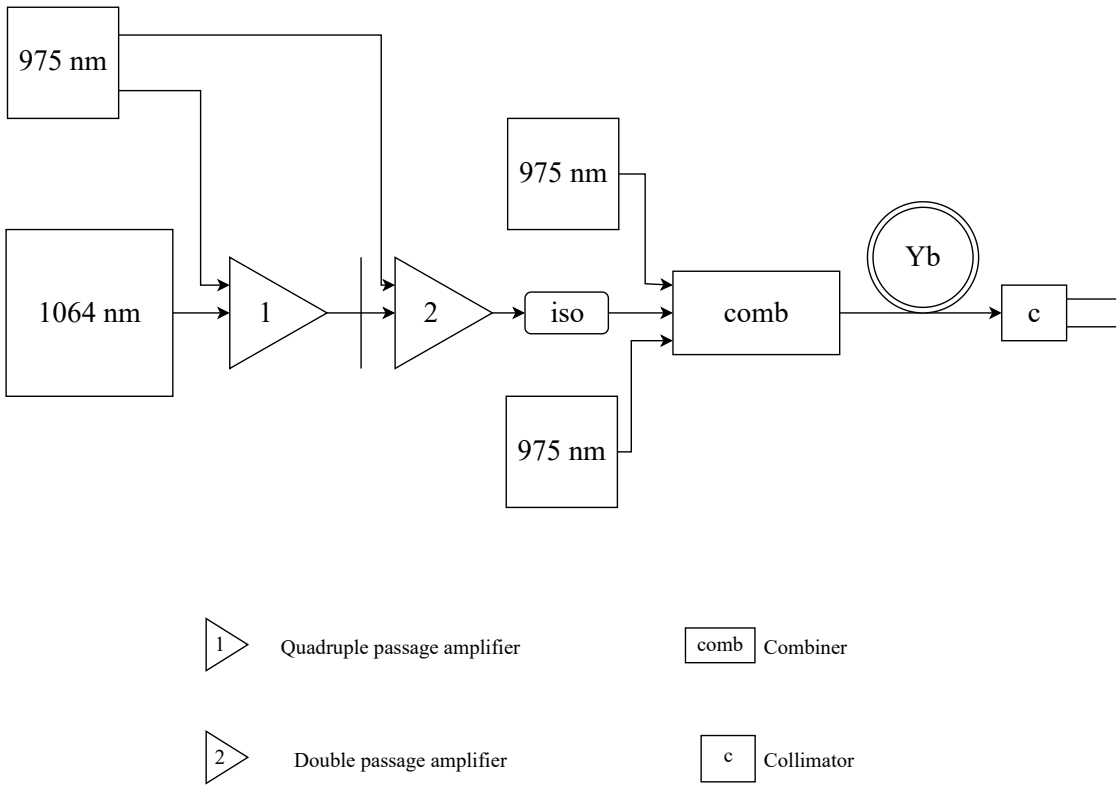

Figure 5.27: Architecture of the high-power amplifier after the pre amplifying module. The high-power amplifier makes the laser reach suitable power levels for non-linear conversion.

In this final amplifier, the combiner is there to combine both pump lasers and the signal

laser in the same channel that goes to the ytterbium fibre. The collimator is there to obtain an output beam the closest to a collimated beam. The collimator is composed of several lenses that manage to collimate the beam. It is important to note that the output beam is a Gaussian beam which is intrinsically uncollimated. However, as the Rayleigh range of the beam is large compared to the scale of the system, it can be considered collimated. More details are given in the next section on optical considerations.

With the amplifying module completely assembled, the power of the output laser can be measured when all amplifiers are set on. The laser at 1064 nm can reach safely powers from 1 to 2.5 W. This range of attainable powers is advantageous as it permits flexibility in the experimental setup. Thus, the laser has reached suitable powers for the experiment. Powers from 1 to nearly 2.5 W result in peak powers of 4 to 10 kW. Theoretically, non-linear effects can appear at any input power. The extent to which the effect is observed depends on the input power, however. The process of frequency doubling or SHG is considered to be efficient at about 50 % of efficiency [86]. If 50 % of the 1064 nm laser diode is converted into 532 nm, this would result in about 500 mW of green light.

Unfortunately, the efficiency of SPDC is much lower. The very low efficiency of the process is the reason a pulsed laser source is used instead of a continuous one. Indeed, the peak power is orders of magnitude larger than the mean power. This increases the efficiency of SPDC for the same mean power compared to a continuous laser. Nevertheless, with a mean power of 500 mW, a peak power of 2 kW is expected for the green laser resulting from the first conversion. Considering the very low efficiency of SPDC, being able to increase the power by a factor of 2.5 is significant to observe the generated photon pairs.

5.9 Optical considerations

With the assembly of the amplifiers concluded, the laser that comes out of the module can be exploited to conduct the experiment. As a reminder, the aim is to convert the 1064 nm photons into photons at 532 nm through SHG and then to convert this green light into photons at 800 and 1588 nm with SPDC. To do so, non-linear crystals were chosen and ordered. The non-linear crystals are magnesium oxide doped periodically poled lithium niobate crystals. These MgO:PPLN crystals are manufactured such that a crystal comprises different channels in which the period of the optical axis inversion is different. The different periods help reach different Quasi-Phase-Matching (QPM) conditions. The length of the different domains is also sensitive to thermal effects. For this reason, the crystals are regulated in temperature to obtain the QPM condition for a specific wavelength. The crystals were manufactured by the company Covesion. For the crystal dedicated to the SHG with the pump laser at 1064 nm, the following temperature dependence of the QPM condition is provided.

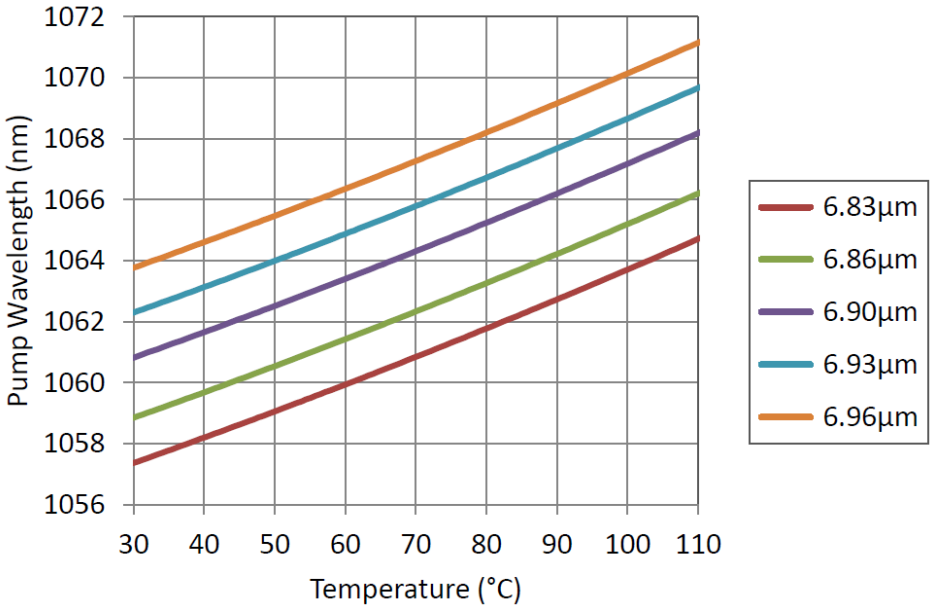

Figure 5.28: Quasi-phase matching condition for the different channels of the crystal. For a specific wavelength, the QPM condition is reached in the different channels at the temperature in abscissa. Figure from Covesion [77].

These values are expected performances, and the actual values might differ slightly. To control the temperature of the crystals, they are encapsulated in specifically designed ovens provided by Covesion. These ovens are connected to temperature controllers that allow to set the desired temperature. The oven and temperature controller are depicted in Fig. 5.29 and 5.30.

Figure 5.29: Oven manufactured by Covesion [77].

Figure 5.30: Temperature controller manufactured by Covesion [77].

The most complicated task is to guide the laser inside the crystal. It is desirable to concentrate at maximum the power of the laser to maximise the efficiency of both processes. Physically, this is achieved by focusing the laser inside the crystal to the smallest spot size possible. However, the crystals cannot withstand a larger peak power density than the limits of the material. For the crystal dedicated to SHG, this limit is less constraining. According to the manufacturer, the SHG crystal should not undergo power densities larger than 50 MW/cm^2. This restriction in terms of power is equivalent to imposing a minimum size or radius of the spot. By making the hypothesis that the power is evenly distributed on the spot, this is equivalent to imposing the spot radius to be larger than 50 µm for a mean power of 1 W. Indeed, we have

$$\frac{P_{\text{peak}}}{\pi\, r^2} = 50 \text{ MW/cm}^2. \tag{5.21}$$

By isolating r, one finds that $r \approx 50$ µm. If a mean power of 2.5 W is considered, which corresponds to a peak power of 10 kW, the radius of the spot should be larger than 80 µm. Similarly, for the SPDC crystal, the supplier has advised not to concentrate the power above a value of 1.5 MW/cm^2. This is equivalent to a radius of 200 µm and 325 µm for the peak power of 2 kW and 5 kW. These values are obtained by assuming that the process has an efficiency of 50% which is highly overestimated to remain cautious and avoid damaging the crystal.

With the different restrictions on the crystals computed, it is possible to design the optical setup of the experiment. Focusing a Gaussian beam inside a crystal is not a straightforward task since many aspects need to be considered. Before diving into the details of the optical design, some theoretical concepts are worth explaining.

As previously explained, a Gaussian beam is a beam of electromagnetic radiation whose transverse amplitude profile follows a Gaussian function. They behave fundamentally differently from optical rays. As Clermont et al. point out, the image waist of a Gaussian beam passing through a converging lens is located at the image focal plane if its waist is located at the object focal length. This goes against the principle in geometrical optics that an object located at the focal plane of a lens is imaged at infinity [87]. The fundamental difference in behaviour is because Gaussian beams follow different laws than classical rays. The propagation of a Gaussian beam is governed by the following equation

$$w(z) = w_0 \sqrt{1 + \left(\frac{z}{z_r}\right)^2}. \tag{5.22}$$

z is the distance between the waist of the beam and the plane at which the beam is considered, w_0 is the waist of the beam and z_r is the Rayleigh range or Rayleigh length that was mentioned in section 4.3.2. It is expressed as

$$z_r = \frac{\pi\, w_0^2}{\lambda_0}. \tag{5.23}$$

The fact that Gaussian beams propagate following Equation 5.22 makes a true collimated beam impossible to reach. Even when collimated by a lens, the beam still propagates according to the equation. The relevant parameter to estimate if a Gaussian beam can be considered collimated is its Rayleigh length. If the optical system remains inside the Rayleigh length of the beam and its scale is significantly smaller, it can be considered collimated. Nevertheless, it is possible to reduce the divergence of a Gaussian beam by making it go through an optical element like a converging lens. The waist of the Gaussian beam must be located at the focal plane of the collimating lens. This has the consequence to modify the waist of the output beam to be equal to the size of the beam at the lens.

In the experimental setup that was assembled up to now, the laser beam exits the optical fibre circuit by a collimator with a diameter of 1.6 mm. The wavelength being equal to 1064 nm, this corresponds to a Rayleigh range of about 2 m. If the first focusing lens remains close to the collimator, the hypothesis of a collimated beam is reasonable. In the case of a collimated beam, Saleh; Teich [88] propose an equation giving the focused waist of the beam after the lens when the incident beam is collimated. The equation is

$$w_0' = \frac{\lambda_0}{\pi\, w_0} f, \tag{5.24}$$

where f is the focal length of the lens. This expression makes the approximation that the lens is thin. Saleh; Teich also explain that the waist of the converged beam is located at the focal length of the lens. It can simply be shown by using the thin lens equation

$$\frac{1}{s} + \frac{1}{s'} = \frac{1}{f}. \tag{5.25}$$

s is the distance from the lens to the waist that is located before the lens and s' is the distance from the lens to the location of the waist after it. If s tends to infinity, the equation predicts that the second waist is located at the focal length of the lens. This result is analogous to ray optics since when the beam is considered collimated, the wavefront striking the lens is similar to a bundle of horizontal rays. However, the spot size is not equal to 0, contrary to what is predicted by ray optics. Equation 5.24 is derived using the formalism of wave optics.

Although geometrical optics is subjected to physical inaccuracies for Gaussian beams, it is interesting to think about the problem with this paradigm in mind as it allows highlighting important behaviours with more simplicity. When an incident beam of parallel rays hits a lens, the angle between the horizontal optical axis and the ray determines where the focus point will be in the focal plane of the lens. This is represented in Fig. 5.31.

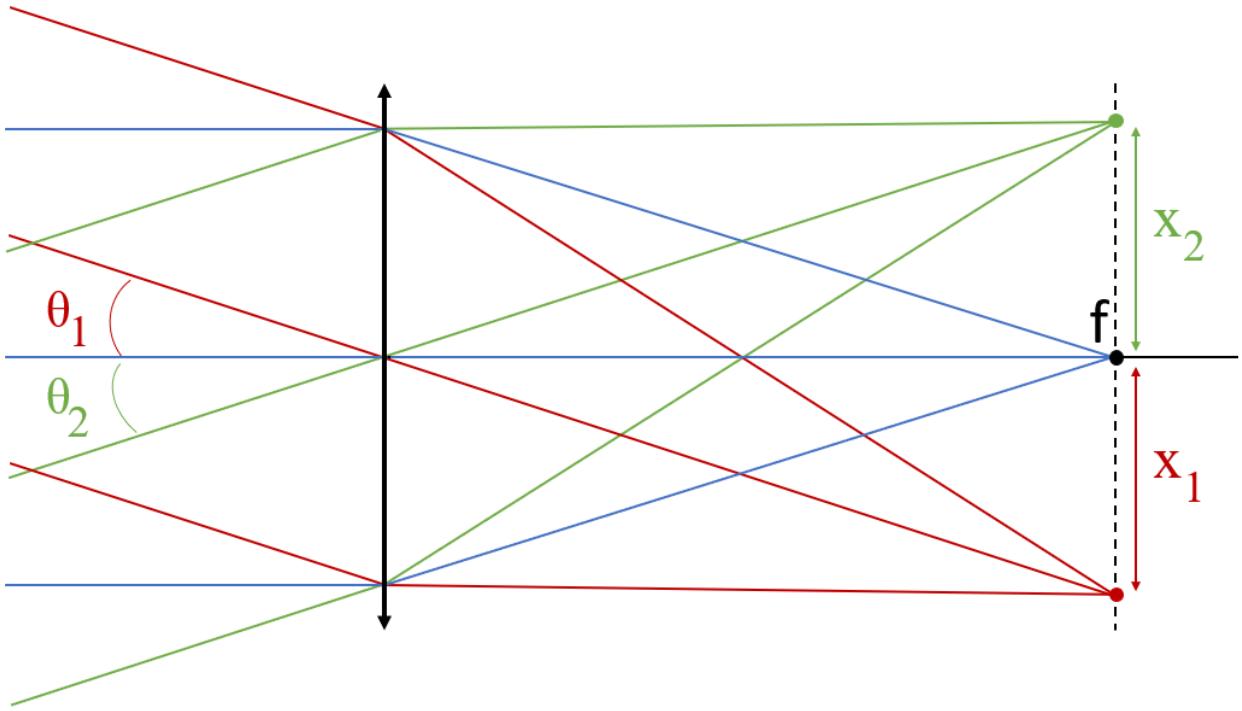

Figure 5.31: Trajectory of different rays striking the converging lens with different angles with respect to the horizontal axis. The angles allow to determine the distances x_1 and x_2 if the focal length f of the lens is known.

