Master thesis and internship[BR]- Master's thesis : Development of a Laser Source of Entangled Photons for Space Quantum Key Distribution[BR]- Integration internship

Auteur : Adam, Marine
Promoteur(s) : Habraken, Serge
Faculté : Faculté des Sciences appliquées
Diplôme : Master en ingénieur civil en aérospatiale, à finalité spécialisée en "aerospace engineering"
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/23289

UNIVERSITE DE LIEGE
FACULTE DES SCIENCES APPLIQUEES

Thesis presented to obtain the degree of:
Master of Science in Aerospace Engineering

Development of a Laser Source of Entangled Photons for Space Quantum Key Distribution

ADAM Marine

Thesis supervisor: HABRAKEN Serge

Committee members: CLERMONT Lionel
HABRAKEN Serge
LOICQ Jerôme
MOREAU Vincent

Academic year 2024 - 2025

Acknowledgments

I would like to thank my thesis supervisor, Serge Habraken, for his availability and the valuable advice he provided throughout my internship at CSL. I am grateful for the subject he proposed, which I found particularly compelling, and for offering me the opportunity to engage with experts in the field. I would also like to express my sincere gratitude to Sélim Chaabani and Antoine Groulard for their continuous support throughout this project. I deeply appreciate the time they dedicated to sharing their knowledge of the subject through insightful discussions, and to assisting me with the experimental aspect of this work. I would like to thank the members of my reading committee for taking the time to read and evaluate my thesis.

I am thankful to the staff of CSL for their warm welcome and for making me feel part of the team. Their willingness to assist and continuous support were of tremendous help during the experimental work. I would like to thank Louison, my fellow intern at CSL, whose presence made this work significantly more enjoyable, as well as Clément, Colin, Ismaël, Jesús and Quentin who made my internship pleasant and enriching.

I wanted to thank my parents for their encouragements throughout my studies, as well as for the insights they provided on this thesis. I am also grateful for my friends and my fellow engineer students from AEES who were continuously showing their support during the realization of this project. Finally, I would like to express special thanks to Dawid and to my everyday companions Katniss and Oscar, who supported me in my most stressful days.

Abstract

With the arrival of new quantum technologies, especially quantum computers, the data security as we know it is at risk because classical encryption protocols are easily decrypted by quantum computers. There is therefore an urgent necessity to develop secure systems, resistant against quantum threats. Quantum key distribution (QKD), which represents the technologies that use both quantum and classical channels to exchange cryptographic keys, could be a solution to this security problem. Indeed, by relying on fundamental principles of quantum mechanics, these distribution protocols enable highly secure transmissions. Among the principles of the technique, the present thesis concentrates on the polarization-entanglement of photons. This quantum property denotes a strong correlation between the polarizations of two photons, such that performing a measurement on one photon instantaneously affects the measurement on the polarization of the other.

The main objective of this project is to implement an entangled photon source that generates pairs of entangled photons with orthogonal polarizations, making them useful in entanglement-based QKD protocols. The design of the source takes inspiration from the Micius satellite, which is a QKD Chinese mission that successfully demonstrated the use of polarization-entangled photons to exchange cryptographic keys. The experimental setup involves a non-linear crystal (PPKTP) located at the center of a Sagnac interferometer (perfectly symmetric loop within which photons propagate in opposite directions). The crystal is pumped by a laser beam at 405 nm to trigger a non-linear phenomenon (spontaneous parametric down-conversion) that annihilates pump photons to create pairs of photons at a wavelength of 810 nm. The present work describes the development of this source and discusses the results that emerged from it.

Detailed correlation measurements, supported by the coincidence counts between two single-photon detectors, confirmed the simultaneous generation of photons in the crystal, marking their entanglement in time. A spectral analysis was performed to verify the wavelength of the photons emitted by the source. This proved that the photons had effectively the same wavelength of 810 nm, highlighting their indistinguishability. Part of the conducted visibility measurements yielded promising results, with a visibility of 92% for photons propagating in the Sagnac loop in one direction. This indicated a great efficiency of the non-linear phenomenon in one pumping direction of the crystal. However, challenges related to the alignment of the setup were identified and appeared to be somehow inhibiting the efficiency of the non-linear phenomenon when the crystal is pumped in the opposite direction. Potential solutions and further improvements of the experiment have therefore been proposed to address these issues, along with the necessary adjustments to make the source suitable for space-based QKD applications.

Contents

List of Figures

List of Tables

List of Acronyms

- **APD** Avalanche PhotoDiode
- **BB84** Bennett-Brassard 1984 protocol
- **BBM92** Bennett-Brassard-Mermin 1992 protocol
- **BBO** Beta-Barium Borate (β-BaB_2O_4)
- **CHSH** Clauser, Horne, Shimony, and Holt
- **CSL** Centre Spatial de Liège
- **DM** Dichroic Mirror
- **E91** Ekert 1991 protocol
- **EPR** Einstein, Podolsky and Rosen
- **EPS** Entangled Photon Source
- **KTP** Potassium Titanyl Phosphate ($KTiOPO_4$)
- **OAM** Orbital Angular Momentum
- **OPA** Optical Parametric Amplification
- **PBS** Polarizing Beam Splitter
- **PPKTP** Periodically Poled KTP
- **PPLN** Periodically Poled Lithium Niobate (PP $LiNbO_3$)
- **PSI** Polarization Sagnac Interferometer
- **QKD** Quantum Key Distribution
- **QRNG** Quantum Random Number Generator
- **QUESS** Quantum Experiment at Space-Scale
- **SFG** Sum Frequency Generation
- **SFWM** Spontaneous Four-Wave Mixing
- **SHG** Second Harmonic Generation
- **SPDC** Spontaneous Parametric Down Conversion

Part I
Introduction

In a world where quantum technologies, particularly quantum computers, are rapidly emerging, the need for new advanced security systems is growing and becoming critical. Given the current geopolitical climate, the imminent arrival of quantum computers able to decipher any encrypted data -past or present- constitutes a global security risk. This has triggered a race against time to develop secure communication systems before quantum computers become available worldwide. There is therefore an urgent need to develop high security communication networks that are robust against quantum threats. This is where quantum key distribution plays a major role, as it allows the unconditionally secure transmission of cryptographic keys. These keys are then used to encrypt and decrypt data in a secure manner, even in a post-quantum world in which quantum computers are widespread.

1 History

The growing need for perfectly secure communication systems led to the emergence of quantum key distribution (QKD). Traditional methods for exchanging secret keys, used to encrypt and decrypt messages, are vulnerable to different kinds of attacks. Indeed, classical communications can always be passively monitored or copied, making it possible for an eavesdropper not to be detected. Furthermore, even the most robust classical cryptographic systems are threatened by the power of quantum computers. This is why it has become imperative to develop cryptographic protocols resistant to quantum attacks.

The first quantum computer ideas emerged in the 1980's, highlighting the urgency to develop secure communication systems. In 1984, the first quantum protocol was proposed to exchange cryptographic keys. This protocol, called the BB84 protocol, is a prepare-and-measure protocol that relies on fundamental quantum properties of particles (typically photons or electrons) to carry information between the communicating parties. In BB84, one (quantum) bit of information is encoded in each particle, representing one bit of the cryptographic key. The protocol is unconditionally secure because any attempt by an eavesdropper to intercept a qubit (quantum bit) and measure its state will alter the key, thereby alerting the communicating parties of their attack.

Starting in 1991, a new type of QKD protocols appeared: the entanglement-based protocols, with the first one being the E91 protocol. These exploit the entanglement of particles to safely transmit cryptographic keys. The phenomenon of entanglement was first described in 1935 by Einstein, Podolski and Rosen but the first application of this property in a cryptographic protocol emerged in 1991. Two particles are said to be entangled if their properties are intrinsically correlated such that a measurement on one of the particles instantaneously affects the state of the other, even separated by huge distances. The motivation to develop entanglement-based protocols came from a desire to enhance the security of simple prepare-and-measure protocols, like the BB84 one. The security of these protocols relies on the fact that, if an eavesdropper performs a measurement on one of the two entangled particles, it also affects the state of the second particle. By analyzing the quantum correlations between the two parties, it can easily be determined if an eavesdropper interacted with the transmission.

Since then, several protocols have been proposed to encode information using entanglement in different degrees of freedom of the particles. In the case of photons, polarization-entanglement appeared to be the most accessible and the easiest to implement. As a result, polarization-entanglement-based QKD has become the most advanced research area in the field, both in laboratory demonstrations and in real-world spatial applications.

2 Context

The performance of current fiber-based quantum communication networks is limited to short distance ranges as optical losses increase exponentially with the fiber length. For this reason, quantum communication systems naturally turned toward space-based solutions. Transmitting information between satellites and ground stations via free-space links indeed allows to cover global-scale ranges. Consequently, many satellites dedicated to the

demonstration of space-borne QKD systems emerged. The first one, launched in 2016, was the Chinese *Micius* satellite [1]. It successfully demonstrated the efficiency of quantum key distributions, using both prepare-and-measure and entanglement-based protocols. Since then, many propositions and launches of space QKD missions have followed.

The European Union is currently developing a complete international quantum communication network through the *EuroQCI* (European Quantum Communication Infrastructure) initiative [2]. This will enable secure communications between the EU members via both fiber-based and free-space channels. In parallel, the European commission proposed the *IRIS*^{2} project (Infrastructure for Resilience, Interconnectivity and Security by Satellite) [3], which consists in the deployment of 290 satellites to form a secure constellation of communication satellites. Some satellites within the *IRIS*^{2} constellation will therefore serve as space platforms for quantum technologies developed under *EuroQCI*. Indeed, three missions are dedicated to the demonstration of space-borne QKD or prototypes: *Eagle-1* [4], *Saga* (Security And cryptoGrAphic mission) [5] and a geostationary satellite with a QKD payload [6]. Among these, *Eagle-1* is particularly noteworthy due to the participation of Belgium to its QKD payload. Belgium's terrestrial infrastructures will also contribute to the *IRIS*^{2} project through its ground stations and fiber-based communication infrastructures. It is within this broader context that the CSL's interest to explore QKD technologies has emerged, motivating the proposal of this thesis.

A proper state of the art will be established later in this paper, following the introduction of the theoretical principles necessary to understand the true relevance of the examples presented.

3 Project Overview and Objectives

With this context in mind, it appears interesting to develop photon sources for space quantum communication applications. Furthermore, entanglement-based QKD protocols seem to be promising for the future of global secure transmissions. As a result, this project aims to develop a laser source of entangled photons that could potentially be later brought onboard a QKD satellite. The goal is for this experimental source to yield good polarization-entanglement quality. The design of the developed source takes significant inspiration from the one onboard the *Micius* satellite, as seen the meaningful performance it demonstrated. Indeed, its particular configuration, which comprises a Sagnac interferometer, enables a high stability and robustness of the instrument. This allows to obtain high generation rates of entangled-photon pairs.

The present work thereby describes the different steps and preliminary computations that were required to design such a source, alongside the difficulties that were encountered and the trade-offs that had to be made. It will be attempted to characterize the source performance and efficiency and to investigate potential improvements to make it suitable for space.

This thesis articulates as follows: technical concepts are first introduced to support the theoretical principles that are used and implemented afterwards. A complete state of the art of entangled photon sources and space-borne QKD technologies is then established. Afterwards, the design and implementation of the experimental setup is detailed, applying the technical concepts that have been presented. Following the practical implementation of the source, the results it yielded are analyzed and discussed, allowing to determine its performance and the entanglement quality of the photon pairs it generates. Finally, the constraints that might limit the source performance are outlined and potential solutions as well as possible improvements to make it space-suitable are investigated.

Part II
Technical Concepts

The following sections present different technical concepts to provide the theoretical foundations necessary to understand the experimental work described later and to interpret its outcomes. The fundamental concepts of quantum mechanics are first introduced, forming a theoretical basis for quantum key distribution protocols. Nonlinear optical processes are then discussed, with a particular focus on the phenomenon of spontaneous parametric down-conversion. Afterwards, the Gaussian beam theory is rapidly reviewed to improve understanding of how light beams propagate within the experimental setup. Finally, the working principle of the Sagnac interferometer, which will be implemented in the scope of this experiment, and its relevance to this work are examined.

4 Quantum Mechanics Theoretical Background

Some fundamental principles of quantum mechanics are first introduced to provide a theoretical background sufficient to understand the techniques and phenomena presented in the following sections.

4.1 Representation of a Quantum System

In quantum mechanics, the state of a quantum system is represented by a vector $|\psi\rangle$, which is normalized in a Hilbert space[1]. This state vector can be expressed as a linear combination of the orthonormal basis vectors of this space. For example, the polarization state of a photon can be described in the rectilinear basis, composed of the horizontal $|H\rangle$ and vertical $|V\rangle$ vectors. In that case, the general polarization state of a photon is given by:

$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle\,,$$

where α and β are complex coefficients, such that the state is normalized ($|\alpha|^2 + |\beta|^2 = 1$). More specifically, horizontally and vertically polarized photons are respectively described as

$$|\psi_h\rangle = |H\rangle \quad \text{and} \quad |\psi_v\rangle = |V\rangle\,,$$

which form an orthonormal basis. The polarization of a photon can also be represented as a superposition of those states, like a diagonally polarized one which would have the following polarization state vector:

$$|\psi_d\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$$

or a photon with an anti-diagonal polarization:

$$|\psi_a\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}.$$

However, in the diagonal basis composed of the diagonal $|D\rangle$ and anti-diagonal $|A\rangle$ vectors, the polarization state of a diagonally polarized photon is $|\psi_d\rangle = |D\rangle$ and the state vectors of photons with horizontal and diagonal polarizations are

$$|\psi_h\rangle = \frac{|D\rangle + |A\rangle}{\sqrt{2}} \quad \text{and} \quad |\psi_v\rangle = \frac{|D\rangle - |A\rangle}{\sqrt{2}}.$$

4.2 Measurement of a Quantum System

The measurement of a quantum system projects, with a certain probability, its state onto one of the base vectors of the corresponding Hilbert space. This probability depends on the inner product between the measurement outcome and the system state vector. Returning to the rectilinear basis example, the probability of the measurement to yield a horizontal polarization when the photon is in a state $|\psi\rangle$ is given by[2]:

$$P_h = |\,\langle H|\psi\rangle\,|^2.$$

[1] Hilbert space: linear space over the complex number field [7].

[2] The notation $\langle\alpha|\beta\rangle$ represents the inner (scalar) product between the quantum state vectors $|\alpha\rangle$ and $|\beta\rangle$. This notation is equivalent to the form $|\alpha\rangle^\dagger\,|\beta\rangle$, where $|\alpha\rangle^\dagger = \langle\alpha|$ denotes the conjugate transpose of the vector $|\alpha\rangle$.

Thereby, the probability of measuring a horizontal polarization when the photon is initially in the vertical polarization state ($|\psi_v\rangle = |V\rangle$) is zero, due to the property of an orthonormal basis. Moreover, this probability becomes

$$P_h = \left|\langle H|\frac{|H\rangle + |V\rangle}{\sqrt{2}}\rangle\right|^2 = \left|\frac{\langle H|H\rangle + \langle H|V\rangle}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

for a photon with diagonal polarization. Hence, if a polarization measurement is performed on a diagonally polarized photon in the rectilinear basis, there is a 50% chance that the outcome is a horizontal polarization and, analogously, a 50% chance that it is vertical.

4.3 Conjugate Bases

Two bases of a Hilbert space are said to be conjugate -or mutually unbiased- if the projection of a state vector from one basis onto any vector of the other results in vectors of equal lengths. This means that, if a quantum system is prepared in a state from a given basis and measured in the conjugate basis, all possible outcomes are equally likely. This property is fundamental to the security of some of the quantum key distribution protocols presented below as measuring a quantum state in the wrong basis disturbs it and yields a random outcome, making eavesdropping detectable. The previously presented rectilinear and diagonal bases serve as an example of conjugate bases. This principle is illustrated in Figure 1 which represents rectilinear polarization filters that deflect vertically polarized photons to the right and those with a horizontal polarization to the left. It can be seen that, if a diagonally polarized photon is sent into this polarization filter, it will be deflected to the left half of the time and to the right the rest of the time.

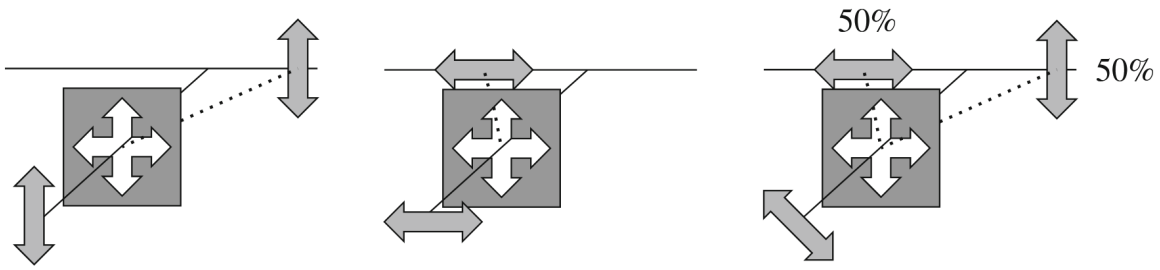


Figure 1: Deflection of vertically, horizontally and diagonally polarized photons by rectilinear polarization filters. Figure from Wolf [8].

4.4 Entanglement

In quantum mechanics, it is possible for two or more particles to be correlated in such a way that measuring the state of one particle has an instantaneous effect on the state of the other(s), even if the particles are located at huge distances from each other. These strongly correlated particles are said to be entangled and their entanglement is basis-independent. This phenomenon was famously referred to by Einstein as a *spooky action at distance*, as it seemed to defy the laws of physics of that time with information seemingly traveling faster than the speed of light. In 1935, these non-local correlations led Einstein, Podolsky and Rosen to argue that the quantum mechanics theory was not complete enough to describe the physical reality [9]. Indeed, the EPR (Einstein, Podolsky and Rosen) paradox emerged: if the position of the first entangled particle is measured, the position of the second one is known with certainty, the same applies for their momentum. However, they believed that measuring the first particle could not possibly affect the second one, such that there was an apparent violation of the Heisenberg uncertainty principle which bounds the product of the position and momentum uncertainties. Therefore, they proposed the existence of some unknown deterministic *hidden variables* in a quantum system, thereby making the quantum theory more complete with a restored local realism[3].

Later on, Bell published a paper from which derived the *Bell's inequalities*, setting an upper limit on the strength of the correlation between two particles if a local realism is supposed [10]. However, correlations

[3]Locality: no information or influence can travel faster than the speed of light, realism: the properties of a particle are not modified when measured.

between quantum systems -especially entangled particles- appeared to violate Bell's inequalities. This renders the EPR theory of local realism at least partially erroneous. These inequalities are now mostly used in a modified form, which is more accessible experimentally. It was proposed by Clauser et al. in 1969 [11] and is designated as the CHSH (Clauser, Horne, Shimony, and Holt) inequality from there on. Years later, experimental proofs of this inequality were implemented, starting with Freedman and Clauser's experiment [12], later improved by Aspect [13]. Violating Bell's inequalities with quantum systems measurements, these experiments showed that the hidden local variable theory was indeed invalid. This suggested the non-locality and/or non-determinism of quantum mechanics.

Nowadays, the entanglement between particles is defined as the inability to express the system quantum state as a tensor product of the individual particle states. For example, the state $|\psi\rangle$ of a system composed of two entangled particles (named particle 1 and particle 2) cannot be written as a tensor product, such that:

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle\,,$$

where $|\psi_1\rangle$ and $|\psi_2\rangle$ would represent the states of particles 1 and 2, respectively. Therefore, the state of a particle in an EPR pair[4] cannot be described without the state of the other one. In the case of two entangled photons that can take parallel or orthogonal polarizations ($|H\rangle$ and $|V\rangle$ for example), the system is in a superposition of basis states. This joint state cannot be factorized into individual photon states. It can be expressed as either:

$$|\psi\rangle = \frac{|H_1H_2\rangle + e^{i\phi}\,|V_1V_2\rangle}{\sqrt{2}} \tag{1}$$

or

$$|\psi\rangle = \frac{|H_1V_2\rangle + e^{i\phi}\,|V_1H_2\rangle}{\sqrt{2}}, \tag{2}$$

where ϕ is the relative phase between the two photons and the notation $|\alpha\beta\rangle$ is equivalent to the tensor product $|\alpha\rangle \otimes |\beta\rangle$. Two correlated particles can be entangled in various degrees of freedom like, for example, polarization, spatial position, time of emission, energy or orbital angular momentum among others. As this paper covers the development of a polarization-entangled photon source, the focus will be on entanglement in the polarization degree of freedom.

Entangled particles can exhibit different degrees of entanglement, which are characterized by their *entanglement quality*. Some quantum states of n-particle systems display a maximal entanglement. In the case of two-particle systems, there exist four maximally entangled states, known as the *Bell's states*. Considering two photons entangled in polarization, decomposed in the rectilinear basis for example, these states are expressed as:

$$|\Phi^+\rangle = \frac{|H_1H_2\rangle + |V_1V_2\rangle}{\sqrt{2}}, \tag{3}$$

$$|\Phi^-\rangle = \frac{|H_1H_2\rangle - |V_1V_2\rangle}{\sqrt{2}}, \tag{4}$$

$$|\Psi^+\rangle = \frac{|H_1V_2\rangle + |V_1H_2\rangle}{\sqrt{2}}, \tag{5}$$

$$|\Psi^-\rangle = \frac{|H_1V_2\rangle - |V_1H_2\rangle}{\sqrt{2}}, \tag{6}$$

where the subscripts 1 and 2 correspond respectively to the first and second particle. These states represent entangled states (see Equation 1 and 2) with a relative phase of 0 or π between the particles. For a system of two entangled photons, the first two Bell's states, $|\Phi^+\rangle$ and $|\Phi^-\rangle$, represent a system in which both photons have the same polarization. There is a probability of $\frac{1}{2}$ that both photons have a horizontal polarization and a probability of $\frac{1}{2}$ that their polarization is vertical. The last two states, $|\Psi^+\rangle$ and $|\Psi^-\rangle$, are quantum systems in which the entangled photons have orthogonal polarizations, with a 50% chance that the first photon is horizontally polarized and 50% chance that it is the second one.

[4] An EPR pair of particles designates a pair of entangled particles. This is a reference to the EPR paradox presented previously.

5 Quantum Key Distribution

To ensure secure communications, two parties -usually named Alice and Bob- need to encrypt and decrypt their messages with secure keys, requiring to exchange these keys. Quantum key distribution, QKD in short, describes cryptographic[5] techniques that employ quantum channels to transmit keys and allow both communicating parties to detect any eavesdropper, referred to as Eve. The keys consist of a sequence of *qubits* (quantum bits) which can, like classical bits, take the value 0 or 1. However, unlike classical bits, qubits also possess the quantum property of being in a superposition of these two states, allowing them to contain much more information.

QKD can be implemented through a variety of protocols, the most used being based on photons or, sometimes, on electrons. As the development of a polarization-entangled photon source is presented in this paper, only protocols that encode information in the photons polarization will be investigated. In such quantum key distribution protocols, the value of the qubit depends on the polarization state in the encoding basis. For example, in the rectilinear and diagonal bases respectively, a linear horizontal or diagonal polarization represents the value 0 while a vertical or anti-diagonal one represents a bit with the binary value 1, as depicted in Table 1.

Basis	**Bits**	
	0	**1**
Rectilinear	↔	↕
Diagonal	↘	↗

Table 1: Bit values and corresponding photon polarization states for different encoding bases.

The security of these cryptography protocols relies on the use of conjugate bases of polarization measurement. This ensures that any eavesdropper who attempts to intercept the key will introduce some errors in it. Commonly used bases are the rectilinear and diagonal ones which regroup non-orthogonal states of polarization. Therefore, if one party sends a photon prepared in, for example, a state of the rectilinear basis and another measures it in its conjugate basis, the diagonal one, the result will be entirely random because of the properties of conjugate bases. The collapse of the photon polarization state into one of the conjugate basis states results in a loss of the information previously carried by the photon and ensures the security of the transmission as it minimizes the chance that an eavesdropper learns useful bits of the key.

Beyond the basic principles, there exist several types of QKD. For instance, depending on whether the protocol relies on discrete single-photons properties (like polarization) or on continuous light wave properties (like phase or amplitude), the key distribution is said to be *discrete-variable* or *continuous-variable*. Other QKD types are also investigated to enhance the protocols security, such as *measurement-device-independent QKD* which eliminates the need to trust detectors or simply *device-independent QKD* which removes trust in any device. Alongside quantum key distribution techniques, post-quantum cryptography has emerged. Like QKD, this approach aims to protect communications but without resorting to quantum techniques. Indeed, post-quantum cryptography relies on classical algorithms theoretically resistant to attacks from quantum computers.

The following sections focus on common discrete-variable QKD protocols.

5.1 BB84 Protocol

In 1984, Bennett and Brassard proposed the BB84 protocol [7], which was the first cryptography protocol based on quantum mechanics. Although it could not be employed with the experiment presented in this paper, this QKD protocol remains worth mentioning for its ease of understanding and implementation.

[5]Cryptography is, as stated by Ekert, a "mathematical system of transforming information so that it is unintelligible and therefore useless to those who are not meant to have access to it" [14]. This is achieved through secure keys, known only to the communicating parties, which are used to encrypt and decrypt the transmitted data.

The BB84 protocol uses both quantum and classical channels to ensure secure transmission of the cryptographic keys as well as the detection of any eavesdropper that might have intercepted and measured some photon polarizations. The functioning of this protocol is summarized in Table 2 and occurs as follows: Alice, the emitter of the message and thus of the secure key, first sends random sequences of bits prepared randomly in one of the two chosen bases of polarization. Due to transmission losses or imperfections in Bob's measurement instruments, he is not able to measure the polarization of all the photons sent by Alice. Therefore, some information is already lost at this stage of the key exchange.

Quantum transmission	Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
	Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
	Photons Alice sends	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕
	Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
	Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
Public discussion	Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
	Alice says which bases were correct			OK		OK			OK				OK		OK	OK
	Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
	Bob reveals some key bits at random					1									0	
	Alice confirms them					OK									OK	
Outcome	Remaining shared bits			1					0				1			1

Table 2: Example of a BB84 application from Bennett and Brassard [7].

Afterwards, Bob publicly communicates the timestamps of the photons he detected, along with the random sequence of bases he used to measure their polarization. Alice then responds with the positions of the qubits measured in the correct bases, which match the ones she used to prepare the photons. The polarizations measured with an incorrect basis, and the qubits that were not detected by Bob, are now discarded to ensure that Alice and Bob possess the same key. Amongst the qubits measured with the correct basis, Bob will tell Alice, via a classical channel, some values selected randomly. This will allow them to determine if an eavesdropper perturbed the communication or not. Indeed, if a third party had intercepted a photon and measured its polarization in the wrong basis, its polarization state could have collapsed in an erroneous state, potentially introducing some errors in the bits measured by Bob. Therefore, if Alice confirms that the bits disclosed by Bob have the same value as the ones she sent, this means that there is a high probability that no eavesdropper was present.

However, Eve has only 25% chance of introducing some errors in the key received by Bob (50% chance of choosing the wrong basis and then 50% chance of the measurement to collapse in the wrong state). Hence, to maximize the likelihood of detecting an eavesdropper, Bob usually makes a much larger number of bit values public than the one presented in this example. Once Alice has confirmed that the communication of the key was secure, both parties know which bits are useful and correct (bottom line of Table 2) and these compose the secret key they will use to encrypt and decrypt their communication.

Theoretically proposed in 1984, the BB84 protocol was later proven to be realistically usable in 1989 by Bennett and Brassard themselves thanks to the transmission of a 403-bit cryptographic key over a 30 cm free-space channel [15]. This protocol is theoretically unconditionally secure. This security has been experimentally tested and confirmed multiple times afterwards [16, 17] as the BB84 protocol remains one of the most used protocols in QKD.

Quantum cryptography systems that encode information in the polarization of photons, like the BB84 protocol, usually employ similar encoding and decoding devices. A typical QKD system based on polarization coding, composed of Alice's encoder and Bob's analyzer, is represented in Figure 2 and its principle is detailed hereafter [18]. The four laser diodes of Alice's system emit photon pulses with four different linear polarizations: vertical, horizontal, diagonal and anti-diagonal. Depending on the qubit value she wants to transmit to Bob, Alice chooses to trigger one of the four diodes, randomly selecting one of the two bases. LD 1 and LD 2 represent the emission of photons with a polarization state prepared in the rectilinear basis and LD 3 and LD 4

in the diagonal basis. These photons -one photon corresponding to one qubit- are then recombined by some beam splitters and the beams are attenuated by a filter to obtain pulses that contain less than one photon on average. Alice then sends her polarization-encoded photons to Bob through a quantum channel, which is either free-space or an optical fiber.