If a supposed collimated beam is collimated with a certain defect represented by the angle θ, the deviation from the actual focal point f follows the equation

$$\begin{aligned} x &= f \, \tan\theta \\ &\approx f \, \theta, \end{aligned} \tag{5.26}$$

if the paraxial approximation is respected. The value of x can be interpreted as the radius of the focused spot and is determined by the collimation error. In the case of Gaussian beams, the beam reaches the lens with a non-horizontal profile. Up to one radius away from the centre of the Gaussian beam, the beam strikes the lens with an incidence angle. Figure 5.32 depicts the propagation of a Gaussian beam reaching a converging lens.

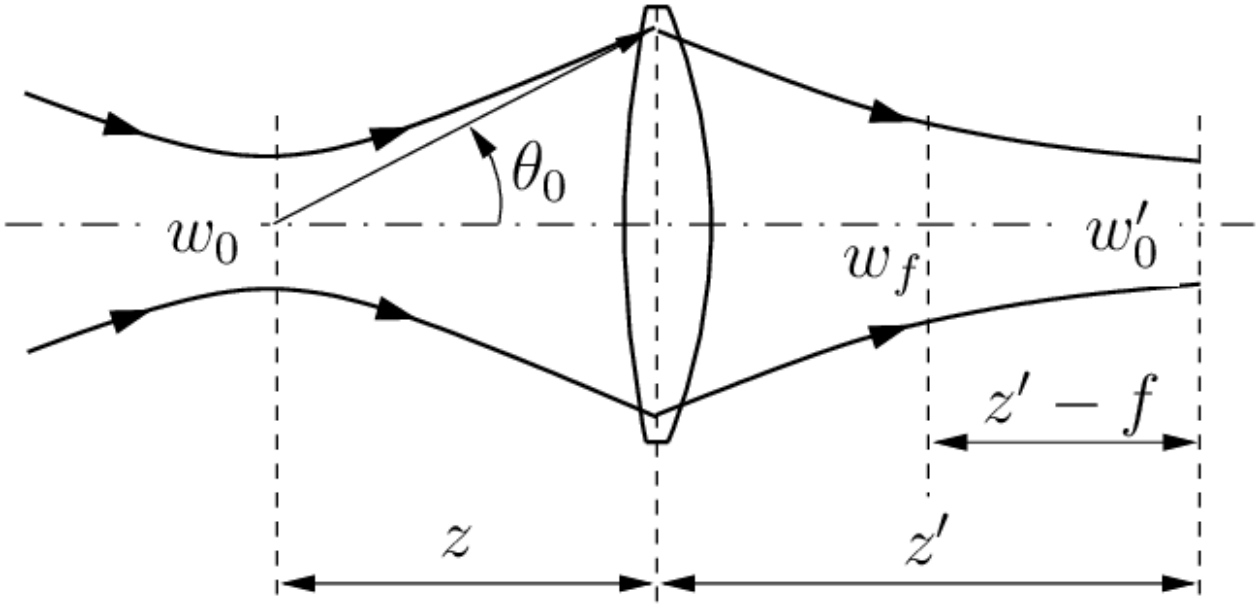

Figure 5.32: Gaussian beam reaching a lens. The angle θ_0 is the maximum angle of incidence of the Gaussian beam. This angle will determine the size of the spot. Figure from Moskalev [89].

Since the beam has an incidence angle, it will not be focused at a point but in a spot. This qualitative description illustrates the fact that the spot has a spatial extension for Gaussian beams, unlike ray optics.

Figure 5.32 is useful to visualise the angle at the extremities of the beam. Although, a collimator is welded at the end of the optical fibre, a truly collimated beam is impossible to achieve. In reality, a beam reaching a lens has always an angle of incidence because of its nature and the collimation defect. The defect amplitude depends on the device.

The geometrical optics approximation is interesting for a qualitative description. However, to design the optical setup, the results of Gaussian optics are privileged to select the focal lengths and compute the spot size. They are more accurate to describe Gaussian beams than geometrical optics.

Equation 5.24 is valid if the beam is considered to be collimated. In the assembly, the laser exits the circuit by the collimator. A collimated beam is characterised by a constant radius along the propagation which is impossible according to the intrinsic properties of Gaussian beams. However, the variation of the Gaussian beam radius can be considered low when the lens remains within the Rayleigh range of the beam as explained earlier.

Another factor needs to be taken into account when dimensioning the lenses. Perfect Gaussian beams do not exist either, and optical elements tend to deteriorate the beam quality. The quality of a laser beam is expressed by the factor M^2. It represents the deviation of the divergence angle of a beam compared to a diffraction-limited one [90]

$$\theta = M^2 \frac{\lambda}{\pi\, w_0}. \tag{5.27}$$

The parameter M^2 is a manner to model the disparity between a Gaussian beam for which it is equal to 1, its minimum value, and a real laser beam. For the application developed in this work, its effect is to increase the size of the spot. In the end, the power is distributed on a larger surface than the one predicted by Equation 5.24. It is also worth mentioning that it is difficult to estimate accurately since a real laser beam has a complex intensity profile and the factor M^2 is only an approximation to model the deviation between the real profile and a Gaussian beam intensity profile. Both the collimated approximation and the M^2 factor are limitations to the accuracy of the computed spot sizes. Nevertheless, the M^2 factor predicts that the size of the spot will be larger than expected and thus less dangerous for the crystals. However, this will limit the extent to which computations can predict the efficiency of the processes.

Another problem appears with the necessity to focus the laser beam to a spot inside a crystal. The crystal refractive index is larger than the one in the air. The incoming light rays are refracted at the interface between the crystal and the air because the refractive index changes. Nemoto studied the impact of a dielectric interface on the beam waist after the interface. Nemoto derived from the complex beam parameter that the beam waist size is not impacted by the interface. The size the waist would reach in the first medium determines the beam waist in the second medium. In the case where the first medium is air and the second is a non-linear crystal, the waist size can be computed according to relations in the air which exhibits a refractive index close to 1. The relevant effect of the dielectric interface is to shift the waist of the beam. Depending on the propagation direction, the waist is either shifted in the propagation direction or the opposite one. Figure 5.33 represents the waist shift after a dielectric interface.

In the experimental setup, laser beams converge from the air into the dielectric crystal. The bottom part of Figure 5.33 is relevant for the application. After passing through the crystal, the beam escapes the medium with a larger refractive index to the medium with a lower refractive index. This is illustrated in the bottom of Fig. 5.33 by switching all indices with $n_1 > n_2$ and inverting the propagation direction.

Nemoto proposes the following formulas to evaluate the magnitude of the waist shift [91]

$$(\Delta z)_a \equiv z_2 - z_1 = (n_2/n_1 - 1)\, z_1, \qquad \text{with} \quad z_1 > 0, \tag{5.28}$$

$$(\Delta z)_b \equiv |z_2| - |z_1| = (n_2/n_1 - 1)\, |z_1|, \qquad \text{with} \quad z_1 < 0. \tag{5.29}$$

In the developed experimental setup, laser beams are focused inside crystals and exit the crystals afterwards. At the entrance and exit of the crystal, the waist is shifted in the propagation direction. It is also possible to represent it with geometrical optics. When a light ray reaches the interface between two mediums, it is refracted according to the Snell-Descartes law

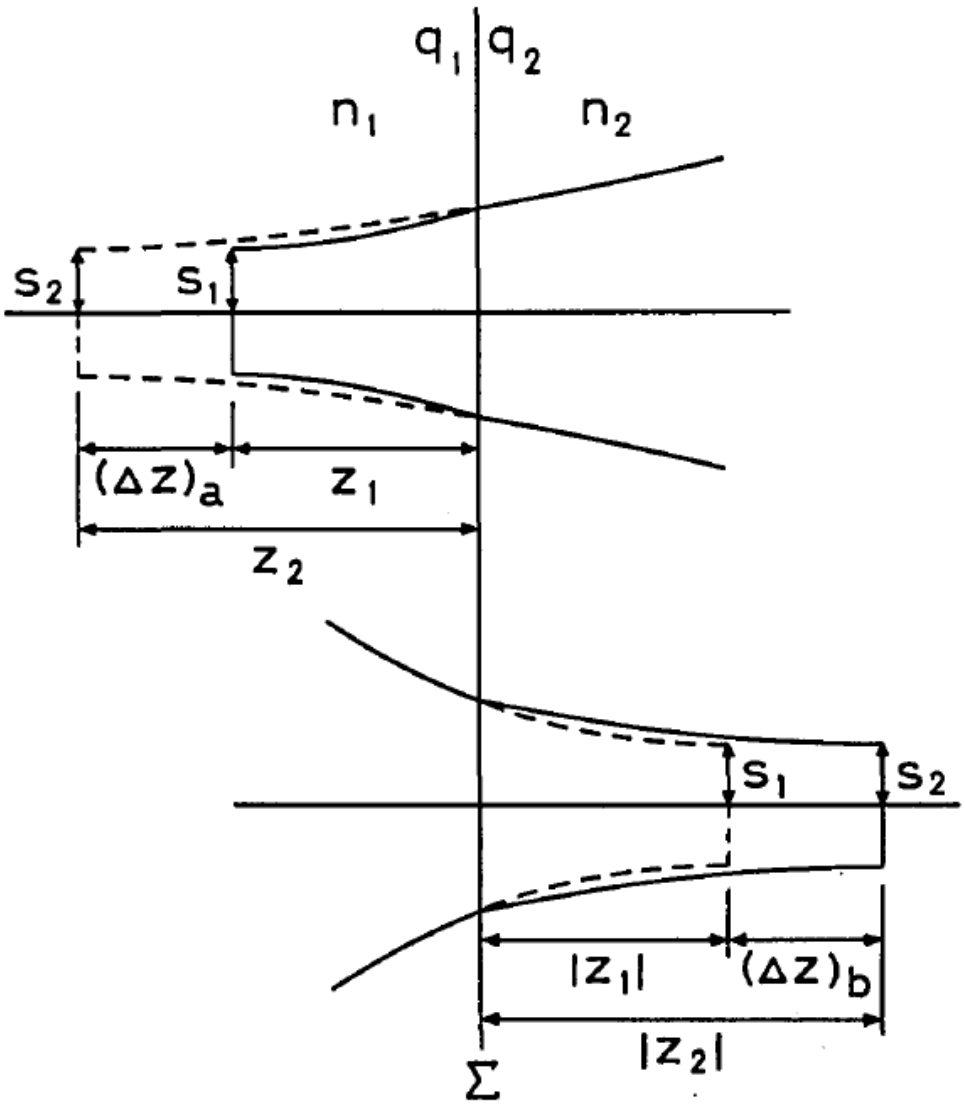

Figure 5.33: Waist shift generated by the transmission of a Gaussian beam through a dielectric interface. In this case $n_1 < n_2$, and Σ is the interface. q_1 and q_2 are the complex parameters of the beam in both mediums and must remain equal. The propagation direction is from left to right. Figure from Nemoto [91]

$$n_1 \sin\theta_1 = n_2 \sin\theta_2. \tag{5.30}$$

If the second medium has a refractive index larger than the incident medium, the angle between the normal at the surface and the light ray in the second medium is smaller. One way to intuitively understand the way the waist is shifted is to apply the Snell-Descartes law with the assumption that the waist size is unchanged. This is what is depicted in Fig. 5.34.

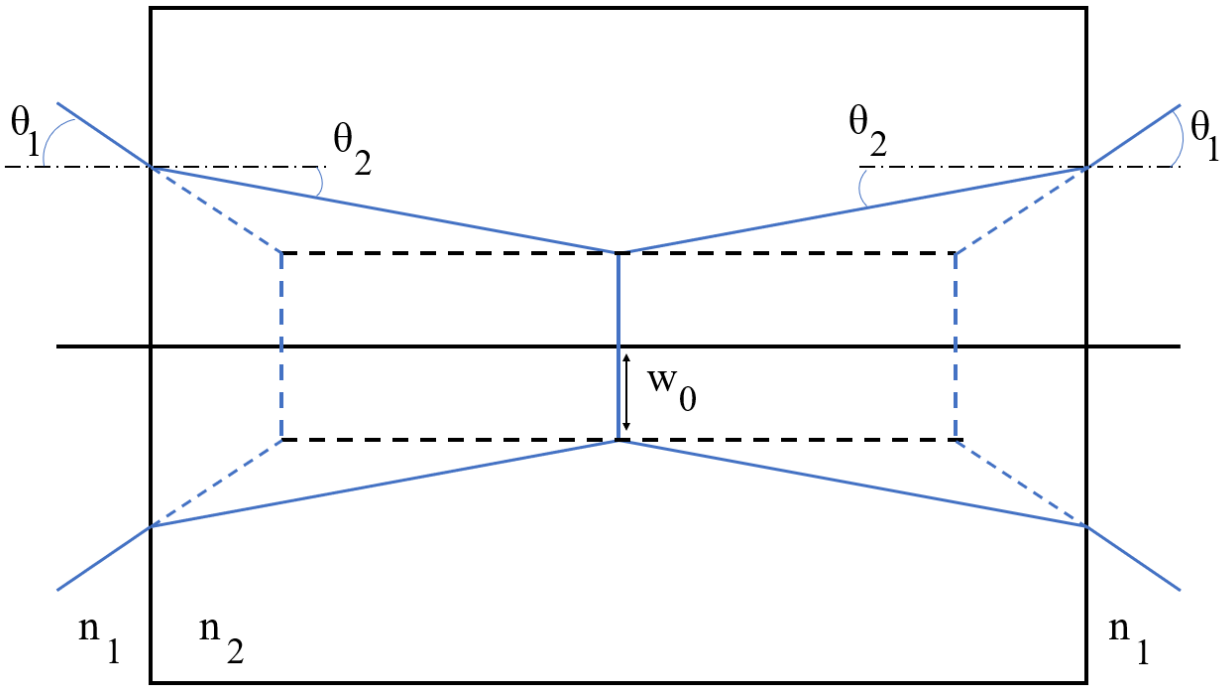

Figure 5.34: Waist shift that results from the modification of refractive index between the two mediums with $n_1 > n_2$. The propagation direction is from left to right. The blue dashed lines represent the trajectory of the light rays and the waist of the beam if there was no crystal from the perspective of air. The complete lines are the actual trajectory and waist of the beam.

As the refractive index in the crystal n_2 is larger than the one of air n_1, the angle of incidence θ_1 is larger than the angle of refraction θ_2 and the waist is located further than in the air. Figure 5.34 depicts this behaviour on the left. At the exit of the crystal, the light rays escape with a refraction angle θ_1 that is larger than the incidence angle at the exit interface θ_2. A beam propagating solely in the air would have its waist located closer to the exit interface.

To compute the waist shift according to the expressions of [91], it is necessary to know the refractive index of the crystal. The crystal refractive index is estimated using the Sellmeier equation for lithium niobate. Jundt proposed the following expression for the equation for lithium niobate

$$n_e^2 = a_1 + b_1 f + \frac{a_2 + b_2 f}{\lambda_0^2 - (a_3 + b_3 f)^2} + \frac{a_4 + b_4 f}{\lambda_0^2 - a_5^2} - a_6 \lambda_0^2. \tag{5.31}$$

The different coefficients a_i and b_i were computed by Gayer et al. [93]. They are given in Figure 5.35

The wavelength is expressed in microns. The parameter f is the square of the temperature in degrees Kelvin with an offset to make it vanish at the reference temperature of 25.5°. Its expression is

$$f = (T - 24.5)(T + 570.82), \tag{5.32}$$

where the temperature T is in °C [92]. Equation 5.31 with the coefficients computed by Gayer et al. is used by the supplier Covesion to compute the refractive index of their crystals [94].

Parameters	5% MgO-doped CLN		1% MgO-doped SLN
	n_e	n_o	n_e
a_1	5.756	5.653	5.078
a_2	0.0983	0.1185	0.0964
a_3	0.2020	0.2091	0.2065
a_4	189.32	89.61	61.16
a_5	12.52	10.85	10.55
a_6	1.32×10^{-2}	1.97×10^{-2}	1.59×10^{-2}
b_1	2.860×10^{-6}	7.941×10^{-7}	4.677×10^{-6}
b_2	4.700×10^{-8}	3.134×10^{-8}	7.822×10^{-8}
b_3	6.113×10^{-8}	-4.641×10^{-9}	-2.653×10^{-8}
b_4	1.516×10^{-4}	-2.188×10^{-6}	1.096×10^{-4}

Figure 5.35: Coefficients intervening in the Sellmeier equation for lithium niobate. Figure from Gayer et al. [95].

The crystals manufactured by Covesion are doped at 5% with MgO.

5.10 Optical design

All the different aspects that were explained before need to be taken into account in the optical design. The dimensions of the crystals are also crucial to optimise the setup. The crystal for SHG is 3 mm long, 10 mm wide and 1 mm thick. The crystal for SPDC is 10 mm long, 10 mm wide and 1 mm thick. The channels inside the crystal have a square section of 1 mm side. As a reminder, the minimum waist sizes in the first crystal are 50 µm or 80 µm for a peak power of 4 kW or 10 kW respectively. For the SPDC crystal, the minimum waists are 200 µm or 325 µm.

In an attempt to maximise efficiency, Boyd and Kleinman investigated SHG with focused Gaussian beams [96]. They derived that the best spot to focus the laser beam is at the centre of the crystal. As a consequence, ensuring that the waist of the Gaussian beam is positioned at the centre of the crystal maximises efficiency. By positioning the different lenses adequately, this condition is easily met. They also derived a set of two conditions that maximise the efficiency of the process:

$$\frac{L}{2z_r} = 2.84 \quad \text{and} \quad \Delta k\, L = 3.2. \tag{5.33}$$

It might be surprising that the second expression imposes a phase difference greater than 0 as it goes against the QPM condition. This is due to the nature of Gaussian beams which imposes to consider the phase difference different than 0 as it is not homogeneous according to Smirr. This phase difference depends thus directly on the period of the inversion of the susceptibility of the material and so the size of the domains [97], which depends on the temperature of the crystal. The value $2z_r$ is called the confocal parameter and the ratio of the length of the crystal over the confocal parameter is the focusing parameter.

Smirr performed a similar experiment to the one developed in this work with a PPLN crystal and a pump laser of 5 W at 1564 nm. They studied the impact of the different parameters and particularly the temperature of their crystal and the waist of the focused spot on the efficiency of the process. Their results are displayed in Fig. 5.36.

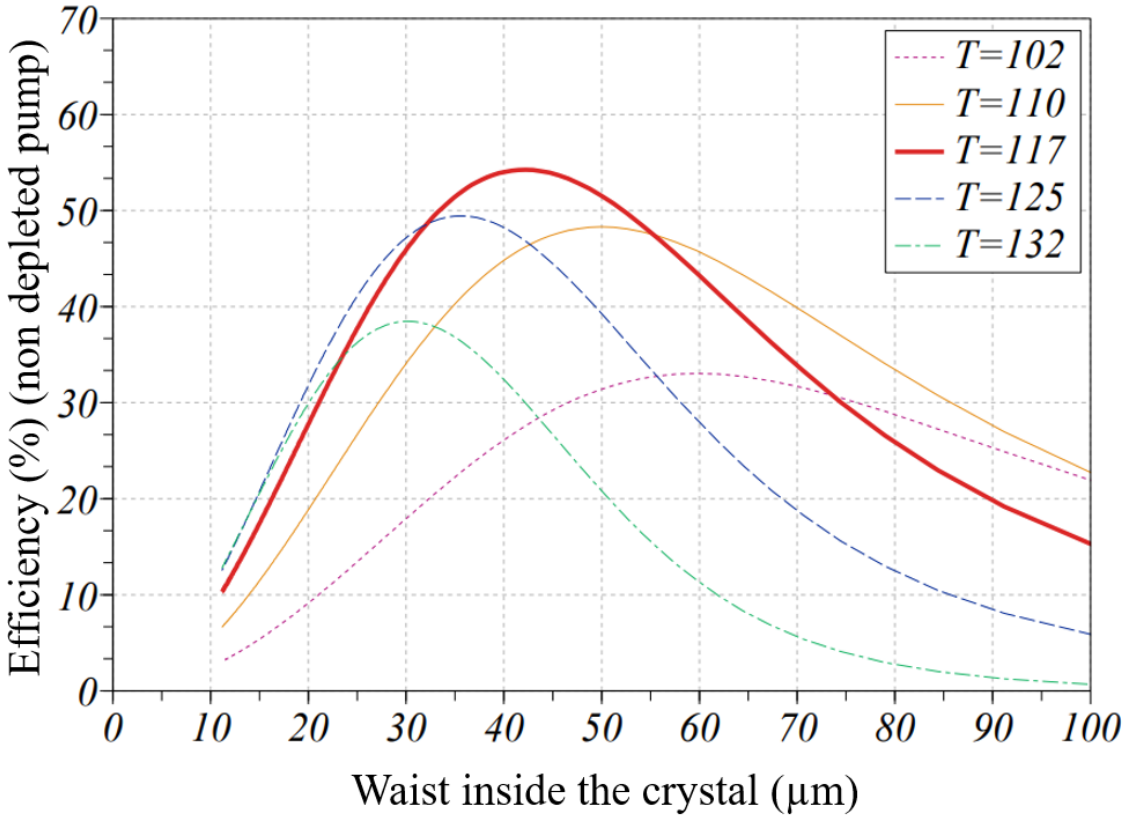

Figure 5.36: Efficiency of the SHG process measured from different conditions of phase difference and focusing parameter. The phase difference is equivalent to the temperature when the crystal properties are known and the focusing parameter can be expressed as the waist of the beam in the crystal. The crystal was 2 cm long for this experiment. Figure adapted from Smirr [97].

The maximum efficiency is achieved when Equation 5.33 is respected which corresponds to a waist of 42 µm and a temperature of 117°C. The temperature for which the phase difference is equal to 0 is 102°. One can see that this temperature is not optimal for the process. Although the dimensions do not agree, the behaviour of the experiment performed in this work should be similar to the one observed in Smirr's experiment and their figure is useful to qualitatively understand the process.

In the experiment developed for this work, by imposing the optimal ratio of the length of the crystal over the confocal parameter, the optimal size of the waist is 13 µm for SHG. This smaller value is consistent with the fact that the crystals supplied by Covesion are much smaller. Thus, the optimal Rayleigh range is smaller and so is the waist. However, this value is much smaller than the minimum waist allowed in the crystal not to damage it. therefore, it is impossible to reach the optimal conditions in the crystal. With a larger waist than the optimal one, the setup developed in the present work's experiment lies on the right side of the optimum in Fig. 5.36 and thus, the efficiency will only increase as the beam is focused more tightly.

For SPDC, Covesion mentioned that a good rule of thumb is to focus the beam such that the Rayleigh range is equal to half the length of the crystal. Similarly, this condition leads to a waist of 30 µm which is smaller than what the crystal can handle. As a consequence, the aim is to focus the laser beam at the centre of the crystal and to have the waist slightly larger than the smallest spot the crystal can withstand.

One last important remark is that in order to generate non-linear effects, the light wave entering the crystal should have an extraordinary polarisation. Concretely, this corresponds to a polarisation parallel to the thickness of the crystal. This remark is valid for both crystals.

With all the different aspects explained to this point, it is now possible to carry on the optical design. The optical setup of the experiment is depicted in Fig. 5.37.

The laser light at 1064 nm comes out of the fibre through the collimator at its end. This laser beam is directed thanks to mirrors to the SHG module. The mirrors can be turned and adjusted to fine-tune the position of the laser beam. This allows to accurately direct the beam in the right channel of the crystal. To ensure that light entering the crystal has an extraordinary polarisation, a rotating polariser is used in conjunction with a rotating HWP. The polariser can be set to be aligned with the extraordinary polarisation and guarantee that all light penetrating inside the crystal is polarised adequately for doubling. The HWP can be rotated such that light has the correct polarisation upon reaching the polariser. If the polarisation of the light matches the polarisation of the polariser, the maximum amount of light is transmitted. Thus, once the polariser is set in the right position, the HWP can be rotated until the maximum light power is measured.

A set of two plano-convex lenses surround the SHG crystal to focus the laser beam and collimate it afterwards. In Fig. 5.37, a lens at a certain wavelength means that the anti-reflective coating is adapted to avoid reflections at the specified wavelength. Collimating the beam after the focusing is more appropriate to use two movable dichroic mirrors to reflect only the useful part of the incident radiations. Light at 532 nm is reflected by the mirrors while the remaining 1064 nm wave is transmitted. The DMs separate the two components of the beam.

The 532 nm light is then conveyed to the second set of lenses and the crystal. Similarly, two plano-convex lenses are positioned around the crystal to focus the 532 nm light in the crystal and the output is then collimated again for simplicity. Right after the crystal and the collimating lens, three electromagnetic waves are superimposed and it is necessary to separate them to measure the output of the SPDC. A first dichroic mirror reflecting the light

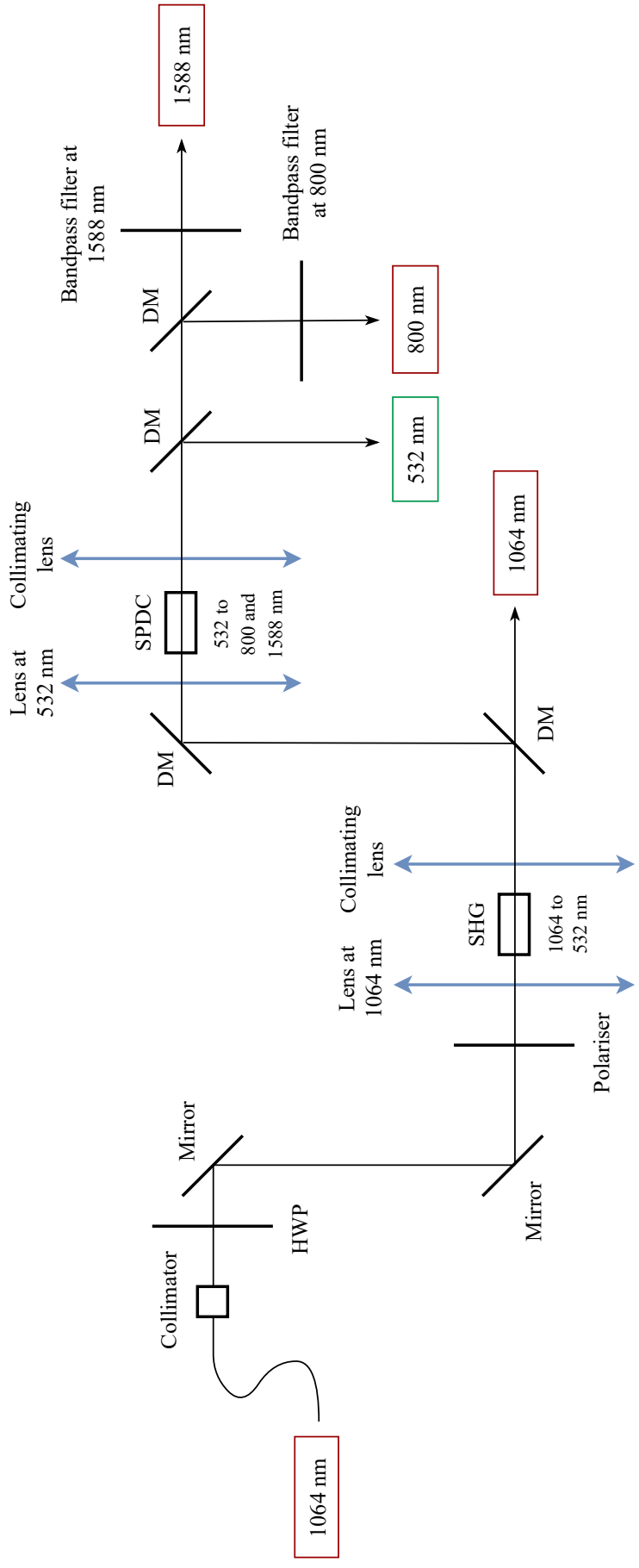

Figure 5.37: Conceptual optical design. The purpose of the setup is to focus the laser beam in the crystals at their centre. To guarantee the appropriate polarisation, a half-wave plate is used with a polariser. After each focusing, the output beams are collimated with converging lenses. The dichroic mirrors filter the output signal after the crystals. HWP: Half-wave plate. DM: Dichroic mirror

at 532 nm separates the signal and idler waves from the pump wave at 532 nm. Afterwards, another dichroic mirror manufactured to reflect the wave at 800 nm and transmit the wave at 1588 nm separates the two components. Finally, on both sides, a bandpass filter at the right wavelength is placed to minimise the amount of stray light.