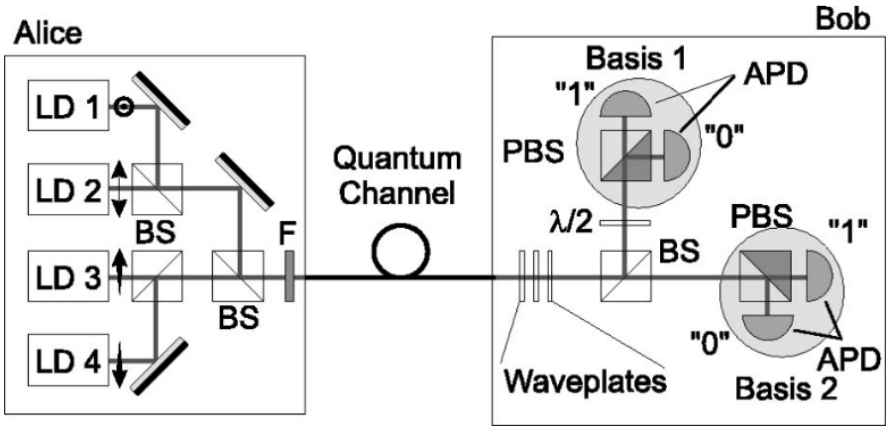


Figure 2: Representation of a typical QKD system based on polarization coding. LD = Laser Diode, BS = Beam Splitter, F = neutral density Filter, PBS = Polarizing Beam Splitter, $\frac{\lambda}{2}$ = half-waveplate and APD = Avalanche PhotoDiode. Figure from Gisin et al. [18]

Following that, the photons are received by Bob and their polarization is determined by its analyzer. As optical fibers may depolarize photons, a set of waveplates is used to recover their initial polarization. A beam splitter then randomly redirects the photons toward one of the two decoders, each corresponding to one measurement basis (either rectilinear or diagonal). Photons transmitted by the beam splitter are analyzed in the rectilinear basis (Basis 2 in the figure), where a PBS reflects horizontally polarized photons and transmits the vertically polarized ones. One photon-counting detector is placed at each output ports of the PBS to register the qubits values. Photons reflected by the beam splitter are rotated by 45° as they pass through a half-waveplate. Their polarization state is then analyzed in the diagonal basis (Basis 1 in the figure) by a PBS and two photon-counting detectors, likewise to what has been described earlier.

5.2 Entanglement-Based QKD

Simple *prepare-and-measure* protocols -like the BB84 protocol- where Alice prepares a photon in a quantum state and Bob measures this state, rely on the assumption that the devices for emission and measurement of both communicating parties are perfect. This allows to consider certain attacks obsolete (for example, see the photon number splitting attack in the next section). Reliance on this assumption, which often diverges from reality, can be avoided by using entangled particles protocols, where both Alice and Bob receive a photon of an EPR pair. Moreover, entanglement-based protocols ensure an enhanced security, compared to prepare-and-measure protocols, thanks to the quantum entanglement properties. Indeed, the interception of one of the two photons by an eavesdropper will disturb their entanglement, making it easier for Alice and Bob to detect Eve.

Ekert was the first to introduce a QKD entanglement-based protocol (E91) in 1991 [14]. Both parties receive one of the entangled photons from a pair, which are assumed to be maximally entangled, and measure its polarization state in a random basis (they have to choose between three conjugate bases). Afterwards, they publicly communicate the bases they used and separate their measurements into two groups: the qubits measured in matching bases and the ones for which the bases do not concord. They then announce via a public channel the polarization they measured for photons of the second group, which allows them to perform a Bell test without discarding any useful bit. The Bell test is based on Bell's inequality to characterize the strength of the correlations between two photons. If the test reveals that the particles are not maximally entangled, this means that Eve probably intercepted and measured a photon polarization, thus reducing the entanglement. This can also mean that external perturbations interfered with the transmission. Nonetheless, if the test shows that the particles remain entangled, a secret key can still be extracted from the data, even if the entanglement is not

maximal [8]. Therefore, if it is concluded that no eavesdropper altered the transmission or that Eve only has partial knowledge of the key, Alice and Bob use the results of the polarizations they measured in the same bases as the cryptographic key. By relying on the violation of the Bell's inequality to verify its security, the E91 protocol is independent from the efficiency and precision of the devices, which makes it more secure and robust than the BB84 protocol [8, 19].

Following Ekert's idea of an entanglement-based protocol, Bennett, Brassard and Mermin proposed the BBM92 protocol in 1992 [20], an entangled version of BB84. Alice and Bob follow a process similar to the BB84 protocol but, instead of Alice preparing the photons and Bob measuring their polarization, they now both measure the polarization states in random bases. Like in the 1984 protocol, they publicly communicate the bases they used (usually either rectilinear or diagonal) and then discard all qubits measured with mis-matched bases. They then compare, via a classical channel, at least half of the values they obtained, use them to determine if an eavesdropper disturbed the communication and finally use the remaining bits as the key if they concluded that Eve did not spy on them. Like E91, BBM92 ensures the key transmission security thanks to the properties of entangled photons. It therefore does not require to make any assumption about the accuracy and efficiency of the devices. However, it is less efficient than E91 as useful bits have to be compared in order to detect any eavesdropper, which reduces the length of the key for a given number of transmitted photons. Finally, this protocol has a simpler implementation than the E91 protocol because it does not rely on a Bell's test and there is thus no need to carry out correlation measurements and statistical computations.

These entanglement-based QKD protocols are overall more secure than the simple prepare-and-measure ones but they are more difficult to implement due to the need of an entangled photon source [19]. Oppositely to the source, the analyzers used to decode keys encoded in the polarization of entangled photons are relatively easy to implement [18]. A general representation of such system is shown in Figure 3. First, a two-photon source sends one photon from an EPR pair to Alice and the other to Bob through quantum channels. The polarization rotator located at the entrance of each analyzer is randomly rotated to select the basis in which the photon polarization is measured. A PBS then sorts the photons based on their polarization, and their qubit values are registered by photon-counting detectors.

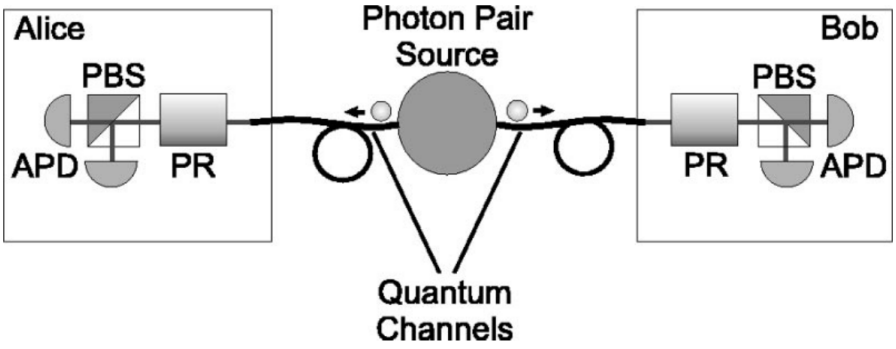


Figure 3: Representation of a typical QKD system based on polarization-entangled photons. APD = Avalanche PhotoDiode, PBS = Polarizing Beam Splitter and PR = active Polarization Rotator. Figure from Gisin et al. [18].

5.3 Protocols Security

When studying the security of a key transmission, one must assume that the eavesdropper who would interfere with the communication has access to any kind of technology, even if this technology does not currently exist. The first advantage of quantum communication protocols is the *no-cloning theorem*. It has been demonstrated that no arbitrary unknown quantum state can be perfectly replicated without altering the initial photon state [21, 22]. This prevents any eavesdropper simply "copying" a photon polarization without disturbing the key transmission. On top of this first degree of security, the previously presented QKD protocols have been developed to be resistant against typical third-party attacks [8], the main ones being:

- **Intercept and resend attack:** Eve intercepts a photon sent by Alice, measures its polarization and then sends it to Bob. As explained before, if Eve chooses the wrong measurement basis, the polarization state

of the photon will collapse randomly in one of the two basis states which might introduce errors in the key. In order to detect an eavesdropper who might intercept and resend some qubits, Alice and Bob compare a part of their key. Thereby, if the number of diverging values exceeds a predetermined threshold (the *qubit error rate* they agreed on), they can conclude that Eve has interfered with their communication and discard the key.

- **Photon number splitting attack:** If Alice's source is not perfect and emits more than one photon at a time, Eve can intercept one photon and isolate it from the others, thus letting Bob receive an unaltered photon directly coming from the source. Eve stores this photon until Alice and Bob publicly communicate the bases they used and can therefore measure its polarization in the correct basis without being detected.

  Ideally, Alice should use a true single-photon source to counter this attack but such sources do not exist. Therefore, she can use weak coherent laser pulses which have an average photon number emission per pulse lower than 1. She can also choose to use decoy states. This means that she sends qubits, with an additional less efficient non-single photon source, such that it modifies the rate of multi-photon supposedly emitted by the source. Meanwhile, Eve still assumes the single-photon rate that should be emitted by one source. If Bob and Alice agreed beforehand on the timestamps of the qubits that would be decoy states, it allows them to exchange quantum keys safely without the need for a perfect or weak coherent laser source.

  Since the probability of creating two pairs of entangled photons simultaneously in an entangled photon source is very low, entanglement-based protocols are considered to be more resistant to the photon number splitting attack than the prepare-and-measure protocols [8]. This represents another advantage of QKD protocols based on entangled photons.

- **Coherent attack:** Even if entanglement-based QKD protocols are more resistant to some attacks, such as photon number splitting, and allow a better detection of intercept and resend eavesdropping, they remain subject to coherent attacks. These represent a powerful type of eavesdropping which involves Eve entangling her own quantum system with Alice and Bob's one. It allows her to store her quantum states in a quantum memory and then to perform a joint measurement on multiple qubits after Alice and Bob have shared publicly the measurement bases they used. As Eve effectuates her attack simultaneously on all the photons she intercepted, she is said to measure the qubits coherently, hence the "coherent attack" name [18]. This type of eavesdropping introduces minimal error into the key, such that there is a low probability for Eve to be detected.

  Simple prepare-and-measure protocols like the BB84 protocol have been proven to be secure against coherent attacks if a true single photon source and perfect devices are assumed [17]. Moreover, entanglement-based protocols, such as E91, are theoretically secure against this type of eavesdropping because performing a Bell test allows to detect the presence of an eavesdropper. However, if Eve performs a coherent attack that only slightly reduces the correlation between Alice and Bob's entangled qubits, they can assume that the non-perfect entanglement of their qubits might come from technical imperfections. Therefore, *privacy amplification* is often used after error correction protocols to ensure a secure transmission. Indeed, even though Alice and Bob share the exact same key after correction, there remains a chance for Eve to know a non-negligible part of this key. Privacy amplification involves shortening the key shared by Alice and Bob to reduce Eve's knowledge [23]. Typically, this is performed by applying a random "hash function", determined beforehand by the communicating parties, to the corrected key. It enables the sharing of a common shortened key by Alice and Bob and ensures the information Eve possesses becomes negligible.

- **Detector side channel attack:** This refers to attacks on the hardware used to implement the protocol rather than on the protocol itself. Indeed, they take advantage of the imperfection of single-photon detectors [8]. There exist different examples of this attack such as the time shift attack in which Eve exploits the difference of detection efficiency for different qubits values. This imperfection of the detectors allows her to manipulate the information transmitted between Alice and Bob by delaying some of the photons. Another example is the detector blinding attack where Eve sends bright light into Bob's detectors to saturate them. They are therefore not able to detect single-photons anymore. This allows Eve to control when Bob's detectors click by sending strong pulses of light.

  Detector side channel attacks can be mitigated through accurate device characterization and testing, active monitoring to detect any leakage of information or even with decoy states for certain attacks. More

recently, a new type of QKD protocol which does not require the single-photon detectors to be trusted[6] has been proposed [24]. It ensures the security of the transmission without relying on assumption about the detection devices performance and accuracy. These robust protocols are referred to as *measurement device-independent* and are resistant against detector side channel attacks.

- **Denial of service attack:** The sole aim of this attack is to disrupt communication, without attempting to learn the cryptographic key exchanged to secure it. To do so, Eve can destroy -or render partially degraded- the quantum channel that Alice and Bob use to communicate, by either physically severing optical fibers or obstructing a free-space link. The attacker can also blind Bob's detectors by injecting strong light pulses or random noise, such that he misses or misinterprets incoming qubits. Consequently, the qubit error rate is so high that the key is rendered unusable.

  This type of attack is particularly limiting in QKD, as it is more accessible and easier to carry out than attacks on the protocols. Therefore, quantum communication systems need to be protected against denial of service attacks. For example, the link between Alice and Bob can be physically secured and a classical fallback encryption system may be implemented to serve as a backup channel, if the quantum link were to fail [25]. Moreover, redundancy can be incorporated into the cryptographic keys. Like in classical communications, the redundancy of the links could also offer protection against denial of service attacks but, due to the current cost and complexity of quantum links, this is not yet a widespread solution. However, this limitation is expected to diminish when QKD networks become globally available [26].

On top of the different protections against typical third-party attacks, the security of QKD protocols also relies on several assumptions -known as security assumptions. Indeed, the protocols are often said to be *unconditionally secure* but this solely means that no assumption is made about Eve's technology, except for the fact that quantum mechanics theory is correct and complete [27]. However, this does not exempt Alice's and Bob's systems from assumptions that are conditional to the security of the transmission. For example, Alice is assumed to send phase-randomized coherent states to Bob. This means that she sends laser pulses composed of photons with random phases and whose photon number distribution follows a Poisson distribution. Additionally, the detection efficiencies of Bob's single-photon detectors (or of both Bob's and Alice's detectors in an entanglement-based protocol) are assumed to be identical. Another assumption concerns the use of the cryptographic key itself. One-time pad encryptions are typically assumed to be the method of choice to encrypt a communication. In a one-time pad, the message is combined with a random key, resulting in a ciphertext. The ciphertext sent to Bob reveals no information about the initial communication text unless it is decrypted with the correct key. This enables secure communications but only under two conditions: the random key must be as long as the message and it should only be used once. These underlying assumptions are critical to make the link between the theoretical security of a protocol and its practical implementation, and they must be accounted for to ensure secure QKD transmissions.

6 Non-Linear Optics

Non-linear optics is a key element in QKD as some non-linear phenomena enable the creation of entangled photon sources. To better understand the principles of non-linear optics, it is helpful to review the basics of classical linear optics: the behavior of a medium crossed by an electromagnetic wave is described by its electric polarization (P) i.e. its electric dipole moment per unit volume [28]. In an isotropic medium, it is usually expressed as follows:

$$P = \varepsilon_0 \chi E, \tag{7}$$

where ε_0 is the electric permittivity of free space, χ the electric susceptibility of the medium and E the wave electric field. This expression of the polarization as a linear function of the wave electric field is in fact an approximation valid only when the amplitude of the field is small enough. Indeed, the general form of the electric polarization of a medium is

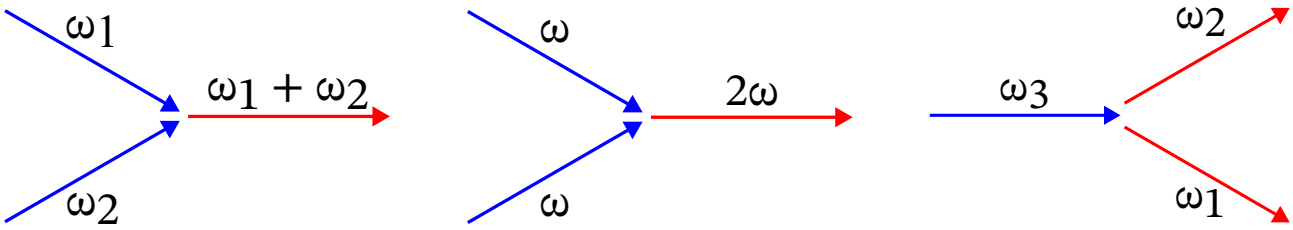
$$P = \varepsilon_0 \chi^{(1)} E + \varepsilon_0 \chi^{(2)} E^2 + \varepsilon_0 \chi^{(3)} E^3 + \dots \tag{8}$$

[6] However, the source still needs to be trusted and thus well characterized.

This confirms that, when the amplitude of the electric field is small, the non-linear terms are negligible, reducing the expression to the linear optics approximation (Equation 7). However, non-linear effects become non-negligible when using laser sources which have a field strength large enough to induce higher-order effects.

In the first order term of Equation 8, $\chi^{(1)}$ characterizes the linear optical properties of the medium and does not allow the coupling of waves. Therefore, two waves propagating in the same linear medium can interfere with each other but it does not influence their propagation [29]. This is not the case for the second-order term which is the most interesting when aiming to produce entangled photon pairs. Indeed, $\chi^{(2)}$ describes the second-order non-linear effects (three-wave interactions) and allows different phenomena to occur [28, 29], the main ones being:

- Sum frequency generation (SFG): two photons oscillating at different frequencies, ω_1 and ω_2, are annihilated in a non-linear medium. The medium then responds by generating a photon oscillating at a frequency given by the sum of the incident ones: $\omega_1 + \omega_2$ (see Fig. 4a).
- Second harmonic generation (SHG): also called frequency doubling. It is a particular case of the sum frequency generation where the two incident photons have the same frequency $\omega_1 = \omega_2 = \omega$, resulting in a photon at twice the initial frequency (see Fig. 4b).
- Spontaneous parametric down-conversion (SPDC): also sometimes referred to as parametric fluorescence. It is the reverse phenomenon of sum frequency generation and consists in one photon (called the *pump* photon), at initial frequency ω_3, spontaneously "splitting" into two photons of lower energy, the *idler* and *signal* photons. These are at frequencies ω_1 and ω_2 (see Fig. 4c). Since SPDC is the only non-linear phenomenon used in this experiment, further details about it are provided below.



(a) Sum frequency generation

(b) Second harmonic generation

(c) Spontaneous parametric down-conversion

Figure 4: Feynman diagrams of second order non-linear optical phenomena.

6.1 Spontaneous Parametric Down-Conversion

Spontaneous parametric down-conversion is a particular case of optical parametric amplification (OPA), a second-order non-linear optical phenomenon. In OPA, a strong pump beam interacts with a weaker signal beam in a non-linear medium, leading to the amplification of this signal and the production of another weaker beam -the idler. The idler photons are created thanks to the input energy provided by the signal wave. Classically, it is thus impossible to realize OPA without a signal input. However, in quantum mechanics, it is possible to consider the signal photons state as being the vacuum state. In this case, a high energy pump photon can be annihilated by the non-linear medium, resulting in the generation of lower energy idler and signal photons. SPDC is therefore described as an amplification of the quantum vacuum energy [30, 31]. Defining SPDC as the reverse process of SFG is intuitive but this classical definition does not accurately describe the actual process of spontaneous parametric down-conversion. It is therefore needed to rely on quantum mechanics theory to precisely describe the phenomenon of SPDC (see Couteau's paper [31] for more details on the quantum description of SPDC).

In the right conditions, the spontaneous down-conversion of a pump photon generates a pair of entangled photons (the idler and signal ones, see Figure 5). This phenomenon therefore plays an important role in quantum key distribution, as it can be exploited to develop entangled photon sources for entanglement-based QKD protocols.

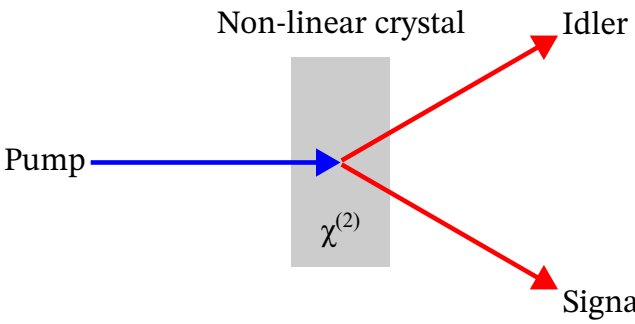


Figure 5: Schematic representation of the spontaneous parametric down-conversion of a pump beam into an idler and a signal wave after going through a non-linear crystal, with a second-order non-linear electric susceptibility $\chi^{(2)}$.

SPDC is an inefficient phenomenon which has a low probability to occur. Its conversion efficiency, defined as the number of down-converted photons per pump photon incident on the crystal, is usually really low. However, this efficiency can be improved thanks to different techniques; conversion efficiencies up to $\sim 10^{-9}$ with periodically poled crystals [32] (see Section 6.5) and $4 \cdot 10^{-6}$ with waveguides [33] have been obtained.

6.2 Phase-Matching Conditions

SPDC is a *spontaneous* process, meaning that it can occur at any time and any point inside the non-linear medium, without the need for an external energy contribution. Moreover, it is a *parametric* process. This implies that the quantum state of the medium remains unchanged before and after the phenomenon has happened [34]. Hence, there is no exchange of energy between the photons and the material medium.

Like the other second-order non-linear parametric phenomena, SPDC thus satisfies the *energy conservation* condition. Indeed, with $\hbar\omega_p$ being the pump photon energy and $\hbar\omega_i$ and $\hbar\omega_s$ the idler and signal ones, the energy conservation writes as:

$$\hbar\omega_p = \hbar\omega_i + \hbar\omega_s,$$

which reduces to the equality:

$$\omega_p = \omega_i + \omega_s. \tag{9}$$

Additionally, efficient SPDC follows the *momentum conservation*, meaning that the wave vector of the pump, idler and signal photons must satisfy the following equation:

$$\mathbf{k}_p = \mathbf{k}_i + \mathbf{k}_s \quad \Leftrightarrow \quad \Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_i - \mathbf{k}_s = \mathbf{0}, \tag{10}$$

with $\mathbf{k}$ the wave vector of the photon inside the non-linear medium. These two principles are represented in Figure 6.

(a) Energy conservation

(b) Momentum conservation

Figure 6: Schematic representation of energy and momentum conservation in a SPDC process.

Equation 10 is equivalent to the statement that the three photons must propagate in phase within the medium. Therefore, when both conservation conditions are met, the interaction of the three photons is said to be *phase-matched* [31]. Phase-matching is required to obtain a high efficiency SPDC but some down-conversion may

still occur when $\Delta\mathbf{k}$ is different from $\mathbf{0}$, leading to a different frequency triplet than the one imposed by the phase-matching condition.

Because the frequencies of the idler and signal photons differ from that of the pump, they propagate differently in the non-linear medium. This is due to *dispersion* as the refractive index of the medium varies with the frequency -and thus wavelength- of the photons, according to the Sellmeier equation [35]. This equation is often used in its reformulated form [36]:

$$n^2 = 1 + \frac{B}{1 - \frac{C}{\lambda^2}} + \frac{D}{1 - \frac{E}{\lambda^2}}, \tag{11}$$

where the wavelength λ is given in micrometers. The coefficients A, B, C, D and E are specific to each transparent material and depend on the temperature.

This dispersion makes it difficult to fulfill the phase-matching condition. To overcome this, *birefringent crystals* are typically used for SPDC. In these materials, the refractive index depends on the photon wavelength but also on the propagation direction and on the polarization of the photon. Indeed, if light does not propagate along the optic[7] axis of the crystal, it is divided into two components: the ordinary and the extraordinary waves. The ordinary wave propagates along the optic axis of the crystal and does not experience birefringence, such that it has a constant refractive index. On the other hand, the propagation velocity of the extraordinary wave depends on the angle its direction forms with the optic axis because of the direction dependence of its refractive index. This birefringence allows an easier phase-matching and yields different types of SPDC (see next subsection for further details) depending on the polarizations of the photons involved.

The momentum of the pump photon being dictated by its wavelength and the refractive index of the medium, it also determines the vector sum of the idler and signal momenta. Consequently, a simple collinear propagation of the down-converted waves cannot always be assumed. Instead, they propagate at a certain angle away from the pump beam to satisfy the phase-matching condition. As a result, the idler and signal photons are emitted along two cones, whose opening angles depend on the generated photon wavelength, as represented in Figure 7. Typically, photons down-converted at lower frequencies will be emitted along cones with larger opening angles (larger diameters) than the higher-frequency photons [37]. The central axes of the two emission cones point in different directions when the idler and signal photons have different polarizations. In birefringent crystals typically used for SPDC, photons with different polarizations experience different refractive indices as they travel through the crystal. This results in different propagation paths [34] such that the rings that appear on a planar cut of the cones (see Figure 7) are centered around different directions.

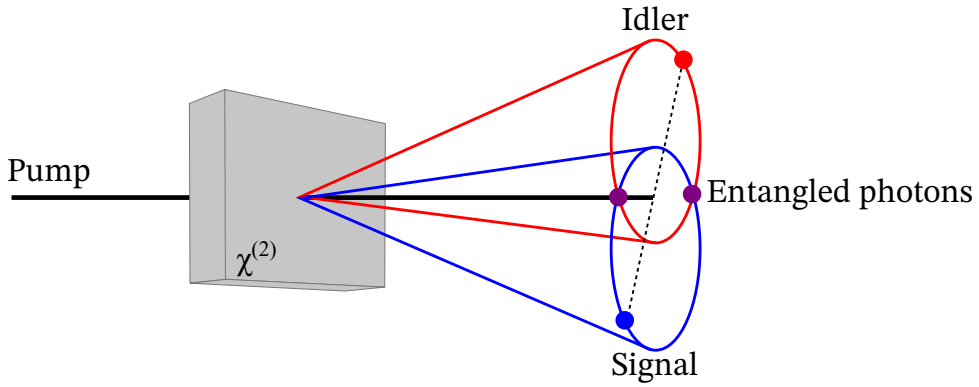


Figure 7: Schematic representation of the cones produced by a degenerate Type-2 SPDC process in a second-order non-linear crystal pumped by a laser beam. The red and blue dots indicate respectively the positions of simultaneously created idler and signal photons. Purple dots represent the polarization-entangled photons located at the two cones intersections. The right side of the schematic represents a transverse planar cut, highlighting the instantaneous positions of the photons during their propagation.

[7]The optic axis of a birefringent crystal is the direction along which light rays propagate without experiencing birefringence, such that their polarization is preserved.

When fulfilled, the phase-matching condition only constrains the wave vectors of the three photons to lie in the same plane (represented by the pump beam and the dotted line in Figure 7), such that the created photons occupy opposite positions[8] with respect to the pump beam. This is due to the transverse momentum conservation which imposes $\Delta k_x = \Delta k_y = 0$, if the pump is assumed to propagate in the z direction [37]. However, the condition does not impose the orientation of this plane. Therefore, there is an uncertainty on the propagation direction of the idler and signal photons, resulting in a circular symmetry because of the numerous orientations that satisfy the phase-matching condition. One can thus observe a ring (cross-section of the cone emission) when looking at the pairs generated by multiple pump photons.

If the pump beam is not purely monochromatic but rather has a certain bandwidth, the rings (cross-sections of the SPDC cones) have a non-zero thickness. This occurs because, if multiple wavelengths are incident on the non-linear crystal, the phase-matching condition will lead to various triplets of wavelengths, resulting in cones of slightly different diameters. As a consequence, the rings appear to be "spread". Moreover, as mentioned earlier, less efficient SPDC can occur even if the phase-matching condition is not perfectly met. Therefore, diverse idler and signal wavelengths combinations may result from the down-conversion of the same input photons. This results once again in cones of varying size and so in "blurred" rings.

6.3 Different SPDC Processes

The outcome of a SPDC process depends on various parameters and can vary from one case to another. Differentiating these kinds of SPDC is important for the comprehension of what follows. The notions relevant for this work are therefore outlined and described in this section.

Based on the frequency of the output photons, the SPDC is said to be either *degenerate* or *non-degenerate*. The degenerate case is a particular form of SPDC in which the idler and signal photons have the same level of energy, such that they are at the same frequency: half of the pump photon frequency. It thus consists in the exact reverse process of second harmonic generation, as one photon at frequency 2ω is annihilated by the non-linear crystal and two photons at ω are created. This degenerate case is useful for QKD application because it produces simultaneously two entangled photons at the same frequency, rendering them indistinguishable. This ensures the security of the key exchange protocol. The non-degenerate case, on the other hand, refers to the creation of two entangled photons at different frequencies. As stated previously, the opening of the emission cones depends on the wavelength of the photons created. Hence, the two cones of a degenerate SPDC process have the same diameter while an asymmetric cone structure appears in a non-degenerate SPDC.

SPDC processes can also be differentiated based on the polarization of the input and output photons. Indeed, there exist three types of spontaneous parametric down-conversion that allow for different tunability of the phase-matching condition:

- **Type-0:** the three photons involved in the second-order process share the same polarization. For example, an ordinary (resp. extraordinary) wave is annihilated and two other lower-energy ordinary (resp. extraordinary) waves are produced by the non-linear medium. This type of SPDC is often used to obtain a maximal efficiency of the process as many birefringent crystals present the highest non-linear coefficients for this type of three-wave interaction [38]. However, the phase-matching condition is challenging to achieve as all three photons have the same polarization and therefore experience very similar but not identical refractive indices during propagation.

- **Type-1:** the signal and idler photons have the same polarization, which is orthogonal to the one of the pump photon. Phase-matching of Type-1 SPDC is usually easier to achieve than for Type-0. Even if this process is not able to produce polarization-entangled photons due to the shared polarization of the idler and signal photons, it is often used to obtain entangled particles in other degrees of freedom such as their emission time, location or phase. Polarization-entanglement can be achieved with a Type-1 phase-matching condition if two birefringent non-linear crystals with orthogonal optic axes are used

[8] The idler, signal and pump photons instantaneous positions always lie on a line, with the pump located between the other two [37].

consecutively [39]. Indeed, by pumping the crystals with diagonally polarized photons, there is a 50% chance that Type-1 SPDC occurs in either of the crystals: in the first one which has a vertical optic axis or in the second one which has a horizontal optic axis[9]. Because of the uncertainty on the crystal in which the down-conversion occurs, the created photons polarization is unknown. The generated states are thus in a superposition of both horizontal and vertical polarizations, resulting in polarization-entangled photons.

- **Type-2:** the output photons have orthogonal polarizations, one of them being the same as the input pump photon polarization. Because the idler and signal photons are emitted with orthogonal polarization states, this type of SPDC enables the production of polarization-entangled photons whose states are characterized by a superposition of orthogonal states. This feature of Type-2 phase-matching makes it suitable for entanglement-based QKD protocols (see Sec. 8.1 for further details).