5.11 Lens selection

Lenses are required to conduct the experiment. A lens is characterised by multiple quantities. The most important is its focal length. In the experiment, lenses are used for two purposes. Some focus the laser beam inside a crystal, while others are used to collimate the beam coming out of a crystal. These two types of lenses are called focusing and collimating lenses in the next part of the discussion.

In Fig. 5.37, both lenses right before the crystals are focusing lenses and the lenses after the SHG and SPDC crystals are collimating lenses. The sole difference between both types of lenses is their position inside the laser beam. The focusing lenses determine the size of the waist inside the crystals according to Eq. 5.24. The equation is valid for collimated beams and depends on the focal length of the focusing lens and the radius of the incident collimated beam. Although perfectly collimated Gaussian beams do not exist, they can be considered collimated when the focusing lenses respect several conditions. They are positioned close to the waist and much less than one Rayleigh range away. To match the conditions, the propagation distance must remain small compared to the z_r. This approximation is useful for its simplicity. Consequently, the aim was to maintain the approximation of collimated beams valid in the current system by ensuring the propagation distances of collimated beams are much smaller than the Rayleigh range of the laser beams.

For a target w_0', the focal length of the focusing lens imposes the value of the radius of the beam reaching the focusing lens w_0. The size of the collimated beam depends on the focal length of the previous collimating lens. A collimating lens must be positioned such that its focal length coincides with the previous beam waist. Afterwards, the image waist lies at the image focal length of the lens. Figure 5.38 represents the collimation process.

For both crystals, the laser light is collimated before reaching the focusing lenses. Therefore, the beam radius that reaches the focusing lens is the radius of the incident collimated beam. To obtain a collimated beam, Fig. 5.38 illustrates that the radius of the collimated beam is constrained by the focal length of the collimating lens. Indeed, since the beam that must be collimated travels a distance f from its waist, its radius increases according to Eq. 5.22. The focal lengths of the collimating lenses have to be chosen such that the dimensions of the collimated beam are suitable afterwards.

In the current system, the beam reaching the focusing lens of the SHG crystal is already collimated by the collimator. However, for SPDC, the collimation is performed by the collimating lens after the SHG crystal. As a consequence, when the focal length of the focusing lens before the SPDC crystal is fixed, the radius of the incident collimated beam is determined. In turn, the radius of the collimated beam imposes the focal length of the collimating lens. The considerations that led to this architecture are detailed hereafter. This discussion

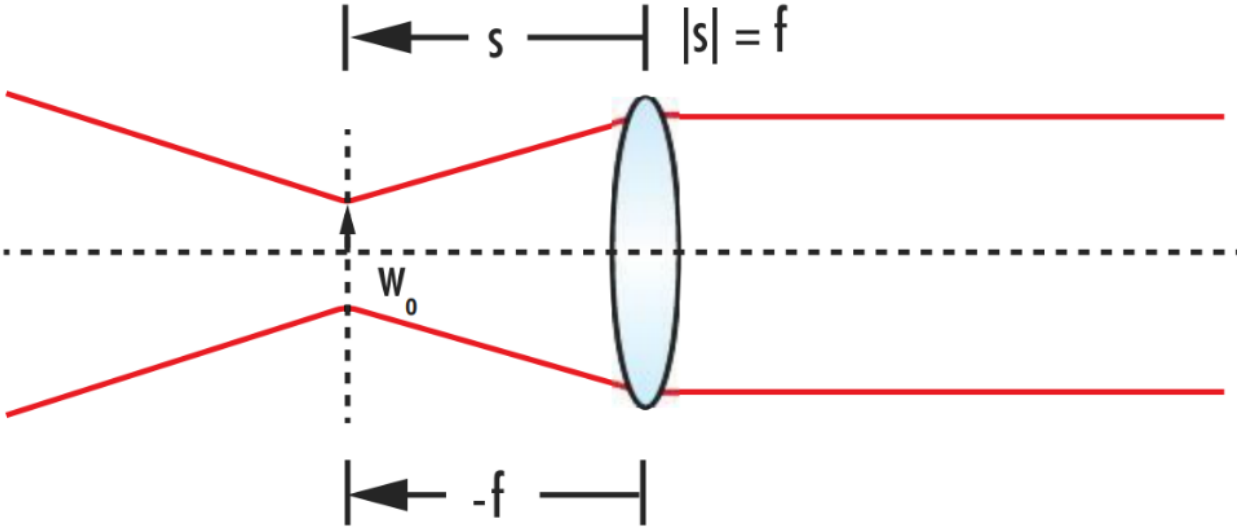

Figure 5.38: Disposition of a lens to collimate a beam. s is the distance from the lens to the waist of the beam. Figure from Edmund Optics [98]

highlights the many dependencies in the system and the influence all the parameters have on each other. With the dependencies clarified, the focal lengths of the different lenses can be selected.

To select the focal lengths of the lenses, the first line of thought consists in using Eq. 5.24 by considering the optimal setup. The objective is to reach the critical spot size inside the crystal. As such, w_0' is imposed equal to the smallest spot size the material can withstand. As a reminder, for the SHG crystal, the smallest spot sizes are 50 and 80 µm for a mean power of 1 and 2.5 W. For SPDC, the minimum spot sizes are 200 µm and 325 µm. By imposing the size of the focused beam in the crystal, it is possible to study the influence of the focal length on the beam waist at both focusing lenses w_0.

To understand the impact of the different parameters on the design, it is possible to plot the focusing ratio in function of the relative scale of the system. The focusing ratio is defined as the ratio of the target beam waist inside the crystal over the beam radius on the focusing lens, which is collimated. The focusing ratio measures the increase in power density between the collimated beam and the spot in the crystal. The relative scale of the system is defined as the focal length of the focusing lens over the length of the non-linear crystal. It is an indicator of the compactness of the system.

In the following discussion, each conversion step is composed of a collimating lens that fixes the size of the incident beam of the focusing lens, the focusing lens which injects the laser into the crystal and the crystal. The combination of focusing lens and crystal is referred to as a module in the following discussion. Moreover, the first focusing lens is studied as if the beam is collimated by a collimating lens instead of the collimator to ensure that the size of the beam out of the collimator is suitable. For a given focal length in each system, the required waist to achieve the critical spot size in the crystal is computed thanks to Eq. 5.24.

Figure 5.39 presents the computations.

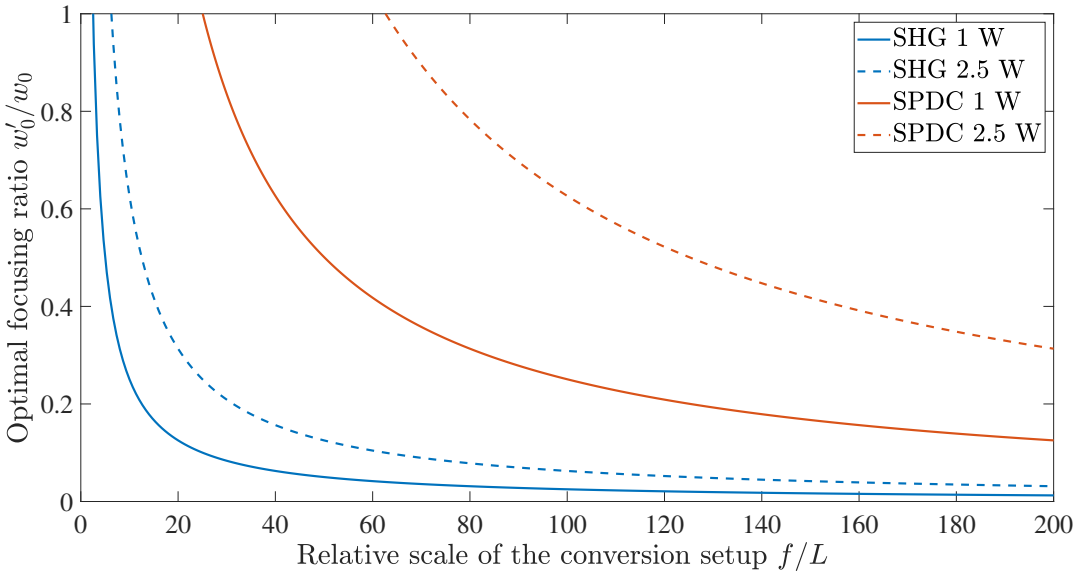

Figure 5.39: Optimal focusing ratio of the lens with respect to the scale of the conversion crystal expressed as the ratio of the focal length on the length of the crystal. The focusing ratio is the ratio of the targeted waist size in the crystal imposed by the material on the size of the beam at the focusing lens. The focusing ratio is optimal because the waist size in the crystal is the critical limit of the material.

The lens selection is a trade-off between different aspects. The differences in the focal length selection for SHG and SPDC in the experiment appear in Fig.5.39. The figure expresses the dependence of the focusing ratio on the size of the system. Physically, a small focusing ratio indicates that the beam reaching the lens is much larger than the spot in the crystal. A large relative scale indicates that the size of the system is large.

There are two manners to observe the figure. One can either look at the variation of the focusing ratio with the relative scale or look at the variation of the scale with the focusing ratio. It is equivalent to either imposing the focal length and computing the required radius w_0 or imposing the size of the beam and computing the focal length such that the appropriate spot size in the crystal is achieved.

In Fig. 5.39, a larger mean power increases the focusing ratio for the same relative scale. Physically, for the same focal length, the size of the optimal spot in the crystal increases and the radius of the collimated beam decreases. As a consequence, the focusing ratio is larger. In the figure, this translates into an increase of a factor of 2.5 between the curves of a specific module for a fixed scale.

The curves are higher for SPDC than for SHG. For the same system scale, the focusing ratio for SPDC is larger which indicates that the optimal collimated beam waist w_0 is closer to the focused spot size w_0'. The first explanation is that the critical spot size is larger. Moreover, the wavelength of SPDC is half the wavelength of SHG. Equation 5.24 predicts that for a larger spot size w_0' and a smaller wavelength, the ratio f/w_0 has to increase either

by increasing f or reducing w_0. In the end, the SPDC module is less compact than the SHG module since the scale of the system is larger for the same focusing ratio.

For both modules, increasing the scale of the system, i.e. the focal length, diminishes the optimal focusing ratio. When the focal length becomes large compared to the system, the optimal size of the collimated beam must be larger resulting in the low focusing ratio. The other way around, the focal length of the focusing lens must be large when the size of the collimated beam is large. Equation 5.24 predicted this behaviour since the spot size is determined by the ratio of f and w_0. For a constant spot size w_0', if the focal length f becomes large, the waist of the incident collimated beam w_0 has to be large and vice versa.

On the contrary, when the scale of the system becomes small, the focusing ratio becomes larger. Equivalently, when the focal length decreases, the radius of the collimated beam reaching the focusing lens must be smaller and eventually closer to the desired spot size. The other way around, when the radius of the collimated beam becomes closer to the spot size in the crystal, the system becomes more compact as a smaller focal length is necessary to maintain the spot size in the crystal constant.

Although reducing the system scale can be advantageous depending on the application, there is a downside. By making the hypothesis the waist of the collimated Gaussian beam is equal to its size w_0, the Rayleigh range of the collimated beam can be computed. To study the dependence of the Rayleigh length on the system parameters, the collimation ratio is defined as the ratio of the Rayleigh range of the incident collimated beam over the length of the crystal. It is an indicator of the validity of the collimation hypothesis. Figure 5.40 represents the collimation ratio as a function of the relative scale of the system.

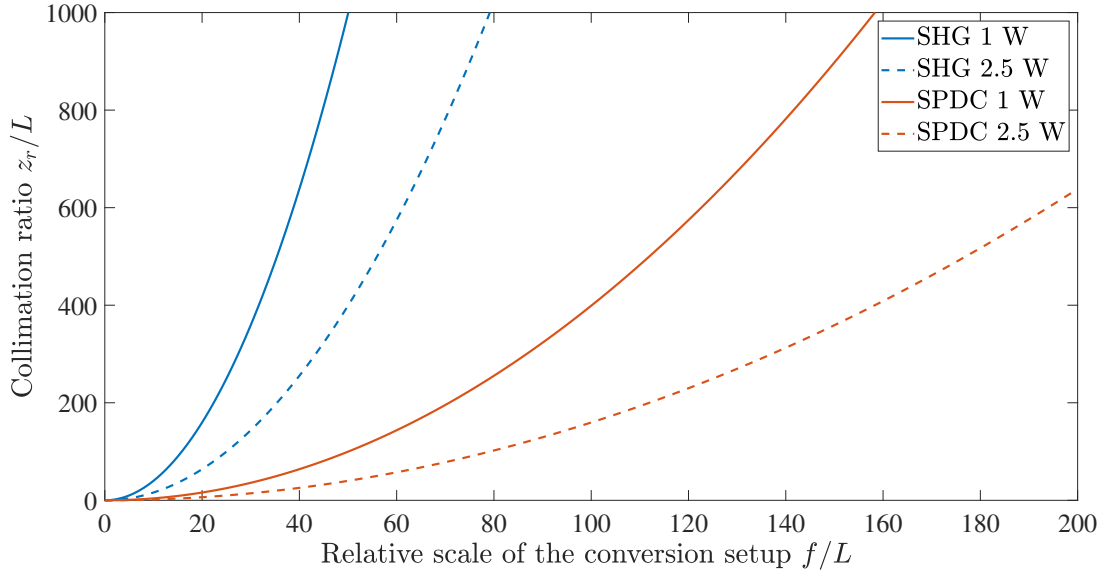

Figure 5.40: Rayleigh range of the collimated beam of adequate size as a function of the scale of the conversion module expressed as the ratio of the focal length on the length of the crystal. The waist used to compute the Rayleigh range is the optimal waist such that the focused spot size is exactly equal to the limit of the material.

For the same system scale, the collimation ratio is larger for a mean power of 1 W than

for a mean power of 2.5 W. The spot size in the crystal is larger when the power is higher. Thus, for the same system scale, the radius of the incident beam w_0 must be smaller, and so is the Rayleigh range.

Another observation is that for the same relative scale, the Rayleigh range for both powers is much larger for the SHG module than for the SPDC module. Since the targeted spot size is much smaller for SHG than for SPDC, for the same scale, the required collimated beam size is larger and its Rayleigh range is larger too.

Finally, as the focal length gets smaller, the Rayleigh range of the beam entering the lens diminishes. This is consistent with the observation that when the scale decreases, the focusing ratio increases and the waist is smaller, closer to the optimal waist in the crystal w_0'.

A small Rayleigh range compared to the system size is detrimental because the hypothesis of collimated beams becomes less reasonable. When the beam reaches a focusing lens, it can be considered collimated if its Rayleigh range is much longer than the propagation distance. Thus, a small Rayleigh range compared to the system heavily constrains the propagation distance for the hypothesis to hold. For this reason, the scale of the system cannot be reduced arbitrarily. The minimal scale the system can reach depends on the application. On the other side, a large Rayleigh range makes the hypothesis of a collimated beam valid, and the hypothesis holds for a much longer propagation distance.

A last remark can be made when the scale of the system is heavily diminished. When the focusing ratio becomes close to 1, the necessity to put a lens in the system is questionable. A ratio close to 1 indicates that the collimated beam reaching the converging lens has a size comparable to the spot in the crystal. Instead of focusing the beam in the crystal, injecting the collimated beam becomes an option. Depending on the application, this might be a suitable solution as it involves less optical components and thus this drastically reduces the scale of the system.

The relevant phenomenon have been illustrated in the previous discussions. In light of these discussions, the direction of the optical design can be chosen in the current application. As the experiment is performed in a lab, the scale of the system is limited by the optical bench size. The compactness of the system is thus an important constraint. There are two degrees of freedom when selecting the lenses to perform a conversion, the focal length and the size of the collimated beam.

5.11.1 System dimensions estimation for SHG

For the focusing inside the SHG crystal, the incident beam is collimated by the collimator at the end of the optical. The collimator is designed such that the beam escapes it with a diameter of 1.6 mm. This size is not a limit of the system since it can be increased voluntarily. In laser optics, it is possible to increase the size of the beam by using two lenses. The first lens has a small focal length to tightly focus the laser beam. Since the waist is small afterwards, the divergence angle is much larger and thus the second lens can be chosen and positioned to collimate the beam with the desired radius.

To determine if it is necessary, the focal length of the focusing lens can be computed by imposing that the radius of the collimated beam is equal to 0.8 mm. In these conditions, the optimal focal lengths are equal to 0.1192 and 0.1885 m for a mean power of 1 W and 2.5 W respectively. Both focal lengths agree with the dimensions of the system and increasing the beam waist would increase them. Moreover, for a collimated beam with a radius of 0.8 mm, the Rayleigh range is about 2 m long. 2 m is much longer than the distance required to make the beam pass through the HWP and the polariser. Moreover, increasing the size of the beam on the lens would increase the focal length. For both reasons, it was estimated that increasing the size of the beam entering the lens in front of the SHG crystal did not present any noticeable advantage. The size of the beam is thus kept as such.

5.11.2 System dimensions estimation for SPDC

For the SPDC module, the situation is not as simple. Because of the more constraining material limitations, the minimal focal length of the focusing lens is much larger than for SHG. Figure 5.41 illustrates the range of focal lengths suitable for the applications.

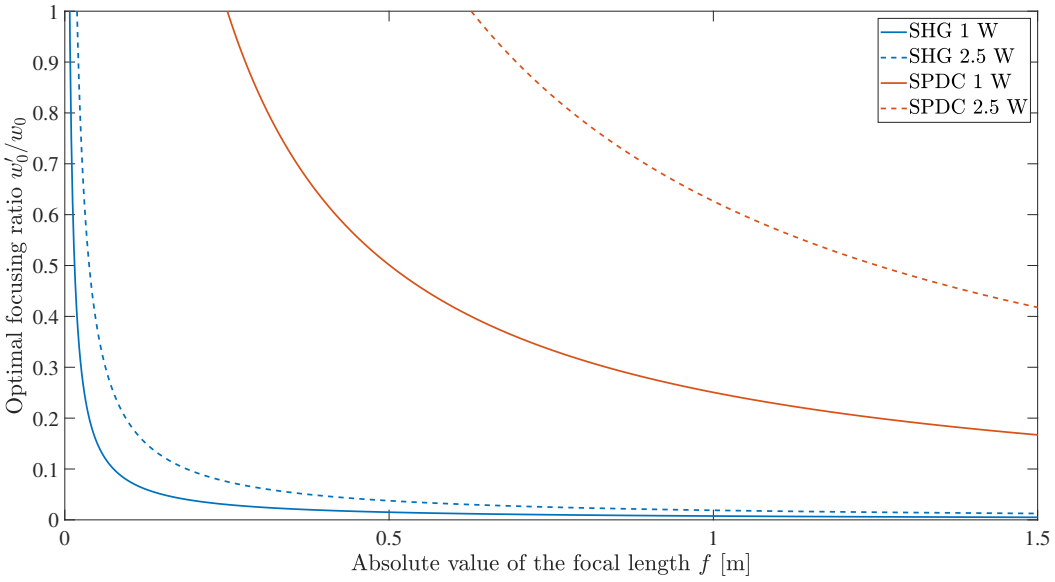

Figure 5.41: Optimal focusing ratio as a function of the focal length of the collimating lens. The minimal focal length which corresponds to a focusing ratio of 1 is much larger for SPDC than for SHG.

The minimum focal length corresponds to a focusing ratio of 1 which is a critical and non desirable because in this case, using a lens becomes pointless. The range of possible focal lengths spans above the minimal value. As the limit is already large compared to the system dimensions, it might be helpful to reduce the system size.

One intuitive possibility is to use a doublet of lenses. A doublet consists of a converging lens followed by a diverging one. Geometrical optics predicts that the combined action of the lenses could achieve the appropriate waist after a much shorter propagation distance.

However, Nemoto [99] suggests that the size of the waist of a converging beam is not modified by an intermediary dielectric plate. Nemoto also studied the effect a converging lens has on an already converging beam. They found that the waist size is not affected by the lens, only its position. Although they studied the case of a converging lens, their results suggest that the waist size is determined by the focusing lens and decreasing the focal length below the minimum is not possible.

The minimal size is the next possibility to minimise the focal length. It corresponds to a focusing ratio of 1, i.e. the collimated beam has the size of the spot in the crystal. In this case, using a lens hardly makes sense. It is interesting to study the case when no lens is used to focus the laser beam inside the crystal and instead, the collimated beam is directly injected into the crystal. There are two limitations to this case.

For a collimated beam whose size is equal to the minimal spot size in the crystal, the Rayleigh range is equal to 25.06 cm or 62.66 cm for a mean power of 1 and 2.5 W. For the hypothesis of a collimated beam to be reasonable, the Rayleigh range of the collimated beam should remain much larger than the propagation distance in the system. It is important to mention that the focusing lens can be located close to the collimating lens, and a short propagation length is not a problem. A small Rayleigh range is especially detrimental when the collimated beam needs to pass through several optical components before the converging lens. In the setup, the collimated beam reaching the focusing lens in front of the SPDC crystal is reflected by the two dichroic mirrors. A Rayleigh range of 25 cm is too small to consider the beam collimated after both mirrors. A Rayleigh range of 63 cm is also restrictive. Such a distance restricts the flexibility of the system as adding optical components increases the propagation distance by a significant margin for the Rayleigh range. Since this source is experimental, maintaining flexibility is valuable to perform other experiments or tests.

The second reason collimating the beam at the right size and injecting it into the crystal is not beneficial is due to the profile of the beam in the crystal. Theoretically, the beam waist of a collimated beam after a collimating lens is located at its image focal plane. The focal length of the collimating lens can be computed from the size of the waist in the SHG crystal thanks to Eq. 5.22. One needs to find the distance z such that the size of the beam is equal to the desired collimated beam size. The distance z is directly equal to the focal length. The expression of z is

$$f = z = z_r \sqrt{\left(\frac{w^2}{w_0^2} - 1\right)}. \tag{5.34}$$

w corresponds to the desired beam radius and w_0 is the waist of the beam. To get a beam whose size is equal to the minimal spot size in the crystal, the focal length of the collimating lens should be about 10 cm long for a power of 2.5 W and 4 cm long for a power of 1 W. Due to the necessity to make the beam pass through dichroic mirrors, it would be extremely difficult to ensure the waist of the beam lies at the centre of the crystal. If the beam waist is not located at the centre of the crystal, the process is less efficient. It is thus not profitable to solely collimate the beam in the crystal in this experiment. Despite the constraint, it is better to use a long converging lens.

5.11.3 Lens dimensions selection

With all the different dependencies of the parameters highlighted, it is possible to choose the lenses used in the experiment. The previous discussion revolves around the possibility of using the exact focal lengths and beam waists to get a spot size equal to the minimum the material can withstand. In practice, however, lenses with arbitrary focal lengths are not available. Thus, it is impossible to get exactly the predicted performances. Instead, it is necessary to find a combination of existing lenses whose performances are close to the optimum and available from a supplier. The domain of acceptable combinations of lenses lies above the curves in Fig. 5.41. A point above the curve corresponds to a combination of focusing focal length and incident collimated beam waist that yields a larger spot than the critical one. Indeed, if the focal length is fixed, a point above the curve corresponds to a beam waist that is inferior to the optimal waist w_0 that gives the critical spot size w_0'. For the same focal length and a smaller beam waist, Eq.5.24 predicts that the spot size becomes larger and thus less dangerous for the crystal. When selecting lenses, their combination should define a point on the figure above the optimal curve of the power considered. The actual lens selection procedure is explained in the next paragraphs.

For the SHG, the previous discussions have concluded that the design was much less constraining than for SPDC. By using the collimated beam that comes out of the collimator, the focal length remains within acceptable bounds. Depending on the mean power of the laser, the focal length should be 0.1192 or 0.1885 m with a smaller focal length resulting in a smaller spot. Fortunately, lenses of 0.2 m focal length are available in the market if the target is to focus the laser beam when the mean power is equal to 2.5 W. If the aim is to focus the laser beam more tightly to get closer to the limit at 1 W, lenses with focal distances of 0.15 m are a suitable option. The choice of the focusing lens for the SHG can be done before the choice of lenses for SPDC.

With the first focal length selected, the characteristics of the focused Gaussian beam can be computed according to Equation 5.24. After the frequency doubling, the converted beam at 532 nm is considered instead of the 1064 nm beam. The wavelength of the generated wave is equal to half the wavelength of the incident laser beam. According to Boyd; Prato, the Rayleigh range is conserved through the process. For the Rayleigh range to remain constant with a smaller wavelength, the waist of the doubled beam must be equal to the waist of the incident beam over $\sqrt{2}$ [76]. The waist of the generated wave is relevant to determine where to put the collimating lens to obtain the appropriate size of collimated beam for SPDC afterwards.

Choosing both focal lengths for SPDC is less straightforward than for SHG. For SPDC, the focal lengths of the collimating lens after the SHG crystal and the focusing lens in front of the SPDC crystal need to be selected. Both focal lengths are determined by the size of the collimated beam reaching the focusing lens. The aim is that the focused spot size in the crystal is close to the smallest spot size possible.

Naturally, the first focal length that is chosen is the focusing lens one. Choosing it from the get-go is difficult. As long as the dimensions agree with the optical bench, many focal lengths are suitable as long as the collimating lens focal length is adapted to yield the adequate size

of the collimated beam. Another possibility is to choose the beam waist at first and adapt it such that the focal lengths of the system do not get too long.

The advantage is that a first value of collimated beam size is imposed by the collimator. A first estimation is to impose the size of the beam entering the focusing lens equal to the size of the beam before the focusing lens of the SHG crystal. For a radius of 0.8 mm for the 532 nm beam entering the focusing lens, the focal length should be about 1.2 or 1.5 m long for a mean power of 1 W or 2.5 W. This is too long for the optical bench. Thus, the size of the collimated beam must be reduced to diminish the size of the system.

As explained earlier, however, the size of the collimated beam cannot be reduced below the size of the spot in the SPDC crystal. From that point on, the objective is to find the size of the collimated beam such that the focal length of the focusing lens is suitable. Therefore, the aim is to find a good compromise between the size of the system, focusing ratio and Rayleigh range and avoid being too close to the minimum focal length.

The complete selection process is to impose a size of the collimated beam, compute the exact focal length required to meet the exact spot size and then select an available lens with a focal length that is close to the required one. Since it is impossible to find a lens with the optimal focal length, it is better to select a lens whose focal length is larger because the real spot size is thus larger than the limit of the crystal. Once the focal length of the focusing lens is selected, the focal length of the collimating lens is computed thanks to the propagation equation of the Gaussian beam at 532 nm resulting from the SHG. Similarly, as lenses with the exact focal length are not available, one needs to use the closest available one. Contrary to the focusing lens, the collimating lens should be selected such that its real focal length is smaller than the required one as it results in a smaller beam size and thus a larger spot size.

If both lenses are chosen as explained, there is no risk of focusing too tight. It is conceivable not to follow these precautions if the increase of focal length compensates for the increase in beam waist and vice versa. Once both focal lengths are chosen, the actual waist in the crystal can be computed. The real waist in the crystal must be larger than the critical one.

In the end, the following combinations of lenses were deemed suitable for the application. It is worth mentioning that combinations for both a mean power of 1 W and 2.5 W were computed. The resulting iterations for the design are expressed in Table 5.1.

f_1 [m]	SHG spot size [µm]	f_2 [m]	f_3 [m]	SPDC spot size [µm]	Focusing ratio [%]
0.2	84.67	0.175	1	339.64	68.12
0.2	84.67	0.125	0.75	354.18	98.77
0.15	63.5	0.15	0.75	223.81	39.44
0.15	63.5	0.175	1	256	38.7

Table 5.1: Iterations of the design. f_1 is the focal length of the focusing lens before the SHG crystal. f_2 is the focal length of the collimating lens before the focusing lens in front of the SPDC crystal. f_3 is the focal length of the focusing lens before the SPDC crystal. The spot sizes are the actual radius of the waist of the beam after passing through the real lenses.

Several lenses were ordered to use different combinations to maintain the freedom of adapting the system. This allows the installation of several setups with different priorities in mind. A more conservative setup adapted for a mean power of 2.5 W can be used while only injecting 1 W inside the system to remain cautious with the crystals. It is worth noticing in Table 5.1 that the size of the system is larger for a power of 2.5 W than for 1 W.