In a birefringent crystal, the refractive index not only depends on the wavelength and polarization of the photons but also on the angle formed by their wave vector and the optic axis of the crystal. Therefore, the SPDC geometry is influenced by these parameters and a modification of this angle leads to variations of both the opening angles and the orientations of the emission cones [37]. As different polarizations of the down-converted photons lead to different cone orientations, Type-0 and Type-1 SPDC produce concentric cones centered around the pump beam (see Fig. 8) whereas Type-2 phase-matching generates cones with distinct orientations.

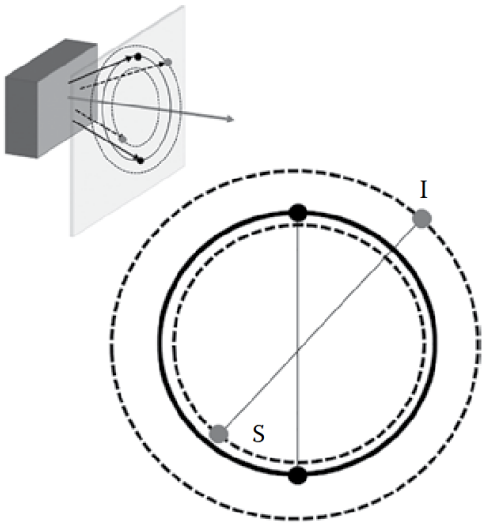


Figure 8: SPDC with Type-1 phase-matching condition. The solid line represents a degenerate case (idler (I) and signal (S) photons share the same wavelength and so a common cone opening angle), while the dotted lines represent a non-degenerate case. Figure from Powers and Haus [40].

Depending on the angle between the pump beam and the crystal optic axis which modifies the overlap of the cones, Type-2 SPDC can present distinct cone configurations, leading to different phenomena [41]. If the pump wave vector and the optic axis form a right angle, the emission cones are concentric and centered around the pump beam, as observed with Type-1 and Type-0 down-conversions. This configuration, where the pump is aligned with one of the crystallographic axes of the birefringent crystal, is called *non-critical* [42]. When the angle is decreased, the axes of the cones move away from the pump propagation direction; the configuration becomes angularly *critical*. This results in the rings intersecting in two distinct points, as depicted in Figures 9b and c. The figures show that, as explained before, the idler and signal photons produced simultaneously by Type-2 SPDC are emitted along two cones and are located on opposite sides of the pump beam. If the pump-optic axis angle is further decreased, the emission cones move farther away from each other and they eventually intersect in a single point, as shown in Figure 9a.

[9]Type-1 SPDC in a crystal with a vertical (resp. horizontal) optic axis generates horizontally (resp. vertically) polarized idler and signal photons.

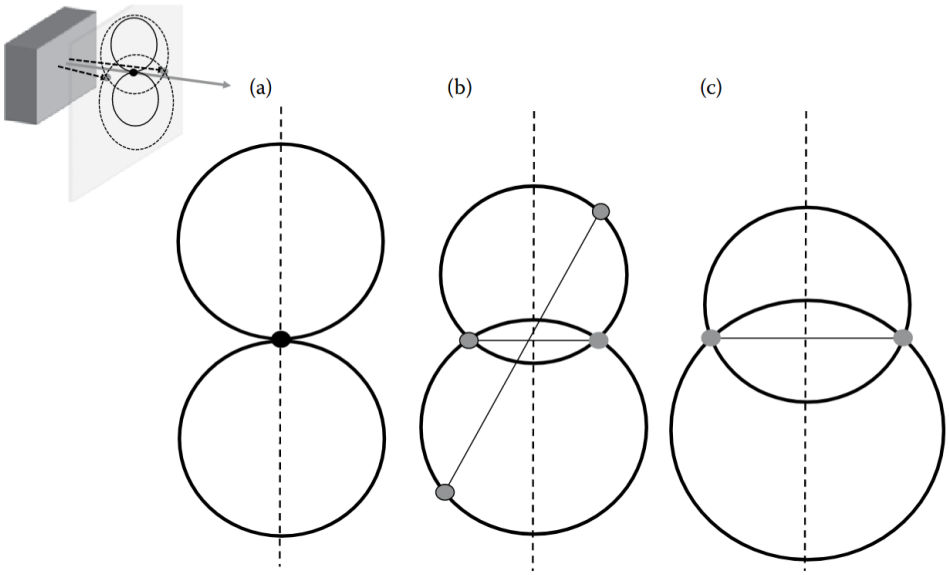


Figure 9: SPDC with Type-2 phase-matching condition. (a) Collinear degenerate case. The pump direction is noted by a black dot. (b) Non-collinear non-degenerate case. Two gray dots connected by a line represent an idler-signal pair. (c) Non-collinear non-degenerate case with an accentuated difference (w.r.t. (b)) between the idler and signal photons wavelengths, resulting in a greater contrast between the rings diameters. Figure from Powers and Haus [40].

With Type-2 phase-matching, the down-converted photons possess orthogonal polarizations. Additionally, each emission cone is composed of photons that share a single polarization. For example, photons in the idler cone are horizontally polarized while those in the signal cone are vertically polarized. Consequently, photons located at the intersections of the cones are equally likely to belong to either cone, such that their polarization is in a superposition of both states (horizontally and vertically polarized in this case). The spatial overlap thus enables the polarization-entanglement of the photons located at the intersection regions. This means that, if a down-converted photon emitted in one of these regions is measured to be horizontally (resp. vertically) polarized, the polarization of the photon from the other region is known to be vertical (resp. horizontal), without any direct measurement [34]. This polarization-entanglement is a fundamental property of Type-2 SPDC and represents a key feature for entanglement-based QKD protocols. Indeed, the polarization-entangled states of the photons introduce intrinsic uncertainty, such that an eavesdropper cannot determine their polarization without performing a measurement.

When the cones intersect in a single point, as depicted in Figure 9a, the geometry is said to be *collinear* given that the pump beam is aligned with the superimposed emission directions of the polarization-entangled photons. Any other case is in a *non-collinear* configuration and the entangled idler and signal photons move away from the pump beam during their propagation. Non-collinear cases are shown in Figures 9b and c, where the pairs of polarization-entangled photons are represented by gray dots located at the intersections of the two rings.

6.4 Potassium Titanyl Phosphate (KTP)

SPDC is typically obtained using birefringent crystals which have large second-order non-linear susceptibility ($\chi^{(2)}$) components. Because of the well-defined internal structure of crystalline materials, the electric field directionality has to be accounted for. Therefore, the second-order non-linear response of the crystal, corresponding to the second-order term of Equation 8, is re-written as [28]:

$$P_i^{(2)} = \varepsilon_0 \chi^{(2)} E^2 = \varepsilon_0 \sum_{j,k} \chi_{ijk}^{(2)} E_j E_k, \tag{12}$$

where the subscripts i, j, k represent the three Cartesian coordinate directions, usually aligned with the crystal principal axes. Injecting the non-linear optical coefficients d_{ij} in Equation 12 [28] yields:

$$\begin{pmatrix} P_x^{(2)} \\ P_y^{(2)} \\ P_z^{(2)} \end{pmatrix} = \begin{pmatrix} d_{11} & d_{12} & d_{13} & d_{14} & d_{15} & d_{16} \\ d_{21} & d_{22} & d_{23} & d_{24} & d_{25} & d_{26} \\ d_{31} & d_{32} & d_{33} & d_{34} & d_{35} & d_{36} \end{pmatrix} \begin{pmatrix} E_x E_x \\ E_y E_y \\ E_z E_z \\ 2E_y E_z \\ 2E_z E_x \\ 2E_x E_y \end{pmatrix}. \tag{13}$$

Depending on the crystal Bravais structure, but also on its internal symmetry, some non-linear optical coefficients can vanish while others can be quite large.

For a sum frequency generation process, the tensor of non-linear optical coefficients allows to couple the electric polarization -so the response- of a non-linear medium in one direction (P_i) to the input wave electric field in other directions (E_j, E_k). Since SPDC corresponds to the reverse process of SFG, the same non-linear susceptibility components describe the phenomenon, therefore contracting into the same non-linear coefficients as the ones presented in Equation 13. Hence, the choice of crystals for spontaneous parametric down-conversion is driven by the magnitude of the d_{ij} coefficients corresponding to orientations of the waves electric fields relevant to the experiment. As the coefficients of interest depend on the polarization configuration of the SPDC process, the choice of the birefringent crystal also relies on the type of phase-matching condition (Type-0, 1 or 2). For instance, the aim of this work is to generate both vertically and horizontally polarized photons thanks to Type-2 down-conversion of pump photons. Therefore, the SPDC crystal material is should either have a high d_{24} coefficient, which links the horizontal and vertical oscillations of the electric field to a response with vertical polarization[10], or a high d_{34} coefficient which links them to a response with horizontal polarization.

Potassium Titanyl Phosphate (KTP[11]) is a birefringent crystal, among many others, that appears to satisfy the requirements for the present experiment. Due to its orthorhombic structure and internal symmetry, the tensor of the non-linear coefficients of KTP reduces to [43]:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & d_{15} & 0 \\ 0 & 0 & 0 & d_{24} & 0 & 0 \\ d_{31} & d_{32} & d_{33} & 0 & 0 & 0 \end{pmatrix}.$$

Because of the shape of this non-linear coefficients tensor, KTP crystals are often employed for all types of SPDC generation. This birefringent material has many advantages [44] such as high non-linear coefficients (given here when the non-linear crystal is pumped at 1.064 μm):

$$\begin{aligned} d_{15} &= 1.9 \text{ pm/V}, \\ d_{24} &= 4.2 \text{ pm/V}, \\ d_{13} &= 2.2 \text{ pm/V}, \\ d_{23} &= 2.7 \text{ pm/V}, \\ d_{33} &= 17.4 \text{ pm/V}, \end{aligned}$$

a wide transparency range (low absorption between 375 nm and 4.2 μm) as well as a good phase-matching tunability due to its thermal properties. KTP is thus a suitable candidate for this experiment, given its notable properties and its satisfactory d_{24} non-linear coefficient value.

6.5 Periodic Poling

To maximize the efficiency of entangled photon sources, periodically poled non-linear crystals are exploited, the most efficient being used in collinear SPDC configuration [42]. The signs of the non-linear coefficients of such

[10] Considering that x is the wave propagation direction, y represents a linear vertical polarization direction and z a horizontal one.

[11] KTP is short for the chemical formula $KTiOPO_4$.

crystals are permanently inverted in a periodic pattern along the propagation direction, thanks to the application of a strong electric field (see Figure 10).

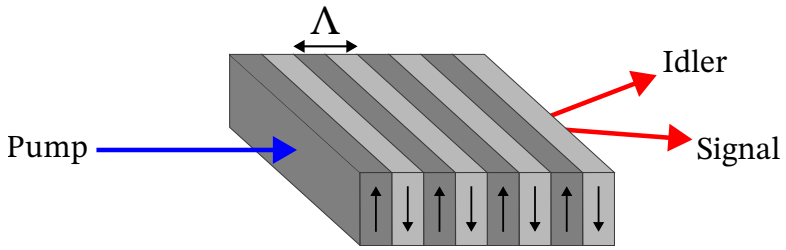


Figure 10: Representation of a periodically poled crystal, used for SPDC, with its periodically inverted non-linear domains. Each domain has a length of $\frac{\Lambda}{2}$.

Hence, considering the crystal poling period Λ, the phase-matching condition can be reformulated as:

$$\mathbf{k}_p = \mathbf{k}_i + \mathbf{k}_s + \frac{2\pi}{\Lambda}\mathbf{x} \quad \Leftrightarrow \quad \Delta\mathbf{k} = \mathbf{k}_p - \mathbf{k}_i - \mathbf{k}_s = \frac{2\pi}{\Lambda}\mathbf{x}, \tag{14}$$

with $\mathbf{x}$ the periodic modulation direction, usually aligned with the pump beam. This equality is referred to as *quasi-phase-matching* as it allows a higher flexibility of the phase-matching condition fulfillment and is represented in Figure 11. Indeed, Λ is a free parameter that can be tuned, for example through thermal expansion or contraction of the crystal, for the SPDC phenomenon to yield different idler and signal frequencies than the ones determined by the classical birefringent phase-matching. When the phase-matching condition is not perfectly respected, the phase mismatches accumulate such that the waves eventually interfere destructively within the crystal. Periodically inverting the signs of the non-linear coefficients allows to compensate this spatial walk-off between the three waves, thus obtaining a triplet of in-phase photons that satisfy the energy and momentum conservation.

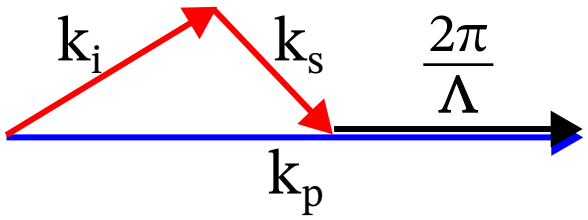


Figure 11: Schematic representation of momentum conservation in a quasi-phase-matched SPDC process in a periodically poled non-linear crystal of period Λ.

In classical birefringent crystals, an increase of the crystal length increases the likelihood of destructive interferences between the waves, thereby reducing SPDC efficiency. Periodic poling then allows the use of longer crystals as quasi-phase-matching prevents these kind of interferences from occurring. Longer crystals being used, more pairs of entangled photons are potentially generated within the non-linear crystal, which increases the SPDC efficiency. Moreover, the periodicity of the structure eliminates the spatial walk-off between the idler and signal photons at the crystal output [45], favoring a high collection efficiency.

As noted previously, periodic poling can be tuned through temperature modulation. Indeed, modifying the temperature will either expand or contract the crystal, thus modulating the length of the periodic domains (Λ). Thereby, different triplets of wavelengths can satisfy Equation 14, which leads to a great tunability of the SPDC source. Quasi-phase-matching also enables simpler geometries because the periodically poled crystals are prepared to be used in a specific orientation, often with the pump beam being orthogonal to the input face of the crystal. Therefore, there is no need to tilt the crystal, allowing a simpler alignment and a more compact layout.

7 Gaussian Beams

The laser nature of a light source enables non-linear optical processes, like SPDC, but it also introduces additional considerations in the computations due to the Gaussian nature of laser beams. Thereby, a reminder about Gaussian beams and the equations used to describe their geometry and focusing is presented hereafter.

Gaussian optics relies on the *paraxial approximation* to describe the behavior of light rays propagating through optical systems. This approximation assumes that the rays forming large angles with the optical axis of the system have a negligible contribution to the behavior of the whole beam, allowing for small-angle approximations. The solution of the wave equation under the paraxial approximation presents the shape of a Gaussian distribution, hence the name *Gaussian beam*. In addition to their Gaussian-shaped intensity profiles, Gaussian beams present a particular wavefront. Indeed, it is planar at the beam waist -minimum beam radius- and becomes spherical when the beam diverges away from the waist. This ensures minimal diffraction losses during propagation.

Monochromatic laser cavities are usually intended to produce light beams in the fundamental transverse electromagnetic mode (TEM_{00}), which presents a Gaussian-shaped intensity profile. TEM_{00} is typically preferred as it is the most stable mode, because it oscillates within a cavity with the lowest losses, and maintains its Gaussian nature during propagation [46]. Laser cavities are thus designed to maximize the diffraction losses of higher-order transverse modes to suppress them, therefore selecting the fundamental one.

7.1 Geometry of a Gaussian Beam

The geometry of a Gaussian beam, depicted in Figure 12, can be entirely described by its wavelength λ and waist size ω_0 [47].

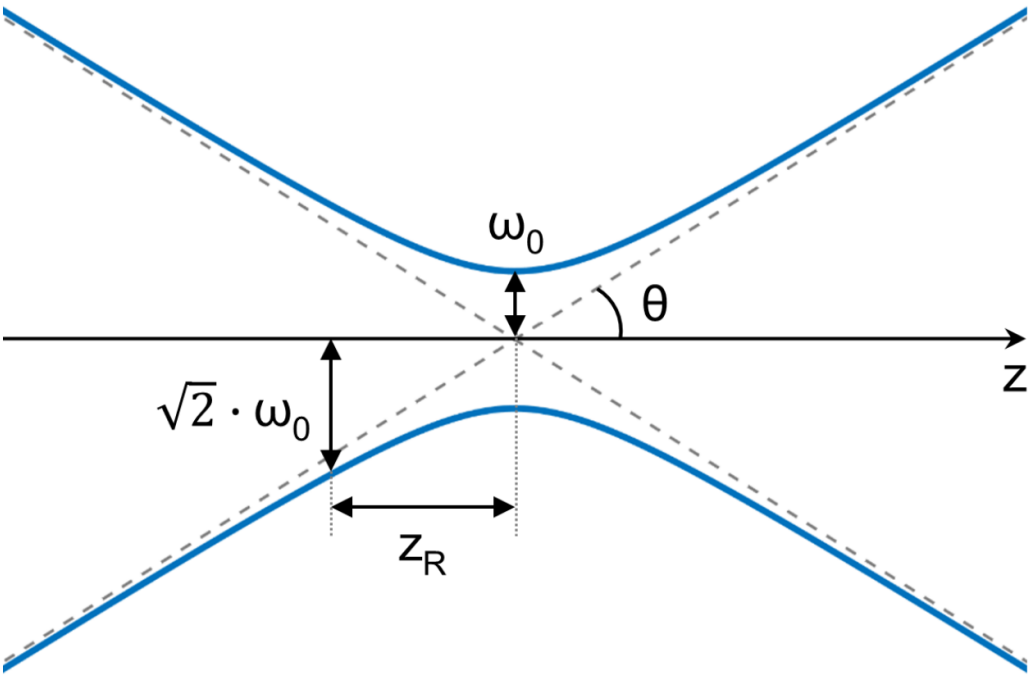


Figure 12: Geometry of a Gaussian beam with ω_0 being its waist, z_R its Rayleigh range, θ its half divergence angle and z the light propagation direction. Figure from Soliman [48].

The Rayleigh range z_R corresponds to the distance, measured from the waist, at which the cross-section of the beam has doubled. It is computed as follows:

$$z_R = \frac{\pi\omega_0^2}{\lambda}.$$

This means that the radius of the beam ω is such that:

$$\omega(z_R) = \sqrt{2} \cdot \omega_0.$$

The general form of the beam radius

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z}{z_R}\right)^2} \tag{15}$$

is a hyperbola that presents a minimum ($\omega = \omega_0$) at $z = 0$. It determines the distance from the beam center at which the intensity reaches $1/e^2 \approx 13\%$ of the on-axis intensity. As mentioned previously, the wavefront of a Gaussian beam becomes spherical when the beam diverges away from its waist. The radius of curvature of its wavefront is therefore given by the following expression:

$$R(z) = z \cdot \left(1 + \left(\frac{z_R}{z}\right)^2\right).$$

The last parameter describing the geometry of a Gaussian beam relevant to this paper is the half angle of divergence θ which, once again, can be completely described by the beam wavelength and waist:

$$\theta = \frac{\lambda}{\pi \omega_0}.$$

7.2 Focusing a Gaussian Beam

As seen from the distinct characteristics of Gaussian beams, the representation of the focusing of light rays is different depending on whether classical geometric optics or Gaussian optics is considered. Therefore the equations employed to mathematically describe the behavior of a laser through thin lenses are recalled below. To draw a parallel with classical geometric optics, the waist ω_0 of the beam entering the lens is referred to as the "object", while the waist of the beam exiting the lens (ω_0') is called the "image" [47]. Moreover, the distance between the object and the lens is noted s and the one between the image and the lens is s'. All of these notations are shown in Figure 13.

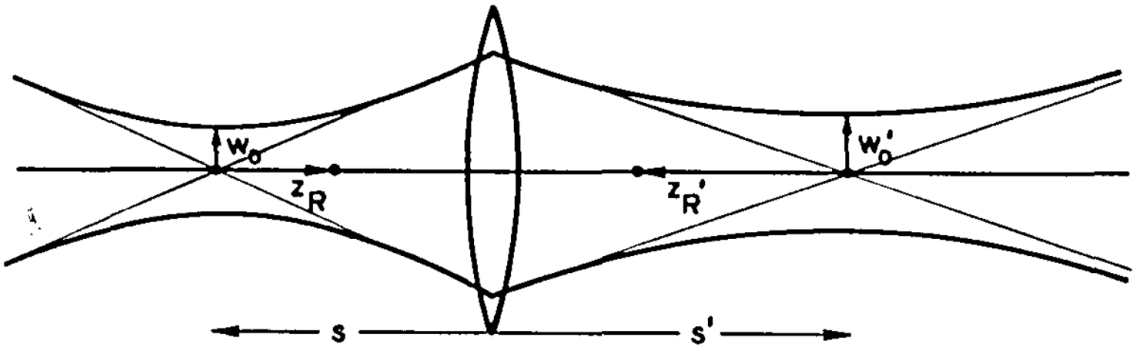


Figure 13: Focusing of a Gaussian beam through a positive thin lens with real object and image. ω_0 and z_R respectively represent the waist and Rayleigh range of the input beam and ω_0' and z_R' the ones of the output beam. s and s' respectively correspond to the distance of the object and image waists to the lens. Figure from Self [47].

When thin lenses are considered, the radii of the input and output Gaussian beams remain unchanged at the lens location. However, they modify the waist size when focusing the beam. Analogously to how a classical thin lens affects the object and image sizes, a thin lens crossed by a Gaussian beam relates the object and image waists with the following expression:

$$m = \frac{\omega_0'}{\omega_0} = \frac{1}{\left((1 - \frac{s}{f})^2 + (\frac{z_R}{f})^2\right)^{\frac{1}{2}}},$$

where m represents the lens magnification. The relation between the distance of the object and image waists to the thin lens and the focal length f of the lens is given by:

$$\frac{1}{f} = \frac{1}{s'} + \frac{1}{s + \frac{z_R^2}{s-f}}.$$

Normalizing this equation with the focal length of the lens [47] leads to:

$$\frac{s'}{f} = \frac{\frac{s}{f} - 1}{(\frac{s}{f} - 1)^2 + (\frac{z_R}{f})^2}. \tag{16}$$

The solution $\frac{s}{f} = \frac{s'}{f} = 1$ shows that, when the object waist is located at the front focus of the thin lens, the image is located at the back focus of the lens. It can also be noted that, unlike the corresponding classical expression

$$\frac{s'}{f} = \frac{1}{\frac{s}{f} - 1},$$

where s' tends toward infinity when s tends toward f, the Gaussian optics expression (Equation 16) does not present any asymptote at $s = f$. This means that, even if the object is located at focal length from the lens, the output beam is not perfectly collimated as the image is not located at infinite distance from the lens but rather at its back focus. These characteristics of Gaussian beams focused by thin lenses have to be accounted for during the predesign of the experiment detailed in this paper.

7.3 Beam Quality

The last important parameter that needs to be taken into account when dealing with lasers is the beam quality factor M^2. It characterizes the deviation of the beam's intensity profile from a perfect Gaussian; the closer M^2 is to 1, the more the real laser beam tends toward a perfect Gaussian beam. This factor is usually specified by the laser manufacturer but it can be determined theoretically with [49]:

$$M^2 = \frac{\pi \omega_0 \theta}{\lambda}.$$

It modifies the Rayleigh range of the beam according to the following expression [50]:

$$z_R = \frac{\pi \omega_0^2}{M^2 \lambda},$$

which affects all of the beam's geometry due to the dependency of the geometric parameters on the Rayleigh range. Once again, this parameter has to be accounted for when pre-dimensioning the setup.

7.4 Waist Shift of a Gaussian Beam

When a Gaussian beam crosses a plane interface, a shift of its waist occurs. This waist shift is defined as the distance between the waist position of the beam incident on the interface and its position after being transmitted by this interface [51]. Figure 14 illustrates this effect.

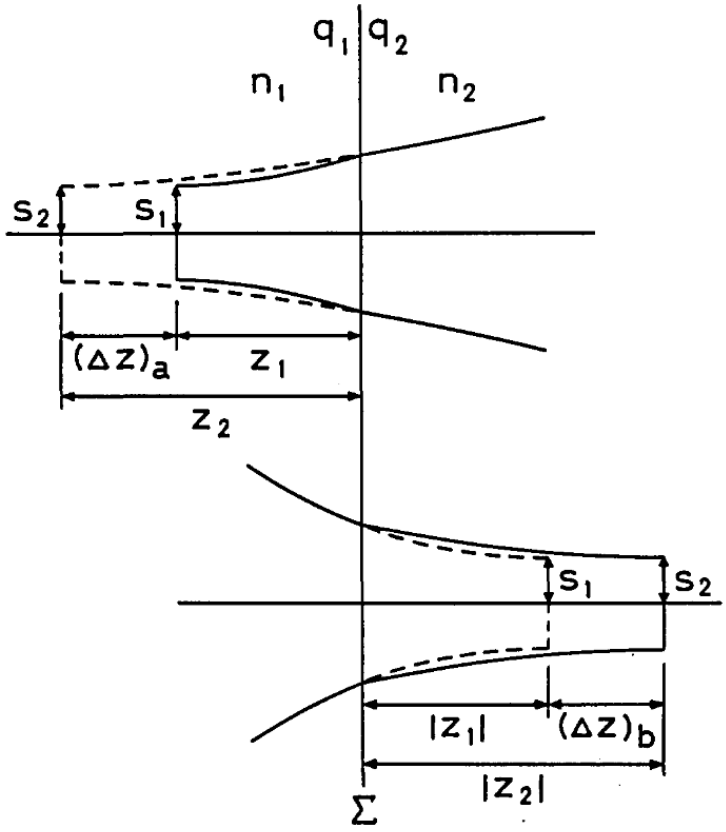


Figure 14: Schematic of the waist shift experienced by a Gaussian beam when it crosses a plane dielectric interface Σ, from a dielectric medium of refractive index n_1 toward one of refractive index n_2 (crossing from left to right), with $n_1 < n_2$. Dotted lines indicate a virtual waist. q_1, q_2 are the complex beam parameters, z_1, z_2 the distances of the beam waists to the interface, s_1, s_2 the waist sizes and $(\Delta z)_a, (\Delta z)_b$ the waist shifts. Figure from Nemoto [51].

The upper part of the figure shows the case of a divergent beam incoming on the interface. The waist of the transmitted beam, in the second medium, is therefore virtual. The lower part of the figure represents the opposite case, namely a convergent beam incident on a plane interface, such that the waist of the transmitted beam is now real. The waist shifts of the two cases are defined as [51]:

$$(\Delta z)_a = z_2 - z_1 = \left(\frac{n_2}{n_1} - 1\right) \cdot z_1, \tag{17}$$

when z_1 is positive and

$$(\Delta z)_b = |z_2| - |z_1| = \left(\frac{n_2}{n_1} - 1\right) \cdot |z_1|, \tag{18}$$

when z_1 is negative (s_1 is located behind the interface). Both waist shifts are positive when $n_1 < n_2$ [51], which means that the waists of the transmitted beams are located farther away from the interface than the waists of the incident beams. It is important to note that, although the waist position is modified by an interface ($z_1 \neq z_2$), its size does not vary ($s_1 = s_2$). These considerations will be useful when attempting to focus a laser beam inside a non-linear crystal.

8 Sagnac Interferometer

The interferometer, named after its inventor, was initially proposed by Sagnac in 1913 to demonstrate the existence of aether[12] and the effect that a motion through this medium had on light propagation [52]. He

[12]The aether theory proponents believed in the existence of an undetectable medium -the aether-, spread across the entire universe, which would support the propagation of light waves, analogous to how air allows sound waves to propagate.

intended to show the alteration of an interference pattern as the system was rotated through the aether. As represented in Figure 15, a beam splitter is used in this interferometer to split the light beam into two and mirrors are arranged so that the split beams can navigate in opposite directions in a closed loop. The beam splitter and the mirrors are generally placed to form a triangular or rectangular loop. When the interferometer is static, the beams travel along the exact same path, in opposite directions, before being recombined at the beam splitter. The principle of the Sagnac interferometer lies on the rotation of the loop in a given direction such that the counter-rotating beams have different relative velocities with respect to the rotating frame. Both the source and detector are rotating with the setup.

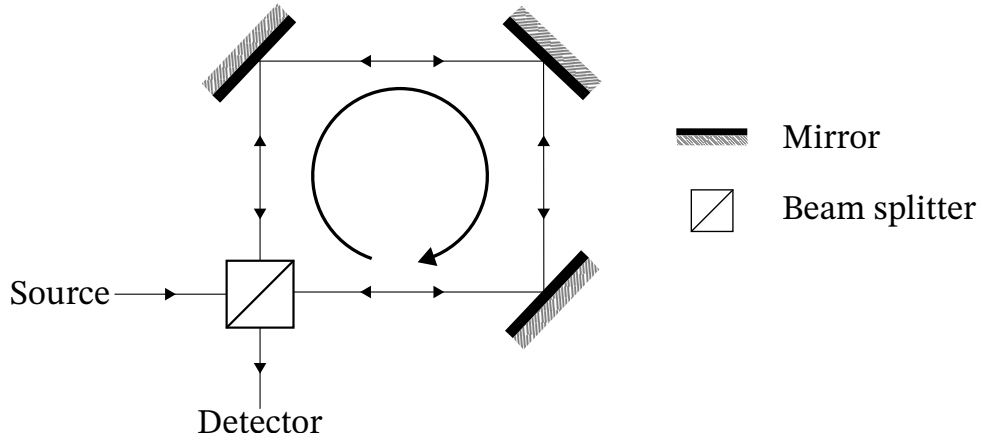


Figure 15: Schematic of a simplified Sagnac interferometer. The incoming light beam is split by a beam splitter. The whole setup rotates in the clockwise direction, as depicted by the central arrow.

Indeed, the wave propagating clockwise around the interferometer travels in the same direction as the beam splitter; it "chases" the beam splitter. While on the other hand, the beam traveling in the counter-clockwise direction is "going away" from the beam splitter. Thereby, because of the invariance of the speed of light with respect to an inertial frame, the rotation causes the separated beams to cover slightly different distances before they interfere at the beam splitter. This results in a relative phase between the two waves that depends on the rotation velocity and leads to a spatial shift of the interference fringes. Sagnac interpreted this effect -now referred to as the *Sagnac effect*- as a proof of the aether existence.

Even if this medium theory has now been proven to be false, the Sagnac interferometer and effect still serve in various other applications. In many navigation systems, they are used to detect inertial rotations with respect to a fixed frame of reference, defined by distant stars and galaxies [53]. For example, modern gyro-compasses use the Sagnac effect to measure the Earth's rotation. By assessing the resulting differences in the light velocity components, a gyro-compass is able to compute the orientation of its coordinate system with respect to the Earth's rotation axis, therefore determining the true North direction. Other navigation instruments use Sagnac interferometers to measure angular velocity, either in ring laser gyroscopes that operate in free-space or in fiber optic gyroscope configuration. The Sagnac interferometer geometry can also be used statically to generate entangled photon pairs, as presented in the next section.

8.1 Entangled Photon Sources

In the scope of this project, the Sagnac interferometer is used in its static configuration, not to exploit the Sagnac effect, but rather to take advantage of its symmetric geometry. Indeed, it makes a suitable entangled photon source (EPS) thanks to its perfectly counter-balanced paths. With the aim of producing entangled photons for quantum key distribution, a non-linear crystal is inserted in the center of a triangular Sagnac loop to produce SPDC, as depicted in Figure 16. The beam splitter and the symmetric arms then introduce an uncertainty on whether the down-converted photons were generated by a pump photon that traveled the loop clockwise or counter-clockwise. At the output of the interferometer, their states are thus a superposition of both possibilities which allows to produce entangled photon pairs. Assuming Type-2 SPDC, which generates pairs of photons

with horizontal and vertical polarizations, the entangled state of the system is given by:

$$|\psi\rangle = \frac{|HV\rangle_{\circlearrowright} + |HV\rangle_{\circlearrowleft}}{\sqrt{2}},$$

with the arrows denoting the clockwise ($\circlearrowright$) and counter-clockwise ($\circlearrowleft$) propagation direction within the loop.

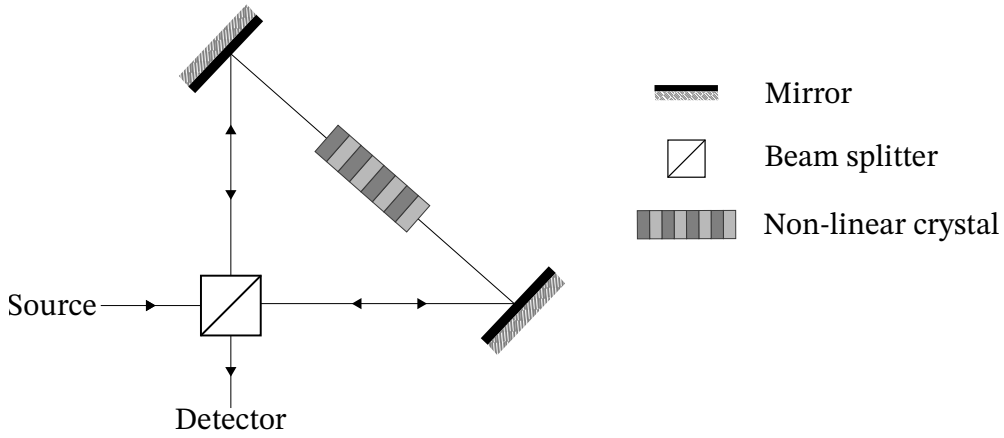


Figure 16: Schematic representation of a static Sagnac interferometer used for QKD purposes.

Using a polarizing beam splitter (PBS), instead of a simple beam splitter cube, with diagonally polarized pump photons enables the random sorting of the photons. Indeed, the PBS randomly projects the photons in a vertical or horizontal polarization state (analogously to Figure 1), thus arbitrarily reflecting and transmitting them. This introduces an uncertainty on the path taken by the photons. Once the spontaneous down-conversion has occurred in the crystal, the generated photons are again sorted by the PBS based on their polarization: they are sent toward different output ports if the SPDC is of Type-2 (idler and signal photons have orthogonal polarizations) and to the same port otherwise. A polarization Sagnac interferometer (PSI) which includes a SPDC Type-2 phenomenon is represented in Figure 17.

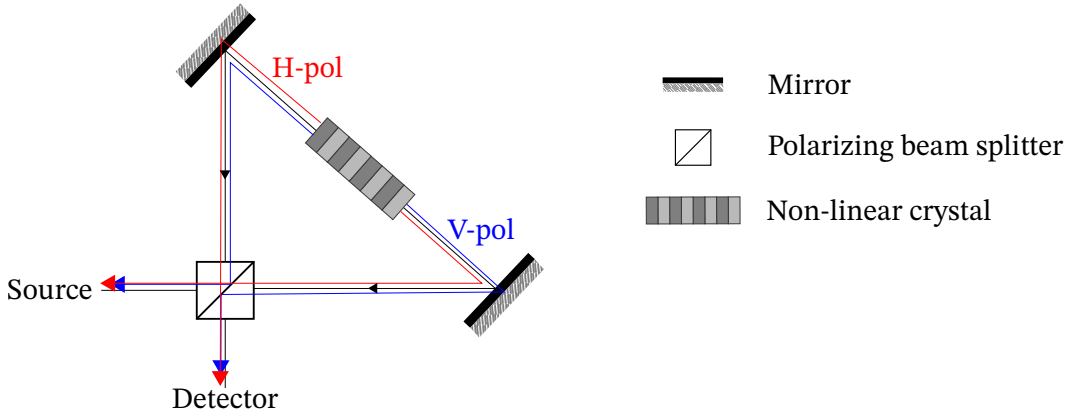


Figure 17: Propagation directions of the horizontally and vertically polarized photons, respectively represented by red and blue lines, down-converted by Type-2 SPDC. The red and blue arrows indicate the propagation of the down-converted photons when they exit the interferometer.

The uncertainty is exploited to ensure a high security of the QKD protocols. In fact, an eavesdropper cannot identify the photon rotation direction due to the Sagnac intrinsic symmetry. As a result, they cannot deduce its polarization unless they measure it, then risking to be detected. This is why it is important for the paths taken by the counter-rotating photons to be indistinguishable. Indeed, if the beams traveling in opposite directions are distinguishable because the paths they took were not perfectly symmetric, an eavesdropper (Eve) could determine if a given photon traveled clockwise or counter-clockwise around the Sagnac loop. Therefore, based on its propagation direction, Eve could assess if the photon was transmitted or reflected by the PBS and thus determine its polarization without measuring it. Type-2 SPDC implemented in a Sagnac interferometer

is thus of great utility in entanglement-based QKD protocols because it allows to send one photon from each pair toward distinct detectors, while preserving the uncertainty on their polarization. Indeed, there are both H and V photons at each output port of the PBS, as illustrated in Figure 17, and the polarization of one photon is unknown until it is measured.

In addition to the indistinguishability of the interferometer arms, ensured by the orientation of the mirrors and of the PBS, the non-linear crystal used to generate entangled photons needs to be perfectly centered in the loop for the protocol to remain secure. Otherwise, the pump photons rotating clockwise for example could be down-converted before/after the photons rotating in the opposite direction. The idler and signal photons that propagate clockwise would then spend more/less time in the loop than the counter-clockwise traveling ones, resulting in a higher/lower probability for them to be affected by external factors (vibrations, temperature fluctuations, ...). Therefore, if Eve is assumed to have access to any technology -currently known or unknown-, these alterations of the photon states could inform her about the direction in which the photons rotated, and so about their polarization like in the previous example. Moreover, if down-converted photons travel a longer path in the loop when they propagate clockwise, they diverge for a longer duration compared to counter-clockwise propagating photons. This results in a larger spatial extension of the beam, making the photons distinguishable.

8.2 Advantages of a Sagnac Interferometer as an EPS

The Sagnac interferometer geometry might be preferred for the development of an entangled photon source over a simple linear architecture[13] for several reasons. First, a linear architecture is incompatible with collinear Type-2 SPDC (see Section 6.3), which is one of the most efficient and convenient configuration for QKD thanks to its high collection efficiency and the indiscernibility between the down-converted photons. Indeed, a linear architecture is not appropriate because the idler and signal photons are either not spatially separated or, if a PBS is employed to split them up, they become distinguishable and therefore useless. One could also use a simple beam splitter to split them but half of the pairs would be wasted when both photons exit the same port of the beam splitter. Consequently, as Type-2 SPDC is often sought in QKD protocols for its polarization-entanglement properties, Sagnac interferometers are usually a suitable choice in this context. Moreover, the Sagnac configuration tends to be more compact than a linear one, where large distances must be imposed between the non-linear crystal and the detectors to spatially separate the down-converted photons for collection, in a non-collinear configuration. This compactness facilitates the alignment of Sagnac interferometers as well as their integration into larger systems, such as satellites.

Due to its symmetric geometry, the Sagnac interferometer is intrinsically robust and stable [54, 55, 56, 57, 58]. Even if an external perturbation (e.g., vibration or temperature fluctuation) were to disturb the setup alignment or the propagation of the beams, both counter-propagating beams would suffer from the same perturbation. This would maintain the symmetry of the optical paths and, consequently, the precision of the Sagnac interferometer. For the same reason, a Sagnac interferometer requires less stringent alignment than other configurations as deviations from the ideal layout affect both paths equally. This symmetry also enables a high phase stability because any phase mismatch occurring in the Sagnac loop is compensated when the photons recombine at the PBS. This represents a key feature for efficient QKD protocols as a strong phase stability enables the production of entangled photon pairs with a high entanglement quality and avoids the need for active phase stabilization. Finally, the Sagnac symmetry introduces an uncertainty on the polarization of the photons once they exit the interferometer, allowing for a high entanglement quality.

Overall, a Sagnac interferometer combined with a spontaneous parametric down-conversion process constitutes an efficient source of entangled photon pairs with high entanglement quality. Its intrinsic symmetry provides it with different properties, including low requirements on the alignment, compactness and robustness. It is particularly its compatibility with Type-2 SPDC and inherent phase stability that make it well-suited for QKD entanglement-based protocols, and so adapted to the present experiment.

[13] In a linear EPS architecture, the pump photons are directly incident on the non-linear crystal and then the down-converted photons are simply collected at its output.

Part III
Practical Implementation

The theoretical foundations needed to understand the objectives and development of this experiment have been presented. This part of the work now focuses on the practical implementation of the experiment. It begins with a state of the art, which introduces the types of entangled photon sources currently used for QKD purposes and various QKD satellite missions. Afterwards, the experimental setup implemented at CSL is described, followed by the presentation and the analysis of the results obtained.

9 State of the Art

Before describing the conducted experiment, an overview of current relevant QKD technologies is presented to contextualize the work. The attention is first directed toward entangled photon sources: reviewing the different architectures that exist, the types of entanglement they are based on, their use for quantum communication and their current limitations, along with ongoing improvements investigated to overcome them. Then, practical implementations of entanglement-based QKD protocols onboard satellites are discussed, first with the pioneer in the domain, the Micius satellite. Other relevant QKD satellites, that are either currently operational or planned for launch, are then introduced. Finally, the challenges that remain for these satellites are outlined. This state of the art aims to situate the present work within the framework of technological research and development, and to highlight the ongoing challenges and improvements in the field.

9.1 Entangled Photon Sources for Quantum Communication

Entangled photon sources, EPS in short, are fundamental components in entanglement-based QKD protocols. They vary in architecture, in the type of entanglement they produce and in the potential of their integration into quantum communication systems. These characteristics confer distinct properties to the sources, such as pair generation rate, entanglement quality and overall performance.

9.1.1 EPS Architectures

Entangled photon sources are designed to generate pairs of photons in order to encode information in their entangled degrees of freedom, representing a key resource for QKD. High-energy photons are typically down-converted into pairs of lower-energy photons through spontaneous parametric down-conversion, a non-linear second order process presented in Section 6.1. Different non-linear crystals can be used to implement SPDC, depending on the type of entanglement that is sought. The most common crystals employed in EPS based on SPDC are Beta-Barium Borate (BBO), periodically poled KTP (PPKTP) and periodically poled Lithium Niobate (PPLN), which have high non-linear second-order coefficients. The periodic poling of PPKTP and PPLN enables high SPDC efficiency, which leads to high generation rates of entangled pairs, and allows a good tunability of the quasi-phase-matching condition. PPKTP is well adapted to telecommunication wavelengths, making it ideal for QKD communications. On the other hand, the compatibility of PPLN with waveguide integration makes it suitable for integrated quantum photonics [59] (see Sec. 9.1.3). However, those crystals are usually more sensitive to external perturbations than PPKTP crystals. Although BBO efficiency is lower than that of the others, it is still employed for spontaneous parametric down-conversion for its large range of transparency, high damage threshold and relatively high non-linear coefficients [60, 61].

Another non-linear process, the spontaneous four-wave mixing (SFWM), is also used in EPS to generate pairs of entangled photons. This third-order non-linear process involves two pump photons interacting to generate a pair of entangled photons. Unlike SPDC, SFWM does not strictly require phase-matching through birefringent or periodically poled crystals. It rather relies on geometric dispersion, which can render its implementation more complex. Nevertheless, this offers a larger choice of materials, like the ones with centro-symmetric structures used in optical fibers. The non-linear crystals with high third-order coefficients, used for SFWM, are usually

robust and CMOS-compatible[14], making four-wave mixing well-suited for EPS integrated on miniaturized circuits [62]. Moreover, the compatibility of these crystals with telecommunication wavelengths allows a good integration into existing fiber-based networks [63]. In comparison with SPDC, the third-order nonlinearities exploited in SFWM are inherently weaker than the second-order ones, thus necessitating higher pump powers.

In addition to these processes, other techniques have been investigated for the generation of entangled photons but they currently remain at the experimental stage due to various challenges. For example, quantum dots are semi-conductor crystalline nano-structures able to emit entangled photons on demand but these are not yet adapted to QKD utilization due to the distinguishability of the photons they emit and the non-consistency of their creation [64]. Radiative cascades in atomic systems may also be used to generate entangled photons but they require complex hardware like a cooler for the laser or a vacuum system, which, for now, renders them impractical and difficult to implement into QKD networks [65]. These new technologies are not yet mature enough to be preferred over SPDC or SFWM which present high performance and efficiency of entanglement. Even if spontaneous four-wave mixing presents advantages for on-chip EPS, it remains less known than SPDC which has been used since around 1970 [66]. This explains why spontaneous parametric down-conversion remains widely used to create entangled-photon pairs.

The performance and efficiency of a source not only depend on the process used to generate entangled photons but also on its geometry. The Sagnac configuration presented in Section 8 is currently the most widely used in quantum communications due to its numerous advantages. Indeed, because of its perfect symmetry, a Sagnac interferometer possesses a great phase stability and resistance to external disturbances. Additionally, the indistinguishability of its counter-propagating paths offers the uncertainty necessary to ensure the security of QKD protocols based on polarization-entangled photons (see Section 8.2 for more detailed advantages). As mentioned previously, linear configurations, in which the non-linear crystal is pumped unidirectionally and the down-converted photons do not interfere, do not provide this uncertainty. They are easier to implement and to align than Sagnac interferometers but more sensitive to instabilities. Therefore, these types of EPS are typically rather used in laboratory demonstrations than in real QKD applications. More complex EPS geometries are employed when the time and OAM degrees of freedom of the photons (see next section) are wanted to be entangled. For example, time-entanglement is usually realized with Franson interferometers or asymmetric Mach Zender interferometers whose different arm lengths are used as delay lines. Some OAM-entangled photon sources use linear configurations and others are exploring the use of interferometric methods but these EPS remain at the experimental stage. It is thereby premature to draw general conclusions about these.

The architecture of an entangled photon source depends on its intended purpose and context of application. The first step is to determine in which degree(s) of freedom of the photons have to be entangled. The different types of entanglements are presented in the next section.

9.1.2 Entanglement Types Used for QKD

Polarization-entanglement is the most exploited form of entanglement, both in laboratory settings and real-world QKD implementations. This is due to its relatively straightforward implementation and compatibility with free-space communication systems. Additionally, the polarization analyzers that receive polarization-entangled photons during key exchanges are convenient to set up and efficient [18]. However, the amount of information that can be encoded in the polarization of photons is quite restricted because it only offers binary encoding, thus limiting the keys to one qubit of information per photon. This limitation is a critical factor for quantum key distribution as it restricts the key rate, which should be high to achieve secure and efficient communications. To overcome this, the entanglement of other photonic degrees of freedom is explored with the aim of increasing the key rates and enhancing the performance of QKD protocols.

The *energy-time-entanglement* of photons can be used for QKD purposes. It refers to strong correlations between the energy (frequency) of two photons in a pair, as well as between their time of emission. This

[14]Being CMOS (Complementary Metal-Oxide-Semiconductor)-compatible means that the material is compatible with the process used to manufacture electronic circuits, such that it is easily integrated in on-chip circuits.

type of entanglement is usually achieved via SPDC in non-linear crystals, which can also simultaneously lead to polarization-entanglement in the right configuration. Energy-time-entanglement is exploited through *phase coding*, which relies on the relative phase between two photons of an EPR pair to carry information [67]. As represented in Figure 18, Alice and Bob each receive one photon from a pair generated by an EPS. Their analyzers usually consist of unbalanced interferometers (known as Franson-type interferometers), which correspond to two measurement bases [18]. Each interferometer consists of two arms of different lengths: a short arm and a long arm.

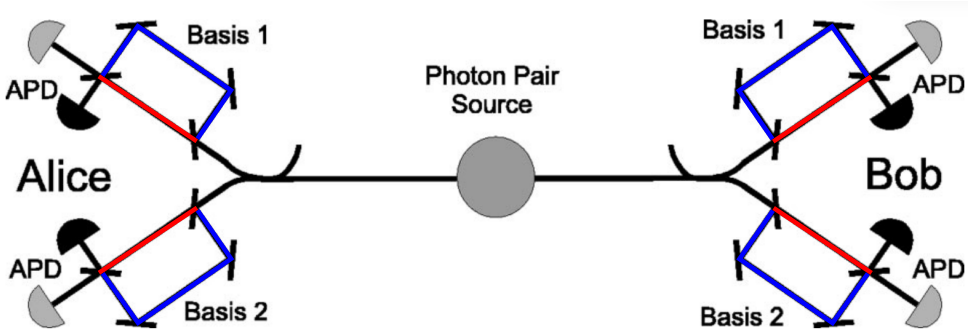


Figure 18: QKD system based on phase coding in energy-time-entangled photons. The long arms of the interferometers are represented in blue and the short arms in red. APD means Avalanche PhotoDiode. Colorized figure, originally from Gisin [18].

When the photons reach Alice's and Bob's analyzers, they randomly choose to go toward one of the interferometers, in one basis. A beam splitter then randomly directs them into either the long or short arm of the interferometer. The path followed by the photons determines the relative phase between Alice's and Bob's photons, leading to distinct interference patterns that correspond to different qubits values. The interferometers are designed such that, if both photons followed the same path length (short-short or long-long), this leads to constructive interferences and to destructive interferences otherwise (short-long or long-short). If the arrival time of the photons is divided in more than two time-bins[15] (beyond just short and long time-bin paths) by more complex interferometers, more information can be encoded in the energy-time-entanglement of a single photon pair. This enables much higher key rates than protocols based on polarization-entanglement, conferring phase coding a substantial advantage for QKD. As in the E91 protocol, Bell tests are performed to verify the security of the key transmission because, if an eavesdropper attempts to spy on the communication, the entanglement quality is diminished.

On top of polarization- and energy-time-entanglement, photons can also be entangled in another degree of freedom: their *orbital angular momentum* (OAM). Only certain light modes, such as Laguerre-Gaussian modes for example, possess an OAM which is a physical property that describes the structure of their wavefront [68]. Photons can carry multiple discrete values of orbital angular momentum, supposedly an infinity, which enables a high key rate and security of the QKD protocols along with a strong resilience to noise -like solar noise. However, atmospheric turbulence can lead to a decoherence of OAM-entangled photons [69, 70].

While polarization-entanglement and energy-time-entanglement have been demonstrated in real-world QKD applications around the year 2000 [71, 72], OAM-entanglement demonstration came later. The first quantum key based on OAM-entanglement has been successfully exchanged over a 210 m free-space link in 2014 [73]. Since then, other experimental proofs have followed, with the most notable being the 2016 experiment that transmitted the words "Hello world!" almost perfectly between two Canary Islands, over a distance of 143 km [74]. Although this demonstration did not implement a full QKD protocol, it remains the longest free-space link over which information was transmitted using OAM-entangled photons.

Polarization encoding currently leads the field in free-space QKD due to its simplicity of implementation

[15]Time-bins are represented by a division of the delay between the detection of one photon from a pair and that of the second into discrete intervals.

and well-known functioning. Notably, a ground-satellite link has already been demonstrated with the Micius satellite [1]. But the need to increase key rates for both efficiency and security of QKD protocols continues to drive research and development of phase- and OAM-encoding technologies. Due to the phase instability of entangled photons, phase encoding is generally more adapted to fiber-links than free-space channels, which explains the slower development of ground-to-satellite phase-based experiments. Nonetheless, some space-borne tests which relate weak coherent pulses to phase encoded QKD have already been conducted. There are significant difficulties in implementing OAM-entangled photon sources and in reliably receiving and analyzing the results of key transmission based on orbital angular momentum protocols. Therefore, long-distance real-world applications remain challenging to achieve. Despite these challenges, OAM encoding remains an active area of research because of its promising potential to increase the performance of QKD protocols.

9.1.3 EPS Miniaturization

EPS miniaturization is a topic of ongoing investigation in quantum technologies. Integrating a quantum system on a small chip is referred to as *integrated quantum photonics*. Researches have led to on-chip entangled photon sources with areas varying from a few cm^2 down to $\sim$ 1 mm^2 [75]. This compactness is a key feature for satellite-based QKD, where the weight and space taken by the instruments are critical. It also makes QKD technologies more accessible and easily scalable for mass production. The large optics and non-linear crystals that compose conventional EPS are often fragile and sensitive to external perturbations and misalignment. By incorporating the optical elements within waveguide structures, integrated quantum photonics enhances the stability and efficiency of these sources. Moreover, using minimal materials improves the robustness of the entangled photon sources and their resistance to the harsh spatial environment, which highlights the relevance of miniaturization research for space-based QKD.

Several space missions, such as SpooQy-1 which uses the Small Photon-Entangling Quantum System (SPEQS) [76] or the german CubeSat QUBE [77], seek to test miniaturized EPS technologies. However, these platforms are not yet fully integrated on-chip systems as they rely on sources made of miniaturized bulk optics. The need for miniaturization is driving the rapid development of on-chips EPS, though their current advancement remains at the laboratory demonstration stage. Entangled QKD protocols based on photonic integrated chips have been demonstrated using both polarization- [78] and energy-time-entanglement [79]. OAM-entangled photon sources have also been successfully miniaturized [80] but not yet applied in full QKD protocols, attesting of the emerging status of technologies based on OAM-entanglement. While on-chip sources are rapidly evolving and achieving high efficiencies, some challenges persist like optimizing the entanglement quality of the photons or integrating efficient filtering and detectors within the chips [81, 82]. Nonetheless, the miniaturization of entangled photon sources is showing potential for global quantum communication networks because of their compatibility with existing fiber-based networks and suitability for satellite payloads.

9.2 QKD Satellites

Nowadays, space-based QKD technologies are an active research area. Indeed, many QKD satellites are already operational or soon to be launched to test a variety of sources and quantum communication protocols. Before presenting examples of these missions, it is important to comprehend the importance of space-borne platforms and thus of free-space quantum transmissions.

9.2.1 QKD Transmission Channels

Quantum key distribution systems typically rely on both classical and quantum communication channels. There are two types of quantum transmission channels: *free-space* links and *optical fibers*. The main differences between them lie in their ability to preserve a quantum signal and the accessible range for the communication.

The signal stability and protection from external perturbations offered by optical fibers often make them the channel of choice for transmission of photons over short distances. However, signal loss in common fiber networks grows exponentially with the distance, typically limiting them to 100-150 km unless quantum repeaters or trusted nodes are employed [83]. Some experiments have also investigated the use of ultra-low-loss

optical fibers combined with high-efficiency detectors, enabling QKD over larger distances like the Boaron et al. experiment realized over 421 km of fibers [84]. While promising, theses technologies are not commercially available yet.

Trusted nodes can extend fiber-based quantum transmissions to longer distances by relaying the signal at trusting intermediate stations. These nodes decrypt the quantum key they receive before re-encrypting and forwarding it, allowing to overcome the distance limitations of classical optical fibers. A large number of nodes is often needed due to the short transmission ranges of fibers. If one node is compromised, the entire system can fail. Therefore, trusted nodes require high levels of physical and operational security, making them complicated to implement globally or within existing networks. Despite these challenges, QKD networks using trusted nodes become common for long distance communications. Examples include the 2000 km long Beijing-Shanghai Backbone Network for QKD and its 32 relay stations [85] or the numerous European metropolitan QKD networks [86]. Nevertheless, due to their high security need and operational complexity, researchers are currently trying to develop higher security nodes as well as more robust operational protocols. Ongoing researches are also focusing on the development of *quantum repeaters*, which aim to improve fiber-based transmissions thanks to the storage of entangled states, therefore avoiding the need to trust intermediate stations. However, quantum repeaters require complex hardware and cryogenic cooling. Additionally, the quantum memory technologies on which they rely are not mature yet. While individual components of quantum repeaters have been demonstrated in controlled laboratory environments, they are not operational yet and still under development.

Even if the transmission range of the optical fibers is continuously improving, it remains limited thus indicating the need for larger-scale communication channels. Moreover, satellite-to-ground free space links are essential in a truly global QKD network, which are not realizable with a fiber-based channel. Free-space links avoid the signal losses inherent to optical fibers over long distances but atmospheric turbulence can affect them. Many ground-based demonstrations of free-space QKD have been successfully conducted at local-scales. Additionally, an effective ground-to-satellite free-space link has been established by the Micius satellite [1], which implemented a working QKD protocol. This indicates that free-space channels are promising for global-scale quantum key distribution but their efficiency remains an active research area. Indeed, ongoing efforts focus on mitigating weather and turbulence effects on communications, as well as improving the time-synchronization between ground stations and satellites.

The last challenge for transmission channels is the global integration of space-borne QKD systems with existing fiber networks [87]. The ground stations required to exchange keys with QKD satellites are complex instruments which are not commonly commercially available. Consequently, existing optical fiber networks are expected to make the link between ground stations and end-users in urban areas. While some partial solutions have already been demonstrated, the global integration of a hybrid QKD network remains under development.

9.2.2 Micius, a Pioneering QKD Satellite

Micius is a low-Earth orbit satellite, developed by the Chinese academy of Science as part of the Quantum Experiments at Space-Scale (QUESS) project. Launched in 2016, it was the first satellite entirely dedicated to the demonstration of quantum technologies. Indeed, some photonic experiments had already been realized on satellite platforms, such as the demonstration of the uplink transmission of single-photons [88] or detector experiments onboard the ISS, but none implemented full QKD protocols. With its multiple payloads[16], this satellite successfully performed several quantum experiments: both uplink and downlink quantum key distribution, the generation and distribution of entangled-photon pairs as well as quantum teleportation. Micius' major achievements are detailed hereafter [1].

Satellite-to-ground QKD experiment:
The satellite successfully transmitted quantum keys, encoded in the polarization of photons, to multiple ground stations (including one in Austria) in a BB84 protocol. Decoy states are used to ensure the protocol security (see Section 5.3 for more details about decoy states). Onboard the satellite, the decoy-state QKD transmitter

[16] Micius' three main payloads are a QKD transmitter, a source of entangled photons and a quantum teleportation receiver.

consists of several laser diodes that send laser pulses through a BB84 encoding module [89]. A beacon beam (green laser) is then added to the beam exiting the encoding module for spatial tracking of the satellite and time-synchronization. Another one is also used as a polarization reference. At the ground station, a telescope receives the beams and separates the beacon photons from the decoy-state ones, which are then analyzed by a BB84 decoder. The principles of BB84 encoder and decoder are represented in Figure 19. These are nearly identical to the typical polarization coding system previously presented in Figure 2.