Increasing the power injected in the crystals is interesting to increase the number of photons that are generated. For the same crystal, a larger power makes the minimum spot size larger. This results in an increase of the ratio f_3/w_0. In the current design, a focal length of 1 m for f_3 is already close to the limits the optical bench permit. For this reason, it is not profitable to increase the power of the laser for the experiment since increasing f_3. In a real application, increasing the number of photons that the source generates might be profitable to increase information transfer. However, this needs to be put in perspective depending on the QKD protocol as some rely on single-photon pulses.

Plano-convex lenses were ordered to conduct the conversions. Plano-convex lenses are suitable to focus Gaussian beams and collimate them. To avoid aberrations as much as possible, the lenses are set such that their plane face is pointed towards the crystal. This helps reduce spherical aberrations.

The ordered lenses share a diameter of 2.54 cm. The smallest focal length is 15 cm. This leads to an F# of 5.91. A larger F# is beneficial to reduce spherical aberrations. Spherical aberrations are proportional to the angle of incidence between a light ray and the surface of the spherical side of the lens. A large F# guarantees that the angle of incidence between the beam and the lens is smaller at the edge of the beam. 5.91 is already considered to be a large F#, and since it is obtained for the lens with the smallest focal length, other lenses possess a larger F# and spherical aberrations are even less of a concern.

5.12 Experimental layout

The different blocks of the experimental setup are depicted in the following pictures.

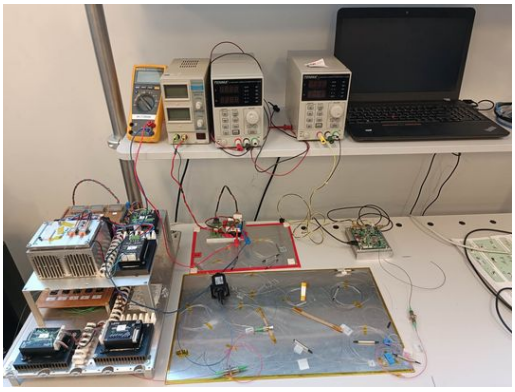

Figure 5.42: Picture of the preamplifier.

Figure 5.43: Picture of the high-power pump diodes station.

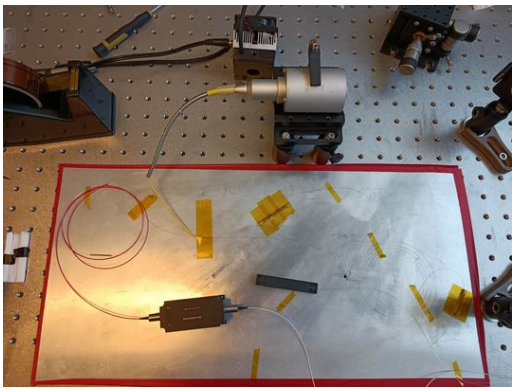

Figure 5.44: Picture of the high-power amplifier.

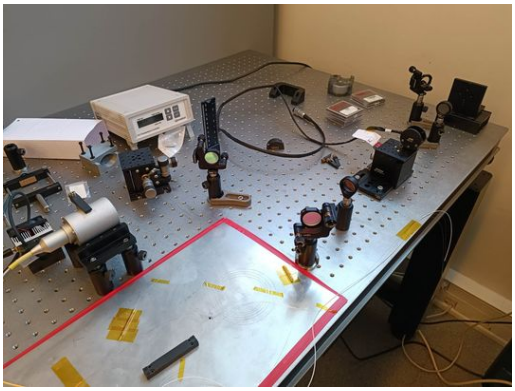

Figure 5.45: Picture of the SHG layout.

The SHG module is depicted in Fig. 5.45. The two mirrors following the collimator lead to the focusing lens. The collimating lens is positioned after the crystal afterwards. Due to delivery delays, the HWP and polariser are not installed yet.

The alignment of the optical elements was performed at low power. The next step is to align the lenses and focus the laser beam inside the crystal. To generate non-linear effects, the power of the laser has to be increased above the alignment powers. Focused laser beams have to be manipulated with caution because the power density they reach is dangerous. Moreover, since the human eye is not sensitive to the wavelength of 1064 nm, the laser is especially dreadful. For safety reasons, it was decided not to pursue the experiment because the setup did not meet safety requirements. Before attempting to conduct conversions, the

next step will be to secure the experimental setup. Afterwards, the efficiency of the SHG can be characterised. Finally, the SPDC module can be installed, aligned and characterised.

5.13 Transposability of the source to space

As this work focuses on FSO QKD, the transposability of the system to space is an important question. The source presented in this section was built and developed in a laboratory. Compared to space, a laboratory is much more convenient. Space is a demanding radiative medium. Many energetic particles or electromagnetic radiations can degrade the components.

Semiconductor laser diodes are being developed for quantum technologies in space applications [100]. Consequently, the laser diodes are not a critical part of the system. On the other hand, optical fibres are subjected to developing colour centres when exposed to radiation. These colour centres lead to signal deterioration. Their apparition is conditioned by several parameters like the temperature, dose rate and doping material among others [101]. To minimise these detrimental effects, it is necessary to create specific fibres of pure silica or design radiation shields for the components that rely on optical fibres [102].

The necessity to regulate the crystals in temperature introduces challenges for a space application. To maintain a crystal at a specific temperature, the heat loss of the component has to be compensated exactly. This heat loss needs to be controlled and understood to avoid detrimental effects on the optical components of a space system.

The first step towards controlling this heat loss is to estimate its magnitude. To do so, it is necessary to understand the different heat fluxes in the system. In space, the two remaining heat transfer mechanisms are conduction and radiation since convection is impossible without air.

In the current source, the crystals are heated thanks to ovens. Inside the ovens, the crystals are positioned on a plate. They are in physical contact with nothing else in the system. As a consequence, the sole heat transfer by conduction is from the crystal to the heater. Moreover, for the plate to transmit heat to the crystal, the temperature of the plate must be larger than the temperature of the crystal. As a result, the hypothesis that the crystal does not lose heat through conduction is appropriate.

Before trying to compute the total heat loss, it is necessary to determine the different sources of heat loss of the components of the system. From the perspective of the crystals, heat is provided by the plate they are positioned on and heat is lost through radiation. As the temperature of the crystals is beyond absolute zero, they naturally emit electromagnetic radiations. The amount of thermal energy any body heated at a temperature T emits is described by the Stefan-Boltzmann law

$$M = \sigma \epsilon T^4, \tag{5.35}$$

with M the power radiated per unit surface, σ the Stefan-Boltzmann constant and ϵ the emissivity of the body. Black bodies have an emissivity equal to 1. Rigorously, the crystals

also receive heat through radiations from their environment. Their environment is composed of the ovens and their environment. In space, the environment of the ovens is either the satellite or the cosmic background. However, it is very unlikely that the oven would be exposed to the cosmic background.

The crystals are integrally encased in the plastic envelope of the ovens except for the two holes that allow light to enter the crystal and escape it, as observed in Fig. 5.29. The temperature of the casings of the ovens and the temperature of the satellite depend on many aspects that include the orbit parameters and the layout of the instrument on board the satellite among others. Both quantities are difficult to estimate without proper parameters.

The second contributor to the total heat loss originates from the ovens. To maintain the temperature constant, the ovens provide the crystals with exactly the amount of heat they lose because of radiation. The ovens exhibit losses: their power consumption is larger than what the crystals need. These losses are part of the total heat loss of the system. Unfortunately, the exact power consumption of the ovens is unknown. Moreover, the ovens also lose heat by conduction with the platform they are positioned on and by radiation since their temperature is above the absolute zero.

The total heat loss is composed of the heat lost by the ovens and the heat lost by the crystals. The ovens lose heat by conduction and radiation and the crystals lose heat by radiation. The relevant heat loss of the crystal is the part of the radiation they emit that is not absorbed by the ovens. To accurately estimate the total heat loss, it is necessary to consider all the different heat fluxes between the elements and solve the heat transfer equations. To solve the equations, the detailed characteristics of the crystals and the ovens are required. However, the emissivities of the ovens, the crystals, as well as the temperature of the ovens casings are difficult to estimate without detailed computations and data. Since the aim of this discussion is to get an order of magnitude of the heat loss, a much simpler model can be used. The emissivity of a body at a specific wavelength follows the conservation of energy

$$\alpha_\lambda + \rho_\lambda + \tau_\lambda = \epsilon_\lambda + \rho_\lambda + \tau_\lambda = 1, \tag{5.36}$$

where ρ_λ is the reflectivity of the material, τ_λ is its transmissivity and α_λ its absorptivity. The three quantities are evaluated at the wavelength λ. According to Kirchoff's law of radiation, the emissivity is equal to the absorptivity. At the range of temperature the crystals are heated, the spectrum they emit lies in the mid to long-wavelength infrared range. The peak wavelength of the crystal at 120°C is 7.371 microns while the peak wavelength of the 33°C crystal is 9.465 microns according to Wien's law.

According to Covesion, the crystals are highly absorptive beyond 4000 nm [103]. Their emissivity is thus relatively close to 1 at their peak wavelength. A relevant estimation of the heat they lose is thus to compute the emission of a black body of the same total surface at the same temperature. The radiation heat losses are equal to 0.0428 and 0.3061 W for the crystal at 33°C and 120°C respectively. The magnitude of their losses is low. Moreover, as the crystals are encased in the ovens, most of their radiation is absorbed by the casings of the ovens which are connected to a platform.

The temperatures of the ovens is necessary to estimate the heat they dissipate by radiation but they are difficult to estimate. Qualitatively, the temperature of the ovens is slightly larger than the optical platform because of the electrical losses and the heat they absorb from the crystals. The total amount of heat lost by radiation by the crystals is small as computed in the previous paragraph. The electrical losses depend on the efficiency of the ovens. It is proportional to the amount of heat the crystals lose since the ovens provide the right amount of heat to maintain their temperatures. As a rough approximation, the total amount of heat lost by both systems is estimated to be twice the heat the crystals lose. This is an overestimation since the crystals dissipate less heat than computed and a part is absorbed by the ovens. The total heat loss is thus equal to 0.7 W in this approximation. Most spacecraft radiators reject between 100 and 350 W of internally generated heat [104] and 0.7 W represents a minor contribution.

Although the magnitude of heat dissipation is low, the part of the radiation of the crystals the ovens absorb and the excess losses intrinsic to the ovens' electrical power have to be evacuated such that the sensitive equipment of the satellite is not heated above its nominal temperature. The excessive heat the ovens absorb can be evacuated by conduction to the satellite platform. By ensuring that heat flows towards a heat dump, the equipment is safe.

Some considerations are important to point out. First, the model presented in the previous paragraph excludes the influence of the environment on the system by considering it to be a heat dump without considering its contribution in heating the system. The discussion is based on a very simple model that could be improved to obtain accurate values.

Moreover, in a real LEO, the temperature of the spacecraft depends heavily on the eclipse cycles and oscillates significantly. To ensure the good function of the optical platform, the influence of the temperature oscillations on the optical payload should either be controlled or the system should be optimised such that temperature oscillations do not influence the performance. In that regard, the crystals are sensitive equipment whose temperature should be maintained at any time to warrant good conversion efficiencies. The influence of the orbit was not taken into account in this discussion.

A final remark concerns the necessity to heat the crystals. In the state of the experiment presented in this work, the crystals have to be heated for the conditions of phase-matching to be met. Heating the crystals is necessary because the period of the domains is imposed by the manufacturer. Through thorough computations and design, it is possible to manufacture a crystal whose working temperature for the application is exactly the operating temperature of the optical payload. This would avoid the requirement to heat the crystals but the temperature of the crystal would still need to be controlled along with the temperature of the optical layout. This would reduce the heat transfers between the components.

6 Conclusions

This thesis is part of the scientific initiative aimed at developing free-space Quantum Key Distribution technologies. It offers an overview of the challenges towards global implementation to allow future works to dive into the details of some specific elements. It started by establishing the fundamental concepts to understand the principle of QKD.

Afterwards, the main types of practical implementations were presented and explained. A short description of the state of the art of optical fibre QKD illustrated the current technology limitations. The nature of optical fibres requires solutions to their intrinsic limitations, and free-space QKD appears as a convenient answer to the short propagation distance of optical fibres. However, fibres present noticeable advantages in cities where the propagation distance is small.

Many efforts are dedicated to research on the technology in the hope of dealing with the different obstacles towards global free-space QKD systems. The Earth's atmosphere induces constraints that do not affect optical fibres. This paper covered many challenges associated with each part of the propagation by following the photons from the source on board a satellite to the receiver on the ground. At the time of this thesis, the key rates are insufficient to provide secure communications at a large scale, especially during the day. Nevertheless, the efforts of the scientific community to increase the secret key rate lead to promising solutions. Their simulations and experiments suggest that the secret key rate is improvable significantly and that day operation is manageable. Micius proved that satellite QKD is an efficient technique with great potential. It also demonstrated that combining optical fibre networks for short distances on ground with satellites was a reliable manner to integrate free-space QKD with optical fibre networks.

Following the qualitative description of the hurdles towards global QKD systems, an experimental photon source was presented with the design steps that dictated its characteristics. The principles of non-linear optics were introduced to understand how to generate suitable photons for QKD. The elaboration of this photon source from simple laser diodes involved assembling amplifiers with optical fibres and micro-optical components. The laser diode power was increased to reach appropriate levels for a laboratory and keep flexibility in its magnitude thanks to a series of one four-pass amplifier, a double-pass amplifier and a high-power single-pass amplifier.

After the laser of suitable power was built, an optical design centred around the non-linear crystals was studied and proposed. The design process highlighted the dependence of the relative scale of the system on the laser beam parameters. The material limitations of the non-linear crystals constrain the size of the system. Moreover, this discussion illustrated that it is impossible to reduce arbitrarily the size of the system without deteriorating the collimation of the laser beam. Consequently, any transmitting system has to be designed according to the typical travelling distance of the different beams involved.

7 Perspectives

In light of the insights provided by the points made throughout this thesis, some perspectives emerge naturally. Some are concrete extensions of the work performed in the frame of this thesis, while others are general initiatives.

In complement to the qualitative explanation of the principle of QKD, a mathematical description could be useful to illustrate some of the behaviours. Similarly, a mathematical formalism could be interesting to derive to describe the propagation of electromagnetic waves through the optical fibres and the atmosphere. A rigorous model would be helpful to make simulations and describe quantitatively the detrimental effects on the signals. Moreover, as the experimental source relies on non-linear optics phenomena, a detailed description based on Maxwell's equations becomes indispensable to quantify the efficiency of the processes. A mathematical model would bring interesting insights to optimise the process. Therefore, an interesting perspective is to adopt a mathematical point of view on the different topics explored in the paper.