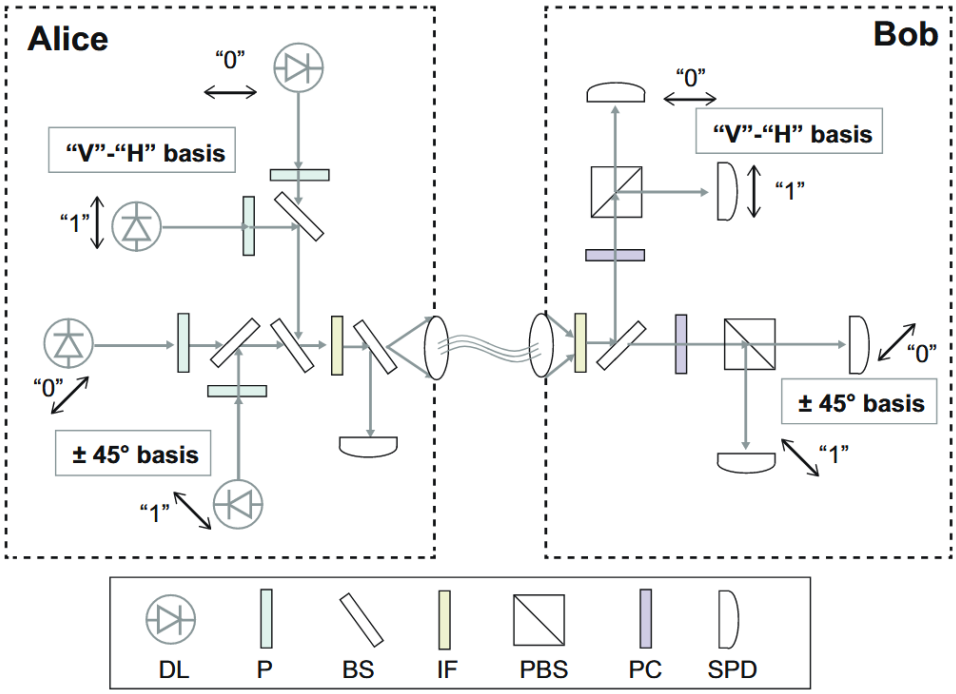


Figure 19: Principle of a BB84 transmitter and receiver. Alice's transmitter is made of four laser sources. The polarization of each beam is set by a linear polarizer, thus encoding BB84 information into the polarization of photons. Afterwards, the data beams are combined by beam splitters, forced through an interference filter to remove spectral information and then sorted by another beam splitter. The rays reflected by the BS are used to monitor laser pulses while the ones transmitted by the BS are sent toward Bob's decoder. There, the photons are randomly separated by a beam splitter, which determines their measurement bases, and their polarization is finally analyzed. If a single detector fires, Bob's records the qubit value for the key. In any other case, a multi-detection event leads to the simultaneous firing of multiple detectors, so the photon is discarded. DL = data laser, P = linear polarizer, BS = beam splitter, IF = interference filter, PBS = polarizing beam splitter, PC = polarization controller and SPD = single-photon detector. This setup was implemented by Hughes et al. [90] and the figure was colorized by Lu et al. [1].

In addition to the green beacon beam sent by the satellite, the ground station sends a red beam toward Micius for system tracking. Over the course of its mission, the satellite established contact with the ground stations for five minutes every day at midnight. During key exchanges the station-to-satellite distance ranged from 645 km to a maximum of 1200 km, while assuring key rates spanning from 12 kbit/s to 1 kbit/s when the distance was maximal. This experiment demonstrated the efficiency that long-distance free-space QKD communications could reach and how they could fix the distance limitations imposed by fiber-based terrestrial networks.

Besides the satellite-to-ground quantum key distribution, Micius also acted as a trusted relay for the exchange of a cryptographic key between the Xinglong ground station in China and the Graz ground station in Austria that are separated by more than 7000 km. The satellite successfully relayed a secure key of 100 kB, which was used to transmit an encrypted picture of Micius and to conduct a secure video conference lasting 75 minutes [91]. This proved the importance of satellites in the development of an intercontinental quantum distribution network.

Satellite-based entanglement distribution and QKD:
A source of polarization-entangled photons was used to demonstrate the two-downlink transmission of photon

pairs simultaneously to two ground stations separated by large distances up to 1200 km. These pairs are generated by a polarization Sagnac interferometer. The Sagnac-based EPS, onboard Micius, is illustrated in Figure 20 and its functioning has been explained in Section 8.

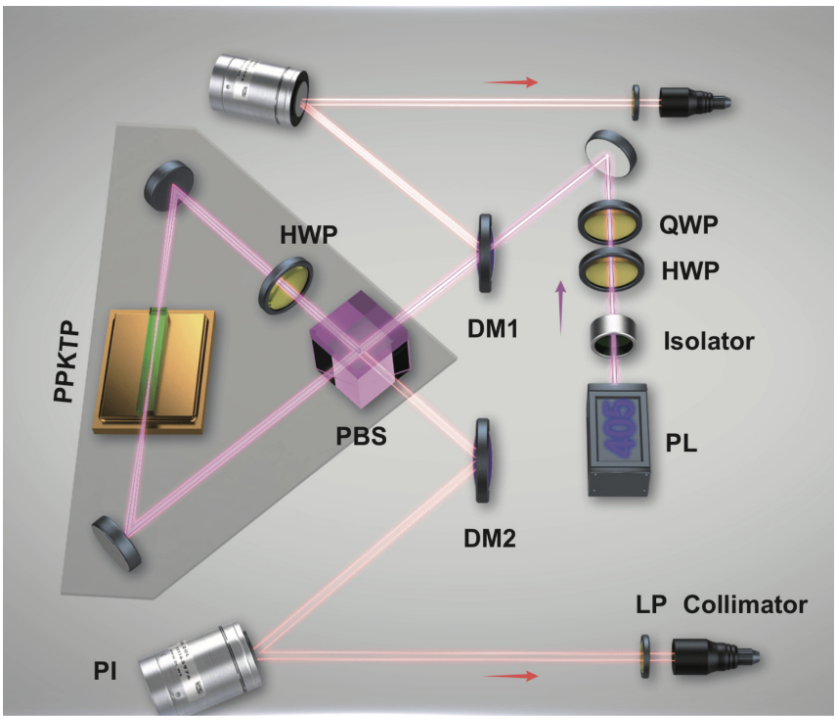


Figure 20: Schematic of the entangled photon source, onboard the Micius satellite. The source uses SPDC, with Type-2 phase-matching in a PPKTP non-linear crystal, to down-convert 405 nm pump photons into 810 nm idler and signal photons. PL = pump laser, HWP = half-waveplate, QWP = quarter-waveplate, DM = dichromatic mirror, PBS = polarizing beam splitter, PI = piezo steering mirror and LP = linear polarizer. Figure from Yin et al. [92].

The satellite distance to the cooperating stations (Delingha, Lijiang and Nanshan in China) varied between 500 and 2000 km. Nonetheless, it reached emissions of almost 6 millions entangled-photon pairs per second. It was computed that, during the 275 s of satellite-ground communications, the efficiency of the two-downlink free-space channel was more than 10 times better than a fiber-based telecommunication channel of the same length [92]. As in the simple QKD payload, the beams of entangled photons are sent simultaneously with reference lasers: an infra-red one for time-synchronization and a green one for tracking. At the ground stations, the photons are analyzed by a succession of optics: a half-waveplate, a polarizing beam splitter and then a Pockels cell (voltage-controlled waveplate). To ensure the photons are still entangled when they reach the ground, their fidelity is verified, and a Bell test is conducted to determine their entanglement quality. The pairs of entangled photons transmitted by Micius reached fidelities of ~ 0.87, while a fidelity of 0.5 is sufficient to conclude to the entanglement of the photons and one of 0.707 indicates a potential violation of Bell's inequality. The Bell tests revealed a violation of the Bell's inequality of ~ 2.37 which shows a great entanglement quality. Indeed, the correlations between two photons are considered quantum in nature when the violation of Bell's inequality surpasses 2 and the entanglement quality is maximal when the violation is 2.83 ($= 2\sqrt{2}$).

Although the entanglement analysis seemed promising, the qubit error rate was too high and the key rate insufficient to perform entanglement-based quantum key distribution. After three years of research, the receiving efficiencies of the Delingha and Nanshan ground stations were improved by using newly built telescopes with improved diameters [93]. This enhanced the key rate while reducing greatly the qubit error rate, thus enabling successful entanglement-based QKD transmissions. Therefore, Micius was able to perform successfully a quantum key exchange with the entanglement-based protocol BBM92, over a distance of 1120 km. The satellite once again demonstrated the significant improvement of performance due to free-space links compared to fiber-based links of the same length, while confirming the conservation of the entanglement of the photons

in satellite-to-ground transmissions.

Ground-to-satellite quantum teleportation:
Micius' third experiment aimed to demonstrate the quantum teleportation of a single photon over distances ranging from 500 to 1400 km. Quantum teleportation refers to the transmission of the state of a particle without transmitting the particle itself. To do so, one photon of an EPR pair is sent to both the emitter (Alice) and the receiver (Bob). Alice then performs a joint measurement, called a Bell state measurement, on the photon from the EPR pair she received and the photon in the state $|\phi\rangle$ that she wants to teleport to Bob. This measurement projects the two photons into one of the four maximally entangled Bell states. This destroys the unknown photon state $|\phi\rangle$ but yields two results she can send classically to Bob. Using Alice's results and the photon he received from the initial EPR pair, which is now collapsed in one of the four Bell states because of its entanglement with Alice's photon, Bob can recreate the unknown photon state $|\phi\rangle$ [1]. Quantum teleportation principle is summarized in Figure 21.

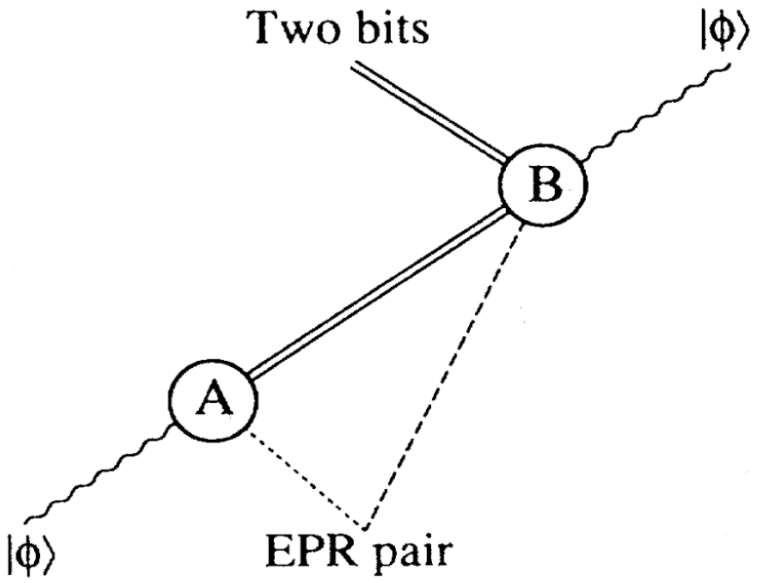


Figure 21: Space-time representation of quantum teleportation, where time increases from the bottom to the top of the figure. Solid line = classical pair of bits, dashed line = EPR pair of particles and wavy line = quantum particle in an unknown state. Figure from Bennett et al. [94].

The first challenge of this experiment, compared to the other ones, was the uplink aspect. Indeed, in uplink transmissions, the turbulence encountered by the beam in the atmosphere occurs at the beginning of its propagation, resulting in beam wandering and broadening. The efficiency of the uplink channel was enhanced by the narrow divergence of the ground station telescope (in Ngari, Tibet) and by the use of a high-bandwidth high-precision APT system[17]at both the transmitter and the receiver to optimize the beam alignment [95]. Moreover, the teleportation of a single photon from the ground to the satellite requires multiphoton interferometry that leads to much lower count rates than simple two-photon experiments.

The ground transmitter for quantum teleportation consists in a highly compact ultrabright four-photon source, which relies on both collinear and non-collinear SPDC to generate multi-photon entanglement. As single-photon detectors are particularly sensitive to spatial radiations, the quantum teleportation detectors on-board Micius are shielded and cooled down to -50°C [1]. The teleportation data showed 911 valid four-photon events detected at the satellite, which led to state fidelities of ~ 0.8, indicating a good entanglement preservation along the uplink channel. Micius appeared as a proof-of-concept by being the first satellite to successfully perform Earth-to-space quantum teleportation. Furthermore, the teleportation was demonstrated over significant large distances.

[17] APT system: Acquisition, Pointing and Tracking

Conclusion:
The Micius mission was planned to last 2 years but, given its success, the satellite realized more QKD experiments until 2021 (5 years after its launch). Even if the QUESS project was a proof-of-concept mission not meant to last over time, it paved the way for space-based quantum key distribution research, with the pioneering experiments it succeeded to conduct. The technologies demonstrated by the satellite showed the feasibility and efficiency of long-distance quantum communications, and offered a potential solution for a global-scale quantum network considering its successful integration in the terrestrial Beijing–Shanghai backbone fiber-based quantum network.

9.2.3 More QKD Satellites

After Micius' success, new QKD satellites emerged to pursue satellite-based quantum communication experiments. Amongst the missions fully dedicated to quantum researches, the following ones can be pointed out:

- SpooQy-1 [96]: Launched in 2019, this Singaporean CubeSat aimed to demonstrate the space-borne generation and detection of polarization-entangled photon pairs. It did not implement proper QKD protocols but its experiments proved the efficiency of photon sources, for entanglement-based QKD, onboard a satellite.

- Jinan-1 [97]: Considered as Micius' successor, Jinan-1 is a Chinese microsatellite which was launched in 2022. It continues to demonstrate long-distance space-to-ground QKD, while putting an emphasis on scaling-up quantum constellations. Indeed, this microsatellite offers diverse advantages for a global-scale quantum network. For example, it weighs less than a sixth of its predecessor weight, making it ideal to be fixed on other space-stations. Moreover, it is capable of exchanging real-time secure keys with portable ground stations. Jinan-1 realized the longest ultra-secure quantum communication, with the intercontinental transmission of images between two ground stations located in China and South Africa, separated by 12 900 km.

- QUBE [77]: This 3-unit German CubeSat was launched in 2024. Its goal is to test two QKD sender modules as well as a quantum random number generator (QRNG). To do so, the satellite is equipped with two quantum payloads (an EPS and a QRNG) and an optical terminal for communication with ground stations. Given QUBE success, a follow-up project -QUBE-II- is planned to be launched in 2025. This 6U-CubeSat will continue to investigate satellite-based QKD performance, as an improved version of QUBE. It will also implement a bidirectional quantum communication channel, while QUBE only implemented downlink transmissions [98].

- Eagle-1 [4]: As part of the European Quantum Communication Infrastructure initiative, the European Space Agency developed, in partnership with many European private companies, the Eagle-1 satellite which is planned for launch in 2025 or early 2026. This satellite will be part of the IRIS^2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) constellation, whose goal is to provide secure communication services to Europe. Eagle-1 will be the first large-scale European QKD satellite and it aims to validate different technologies such as satellite-to-ground quantum transmissions based on decoy-states BB84 protocols and the optical terminal used to communicate with the ground stations.

- QEYSSat [99]: The Quantum Encryption and Science Satellite represents the Canadian effort to participate to a global quantum communication network. Planned for launch in 2026, it will be equipped with both a receiver (Reference Frame Independent Quantum Key Distribution Source of polarization-entangled photons) and a transmitter for QKD.

There exist many more QKD missions that are either already operational or planned for launch. All of these examples show the current craze for quantum secure transmissions, which likely represent the future of global-scale communication.

9.2.4 Current Trends and Challenges

Given the current development speed of QKD technologies, several trends can already be observed. For example, the focus is shifting from individual missions that conduct QKD experiments toward constellations of satellites working together to offer a broader Earth coverage for complete implementations of QKD protocols. Another noticeable trend is the growing number of countries and international agencies that invest in quantum research and in the development of quantum key distribution satellites. All these contributors, led globally by China and closely followed by the EU, are working toward the development of global quantum networks because quantum communication appears to be the most secure option for the near future, where there will be a need of protection against quantum computers.

Despite the amount of ongoing projects of satellites fully dedicated to quantum research or quantum communication demonstration, many challenges remain and solutions are currently being investigated. Several difficulties are linked to the physical transmission of photons between ground stations and the satellites. For instance, atmospheric turbulence can lead to beam wandering, thus deviating the laser beam from the satellite it is pointing toward. Consequently, the pointing precision required to execute QKD might not be achieved, which causes the quantum link to fail. Atmospheric turbulence can also alter a quantum signal through scattering and wavefront distortion. As a result, the weather has a significant effect on quantum communications. Solar noise also greatly affects these transmissions. Its effect depends on the wavelength of the laser used between the ground station and the satellite but operating during the day currently remains difficult overall. The last major challenge faced by present QKD satellites is the persistent need to improve secure key rates, which allows the exchange of longer secure communications. Indeed, increasing these rates is essential for quantum key distribution to become more widespread and accessible, as it enables faster transmission of the communications.

10 Experimental Setup

The current states of entangled photon sources and space-based QKD technologies being introduced, this section presents the experimental work realized in the framework of this project. The experiment is inspired by the EPS onboard the Micius satellite [92] which demonstrated the efficient space application of an entanglement-based QKD protocol over long distances. This work aims to develop a similar efficient and robust polarization-entangled photon source for a potential spatial QKD application. The present section therefore details the experimental setup implemented at CSL, followed by a description of the methodology and an analysis of the results obtained.

The decision to work with a free-space setup, rather than a fiber-based one, was driven by practical considerations. To begin with, CSL's optical experts have a better expertise in free-space optics, facilitating the supervision of this work. Moreover, due to CSL's past experience with free-space experiments, much of the equipment needed to implement the experiment was already available at the company. Finally, even if the generation of entangled photons is often more efficient in fiber-based systems, the Micius satellite demonstrated that a free-space EPS could also achieve high performance. Altogether, these arguments naturally led to the choice of a free-space setup for this experiment.

10.1 Summary of the Experiment

This work aims to develop an entangled photon source, inspired by the one onboard the Micius satellite, for QKD purposes. The goal is to obtain degenerate polarization-entangled photon pairs by pumping a non-linear crystal with near-UV photons, resulting in both the idler and signal photons having a wavelength of 810 nm. To do so, a Sagnac interferometer, which includes a PPKTP crystal able to engender Type-2 collinear SPDC, is implemented. A schematic of the experimental setup is presented in Figure 22. The elements used in the experiment are detailed later, along with the preliminary computations that drove the setup design. Nevertheless, a rapid overview of the experiment is first presented.

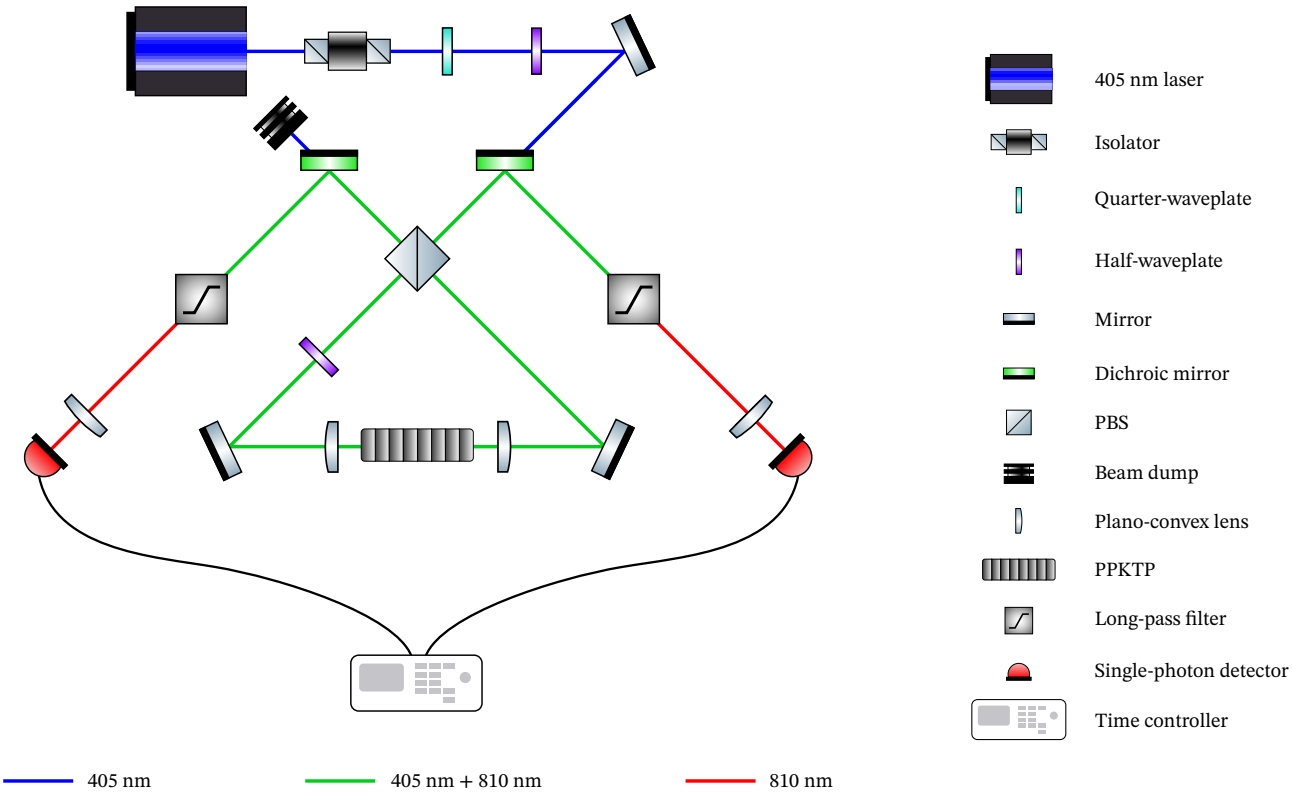


Figure 22: Schematic of the EPS based on a Sagnac interferometer. This setup implemented at CSL was inspired by the EPS onboard the Micius satellite [92].

As explained in Section 8.1, to implement a Sagnac interferometer as an entangled photon source, a polarizing beam splitter must be placed at the interferometer entrance. Moreover, the incoming light should be diagonally polarized for the PBS to split it equally in the two arms of the Sagnac. This ensures an uncertainty on which path the photons followed, later guaranteeing the indistinguishability of the photons spontaneously down-converted by the PPKTP crystal. However, the single-frequency single-mode laser source which is used emits a beam at 405 nm made of vertically polarized photons. Therefore, a quarter-waveplate is first used to ensure the linearity of the light polarization and, then, a half-waveplate rotates the vertical polarization into a diagonal one.

Once the beam reaches the PBS, the polarization state of the diagonally polarized light is equally likely to be collapsed into a horizontal or vertical state. From now on, photons with horizontal and vertical polarizations will be referred to as H and V photons respectively. H photons are transmitted by the PBS and propagate counter-clockwise in the Sagnac loop while V photons are reflected and so rotate clockwise. The non-linear PPKTP crystal, placed at the loop center, is manufactured to spontaneously down-convert V photons with a wavelength of 405 nm into one H and one V photon at 810 nm, with a Type-2 phase-matching condition. Therefore, it needs to be pumped by V photons, so that the polarization of counter-clockwise propagating photons is rotated by a half-waveplate oriented at 45°, located inside the loop. When H photons are incident on a half-waveplate with such orientation, their polarization is rotated to vertical, whereas V photons are transformed into H photons. Figure 23 illustrates the evolution of the polarization of the photons in the Sagnac loop, depending on wether they were transmitted (left diagram) or reflected (right diagram) by the PBS. A plano-convex lens is placed on either side of the non-linear crystal to focus the pump beams inside of it and to collimate[18] the beams of down-converted photons when they exit the PPKTP.

[18] In the context of Gaussian beams, here, "collimated beam" designs the fact that the waist of the beam that passed through the lens is located far from the region of interest. Therefore, the radius of the beam is relatively constant in the loop, resembling a collimated beam in geometric optic.

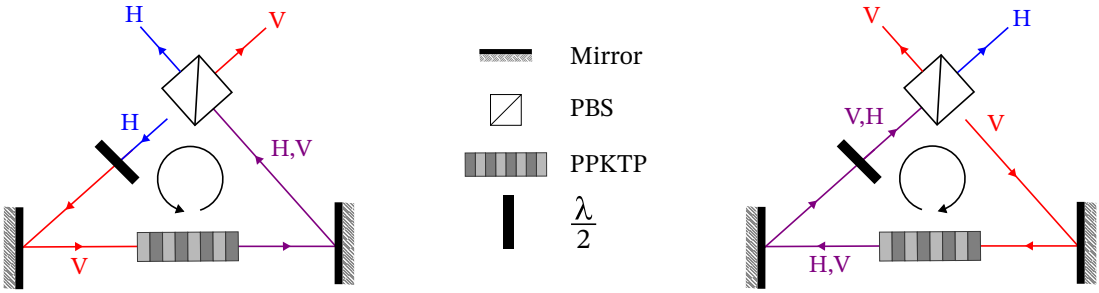


Figure 23: Schematic representations of the photons polarization and propagation direction inside the loop -after being sorted by the PBS- and at the interferometer output. Left diagram: counter-clockwise propagating photons, once they have been transmitted by the PBS. Right diagram: clockwise propagating photons, once they have been reflected by the PBS. H (blue) = horizontally polarized photons, V (red) = vertically polarized photons, purple = presence of both horizontally and vertically polarized photons, $\frac{\lambda}{2}$ = half-waveplate.

As SPDC is an inefficient process, both 405 nm pump photons and down-converted 810 nm photons are traveling in the Sagnac loop but the pump photons need to be filtered out before detection. For that reason, a first filtering is effectuated by dichroic mirrors (DM) aligned with the output ports of the PBS, as shown in Figure 22. These DMs transmit a great part of 405 nm photons and reflect the 810 nm ones, while also reflecting a residual part of the 405 nm beam. Because 405 nm photons are transmitted back toward the laser source by one DM at this point of the experiment, an isolator is placed in front of the source to protect it. The propagation of the higher-energy photons transmitted by the other DM is stopped by a beam dump. As the lower-energy photons reflected by the dichroic mirrors are still mixed with 405 nm photons, long-pass filters are used to isolate the 810 nm photons.

The final stage of the experiment is composed of two single-photon detectors, connected to a time controller which allows to highlight the correlations between the counts registered by both detectors. Converging lenses are placed in front of the detectors to focus the laser beams on their sensor areas. The ability of the EPS to produce polarization-entangled photons will later be demonstrated by measuring coincidences at the detectors between photons produced simultaneously via SPDC. These coincidences will lead to a Bell test which will evaluate the entanglement quality of the photons.

10.2 Optical Components

The experiment and its goal being introduced, this section now describes the optical elements used in the setup, detailing their specifications and function. The alignment procedure is also presented, along with the preliminary computations made to design the experiment while ensuring proper alignment, phase-matching condition, and good performance of the source.

The optical elements presented below are listed in Appendix A, along with their references.

10.2.1 Support Structure

The entire experiment is mounted on a honeycomb optical breadboard, itself fixed on an optical table. These are composed of a steel honeycomb core which is sandwiched between two thin steel layers, pierced by regularly spaced mounting holes. This configuration provides mechanical and thermal stability, ease of alignment and vibration isolation. Additionally, the breadboard allows for transportation of the setup, should the need to displace it occur. All the optical components are mounted on its flat surface, serving as a planar guide parallel to which the laser beam is intended to propagate. The grid pattern of the mounting holes facilitates the planning of the experiment layout as well as the alignment of the optics. The honeycomb cores, as well as the legs of the table, dampen vibrations, thus isolating the experiment from external perturbations. Moreover, the structure and choice of material of both elements offer great thermal stability, which is a key feature when dealing with precise alignment. This mounting approach was chosen to minimize the risk of misalignment induced by accidental motions, ensuring a safe and user-friendly environment when working around the setup.

10.2.2 Laser Source

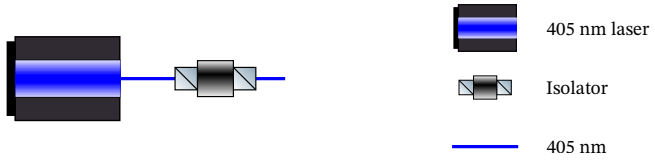


Figure 24: Close-up of the laser source area of Figure 22.

The laser source used in this experiment consists of a diode laser module emitting a continuous single-mode single-frequency laser beam at 405 nm [100]. It was chosen to work with a pump laser at 405 nm due to the general good efficiency of detectors at that wavelength and to the availability of such lasers [101]. Additionally, 405 nm is the wavelength used in the EPS onboard the Micius satellite, which has been demonstrated to work efficiently. The laser module was selected for its tunable low output powers, which enable a safe and adjustable manipulation, for its narrow linewidth and long coherence length. Indeed, a narrow linewidth implies that a small range of wavelengths impinge on the non-linear crystal, resulting in a restricted set of wavelength-triplets that fulfill the quasi-phase-matching condition. This provides a great control and precision of the frequency of the down-converted photons. The narrow spectral width of the laser source provides it with a high coherence length due to their inverse relationship. In a Sagnac interferometer, the laser coherence length must be large enough for the counter-propagating photons to recombine coherently at the PBS, after traveling the Sagnac loop. Furthermore, the coherence length of the pump should be longer than the non-linear crystal length to ensure the efficient generation of entangled photon pairs. As SPDC occurs randomly along the crystal, insufficient coherence could introduce information about the temporality of the down-conversion of the photons [102]. This would lead to a distinguishability of the photon wavepackets inside the crystal and therefore to a weakening of their entanglement.

The choice of a continuous wave laser was influenced by the EPS onboard the Micius satellite. Nevertheless, it offers some advantages over a pulsed laser. Indeed, continuous-wave lasers are usually safer for the optics than pulsed lasers, which can present high peak powers. The laser output powers being low, it is not necessary to verify the power densities it reaches at the optical elements, as their damage thresholds are not exceeded. Moreover, since the pump beam is a continuous-wave, the noise due to residual 405 nm photons is also continuous at the detection. This enhances the readability of the results displayed in Section 10.4 and the distinguishability of the down-converted photon pairs from the pump noise.

The temperature of the laser source is controlled and maintained by a heat sink to ensure the stability of the output powers. Another characteristic of the laser is its Gaussian aspect which is described by different parameters: waist, Rayleigh range, half-divergence angle and quality factor. These allow to understand how the laser beam behaves when interacting with optical elements and how it propagates and diverges throughout the experiment. The specifications of the laser source relevant to this work are summarized in Table 3.

Specification	**Value**
Output power range [mW]	$1 - 40$
Central wavelength [nm]	405
Linewidth [pm]	0.4
Coherence length [m]	~ 1
Beam waist [mm]	0.2 ± 0.05
Half-divergence angle [mrad]	< 1.1
Beam quality	≤ 1.8

Table 3: Specifications of the laser source: model OBIS 405 nm LX 40 mW SF from Coherent [100].

The last important feature of the laser source for the experiment is the polarization of the emitted beam. It should be vertical, with an accuracy of ±5°. Moreover, the beam has a minimum polarization ratio of 100 to 1, meaning that the intensity of the vertical component of the polarization is at least 100 times larger than the intensity of the horizontal component. This shows a good linearity of the polarization.

It was mentioned earlier that, when the light beams are separated by the dichroic mirrors at the output of the Sagnac loop, a portion of the 405 nm rays are transmitted back toward the laser source. To prevent damage to the laser, an isolator designed for 405 nm light is placed in front of the laser module. Thanks to the polarization of the photons, it transmits most of the light emitted by the laser while significantly attenuating any light back-reflected toward the source. The isolator employed in this experiment consists of a Faraday rotator located between two linear polarizers. As depicted in Figure 25, in forward mode, the laser beam first passes through a vertical linear polarizer, then its polarization is rotated by 45° by the Faraday rotator, and it finally exits the isolator through a second linear polarizer oriented at 45°. Therefore, the entrance polarizer is aligned with the polarization of the light emitted by the laser source of the experiment to maximize transmission of the laser output in the forward direction. However, in reverse mode, the light is polarized at 45° by a first polarizer. Then, its polarization undergoes a rotation of 45° in the Faraday rotator, resulting in horizontally polarized light. These rays are then blocked by the second polarizer (vertical) due to the orthogonality of their polarization with the polarizer optical axis.

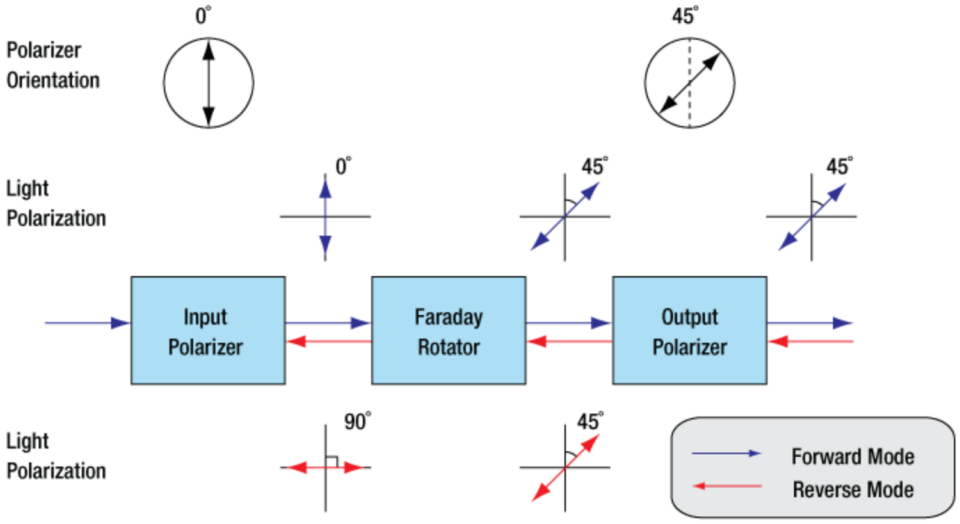


Figure 25: Principle of an optical isolator composed of two linear polarizers and one Faraday rotator. Figure from the Thorlabs website [103].

10.2.3 Waveplates

Figure 26: Close-up of the waveplates area of Figure 22.

Waveplates, also called phase retarders, are used to modify light polarization without decreasing its intensity. These are made of birefringent materials that impose a phase shift between the orthogonal light components as they travel along the fast and slow axes of the crystal. The phase delay introduced by the waveplate depends on the thickness of the material. Indeed, a quarter-waveplate introduces a phase shift of $\frac{\pi}{2}$. This transforms circular and elliptical polarizations of the photons into linear ones and inversely. On the other hand, a half-waveplate, which is usually thicker than a quarter-waveplate, introduces a phase shift of π. Therefore, if the polarization of the photons makes an angle θ with the fast axis of the half-waveplate, it will be symmetrically rotated, resulting

in a polarization oriented at $-\theta$ w.r.t. the waveplate fast axis. Noting θ the angle between a photon linear polarization and the fast axis of a waveplate it is incident on, the transformations introduced by quarter- and half-waveplates can be summarized as follows:

Waveplate type	Input polarization	Output polarization
Quarter-waveplate	Linear, $\theta = 45°$	Right circular
	Linear, $\theta = -45°$	Left circular
	Linear, $\theta \neq \pm 45°$	Elliptical
Half-waveplate	Linear, θ	Linear, $-\theta$
	Left circular	Right circular

Table 4: Summary of the effects of quarter- and half-waveplates on the polarizations of input photons. Input-output relations are reversible. Table from the Newport website [104].

The laser source emits a vertically polarized beam while a diagonal polarization is needed to enter the Sagnac loop. Thereby, a half-waveplate is positioned after the isolator to rotate the orientation of the light polarization. Without the presence of the isolator, its fast axis should theoretically make a 22.5° angle with the vertical direction. Nonetheless, since there is an uncertainty of ±5° on the orientation of the laser beam polarization and since the isolator already rotates this polarization, the half-waveplate exact orientation is determined experimentally. To do so, a linear polarizer oriented at 45° away from the vertical direction is placed behind the waveplate and the light power is subsequently measured with a photodiode. The half-waveplate is then gradually rotated until the light intensity measured after passing through the 45° polarizer is maximal.

Additionally, the polarization of the beam emitted by the laser source is supposed to be linear but, as no device is perfect, it could present a slight ellipticity. Consequently, a quarter-waveplate is placed in front of the half-waveplate to ensure a good linearity of the polarization of the photons. As the exact ellipticity of the laser polarization is not known beforehand, the orientation of the quarter-waveplate must also be asserted experimentally. The same approach as for the half-waveplate is applied: a linear polarizer oriented diagonally is placed behind both waveplates. The quarter-waveplate is then rotated gradually until the intensity of the light measured after the polarizer is maximal.

10.2.4 Sagnac Loop

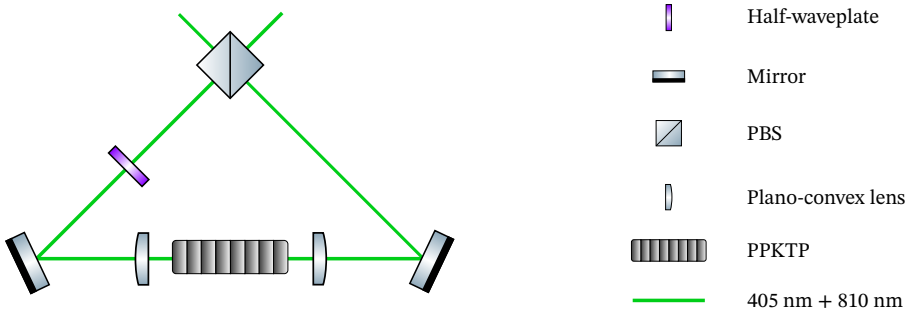


Figure 27: Close-up of the Sagnac loop area of Figure 22.

The point of using a Sagnac interferometer to generate polarization-entangled photon pairs has been presented in Section 8.1. Photons down-converted by Type-2 SPDC have orthogonal polarizations. The fact that these photons are propagating in both directions within the loop therefore allows to introduce an uncertainty on their polarization once they exit the interferometer.

A PPKTP crystal is used to spontaneously down-convert V photons into one V and one H photon, through Type-2 SPDC. The goal of this experiment is to produce perfectly indistinguishable idler and signal photons, as much in their positions within the interferometer as in their polarizations. Therefore, the SPDC collinearity (superimposition of the pump, idler and signal photons) and degeneracy (idler and signal photons have the same energy) are wanted. The employed crystal is manufactured such that, when pumped by a laser beam orthogonal to its entrance face, the angle between the beam linear polarization and the crystal optic axis leads to a collinear configuration (see Section 6.3). Furthermore, degeneracy means that the down-converted photons are wanted to share a common wavelength which, for a reason of energy conservation (see Equation 9), corresponds to twice the pump wavelength.

Depending on the length of the domains of the periodically poled crystal, different wavelength triplets (λ_{pump}, λ_{idler} and λ_{signal}) can satisfy the quasi-phase-matching condition (Eq. 14). The triplets that do not fulfill this condition may be created within the crystal but these most likely vanish through destructive interferences before they exit the PPKTP, due to its periodic structure. Therefore, through thermal expansion, the length of the poled domains is tuned to create degenerate photon pairs. The relation between PPKTP temperature and the wavelengths of the photon pairs created by Type-2 SPDC is specified by the manufacturer of the crystal (Svenska LaserFabriken [105]) and is shown in Figure 28.

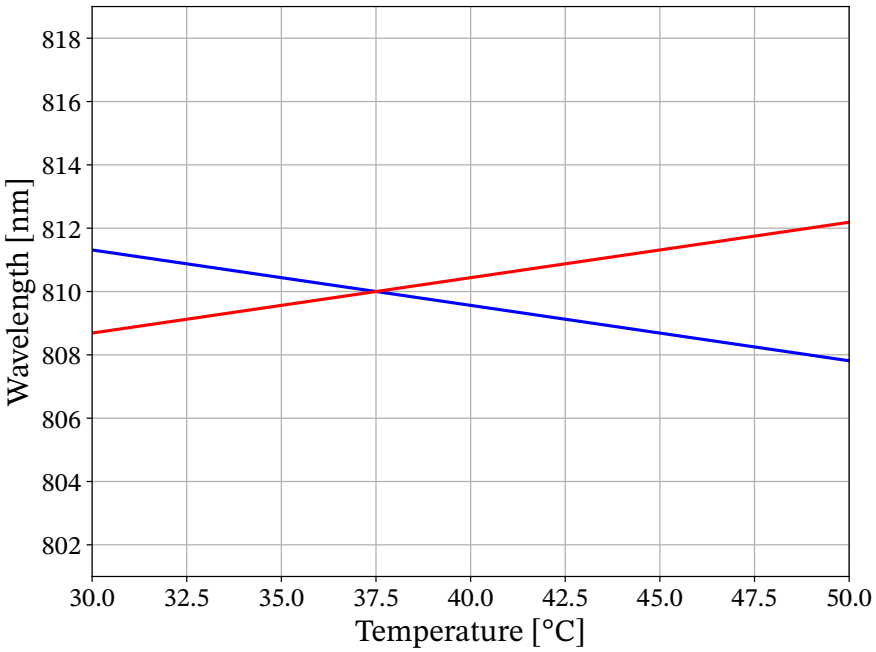


Figure 28: Tuning curve of a PPKTP non-linear crystal pumped with a 405 nm laser beam. It relates the temperature of the crystal to the wavelength of the photons generated through Type-2 SPDC. Each curve represents the behavior of one of the down-converted photons. For example, the red curve can be attributed to the idler photon and the blue one to the signal photon or inversely. Figure adapted from a document obtained via personal communication with the crystal manufacturer, Svenska LaserFabriken [105].

The temperature of the crystal is controlled by a copper heater through conduction, with an accuracy of ±0.1°C. As can be seen in Figure 28, the crystal needs to be maintained at a 37.5°C temperature in order to generate idler and signal photons at the degenerate wavelength of 810 nm. At this temperature, the PPKTP periodically poled domains are $\sim$ 5 μm long, which corresponds to the poling periodicity of Λ = 9.96 μm. This value is now used to determine the orientation of the crystal optic axis, which was not provided by the manufacturer.

To do so, the refractive indices of the pump, idler and signal photons are first expressed as a function of the angle θ, which is formed by their collinear propagation direction and the optic axis of the crystal. This expression is then employed to determine θ. The refractive index of a wave propagating along the extra-ordinary or the

ordinary axis of the PPKTP crystal is denoted by n_e or n_o respectively. These indices depend on the wavelength of the photons and are given by the Sellmeier equation (see Eq. 11). Accounting for PPKTP coefficients in the Sellmeier equation [106], this yields:

$$n_e^2 = 4.59423 + \frac{0.06206}{\lambda^2 - 0.04763} + \frac{110.80672}{\lambda^2 - 86.12171},$$
$$n_o^2 = 3.45018 + \frac{0.04341}{\lambda^2 - 0.04597} + \frac{16.98825}{\lambda^2 - 39.43799}.$$

These relations assume a wave propagation inside the crystal at 20°C. As the PPKTP used in this experiment is maintained at 37.5°C, the formulas need to be adapted using the following temperature-induced variation of the refractive indices [107]:

$$\Delta n(\lambda, T) = n_1(\lambda)(T - 25°C) + n_2(\lambda)(T - 25°C)^2,$$

where n_1 and n_2 are computed based on the KTP temperature-dependence coefficients provided by Emanueli and Arie [107]. This yields the refractive indices of waves propagating along the extra-ordinary and ordinary axes of the crystal, at both 405 nm and 810 nm. With Type-2 SPDC, the polarization of the pump and signal photons have a certain angle w.r.t. the extra-ordinary axis of the crystal while the idler photon polarization is parallel to its ordinary axis. Therefore, their refractive indices (n_p, n_s and n_i) are deduced, considering their respective wavelengths and the orientation of their polarizations w.r.t. the optic axis of the crystal. These are given by the following equations [31]:

$$n_p = \sqrt{\frac{n_e^2 n_o^2}{n_e^2 \cos^2\theta + n_o^2 \sin^2\theta}} \quad \text{with } \lambda = 405 \text{ nm}, \tag{19}$$

$$n_s = \sqrt{\frac{n_e^2 n_o^2}{n_e^2 \cos^2\theta + n_o^2 \sin^2\theta}} \quad \text{with } \lambda = 810 \text{ nm}, \tag{20}$$

$$n_i = n_o \quad \text{with } \lambda = 810 \text{ nm}. \tag{21}$$

Now, knowing the poling period Λ of the crystal, the previous results are injected in the quasi-phase-matching condition (Eq. 14) to determine the angle θ:

$$\frac{2\pi}{\Lambda} = k_p - k_s - k_i \quad \Leftrightarrow \frac{2\pi}{\Lambda} = \frac{2\pi\, n_p(\theta)}{\lambda_p} - \frac{2\pi\, n_s(\theta)}{\lambda_s} - \frac{2\pi\, n_i}{\lambda_i}.$$

Accounting for the values of different parameters ($\Lambda = 9.96\ \mu$m, $\lambda_p = 0.405\ \mu$m, $\lambda_s = \lambda_i = 0.810\ \mu$m), the angle formed by the propagation direction of the photons and the optic axis of the PPKTP crystal is computed:

$$\theta = 74.367°.$$

Coming back to Equations 19, 20 and 21, the refractive indices of the different waves are finally computed:

$$n_p = 1.74, \tag{22}$$
$$n_s = 1.64, \tag{23}$$
$$n_i = 1.76. \tag{24}$$

To ensure a safe manipulation of the crystal, the PPKTP is embedded in an inert substrate, making it stiffer and more resistant to shocks. The substrate embedding configuration, along with the dimensions of the crystal used in this experiment, are presented in Figure 29.

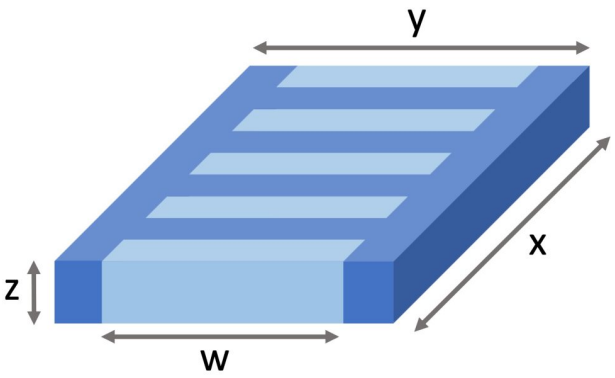


Figure 29: Embedding of the PPKTP crystal (light blue) in an inert substrate (dark blue). w = 3 mm, x = 30 mm, y = 6 mm and z = 1 mm. Figure from the Svenska LaserFabriken website [105].

A long crystal has been chosen to maximize the generation rate of photon pairs and the wavelength purity of the down-converted photons. Moreover, the width of the PPKTP is large enough to facilitate the focus of the laser beams within the crystal. Because it needs to be pumped from both directions in the Sagnac loop, the crystal is sandwiched between two plano-convex lenses, positioned symmetrically around it to focus the beams inside of it. The choice of the focal length of the converging lenses is limited by the spatial disposition of the experiment. Indeed, the more the beam is focused, the better, as it increases the SPDC efficiency but the focal length of the lenses should not be too short to enable the positioning of the crystal and its heater (43 mm long) between the lenses. Moreover, the focal length of the lenses should not be too large because, as will be explained later, the lenses are placed in the interferometer after the base elements (the PBS and the two mirrors) are installed. Therefore, their spacing is limited by the optics already mounted in the setup. Finally, one has to keep in mind that focusing too much the beams leads to a low interaction length with the crystal. There is thus a compromise to make between the power density and the interaction length of the beam waist with the PPKTP.

Opting for a focal length of 5 cm enables a high power density in the crystal[19] and allows the lenses to fit between the positioned mirrors while being spaced enough to leave room for the crystal and its heater. The counter-propagating beams are focused to have their waists at the crystal center to obtain the maximal conversion rate [108]. The crystal is itself located at the center of the Sagnac loop in order to maintain the symmetry of the interferometer. Due to the Gaussian nature of the laser, the new waists of the beams are not located at exact focal length from the plano-convex lenses. Therefore, the evolution of the laser beam radius throughout the experiment is computed to select the optimal position of the lenses. To do so, Equation 15, which gives the radius ω of a Gaussian beam as a function of the distance z to its waist ω_0, is employed. The positions of the lenses are numerically adjusted through trials and errors until the new waists of the beams are located at the exact center of the Sagnac interferometer. Considering that the waist of the beam emitted by the laser source is located at z = 0 (the output of the laser module), the radius of the Gaussian beam as well as the power density resulting from its spot size are computed at different locations and summarized in Table 5 on the following page. This also allows to verify that the focus leads to a power density inside the crystal sufficient for efficient SPDC.

It can be seen in Table 5 that the position of the first lens encountered by the beam is more than 5 cm away from the crystal center, meaning that the focus of the rays occurs slightly behind the focus point of the lens. This table also shows that the tight focus of the beam in the middle of the Sagnac loop gives a high value of the power density. This leads to strong non-linear interactions and so to a high generation rate of photon pairs at the waist of the beam in the crystal. The final point this table highlights is that, when it enters the PPKTP, the laser beam has a diameter of 0.52 mm (radius of 0.26 mm), which is smaller than the crystal thickness of 1 mm. As a result, no part of the beam is lost at the crystal entrance, thus preserving its full intensity when penetrating it.

[19]The damage threshold of the PPKTP crystal has not been specified by the manufacturer but it was assured that the power density range browsed for this experiment would not lead to deterioration of the crystal.

Optical element	**Distance to the initial waist z [cm]**	**Beam radius ω [mm]**	**Power density ρ [W/cm^2]**
Laser output	0	0.2	31.83
PBS	65	0.78	1.51
Converging lens	80.94	0.96	0.97
Crystal entrance	84.75	0.26	13.34
Crystal center	86.25	0.013	5537.06

Table 5: Evolution of the laser beam radius and its power density, depending on the distance to the initial waist located at the laser output. The power densities are computed considering a maximal initial intensity of 40 mW at the laser output and accounting for the attenuation of the beam power when it passes through different optical elements. These values have been verified and confirmed by the *Gaussian beam* software [109].

The waist shift of the beam caused by the interface between air and the PPKTP crystal is now computed to verify the positioning of the two lenses. Based on the waist shift formulas presented in Section 7.4 and on the refractive indices previously computed, the shift is determined. The configuration of the beams entering the crystal corresponds to the scenario illustrated at the bottom of Figure 14, because of the focusing imposed by the converging lenses. First, considering the position of the lenses that focus the beam at the center of the crystal ($z_1 = -15$ mm), the waist shift is computed as:

$$(\Delta z)_b = \left(\frac{n_p}{n_{air}} - 1\right) \cdot |z_1| = 11.10 \text{ mm},$$

where $n_p = 1.75$ (Eq. 22) is the refractive index of the pump wave in the PPKTP crystal and $n_{air} = 1$ is the refractive index of air. This shows that the waist shift causes the beam waist to be located away from the crystal center. An iterative procedure is thereby implemented to determine the optimal position of the lenses. This position ideally aligns the beam waist with the crystal center, ensuring a compensation of the waist shift. This is achieved by iterating on the z_1 value until the following condition is satisfied:

$$|z_1| + (\Delta z)_b = 15 \text{ mm}.$$

15 mm corresponds to the distance between the first air-PPKTP interface met by the beam and the crystal center, which is half of the crystal length. The iterative optimization yields:

$$z_1 = -8.62 \text{ mm} \quad \text{and} \quad (\Delta z)_b = 6.38 \text{ mm}. \tag{25}$$

As a result, the converging lenses must be positioned closer to the mirrors in the Sagnac loop than what was computed, such that the cumulation of their focusing and the waist shift results in the beam waist being located at the crystal center, which corresponds to the center of the loop.

The choice of using two converging lenses within the Sagnac loop rather than a single lens outside the interferometer, like in the Micius satellite EPS, is the result of a comparative study. A third option consisting in two parabolic mirrors located inside the loop rather than using simple mirrors and converging lenses was also considered. The pros and cons of each solution are listed below:

- 2 parabolic mirrors in the loop:
  - Advantages: Using two parabolic mirrors rather than one or two lenses with planar mirrors allows to use less optics, making the setup simpler. They also provide a strong focus of the laser beams, which is needed to enable efficient SPDC. As parabolic mirrors are reflective optics, they are inherently achromatic, meaning they do not suffer from chromatic aberrations when reflecting both 405 nm

and 810 nm rays. Lastly, they "collimate" -still in a Gaussian interpretation- the rays propagating away from the crystal. This facilitates beam handling throughout the experiment as narrower beams are easier to align through optical elements and reduce the risk of partial obstruction.

  - Disadvantages: Parabolic mirrors require extremely precise alignment and complicate the mathematics of initial design computations. Moreover, their focal length imposes the size of the Sagnac loop, thus restricting the flexibility of the setup. As a strong focus of the beams is needed on a relatively short distance, the focal length of the mirrors must be small, leading to a small curvature radius. These types of parabolic mirrors are more difficult to manufacture, and thus to procure, than longer focal length mirrors.

- 1 converging lens outside the loop with 2 planar mirrors in the loop:

  - Advantages: Using only one converging lens simplifies the design computations with respect to parabolic mirrors. Placing it in front of the first dichroic mirror encountered by the rays avoids chromatic aberrations. Indeed, at this point in the setup, only pump rays are present. This avoids issues linked to the simultaneous use at both 405 nm and 810 nm of the optics. Finally, converging lenses adapted to one wavelength in particular, with large focal length, are easily found and procured.
  - Disadvantages: Even if the computations are simplified, using one lens along with two planar mirrors complicates the setup as three optics are needed. Because the lens is positioned outside of the interferometer, where the focus is required, its focal length must be quite large. This results in a weaker focus compared to what would have been achieved with parabolic mirrors or a pair of converging lenses. Furthermore, relevant rays only pass once through the lens. Hence, the beams diverge from their focus in the crystal until they reach the detectors, making them more complicated to handle.

- 2 converging lenses and 2 planar mirrors in the loop:

  - Advantages: Dealing with only planar mirrors and converging lenses leads to simple design computations. Additionally, the use of converging lenses within the Sagnac loop allows for a stronger focus compared to configurations with parabolic mirrors or a single lens. It also simplifies alignment as the lens pair does not affect the setup dimensions. Because they are positioned at one of the final steps of the interferometer alignment, the lenses are easy to adjust or replace if needed. Finally, similar to the 2 parabolic mirrors configuration, the pair of converging lenses "collimates" the beams before they exit the Sagnac loop, which facilitates their handling.
  - Disadvantages: This configuration has the largest number of optics, which complicates the setup and takes up more space. Moreover, as they are located within the Sagnac loop, the lenses are crossed by both 405 nm and 810 nm photons. This might lead to chromatic aberrations.

The key features considered to assess the optimal configuration are a strong focus and an ease of alignment. This naturally led to the choice of a pair of converging lenses located in the Sagnac interferometer along with planar mirrors, which provides both searched characteristics.

Attention is now directed toward the propagation of photons inside the Sagnac loop. Diagonally polarized photons, with a wavelength of 405 nm, enter the PBS by the top right port of Figure 27. H photons are transmitted to the left of the setup while V photons are reflected to the right. V photons, therefore propagating in a clockwise direction, are focused inside the PPKTP crystal by a first plano-convex converging lens. Once down-converted, the idler and signal photons exit the non-linear crystal and the beams are collimated by a second plano-convex lens. Afterwards, the down-converted 810 nm photons as well as the residual 405 nm ones pass through a dual-wavelength half-waveplate (optimized for both 405 nm and 810 nm photons) whose fast axis is oriented at 45° away from the vertical direction. This rotates the vertical polarization of pump photons to a horizontal one and it simply inverses the idler and signal polarizations. The PBS finally separates the idler and signal photons when they reach the exit of the interferometer, which remained collinear until then.

When looking at pump photons propagating in the opposite direction -the counter-clockwise one-, the half-waveplate offers a key feature. Indeed, the PPKTP crystal is manufactured to be pumped by V photons. Hence,

the H photons that enter the loop have to be transformed into V photons for an efficient Type-2 SPDC to occur. The half-waveplate with a diagonal fast axis implements this rotation, resulting in V photons being focused in the crystal, down-converted, collimated and then split at the PBS like the clockwise propagating ones. This polarization rotation needs to be highly precise. If the pump photons are not perfectly vertically polarized upon entering the PPKTP, the crystal birefringence can alter their polarization state, reducing the down-conversion rate. To avoid such distortion, it is important that the pump photons enter the crystal with a linear vertical polarization. This also highlights the importance of the quarter-waveplate placed at the beginning of the setup because, if the polarization of the pump photons is only slightly elliptical, the birefringence of the crystal introduces a phase-mismatch between the orthogonal components of the light polarization. As the beam propagates in the crystal, the polarization then becomes more elliptical, resulting in an inefficient down-conversion.

In addition to flipping the polarization of pump photons, the half-waveplate serves another purpose. Indeed, because of the birefringence of the PPKTP material, horizontally and vertically polarized photons do not propagate at the same velocity in the crystal: H photons travel slightly faster. This results in a temporal walk-off between two photons of a pair. If the down-converted photons do not pass through the half-waveplate after being generated, H photons exit the Sagnac loop before V photons, whatever the PBS port they exit by. Consequently, this could leak information about the polarization of the photons to an eavesdropper as they would not need to measure it to acquire knowledge about it. The half-waveplate thus inverts, in one propagating direction, the phase mismatch imposed by the birefringent crystal, such that down-converted H and V photons are superimposed at both output ports of the PBS. This principle of phase inversion is well illustrated by Meraner's diagram [110], shown in Figure 30. It can be seen that, even if photons are superimposed at one output port of the PBS, photons going toward the bottom of Figure 30c are in advance with respect to the ones propagating to the right of the figure. In fact, in the clockwise direction, the H photon of an entangled pair is in front of the V one and it is transmitted by the PBS. On the other hand, in the counter-clockwise direction, the V photon is in front of the horizontally polarized one and it is reflected toward the bottom of the figure by the PBS, such that both "in advance" photons exit the Sagnac loop by the same port of the PBS.

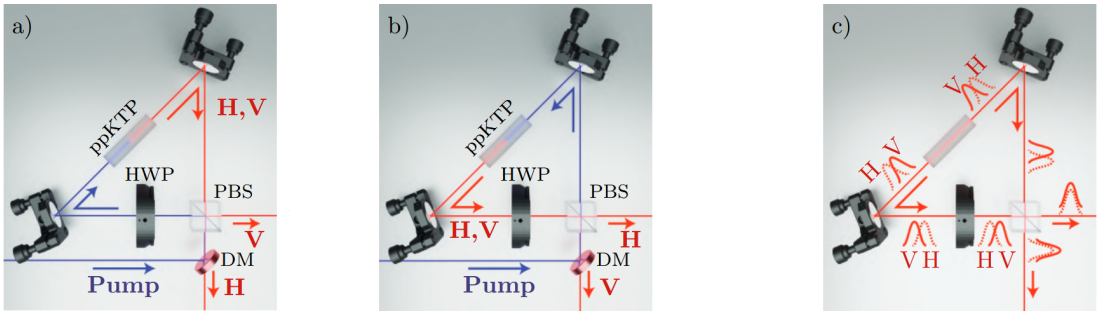


Figure 30: Representation of a Sagnac interferometer which comprises a PPKTP crystal for collinear Type-2 SPDC. Two cases of propagations inside the loop are represented: the clockwise (a) and then the counter-clockwise (b) one. Figure (c) shows the inversion of the temporal walk-off between H and V photons by the half-waveplate (HWP). A dichroic mirror (DM) is used to separate the pump from the down-converted photons outside the interferometer. Figure from Meraner et al. [110].