The solutions proposed to the problems yield promising results. Nevertheless, not all are mature enough to enable sufficient secret key rates. Each solution should be further researched to improve the achievable performance of QKD systems. Particularly, the capabilities of current systems depend heavily on detector performances. As SNSPDs appear helpful in this regard, investigating their transposability to space is a priority. Studying the interoperability of several technologies to address different problems is also necessary. Assessing the combined performances of several systems is critical in evaluating the readiness of the technology. More complex protocols should also be explored as they possess intrinsic advantages.

Concerning the experimental source, it was decided to stop the experiment after the optical alignment of the SHG module for safety reasons. The natural next step is to secure the experimental setup. Once the safety conditions are met, the process can be characterised in detail. The experiment can be conducted with different combinations of optical elements to compare the efficiencies. Moreover, for a single optical layout, studying the evolution of the efficiency of both SHG and SPDC with the amount of power of the input laser would be interesting.

A complete characterisation of the setup is crucial to imagine further experiments. The current experiment can provide a first block for subsequent studies once finalised. Both photons can be used in a variety of manners. A possibility is to use the photon at 800 nm as a heralded photon whose detection indicates the presence of the photon at 1588 nm. Afterwards, the latter can be prepared and sent to an interlocutor. These aspects could be investigated in a following study. A long-term perspective could be to study the possibility, through similar conversions, to perform QKD with longer wavelengths photons or improve the optical design. A more detailed space transposability study would also be important to find solutions to the limitations of the system. This study should compute the heat transfers in the system to accurately evaluate the heat dissipation and its influence on the rest of the satellite platform.

Finally, since the technology is young, concrete guidelines regarding its implementation are lacking. In a collective effort between parties, a set of rules and standards should be discussed and thought out to initiate a progressive migration towards QKD systems. This migration should be carefully planned to smoothly integrate QKD in the current optical fibre networks.

This thesis explored different lines of thought regarding the challenges of QKD technologies. All the explored aspects deserve further investigation. By dedicating efforts to improve the secret key rate through research, the gap between current performance and suitable systems at a global scale will shorten. Moreover, innovative solutions such as exploring operations at larger wavelengths can be decisive in enabling appropriate secure key rates. Considering the advances made in the different domains explored in this work, suitable QKD systems may be close to becoming a reality.

References

1. SEEMANN, Lee. A Historical Overview of Secret Communication and an Introduction to Modern Encryption Methods. 2016.
2. KIRSCH, Zack. *Quantum Computing: The Risk to Existing Encryption Methods* [online]. [visited on 2023-05-27]. Available from: https://www.semanticscholar.org/paper/Quantum-Computing%3A-The-Risk-to-Existing-Encryption-Kirsch-Chow/7a82a44b21bfffb8546496b8d101e5bcf844533c.
3. *IRISS* [online]. [visited on 2023-03-28]. Available from: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-programme/iriss_en.
4. *EuroQCI (European Quantum Communication Infrastructure)* [online]. [visited on 2023-03-28].
5. *Eagle-1* [online]. [visited on 2023-03-29]. Available from: https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Eagle-1.
6. WOLF, Ramona. *Quantum Key Distribution: An Introduction with Exercises*. Vol. 988 [online]. Cham: Springer International Publishing, 2021 [visited on 2023-02-14]. Lecture Notes in Physics. ISBN 9783030739911. Available from DOI: 10.1007/978-3-030-73991-1.
7. SHANNON, Claude E. Communication theory of secrecy systems. *The Bell system technical journal*. 1949, vol. 28, no. 4, pp. 656–715.
8. One-time pad. In: *Wikipedia* [online]. 2023 [visited on 2023-05-27]. Available from: https://en.wikipedia.org/w/index.php?title=One-time_pad&oldid=1156629822. Page Version ID: 1156629822.
9. WOOTTERS, W. K.; ZUREK, W. H. A single quantum cannot be cloned. *Nature* [online]. 1982, vol. 299, no. 5886, pp. 802–803 [visited on 2023-05-27]. ISSN 1476-4687. Available from DOI: 10.1038/299802a0.
10. BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* [online]. 2014, vol. 560, pp. 7–11 [visited on 2023-05-28]. ISSN 03043975. Available from DOI: 10.1016/j.tcs.2014.05.025.
11. HAMMING, Richard W. Error detecting and error correcting codes. *The Bell system technical journal*. 1950, vol. 29, no. 2, pp. 147–160.
12. WILCZEK, Frank. *Entanglement Made Simple* [Quanta Magazine] [online]. 2016-04-28. [visited on 2023-02-17]. Available from: https://www.quantamagazine.org/entanglement-made-simple-20160428/.
13. GHALBOUNI, Joe. *Distribution multi-utilisateur de paires de photons intriqués aux longueurs d'onde de télécommunications*. 2013. PhD thesis. Télécom Paris.
14. CLAUSER, John F. et al. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters* [online]. [N.d.], vol. 23, no. 15, pp. 880–884 [visited on 2023-02-17]. Available from DOI: 10.1103/PhysRevLett.23.880.

15. SHARMA, Purva et al. Quantum Key Distribution Secured Optical Networks: A Survey. *IEEE Open Journal of the Communications Society*. 2021, vol. 2, pp. 2049–2083. ISSN 2644-125X. Available from DOI: 10.1109/OJCOMS.2021.3106659.

16. COMMONS, Wikimedia. *File:Multiplexing diagram.svg — Wikimedia Commons, the free media repository*. 2021. Available also from: https://commons.wikimedia.org/w/index.php?title=File:Multiplexing_diagram.svg&oldid=574059913. [Online; accessed 31-May-2023].

17. DIAMANTI, Eleni et al. Practical challenges in quantum key distribution. *npj Quantum Information* [online]. 2016, vol. 2, no. 1, pp. 1–12 [visited on 2023-02-21]. ISSN 2056-6387. Available from DOI: 10.1038/npjqi.2016.25.

18. HUANG, Donghai et al. Quantum Key Distribution Over Double-Layer Quantum Satellite Networks. *IEEE Access*. 2020, vol. PP, pp. 1–1. Available from DOI: 10.1109/ACCESS.2020.2966683.

19. CAI, Chun et al. Experimental wavelength-space division multiplexing of quantum key distribution with classical optical communication over multicore fiber. *Optics Express* [online]. 2019, vol. 27, no. 4, pp. 5125–5135 [visited on 2023-05-29]. ISSN 1094-4087. Available from DOI: 10.1364/OE.27.005125.

20. DYNES, J. F. et al. Quantum key distribution over multicore fiber. *Optics Express* [online]. 2016, vol. 24, no. 8, pp. 8081–8087 [visited on 2023-05-29]. ISSN 1094-4087. Available from DOI: 10.1364/OE.24.008081.

21. DIXON, A. R. et al. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Optics Express* [online]. 2008, vol. 16, no. 23, p. 18790 [visited on 2023-02-22]. ISSN 1094-4087. Available from DOI: 10.1364/OE.16.018790.

22. WANG, Shuang et al. Twin-field quantum key distribution over 830-km fibre. *Nature Photonics* [online]. 2022, vol. 16, no. 2, pp. 154–161 [visited on 2023-02-22]. ISSN 1749-4893. Available from DOI: 10.1038/s41566-021-00928-2.

23. Quantum key distribution. In: *Wikipedia* [online]. 2023 [visited on 2023-02-22]. Available from: https://en.wikipedia.org/w/index.php?title=Quantum_key_distribution&oldid=1140181383#cite_note-39. Page Version ID: 1140181383.

24. KHALIGHI, Mohammad Ali; UYSAL, Murat. Survey on Free Space Optical Communication: A Communication Theory Perspective. *IEEE Communications Surveys & Tutorials*. 2014, vol. 16, no. 4, pp. 2231–2258. ISSN 1553-877X. Available from DOI: 10.1109/COMST.2014.2329501.

25. *Military Satellite Communications Fundamentals | The Aerospace Corporation* [online]. 2015-09-05. [visited on 2023-05-29]. Available from: https://web.archive.org/web/20150905170449/http://www.aerospace.org/2013/12/12/military-satellite-communications-fundamentals/.

26. Communications satellite. In: *Wikipedia* [online]. 2023 [visited on 2023-05-29]. Available from: https://en.wikipedia.org/w/index.php?title=Communications_satellite&oldid=1156553960. Page Version ID: 1156553960.

27. *6.12 What about scattering? | METEO 300: Fundamentals of Atmospheric Science* [online]. [visited on 2023-02-24]. Available from: https://www.e-education.psu.edu/meteo300/node/785.

28. COMMONS, Wikimedia. *File:Atmosfaerisk spredning-ru.svg — Wikimedia Commons, the free media repository*. 2022. Available also from: https://commons.wikimedia.org/w/index.php?title=File:Atmosfaerisk_spredning-ru.svg&oldid=646132762. [Online; accessed 31-May-2023].

29. DYNES, J. F. et al. Testing the photon-number statistics of a quantum key distribution light source. *Optics Express* [online]. 2018, vol. 26, no. 18, p. 22733 [visited on 2023-06-03]. ISSN 1094-4087. Available from DOI: 10.1364/OE.26.022733.

30. Quantum key distribution. In: *Wikipedia* [online]. 2023 [visited on 2023-02-22]. Available from: https://en.wikipedia.org/w/index.php?title=Quantum_key_distribution&oldid=1140181383#cite_note-39. Page Version ID: 1140181383.

31. COMMONS, Wikimedia. *File:GaussianBeamWaist.svg — Wikimedia Commons, the free media repository*. 2022. Available also from: https://commons.wikimedia.org/w/index.php?title=File:GaussianBeamWaist.svg&oldid=668173127. [Online; accessed 31-May-2023].

32. BEDINGTON, Robert et al. Progress in satellite quantum key distribution. *npj Quantum Information* [online]. 2017, vol. 3, no. 1, pp. 1–13 [visited on 2023-02-14]. ISSN 2056-6387. Available from DOI: 10.1038/s41534-017-0031-5.

33. LIORNI, Carlo et al. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New Journal of Physics* [online]. 2019, vol. 21, no. 9, p. 093055 [visited on 2023-03-09]. ISSN 1367-2630. Available from DOI: 10.1088/1367-2630/ab41a2.

34. CHURNSIDE, James H.; LATAITIS, Richard J. Wander of an optical beam in the turbulent atmosphere. *Applied Optics* [online]. 1990, vol. 29, no. 7, pp. 926–930 [visited on 2023-02-28]. ISSN 2155-3165. Available from DOI: 10.1364/AO.29.000926.

35. BOURGOIN, J.-P. et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. *New Journal of Physics* [online]. 2013, vol. 15, no. 2, p. 023006 [visited on 2023-02-28]. ISSN 1367-2630. Available from DOI: 10.1088/1367-2630/15/2/023006.

36. ARTEAGA-DÍAZ, Pablo et al. Enabling QKD under Strong Turbulence for Wireless Networks with Tilt Wavefront Correction. In: *2019 21st International Conference on Transparent Optical Networks (ICTON)*. 2019, pp. 1–4. Available from DOI: 10.1109/ICTON.2019.8840410. ISSN: 2161-2064.

37. ACOSTA, Valentina Marulanda et al. *Analysis of satellite-to-ground quantum key distribution with adaptive optics* [online]. arXiv, 2021 [visited on 2023-02-14]. Available from DOI: 10.48550/arXiv.2111.06747.

38. BARNHART, Samuel; GUNASEKARAN, Sidaard. *Design and Development of a Coherent Detection Rayleigh Doppler Lidar System for Use as an Alternative Velocimetry Technique in Wind Tunnels*. 2020. Available from DOI: 10.13140/RG.2.2.32670.15688. PhD thesis.

39. GRUNEISEN, Mark T. et al. Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver. *Optical Engineering* [online]. 2016, vol. 55, p. 026104 [visited on 2023-02-14]. ISSN 0091-3286. Available from DOI: 10.1117/1.OE.55.2.026104. ADS Bibcode: 2016OptEn..55b6104G.

40. GRUNEISEN, Mark T. et al. Adaptive spatial filtering for daytime satellite quantum key distribution [online]. 2014, vol. 9254, p. 925404 [visited on 2023-02-14]. Available from DOI: 10.1117/12.2071278. ADS Bibcode: 2014SPIE.9254E..04G.

41. ANISIMOVA, Elena et al. A low-noise single-photon detector for long-distance free-space quantum communication. *EPJ Quantum Technology* [online]. 2021, vol. 8, no. 1, pp. 1–17 [visited on 2023-02-14]. ISSN 2196-0763. Available from DOI: 10.1140/epjqt/s40507-021-00111-0.

42. CALANDRI, Niccolò et al. Superconducting nanowire detector jitter limited by detector geometry. *Applied Physics Letters* [online]. 2016, vol. 109, no. 15, p. 152601 [visited on 2023-03-13]. ISSN 0003-6951. Available from DOI: 10.1063/1.4963158.

43. BEUTEL, Fabian et al. Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Information* [online]. 2021, vol. 7, no. 1, pp. 1–8 [visited on 2023-03-13]. ISSN 2056-6387. Available from DOI: 10.1038/s41534-021-00373-7.

44. BOARON, Alberto et al. Simple 2.5 GHz time-bin quantum key distribution. *Applied Physics Letters* [online]. 2018, vol. 112, no. 17, p. 171108 [visited on 2023-03-13]. ISSN 0003-6951, ISSN 1077-3118. Available from DOI: 10.1063/1.5027030.

45. SEMENOV, Alex D. et al. Quantum detection by current carrying superconducting film. *Physica C: Superconductivity* [online]. 2001, vol. 351, no. 4, pp. 349–356 [visited on 2023-03-17]. ISSN 0921-4534. Available from DOI: 10.1016/S0921-4534(00)01637-3.

46. GOLTSMAN, G. N. et al. Picosecond superconducting single-photon optical detector. *Applied Physics Letters* [online]. 2001, vol. 79, no. 6, pp. 705–707 [visited on 2023-03-17]. ISSN 0003-6951. Available from DOI: 10.1063/1.1388868.

47. MARSILI, F. et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics* [online]. 2013, vol. 7, no. 3, pp. 210–214 [visited on 2023-03-17]. ISSN 1749-4893. Available from DOI: 10.1038/nphoton.2013.13.