Aligning the Sagnac interferometer represents the most tedious part of the experiment, as high precision is needed. Indeed, the counter-propagating beams need to superimpose exactly to ensure perfect indistinguishability of their paths and a coherent recombination at the PBS. To facilitate the alignment of the experiment, the laser beam emitted by the source is directed parallel to the grid of mounting holes on the optical breadboard. This makes it easier to impose 45° and 90° angles between the rays incident on, and the rays reflected or transmitted by, the optics. The light rays are also wanted to remain parallel to the breadboard throughout the experiment such that it is easier to impinge perpendicularly on certain optics. A first mirror reflects the beam exiting the laser module toward the Sagnac loop (see Figure 31). A dichroic mirror, whose role will be detailed later, is already mounted in the experiment at this step of the alignment because it can introduce unwanted reflections and refractions that need to be accounted for during the Sagnac interferometer alignment. Diaphragms calibrated to the height of the laser source are placed as depicted in Figure 31 to determine the optimal orientation of the first mirror and the polarizing beam splitter cube. These also ensure a propagation of the laser beams parallel

to the breadboard. The optimal orientation of the PBS corresponds to a 90° angle between the rays it transmits and the ones it reflects. This results in a perfect overlap of the beams entering and exiting the cube.

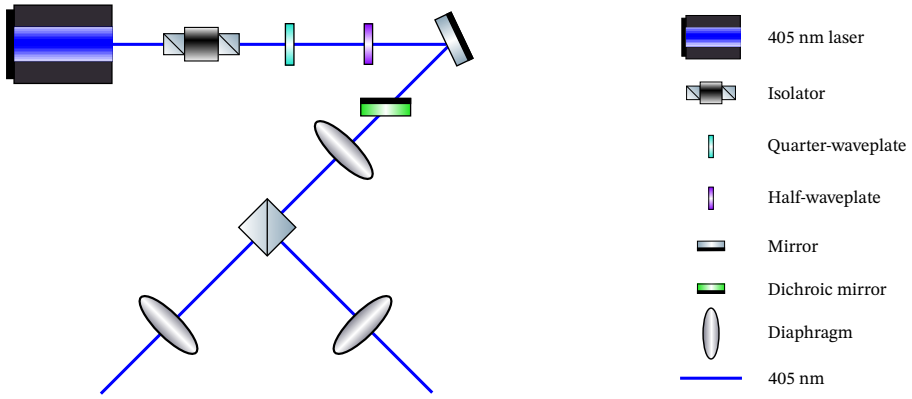


Figure 31: Representation of the experimental setup during alignment of the polarizing beam splitter cube.

The PBS is placed on a 3-axis adjustable platform and all the mirrors used are mounted on kinematic mounts. Once the cube position is fixed, two mirrors with coatings adapted to both 405 and 810 nm are positioned to close the triangular Sagnac loop. They occupy symmetric positions within the interferometer, thus outlining identical arms. The distance between the mirrors is arbitrary set so as to minimize the interferometer surface for a good alignment stability, while ensuring a practical disposition of the optics. They are oriented such that counter-propagating beams perfectly coincide while keeping the rays parallel to the optical table. This is once again verified using diaphragms. The alignment of the mirrors based on the superimposition of the beam spots is challenging to perform with the naked eye due to the small diameters of the beams. A linear polarizer oriented at 45° is thereby placed at the output of the interferometer to reveal a fringe pattern. Indeed, both horizontally and vertically polarized 405 nm photons exit the PBS. The polarizer is therefore used to effectively combine them. The resulting fringes serve as a proxy to verify the overlap of the beams: if they coincide perfectly, no fringe should appear in the central lobe of the beam. A temporary mirror and concave lens are used to project this pattern on a white screen. The alignment setup is as presented in the following figure.

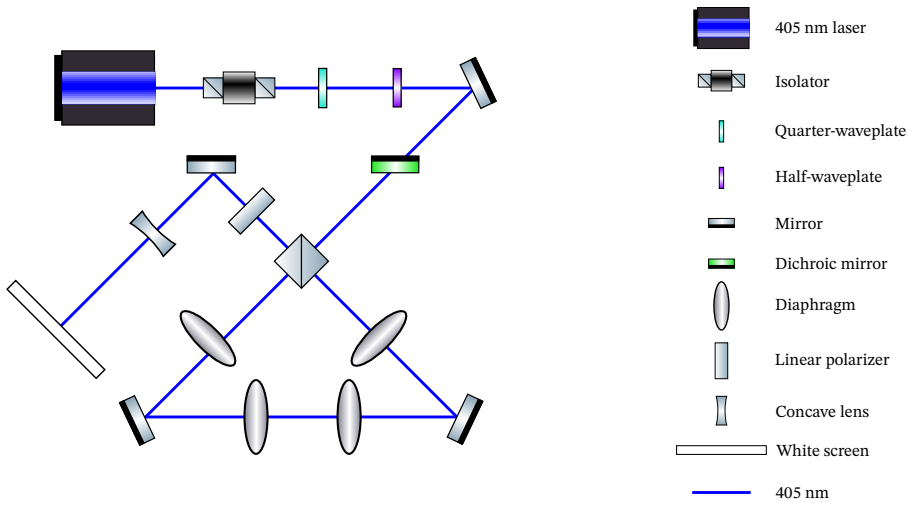


Figure 32: Representation of the experimental setup during alignment of the mirrors inside the Sagnac loop based on fringes pattern.

At this stage of the alignment, the optical elements already set in place (the PBS and the mirrors) are not moved anymore. Once the triangular loop is formed and aligned, the two converging lenses that focus the light rays at the crystal center are introduced in the interferometer. Their positions within the loop are computed numerically (see Tab. 5 and Eq. 25) and adjusted experimentally for the beam spots to coincide at every point in the interferometer. The overlap of the counter-propagating beams is again verified with the absence of a fringe pattern. This alignment step is repeated by introducing and centering the non-linear PPKTP crystal, mounted

on its heater, in the Sagnac loop. Their position is adjusted thanks to the 2-axis movable platform they are fixed on, once more guided by the fringe pattern approach.

10.2.5 Dichroic Mirrors

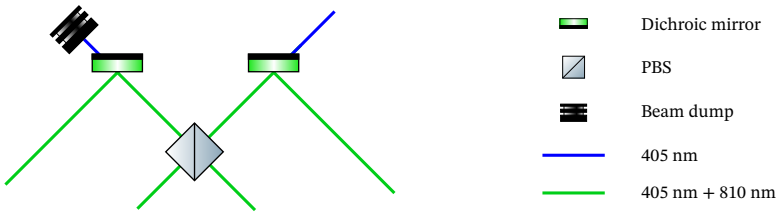


Figure 33: Close-up of the dichroic mirrors area of Figure 22.

Both 405 and 810 nm photons exit the Sagnac loop. However, only the polarization-entangled photon pairs at 810 nm are relevant for this experiment. The pump beam is therefore filtered a first time by shortpass dichroic mirrors (DMs). These can either be used to combine or split beams of different colors, as depicted in Figure 34.

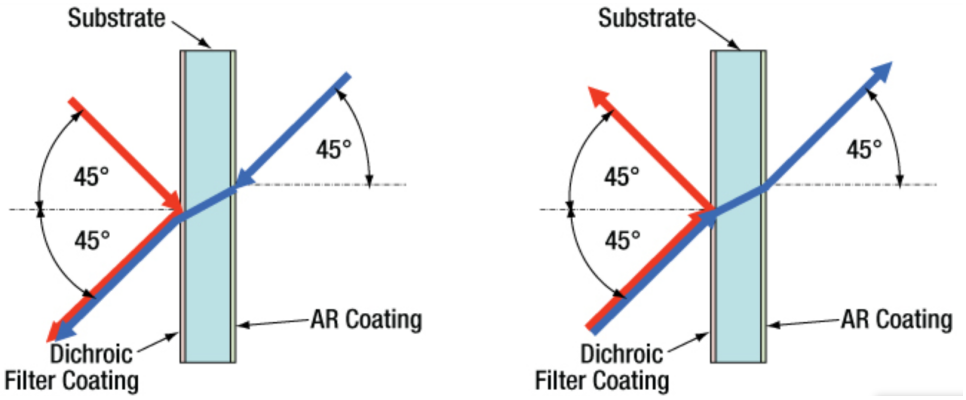


Figure 34: Schematic working principle of dichroic mirrors used to either combine (left diagram) or split (right diagram) beams of different colors. Figure from the Thorlabs website [111].

As pump and down-converted photons need to be spatially separated, dichroic mirrors are rather used in a "splitting" configuration (diagram on the right of Fig. 34) in the scope of this project. Thanks to different coatings, the dichroic mirrors used in this experiment are designed to transmit rays with a wavelength lower than 490 nm and to reflect photons with larger wavelengths. The anti-reflective (AR) coating on one side is thus optimized to transmit rays with short-wavelengths (in particular 405 nm). The dichroic coating on the opposite side also allows the majority of the lower wavelengths to pass through, but it reflects most of the long wavelengths (particularly 810 nm).

As can be seen in Figure 33, the dichroic mirror located near the PBS input port transmits 405 nm rays toward the Sagnac loop. Once the photons have propagated in the interferometer and a part of the pump is down-converted into 810 nm photons, they all exit the loop through one of the two output ports of the PBS. The lower-energy photons are mostly reflected by the DMs and a significant amount of the higher-energy ones are transmitted. On the left of Figure 33, it is shown that 405 nm rays are stopped by a beam dump, which is a device that blocks and absorbs unwanted rays. On the right however, it is not possible to block the propagation with a beam dump as pump photons need to cross the DM from both directions. Hence, it can be seen that the higher-energy photons travel back toward the laser source, which explains the relevance of an isolator to protect it.

It has been previously mentioned that dichroic mirrors can introduce unwanted reflections and refractions in the experiment. Indeed, a substrate is sandwiched between two coated surfaces. The difference of refractive indices of these materials with respect to the air introduces a displacement of the rays passing through the DMs.

Moreover, as the coatings are not ideal, partial reflections may appear at the mirror surfaces, leading to parasitic light beams offset from the primary ones. The principle of these partial reflections is presented in Figure 35.

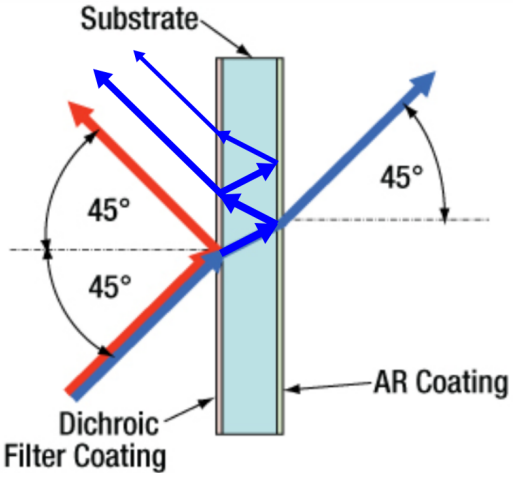


Figure 35: Addition of partial reflections on Figure 34: schematic working principle of a dichroic mirror used to split beams of different colors [111].

Simple geometric computations, confirmed with an experimental measurement, showed that the distance between the primary and secondary reflections was of ~2.5 mm. Unwanted partial reflections induced by the dichroic mirrors are therefore simply neglected throughout the experiment due to their intensities being much lower than that of the primary reflection and because they are spatially separated from it. They have little to no impact on the detections due to their low intensity, and even if they did contribute, they are unlikely to be collected by the detectors as they diverge away from the primary beam.

The two dichroic mirrors used in this experiment are placed at equal distance from the Sagnac interferometer outputs to maintain the setup symmetry. They are aligned thanks to the mounting holes grid of the optical breadboard and are oriented such that they reflect 810 nm photons perpendicularly to the incoming beams. This will later facilitate the alignment of the detectors.

10.2.6 Detection

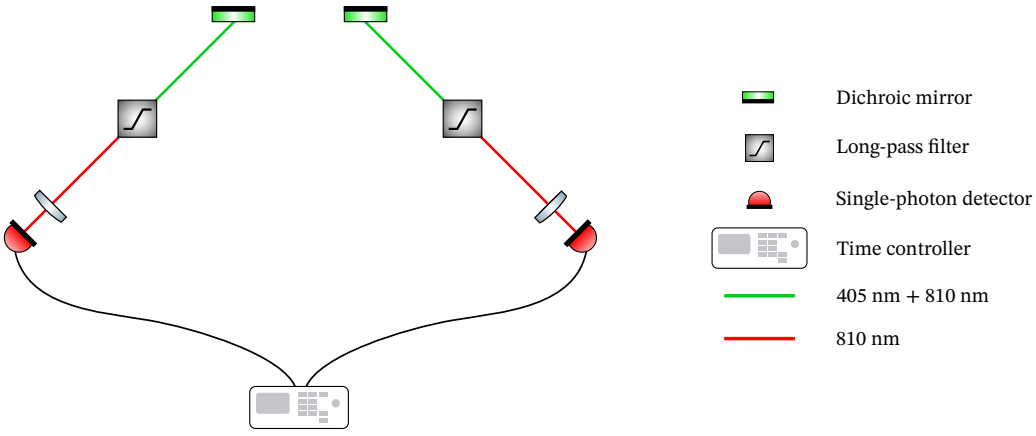


Figure 36: Close-up of the detection area of Figure 22.

The final stage of the experiment is the detection. Indeed, this work aims to develop a laser source of polarization-entangled photons. This objective should be reached at this point as photons down-converted by the PPKTP crystal are normally entangled. Regardless, this achievement must be confirmed to conclude that the source is functioning properly. Single-photon detectors are thus used to determine if pairs of photons generate coincidence events at both detectors. Afterwards, tests are conducted to verify wether their polarizations are

correlated at a quantum level, indicating their entanglement.

The selected detectors use Silicon avalanche photodiodes (APDs) to detect single photons. Avalanche photodiodes are semiconductor devices operated in a particular regime such that, when photons are absorbed, they excite and eject carriers (electrons and holes) via the internal photoelectric effect [112]. The ejected carriers are then accelerated by the strong internal electric field of the APD and they ionize additional atoms as they propagate, triggering an avalanche of carriers. This avalanche process allows to amplify the photocurrent generated by the absorbed photons. Therefore, such photodiodes are sensitive enough to detect single photons. Silicon-based APDs typically respond to photons with wavelengths between 400 nm and 1000 nm. They therefore appeared to be quite suitable for this experiment.

After the beams have exited the Sagnac loop, the dichroic mirrors introduced before filter out most of the pump photons. Some 405 nm photons remain nonetheless in the beams reflected toward the detectors. Furthermore, as single-photon detectors are sensitive devices, the intensity of the beams impinging on it should be significantly low. Therefore, long-pass filters with a cut-on wavelength at 600 nm are placed in the trajectory of the rays to block pump photons. This ensures that saturation of the detectors is never reached, whatever the output power of the laser. Converging lenses are placed behind the filters to focus the beams on the detectors because the smaller the beam spotsize at the detectors, the higher the detection efficiency. As SPDC is an extremely inefficient process, the down-converted photons at 810 nm are in such low quantity that they should not cause any harm to the detectors. The computation of the beam power at the detectors is carried out to verify this affirmation and to determine the amount of long-pass filters needed. To do so, the maximal output power the laser can emit is considered (40 mW) and the transmission and reflection efficiencies of the optical elements are accounted for. The efficiencies used in these computations are summarized in Table 6.

Optical element	**Transmission efficiency [%]**		**Reflection efficiency [%]**	
	At 405 nm	**At** 810 nm	**At** 405 nm	**At** 810 nm
Isolator	80	/	/	/
Quarter-waveplate	99.8	/	/	/
Half-waveplate	99.5	/	/	/
Mirror outside the loop	/	/	95.7	/
Dichroic mirror	95.22	/	3.13	99.34
PBS	92.14	96.62	/	/
Mirror in the loop	/	/	97.5	97.5
Lens in the loop	98.96	99.13	/	/
PPKTP crystal	99.5	99.5	/	/
Dual wavelength half-waveplate	99.5	99.5	/	/
Long-pass filter	$3.99\ 10^{-5}$	95.9	/	/
Lens outside the loop	99.3	99.7	/	/

Table 6: Efficiencies of the optical elements used in the system. Only the ones relevant to the experiment are presented. The PBS transmission efficiencies are given for a horizontally polarized beam. See Appendix A for the references of the optics.

To account for the worst-case scenario in the computations, it is assumed that the laser emits its maximal power of 40 mW and that the conversion rate of 405 nm photons into a pair of 810 nm photons is 10^{-9} (highest

rate achieved in periodically poled crystals as shown in Sec. 6.1). Based on Table 6 and considering that the laser rays pass through all the optical elements as presented in Figure 22, the power of the beams at the locations of the detectors are computed. It must be noted that, when the photons exit the Sagnac loop through the PBS, the beam power is divided into two as 50% of the photons propagate in one detector arm while the other 50% go in the other. When no filter is used, which means that the 405 nm photons are only removed by the dichroic mirrors, the beam power at the detectors is divided as follows:

$$P_{405} = 0.352 \text{ mW},$$
$$P_{810} = 1.185 \cdot 10^{-8} \text{ mW}.$$

This shows that the pump power remains way too high to use single-photon detectors safely. When a long-pass filter is introduced in each detector arm of the setup, these values become:

$$P_{405} = 1.405 \cdot 10^{-7} \text{ mW},$$
$$P_{810} = 1.136 \cdot 10^{-8} \text{ mW}.$$

The powers become manageable for single-photon detectors but the pump intensity is still larger than that of the down-converted photons, making it difficult to differentiate 405 nm from 810 nm photons at the detection. A second long-pass filter, identical to the first one, is therefore added in front of each detector, leading to the following results:

$$P_{405} = 5.607 \cdot 10^{-14} \text{ mW}, \tag{26}$$
$$P_{810} = 1.089 \cdot 10^{-8} \text{ mW}. \tag{27}$$

The pump power now represents less than 0.001% of the power of the down-converted photons. This will help to highlight the coincidences due to 810 nm pairs with respect to the 405 nm noise. The single-photon detectors have a maximal count rate of 20 MHz. This corresponds to a maximal incident optical power of $\sim 10^{-11}$ W ($\sim 10^{-8}$ mW) at 810 nm [113], which should not be surpassed to avoid saturation. The previous power computations have been made assuming the maximum output power of the laser and did not consider potential power losses due to partial obstruction of the beams or to imperfections of the optics and the alignment. Moreover, the 60% photon detection efficiency of the detectors at 810 nm and 10% at 405 nm were not accounted for. Therefore, it can be presumed that Equations 26 and 27 overestimate the real power the beam has when it reaches the detectors. For this reason, the two long-pass filters are judged sufficient to prevent detector saturation.

Adding a third filter can be considered, as it would drastically decrease the number of 405 nm photons, thus leading to an improved signal to noise ratio (defined here as the 810 nm power divided by the 405 nm power). Nonetheless, the signal to noise ratio achieved with only two long-pass filters is already sufficient to distinguish the down-converted photons from the pump ones at detection. Furthermore, the minimal optical power at which the filters were characterized is not specified. It could mean that their filtering performance at a few tenths of mW is not the same as at much lower optical powers, potentially resulting in unknown behaviors. The increase of signal to noise ratio provided by a third filter may therefore not justify the potential unexpected behavior at low powers and the additional inconvenience linked to ordering a new long-pass filter. Consequently, the filtering of 405 nm photons is achieved using only the dichroic mirrors and two long-pass filters, with a cut-on wavelength of 600 nm, placed in front of the detectors.

Now concerning the alignment of the detection zone in the setup, the long-pass filters are positioned perpendicular to the incoming rays to minimize parasitic reflections. A converging lens is then placed in front of each detector. Opting for plano-convex lenses with a focal length of 12 mm allows to focus the beams to a waist diameter of 11.4 μm, while the collection area of the detectors is 100 μm. The tight focus of the beams at the detectors improves the detection efficiency. Finally, the orientation of the detectors is controlled by 3-axis platforms. These enable an optimal orientation that maximizes the count rate.

10.3 Implementation of the Experiment

Figure 37 shows the physical implementation of the experiment presented in Figure 22. Arrows are used to illustrate the direction of propagation of the photons as well as their wavelength.

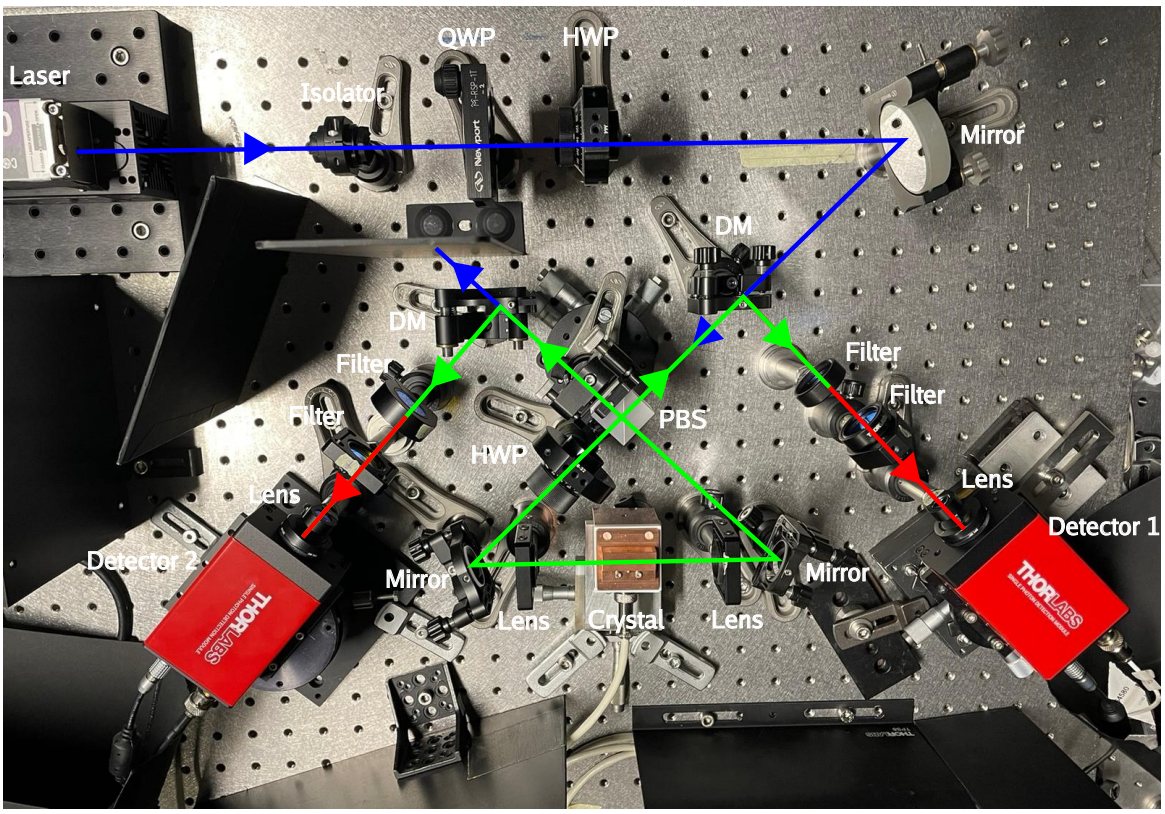


Figure 37: Photograph of the experimental setup. Arrows show the propagation directions of photons from the laser output to the detectors, except in the Sagnac loop and between the isolator and the right DM where photons of the same wavelength propagate in both directions. Blue = 405 nm, Green = 405 and 810 nm, Red = 810 nm. QWP = quarter-waveplate, HWP = half-waveplate, DM = dichroic mirror, PBS = polarizing beam splitter.

To minimize detection noise, dark boxes have been placed around the single-photon detectors. These are shown in Figure 38.

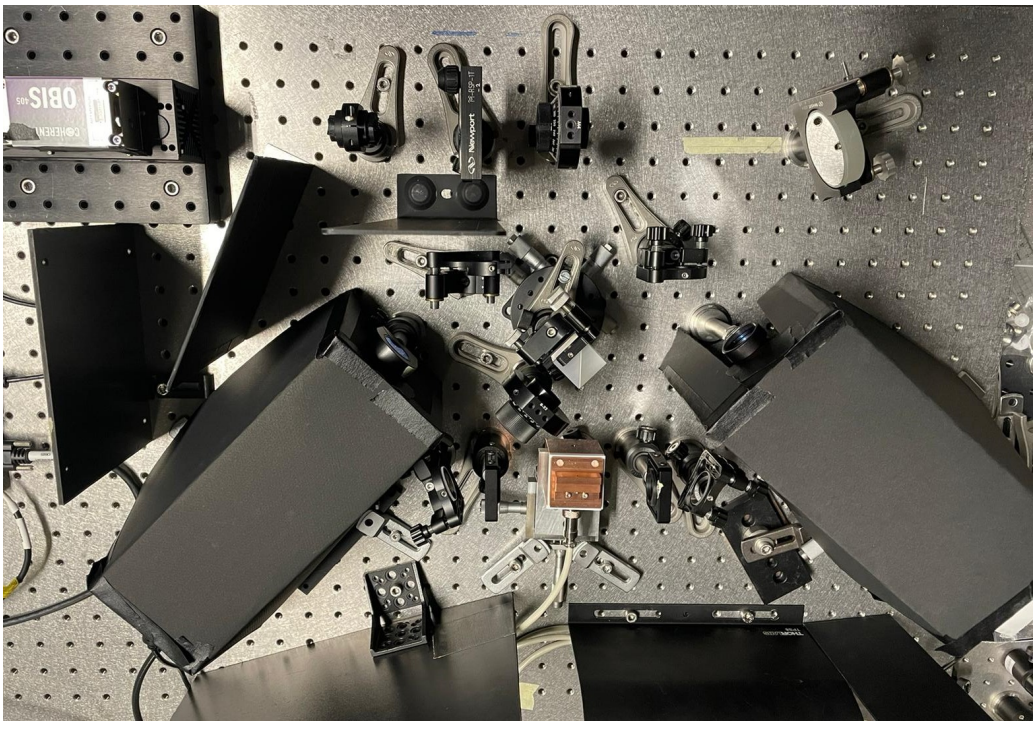


Figure 38: Photograph of the experimental setup, with dark boxes to isolate the single-photon detectors from environmental noise.

Complete darkness can be established around the experiment, such that the only background noise capable of triggering the detectors comes from faint light emissions by the electronic devices. Before data acquisition begins, the detectors need to be characterized and the background noise must be assessed. To do so, the average count rates (number of counts per second) registered by the detectors are measured for different configurations: with both protective caps and isolation boxes, with caps but no box, with neither the caps nor the boxes and with only the isolation boxes covering the detectors. The results are summarized in the table below.

Configuration	**Average count rate [Hz]**	
	Detector 1	**Detector 2**
With caps, with boxes	8	8
With caps, no box	9	8
No cap, no box	6685	1449
No cap, with boxes	92	129

Table 7: Characterization of the dark noise of the single-photon detectors and ambient noise. Detections are carried out in total darkness and with no emission of the laser. A cap refers to a cover that protects the active area of a detector when not in use.

Table 7 confirms that the dark count rate of the detectors (configuration with caps and boxes) remains lower than 100 Hz, which is consistent with the manufacturer's specifications [113]. This conclusion follows from the fact that, even when covered by protective caps and isolation boxes, some parasitic light may still reach the detectors. Therefore, the dark noise intrinsic to the detectors must be lower than 8 Hz -and so lower than 100 Hz- as the measured count rate includes both the dark count rate and the parasitic photons. Moreover, comparing the last two rows of the table highlights the efficiency of the isolation boxes in reducing the background noise. Since these noises appear to be significantly low, both the dark noise of the detectors and the background noise will be neglected when analyzing the data registered by the detectors.

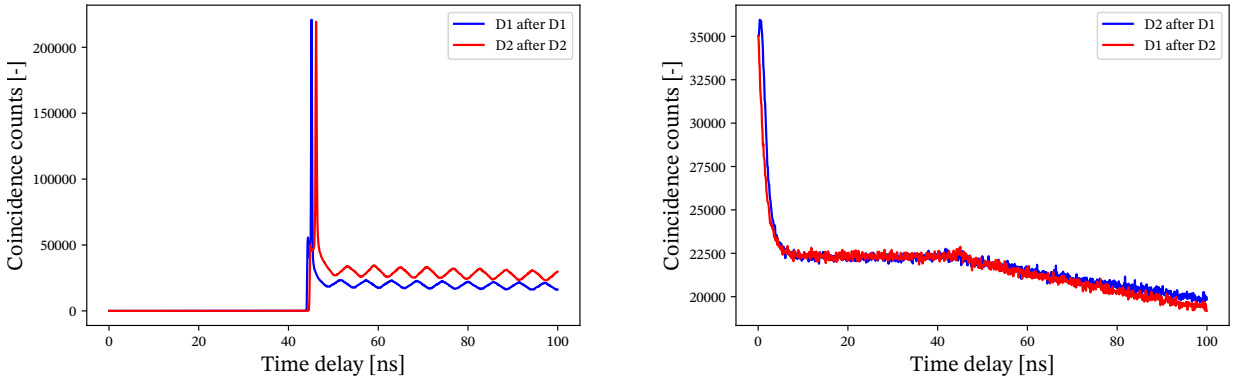
10.4 Analysis of the Results

This section presents the experimental results obtained from the setup described above and discusses their implications. The aim of the experiment was to implement a source of polarization-entangled photons, with orthogonal polarizations and wavelengths of 810 nm. The simultaneous spontaneous creation of photons is therefore verified through coincidence counts. Afterwards, the correlations between the polarizations of the down-converted photons are checked with a Bell test and their wavelengths are finally confirmed with a spectrometer.