48. KORZH, Boris et al. Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector. *Nature Photonics* [online]. 2020, vol. 14, no. 4, pp. 250–255 [visited on 2023-03-17]. ISSN 1749-4893. Available from DOI: 10.1038/s41566-020-0589-x.

49. MÜNZBERG, Julian et al. Superconducting nanowire single-photon detector implemented in a 2D photonic crystal cavity. *Optica* [online]. 2018, vol. 5, no. 5, pp. 658–665 [visited on 2023-03-17]. ISSN 2334-2536. Available from DOI: 10.1364/OPTICA.5.000658.

50. PASCHOTTA, Dr Rüdiger. *Acceptance Angle in Fiber Optics* [online]. [visited on 2023-04-17]. Available from: https://www.rp-photonics.com/acceptance_angle_in_fiber_optics.html.

51. PASCHOTTA, Dr Rüdiger. *Numerical Aperture* [online]. [visited on 2023-04-17]. Available from: https://www.rp-photonics.com/numerical_aperture.html.

52. PASCHOTTA, Dr Rüdiger. *Fibers* [online]. [visited on 2023-04-19]. Available from: https://www.rp-photonics.com/fibers.html.

53. PASCHOTTA, Dr Rüdiger. *Fiber Launch Systems* [online]. [visited on 2023-04-17]. Available from: https://www.rp-photonics.com/fiber_launch_systems.html.

54. NEUMANN, Ernst-Georg. *Single-Mode Fibers*. Vol. 57 [online]. Red. by TAMIR, Theodor; LOTSCH, Helmut K. V. Berlin, Heidelberg: Springer, 1988 [visited on 2023-04-17]. Springer Series in Optical Sciences. Available from DOI: 10.1007/978-3-540-48173-7.

55. COMMONS, Wikimedia. *File:Airy-pattern.svg — Wikimedia Commons, the free media repository*. 2020. Available also from: https://commons.wikimedia.org/w/index.php?title=File:Airy-pattern.svg&oldid=494233218. [Online; accessed 5-June-2023].

56. BABCOCK, H. W. THE POSSIBILITY OF COMPENSATING ASTRONOMICAL SEEING. *Publications of the Astronomical Society of the Pacific* [online]. 1953, vol. 65, no. 386, p. 229 [visited on 2023-03-20]. ISSN 1538-3873. Available from DOI: 10.1086/126606.

57. *Atmospheric turbulence | meteorology | Britannica* [online]. 2023-03-02. [visited on 2023-03-21]. Available from: https://www.britannica.com/science/atmospheric-turbulence.

58. ZHAO, Jiapeng et al. Performance of real-time adaptive optics compensation in a turbulent channel with high-dimensional spatial-mode encoding. *Optics Express* [online]. 2020, vol. 28, no. 10, pp. 15376–15391 [visited on 2023-02-14]. ISSN 1094-4087. Available from DOI: 10.1364/OE.390518.

59. KO, Heasin et al. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Scientific Reports* [online]. 2018, vol. 8, no. 1, p. 15315 [visited on 2023-02-14]. ISSN 2045-2322. Available from DOI: 10.1038/s41598-018-33699-y.

60. BENNETT, Charles H. et al. Experimental quantum cryptography. *Journal of Cryptology* [online]. 1992, vol. 5, no. 1, pp. 3–28 [visited on 2023-03-29]. ISSN 1432-1378. Available from DOI: 10.1007/BF00191318.

61. JACOBS, B. C.; FRANSON, J. D. Quantum cryptography in free space. *Optics Letters* [online]. 1996, vol. 21, no. 22, pp. 1854–1856 [visited on 2023-03-29]. ISSN 1539-4794. Available from DOI: 10.1364/OL.21.001854.

62. URSIN, R. et al. Free-Space distribution of entanglement and single photons over 144 km. *Nature Physics* [online]. 2007, vol. 3, no. 7, pp. 481–486 [visited on 2023-02-20]. ISSN 1745-2473, ISSN 1745-2481. Available from DOI: 10.1038/nphys629.

63. *China launches world's first quantum science satellite* [Physics World] [online]. 2016-08-16. [visited on 2023-03-30]. Available from: https://physicsworld.com/china-launches-worlds-first-quantum-science-satellite/.

64. YIN, Juan et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* [online]. 2017, vol. 356, no. 6343, pp. 1140–1144 [visited on 2023-02-22]. Available from DOI: 10.1126/science.aan3211.

65. MERANER, Sandra et al. Approaching the Tsirelson bound with a Sagnac source of polarization-entangled photons. *SciPost Physics*. 2021, vol. 10. Available from DOI: 10.21468/SciPostPhys.10.1.017.

66. LU, Chao-Yang et al. Micius quantum experiments in space. *Reviews of Modern Physics* [online]. 2022, vol. 94, no. 3, p. 035001 [visited on 2023-04-07]. Available from DOI: 10.1103/RevModPhys.94.035001.

67. LIAO, Sheng-Kai et al. Satellite-to-ground quantum key distribution. *Nature*. 2017, vol. 549, no. 7670, pp. 43–47.

68. LIAO, Sheng-Kai et al. Satellite-Relayed Intercontinental Quantum Network. *Physical Review Letters* [online]. 2018, vol. 120, no. 3, p. 030501 [visited on 2023-03-31]. Available from DOI: 10.1103/PhysRevLett.120.030501.

69. YIN, Juan et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* [online]. 2020, vol. 582, no. 7813, pp. 501–505 [visited on 2023-04-03]. ISSN 1476-4687. Available from DOI: 10.1038/s41586-020-2401-y.

70. *ESA - Eagle-1* [online]. [visited on 2023-06-03]. Available from: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1.

71. ANTONIO.AMENDOLAGINE@ANGELCOMPANY.COM. *SITAEL signs deal with SES on EAGLE-1 for Quantum Cryptography* [SITAEL S.p.A.] [online]. 2022-11-17. [visited on 2023-06-06]. Available from: https://www.sitael.com/sitael-signs-deal-with-ses-to-deliver-satellite-platform-for-europes-eagle-1-quantum-cryptography-system/.

72. *SES + TESAT to develop QKD payload for EAGLE-1 – SatNews* [online]. [visited on 2023-06-06]. Available from: https://news.satnews.com/2023/05/11/ses-tesat-to-develop-qkd-payload-for-eagle-1/.

73. *EAGLE-1: Advancing Europe's Leadership in Quantum Communications* [SES] [online]. 2022-09-22. [visited on 2023-06-06]. Available from: https://www.ses.com/newsroom/eagle-1-advancing-europes-leadership-quantum-communications.

74. *Optical Communication Band - FiberLabs Inc.* [FiberLabs Inc. - Specialty Fiber Amplifiers and Fluoride Fibers] [online]. 2023-03-08. [visited on 2023-04-19]. Available from: https://www.fiberlabs.com/glossary/optical-communication-band/.

75. PRABHAKAR, Shashi et al. Two-photon quantum interference and entanglement at 2.1 µm. *Science Advances* [online]. 2020, vol. 6, no. 13, eaay5195 [visited on 2023-02-14]. Available from DOI: 10.1126/sciadv.aay5195.

76. BOYD, Robert W.; PRATO, Debbie. *Nonlinear Optics*. 3rd edition. Amsterdam ; Boston: Academic Press, 2008. ISBN 9780123694706.

77. *PPLN Guide-Overview* [HC Photonics Corp. - PPLN, PPLT, MgO:PPLN, PPMgO:LN, SHG, SFG, SPDC, DFG, MIR OPO, Waveguide, ridge waveguide, mixers] [online]. [visited on 2023-04-24]. Available from: https://www.hcphotonics.com/ppln-guide-overview.

78. PASCHOTTA, Dr Rüdiger. *Quasi-phase Matching* [online]. [visited on 2023-04-25]. Available from: https://www.rp-photonics.com/quasi_phase_matching.html.

79. COUTEAU, Christophe. Spontaneous parametric down-conversion. *Contemporary Physics* [online]. 2018, vol. 59, no. 3, pp. 291–304 [visited on 2023-02-14]. ISSN 0010-7514, ISSN 1366-5812. Available from DOI: 10.1080/00107514.2018.1488463.

80. LEVERRIER, Anthony et al. Efficiency of entangled photon pair generation in bulk crystals and waveguides - A comparison. *Proc SPIE*. 2006, vol. 6244, p. 17. Available from DOI: 10.1117/12.665319.

81. YARIV, Amnon. *Quantum Electronics* [online]. New York, NY: John Wiley & Sons, 1989 [visited on 2023-05-03]. Available from: https://resolver.caltech.edu/CaltechAUTHORS:20201119-180721356.

82. COMMONS, Wikimedia. *File:Stimulated Emission.svg — Wikimedia Commons, the free media repository*. 2023. Available also from: https://commons.wikimedia.org/w/index.php?title=File:Stimulated_Emission.svg&oldid=728774176. [Online; accessed 7-June-2023].

83. *QD Laser | Through light, the world is evolving* [QD Laser] [online]. [visited on 2023-06-07]. Available from: https://www.qdlaser.com/en/products/list.html.

84. *Parameter Overview of Laser Diodes by Dr. Kamran S. Mobarhan* [online]. [visited on 2023-05-03]. Available from: https://www.laserdiodecontrol.com/laser-diode-parameter-overview.

85. ADMIN. *Passive Optical Components – Optical Circulator* [Fiber Optic Network Products] [online]. 2015-02-13. [visited on 2023-05-07]. Available from: www.fiberopticshare.com/passive-optical-components-optical-circulator.html.

86. ZHU, Heyuan et al. Efficient second harmonic generation of femtosecond laser at 1 µm. *Optics Express* [online]. 2004, vol. 12, no. 10, pp. 2150–2155 [visited on 2023-05-15]. ISSN 1094-4087. Available from DOI: 10.1364/OPEX.12.002150.

87. CLERMONT, Lionel et al. Afocal combinations and focus control for laser launch telescopes. *Journal of Astronomical Telescopes, Instruments, and Systems* [online]. 2020, vol. 6, no. 3, p. 034003 [visited on 2023-05-15]. ISSN 2329-4124, ISSN 2329-4221. Available from DOI: 10.1117/1.JATIS.6.3.034003.

88. SALEH, Bahaa E. A.; TEICH, Malvin Carl. *Fundamentals of Photonics* [online]. Red. by GOODMAN, J. W. New York, USA: John Wiley & Sons, Inc., 1991 [visited on 2023-05-15]. Wiley Series in Pure and Applied Optics. ISBN 9780471839651. Available from DOI: 10.1002/0471213748.

89. MOSKALEV, Igor. Multiwavelength and ultrabroadband solid-state and semiconductor spatially-dispersive lasers. 2004.

90. PASCHOTTA, Dr Rüdiger. *M^2 factor* [online]. [visited on 2023-05-16]. Available from: https://www.rp-photonics.com/m2_factor.html.

91. NEMOTO, Shojiro. Waist shift of a Gaussian beam by plane dielectric interfaces. *Applied Optics* [online]. 1988, vol. 27, no. 9, pp. 1833–1839 [visited on 2023-05-16]. ISSN 2155-3165. Available from DOI: 10.1364/AO.27.001833.

92. JUNDT, Dieter H. Temperature-dependent Sellmeier equation for the index of refraction, n_e, in congruent lithium niobate. *Optics Letters* [online]. 1997, vol. 22, no. 20, pp. 1553–1555 [visited on 2023-05-17]. ISSN 1539-4794. Available from DOI: 10.1364/OL.22.001553.

93. GAYER, O. et al. *Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNbO3 | SpringerLink* [online]. [visited on 2023-05-17]. Available from: `https://link.springer.com/article/10.1007/s00340-008-2998-2`.

94. *Material Properties of Lithium Niobate • Covesion* [Covesion] [online]. [visited on 2023-05-17]. Available from: `https://covesion.com/en/resource/material-properties-of-lithium-niobate/`.

95. GAYER, O. et al. Erratum to: Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNbO3. *Applied Physics B* [online]. 2010, vol. 101, no. 1, pp. 481–481 [visited on 2023-05-17]. ISSN 1432-0649. Available from DOI: `10.1007/s00340-010-4203-7`.

96. BOYD, G. D.; KLEINMAN, D. A. Parametric Interaction of Focused Gaussian Light Beams. *Journal of Applied Physics* [online]. 2003, vol. 39, no. 8, pp. 3597–3639 [visited on 2023-05-17]. ISSN 0021-8979. Available from DOI: `10.1063/1.1656831`.

97. SMIRR, Jean-Loup. *Vers une source de paires de photons intriqués en polarisation de spectre étroit à 1550 nm* [online]. 2010. [visited on 2023-05-23]. Available from: `https://theses.hal.science/tel-00745192`. PhD thesis. Université Paris Sud - Paris XI.

98. *Gaussian Beam Propagation | Edmund Optics* [online]. [visited on 2023-05-21]. Available from: `https://www.edmundoptics.eu/knowledge-center/application-notes/lasers/gaussian-beam-propagation/`.

99. NEMOTO, Shojiro. Waist shift of a Gaussian beam by a dielectric plate. *Applied Optics* [online]. 1989, vol. 28, no. 9, pp. 1643–1647 [visited on 2023-05-09]. ISSN 2155-3165. Available from DOI: `10.1364/AO.28.001643`.

100. FLAHERTY, Nick. *Reliable semiconductor lasers for quantum technologies in space* [eeNews Europe] [online]. 2022-06-02. [visited on 2023-06-08]. Available from: `https://www.eenewseurope.com/en/reliable-semiconductor-lasers-for-quantum-technologies-in-space/`.

101. GOEPEL, Michael. Optical fiber technology for space: challenges of development and qualification. In: *International Conference on Space Optics — ICSO 2014* [online]. SPIE, 2017, vol. 10563, pp. 671–678 [visited on 2023-05-31]. Available from DOI: `10.1117/12.2304198`.

102. Radiation effects on optical fibers. In: *Wikipedia* [online]. 2022 [visited on 2023-05-31]. Available from: `https://en.wikipedia.org/w/index.php?title=Radiation_effects_on_optical_fibers&oldid=1089050281`. Page Version ID: 1089050281.

103. *MgO:PPLN Bulk Crystals • Covesion • MgO:PPLN crystal and waveguide* [Covesion] [online]. [visited on 2023-05-15]. Available from: `https://covesion.com/en/products/mgoppln-crystals-and-chips/`.

104. WIKIPEDIA CONTRIBUTORS. *Spacecraft thermal control — Wikipedia, The Free Encyclopedia*. 2023. Available also from: `https://en.wikipedia.org/w/index.php?title=Spacecraft_thermal_control&oldid=1154931319`. [Online; accessed 8-June-2023].