10.4.1 Coincidence Counts

To begin with, coincidence counts are registered by the detectors. This means that the system records the time delay between detection events from the two detectors. If the time controller, which is connected to both single-photon detectors, indicates a delay of 0 s, it suggests that the two photons arrived simultaneously, resulting in a coincidence event. Simultaneous detections of photons hint toward their simultaneous generation, which is characteristic of pairs produced through SPDC. It can therefore highlight their entanglement, at least in the time degree of freedom, as no other phenomenon in the experiment is expected to simultaneously emit two photons.

To better understand the data collected and the concept of coincidence counts, an example of histograms generated by the time controller during a single acquisition is shown in Figure 39. These histograms represent the number of detection events that occurred close in time as a function of the time delay between these events. The correlations can be either between two successive detections on the same detector or between detections from the two detectors. It can be noted that their overall shape is typical of entangled-photons experiment, indicating promising results.



(a) Auto-correlations

(b) Cross-correlations

Figure 39: Number of coincidence counts plotted against the time delay between two detection events. Acquisition during 1 minute with a laser output power of 4 mW. Maximum time delay of 100 ns with a bin-width of 100 ps. The legend "Di after Dj" means that the start channel of the acquisition is detector j and the stop channel channel is detector i, such that the time delay is computed as the time of detection at the stop channel minus the time of the detection at the start channel.

Figure 39a represents coincidence counts recorded in an auto-correlation mode. In other words, each curve indicates the delay between successive detection events at a single detector. The curve labeled "D1 after D1" therefore shows the frequency at which two successive detections occur at the first detector with a specific time delay. "D2 after D2" refers to the same curve but based on the detections of the second detector. The histograms displayed in Figure 39b show the correlations between photons incoming on the first and second detector. Indeed, the curves represent the time it takes for a detection at the second detector (resp. the first) to occur after the first detector (resp. the second) was triggered by a detection event. An interpretation of these graphs will be detailed later in this section.

The time delay axis is divided into smaller intervals, called time-bins. These define small time-windows during which detection events at these time delays are considered part of the same contribution to the histogram. For example, the bin-width of the detections plotted in Figure 39 is 100 ps. This means that all photon pairs arriving with a time difference ranging from 0 to 100 ps at the detectors contribute to the first bin. Analogously, the second bin counts the photon pairs detected with a delay between 100 ps and 200 ps, the third bin between 200 ps and 300 ps and so on for a thousand time-bins. A maximal time delay of 100 ns is also imposed such that, if two photons are detected with a time difference that exceeds this limit, they are not considered as part of the same event and therefore do not contribute to the histogram. When the data acquisition is performed over an extended period (1 minute in this case), the number of coincidence events accumulates. The resulting histogram shows the frequency at which successive photons are detected with a given time delay, which illustrates the temporal correlations between photon pairs.

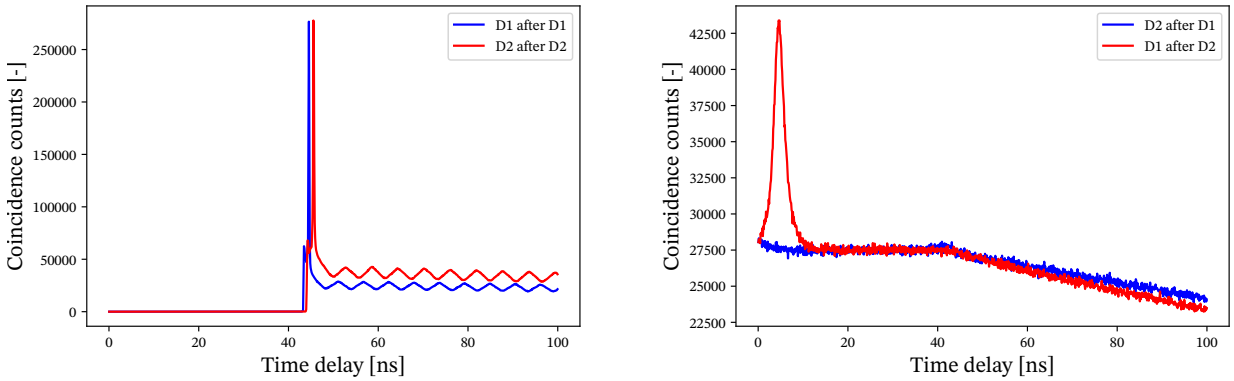
The histogram settings have been fixed with the following values throughout the entirety of the experimental work, as they seemed to provide the most precise and readable data. The bin-width of 100 ps is the smallest that can be imposed by the selected time controller [114]. It therefore yields the most precise results as the time delay axis is divided into a maximal number of time-bins. Moreover, it was chosen to work with a maximal delay of 100 ns because it appeared to yield easily readable histograms. Indeed, if the maximal time delay is too short, the number of distinct bins -calculated as the maximal delay divided by the bin-width- is small, making the graphs difficult to read. On the other hand, the maximum number of time-bins that can be resolved by the time controller is also limited. Thereby, if the maximal time delay is too long, the bin-width becomes large, thus losing information about short time-scale phenomena. Furthermore, 100 ns is larger than the dead time of the single-photon detectors (45 ns [113]). This allows to draw conclusions about the data behavior related to the dead time of the detectors. Due to the symmetry of the system, small time delays between the detections of photons were expected. Therefore, time delays below 100 ns seemed sufficient to analyze the emissions of the source.

When an avalanche of photocarriers has been triggered by the absorption of a photon on the detector APD, it needs to be stopped. The avalanche stopping process is called *quenching*. The *dead time* of a detector is the time required to recover the APD operating voltage after the avalanche has been quenched. During this recovery period, the detector is temporarily unable to register new detection events. The single-photon detectors used in this setup are equipped with an active quenching system, which enables a short dead time of 45 ns and so the achievement of high count rates.

The dead time of the detectors is noticeable in the histograms of Figure 39. Indeed, it can be seen in Figure 39a that almost no successive detections occur with a time delay shorter than 45 ns, when looking at detections from a single detector. This is because, during the dead time of the detector, no photon incoming on the APD can trigger an avalanche, resulting in no coincidence counts during that period. As continuous laser beams are incident on the detectors, they register detection events continuously over time. Therefore, as no photon is detected during the dead time, the most common interval between detections corresponds to that period, resulting in a high peak of the coincidence counts at 45 ns. The stable region that appears in the auto-correlation histograms after the high peak indicates that detections spaced by more than 45 ns occur with a nearly constant probability. Moreover, the small oscillations that can be seen likely come from either timing jitter of the detectors or periodic faint light emissions produced by the surrounding electronic devices. These oscillations can also come from intrinsic instabilities or a periodic behavior of the laser source.

The dead time can also be noticed in Figure 39b, where a flat stable noise is observed until the delay reaches 45 ns. The constant noise level is explained by the randomness of the environmental noise and the continuity of the noise coming from the pump beam at 405 nm. It represents accidental coincidences between uncorrelated detection events. The gradual decrease that follows the constant noise floor is due to the fact that, beyond a delay of 45 ns, both detectors are theoretically fully recovered from any prior detection. Coincidence events occurring with such long delays imply that one detector is triggered much later than the other, while registering no detection event in the mean time. The probability that this happens diminishes with increasing delays. This results in the decreasing tail of the histograms shown in Figure 39b.

Figure 39b presents high coincidence counts for simultaneous detection events at both detectors -when the delay between the detections is null. However, the graph is difficult to read due to the closeness of the peak with the left border of the graph. Therefore, an arbitrary time delay of 5 ns is imposed on the first detector, such that the peak is displaced for a better visibility. The histograms resulting from this artificial delay are displayed in Figure 40.



(a) Auto-correlations

(b) Cross-correlations

Figure 40: Number of coincidence counts plotted against the time delay between two detection events, with an artificial 5 ns delay imposed on the first detector. Acquisition during 1 minute with a laser output power of 4 mW. Maximum delay time of 100 ns with a bin-width of 100 ps. The legend "Di after Dj" means that the start channel of the acquisition is detector j and the stop channel channel is detector i, such that the time delay is computed as the detection time at the stop channel minus the detection time at the start channel.

Comparing Figures 39b and 40b highlights the impact of the imposed delay on the histograms that show correlations between detection events at the two detectors. The strong peak previously observed at a time delay of 0 ns is now clearly visible and appears to be centered around 5 ns because of the imposed delay. It corresponds to the simultaneous arrival of photons at both detectors, suggesting strong temporal correlations. Indeed, considering two photons arriving at the same time at the two detectors, the imposed delay makes the time controller register the detection at the first detector as occurring 5 ns after that at the second detector. Their coincidence event thus contributes to the time-bin centered around 5 ns. This temporal correlation coming from the simultaneous arrival of the photons is typical of entangled-photon pairs generated through processes like the spontaneous parametric down-conversion. The blue curve of Figure 40b does not present a peak anymore because, as detections at the first detector are artificially delayed w.r.t. those at the second detector, the probability that the second is triggered after the first one is drastically reduced. Indeed, the second detector now appears to react before the first one during coincidence events, such that the corresponding time delays (D2 after D1) are negative and therefore not plotted. Consequently, this histogram no longer reflects the correlations of entangled photons.

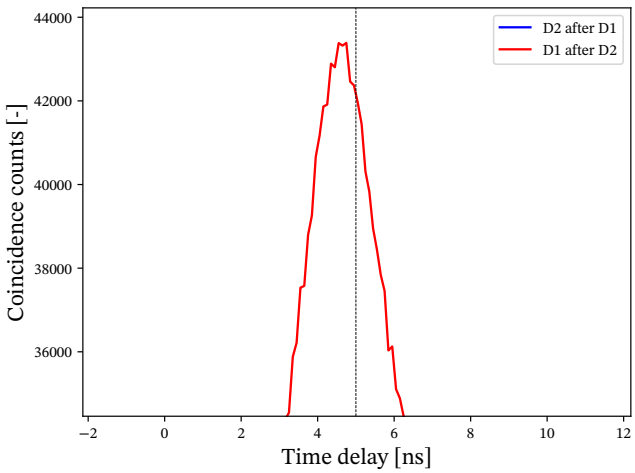


Figure 41: Close up of the peak area in Figure 40b. The dotted line indicates a time delay of 5 ns.

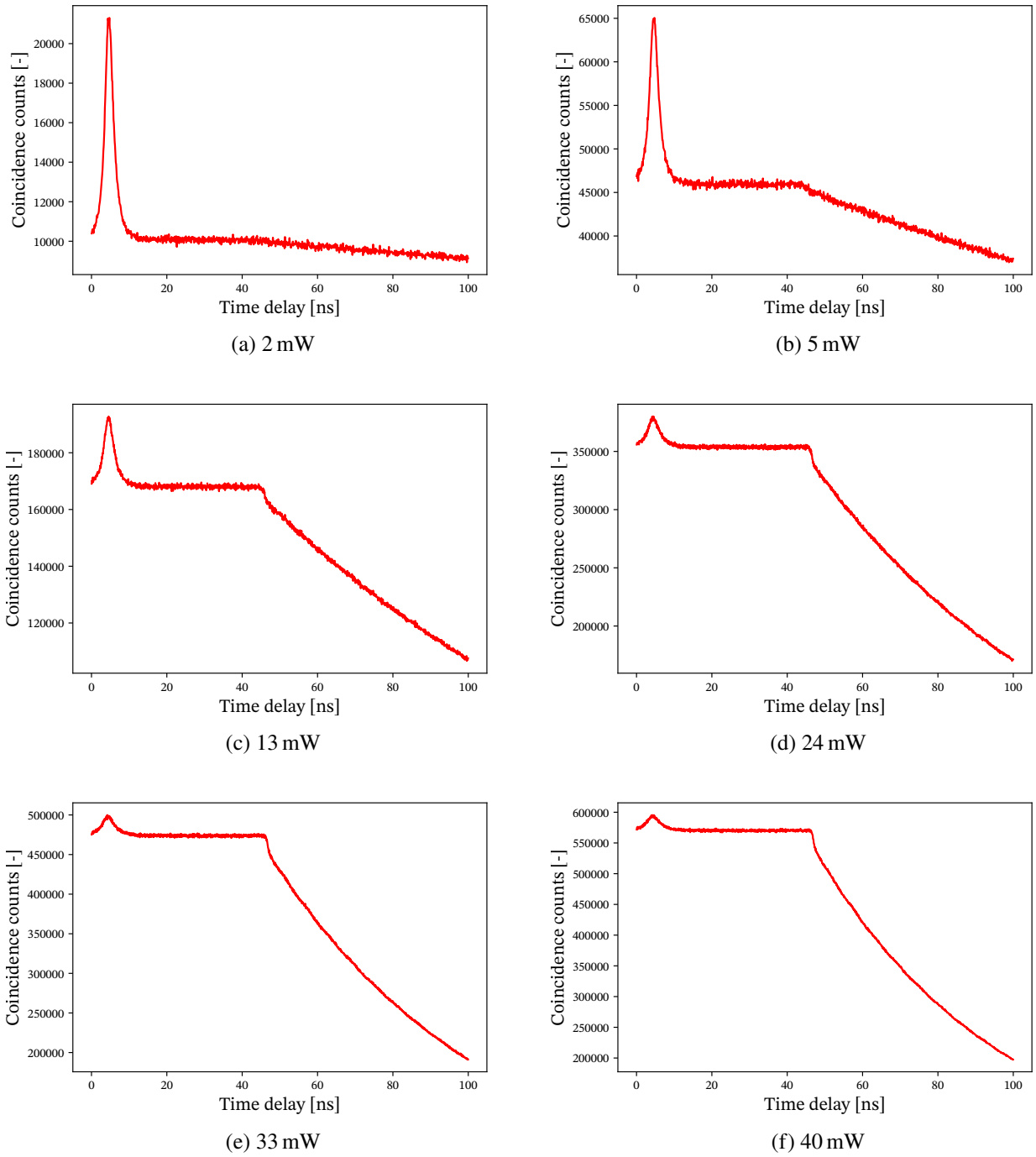
As can be seen in Figure 41, the coincidence peak from Figure 40b is in fact centered around a delay of 4.65 ns rather than exactly around the expected 5 ns. This could be caused by a slight asymmetry in the setup, so that a photon from an EPR pair reaches the first detector before the other arrives at the second detector, resulting in a small real time delay despite their entanglement. The peak width can arise from either distinct timing resolutions between the detectors or from their jitter, which represents their inability to determine exactly the timing of a detection. It may also be due to different optical paths of the photon-pairs, that can result from the generation of down-converted photons at different locations within the non-linear crystal.

In APD detectors, after a photon has been detected and the resulting avalanche of photocarriers has been quenched, some charges can remain trapped in the semiconductor material. Once the dead time of the detector has elapsed, these charges can be released and trigger false detections, potentially leading to spurious coincidence counts. This phenomenon, called *afterpulsing*, is visible in histograms generated in auto-correlation mode (see Fig. 39a and 40a), where a small increase of the coincidence counts can be seen just before the main peak.

The figures presented in this section allowed to highlight the simultaneous detections of photons at the detectors, revealing strong correlations between their timing. As no other phenomenon than SPDC could be responsible for such temporal correlations, this is taken as a strong hint toward the generation of photon-pairs and so their time-entanglement.

The influence of the laser output power on the generation rate of these pairs is now studied. This is done by

analyzing the height of the peak present in the histogram representing the frequency of detection events at the first detector as a function of the time delay following a detection at the second detector ("D1 after D2" curve). As this peak suggests the simultaneous generation of photons through SPDC, its height is a great indicator of the quantity of 810 nm photons that are created. A 5 ns delay is artificially imposed on the first detector to better visualize the coincidence peaks.



(a) 2 mW (b) 5 mW

(c) 13 mW (d) 24 mW

(e) 33 mW (f) 40 mW

Figure 42: Number of coincidence counts plotted against the time delay between a detection at the first detector that follows a detection at the second one. An artificial delay of 5 ns is imposed on the first detector. Acquisition during 1 minute with varying laser output powers. Maximum delay time of 100 ns with a bin-width of 100 ps.

Figure 42 illustrates the variation of the coincidence peak height as a function of the laser output power. It can be seen that, as the power increases, the height of the peak becomes less contrasted with respect to the amount of noise caused by the pump photons. This noise corresponds to the flat region located between the main peak and the decline of counts that starts around a delay of 45 ns. However, despite this reduced contrast,

the total amount of coincidence counts comprised in the peak does indeed globally increase with the laser power, as it can be observed in Figure 43.

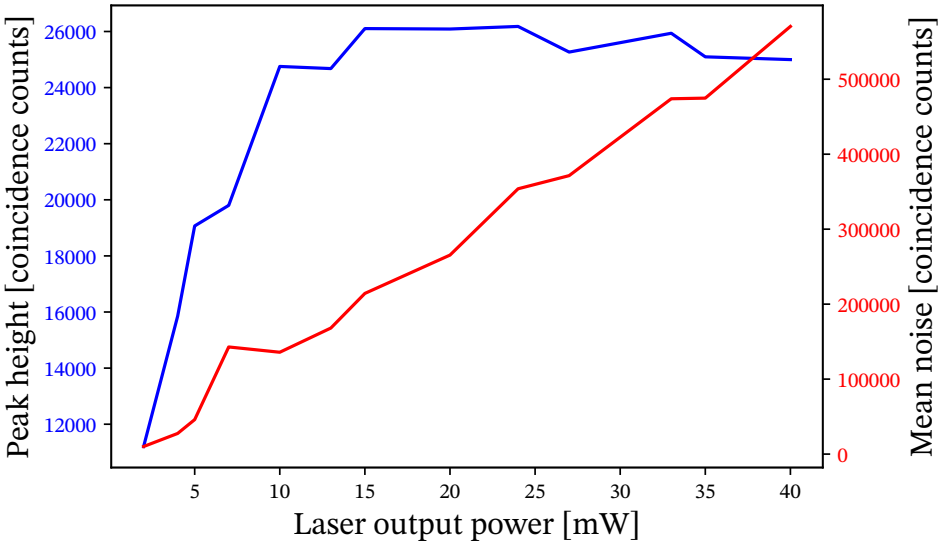


Figure 43: Variation of the peak height and the mean noise of the histograms presented in Figure 42 with the laser output power.

The proportional increase of the noise floor level with the laser power (red curve of Fig. 43) is coherent as more 405 nm photons are emitted by the laser module such that their chance of causing accidental coincidence events is increased. However, the generation rate of 810 nm photons within the crystal is not directly proportional to the pump power. When the laser power is increased, more entangled-photon pairs are indeed generated but much more pump photons go through the PPKTP crystal without interacting with it. This explains why the proportionality between the peak height and the noise level is not constant throughout the histograms displayed in Figure 42, leading to the reduced visibility of the peak. The obtained 810 to 405 nm photon ratio differs from the one computed in Section 10.2.6 in the context of analyzing the effects of long-pass filters. Indeed, the experimental results show a much lower signal-to-noise ratio than what has been previously determined when the laser outputs a maximal power of 40 mW. This is due to the fact that the previous computations accounted for the worst-case scenario in which many 810 nm photons were created and reached the detectors, such that a maximal intensity at the detectors was considered. Therefore, the maximal down-conversion efficiency was considered while, in reality, this efficiency is much lower, such that many pump photons propagate in the crystal without being down-converted. Moreover, the real efficiency of the dichroic mirrors and the filters that are supposed to filter out pump photons might also be lower than expected, thus letting more 405 nm photons being detected.

The amount of photon-pairs detected seems to increase with the laser power, until it reaches an almost constant value. This is noticeable in Figure 43, where the peak height starts to stagnate as higher pump powers are reached. Several phenomena could be at the source of this stagnation of the number of coincidence counts. For instance, the large amount of photons that comes from a high pump power increases the probability of accidental coincidences at the detectors, making it harder to resolve true coincidences. The saturation could also come from an intrinsic limitation of the time controller which can saturate when too many detections are registered by the detectors, potentially leading to the loss of relevant detections. Having high intensities impinging on the crystal might modify its temperature locally, thus inducing thermal effects. These can cause the phase-matching condition to be modified or even induce photorefractive effects, which can therefore lower the SPDC efficiency and so constrain the pair generation rate.

10.4.2 Visibility Measurements and Bell Test

Now that the generation of pairs of photons, that are at least entangled in their temporality, has been strongly supported by the histograms presented in the previous section, visibilities are computed and a Bell test is

conducted to verify whether these photons are also polarization-entangled.

The point is to verify that the polarizations of photons simultaneously detected are indeed anti-correlated. This means that, if one photon from an EPR pair is determined to be horizontally polarized, the other photon should have a vertical polarization. To achieve this, a linear polarizer is introduced in front of each detector. This allows to sort the photons that are detected, based on their polarization. By rotating the polarizers one at a time, specific behaviors should be observed, hinting toward the polarization-entanglement of the photons. Data acquisitions are performed by taking arbitrarily one polarizer (called P1) as the reference and gradually rotating the second one (P2). When the polarizers have orthogonal orientations, e.g. P1 is set horizontally and P2 vertically, the coincidence counts should reach maximal values as the emission of orthogonally polarized photons is expected from the source. On the other hand, when the polarizers are set parallel to each other, the coincidence counts should be minimal because only one photon from each EPR pair is able to trigger a detection event while the other is stopped by the polarizer. Noting C_{max} the maximal number of coincidence counts triggered by photon-pairs and C_{min} the minimal number of counts, the entanglement visibility can be computed as follows:

$$V = \frac{C_{max} - C_{min}}{C_{max} + C_{min}}. \tag{28}$$

Classical physics predicts a visibility $V \leq 71\%$ [54]. Therefore, if the visibility is larger than 71%, Bell's inequality is most likely violated which suggests that the photons are polarization-entangled [115].

As relevant coincidence counts are triggered by pairs of 810 nm arriving simultaneously at the detectors, the number of counts that are considered to compute the entanglement visibility are taken as the height of the peak present in cross-correlation histograms. When a 5 ns delay is imposed on the first detector, this height is defined as the difference between the maximal number of counts recorded for delays between 0 and 10 ns and the mean level of noise which is computed as the mean number of coincidence counts registered for time delays ranging from 10 to 45 ns. This approach allows to isolate the contribution of down-converted photons in the histograms, while discarding the accidental coincidences arising from the pump noise.

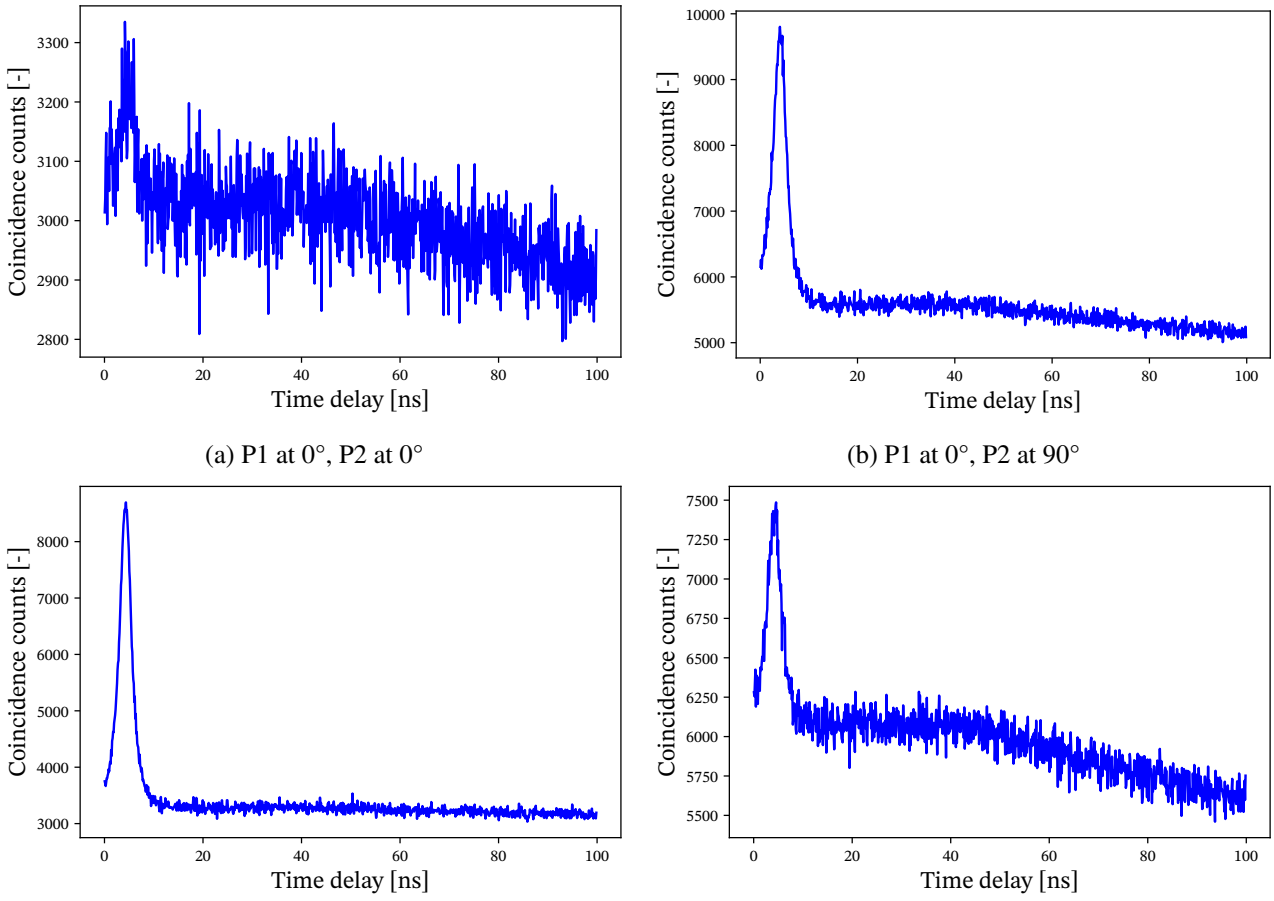
The experiment being manually aligned, it still requires some adjustments to yield satisfying results. Preliminary acquisitions are therefore used to improve the setup alignment through trials and errors. These acquisitions record coincidence counts in four configurations of the polarizers:

1. P1 at 0° with P2 at 0°,
2. P1 at 0° with P2 at 90°,
3. P1 at 90° with P2 at 0°,
4. P1 at 90° with P2 at 90°,

as the height of the peak is expected to be minimal in the first and last configurations and maximal in the others. Considering C_i is the peak height, expressed in coincidence counts, registered in the i^{th} configuration, preliminary visibilities can be computed as follows:

$$V_H = \frac{C_2 - C_1}{C_2 + C_1} \quad \text{and} \quad V_V = \frac{C_3 - C_4}{C_3 + C_4}, \tag{29}$$

where V_H is the visibility computed with the reference polarizer set horizontally and V_V when it is oriented vertically. These give an idea on the probability that the generated pairs of photons violate Bell's inequality, therefore indicating whether the photons are likely polarization-entangled. The optimal settings of the experiment yielded the results shown in Figure 44.



(a) P1 at 0°, P2 at 0°

(b) P1 at 0°, P2 at 90°

(c) P1 at 90°, P2 at 0°

(d) P1 at 90°, P2 at 90°

Figure 44: Number of coincidence counts plotted against the time delay between a detection at the first detector that follows a detection at the second one. An artificial delay of 5 ns is imposed on the first detector. Acquisition during 1 minute with a laser output power of 4 mW. Maximum delay time of 100 ns with a bin-width of 100 ps.

The preliminary entanglement visibilities obtained from these histograms are thus computed with Equation 29:

$$V_H = 86.56\% \quad \text{and} \quad V_V = 58.64\%.$$

When considering a horizontal orientation of the reference polarizer (P1), it is clear from Figures 44a and 44b that the polarizations of photons detected simultaneously are strongly anti-correlated. Indeed, when the linear polarizers located in front of the detectors are set with orthogonal orientations, many coincidence events triggered by photon-pairs are registered. In other words, the peak centered around a delay of 5 ns in this configuration suggests that the photons arrived simultaneously at the detectors as an artificial delay has been imposed. On the contrary, when the fast axes of the polarizers are parallel to each other, almost no photon-pairs are detected simultaneously, as shown by the small peak present in Figure 44a. This is a behavior expected from polarization-entangled photons. The visibility computed supports this as the value of V_H is larger than 71%, thus strongly suggesting polarization-entanglement.

However, the entanglement visibility computed with the reference polarizer set vertically is not satisfying enough to hint toward entanglement. Indeed, Figures 44c and 44d show that the peak of coincidence counts recorded with orthogonal orientations of the polarizers is quite high but the contrast between the height of the two peaks is not large enough to yield a satisfactory entanglement visibility. V_V value of 58.64% therefore indicates that the photon-pairs cannot violate Bell's inequality, despite having apparent anti-correlated polarizations.

The fact that one visibility is quite high while the other is relatively low shows an asymmetry in the setup. In fact, the configuration P1 at 0° with P2 at 90° presents a large peak of coincidence counts corresponding to photons that have propagated in the Sagnac interferometer clockwise. Referring back to the setup photograph

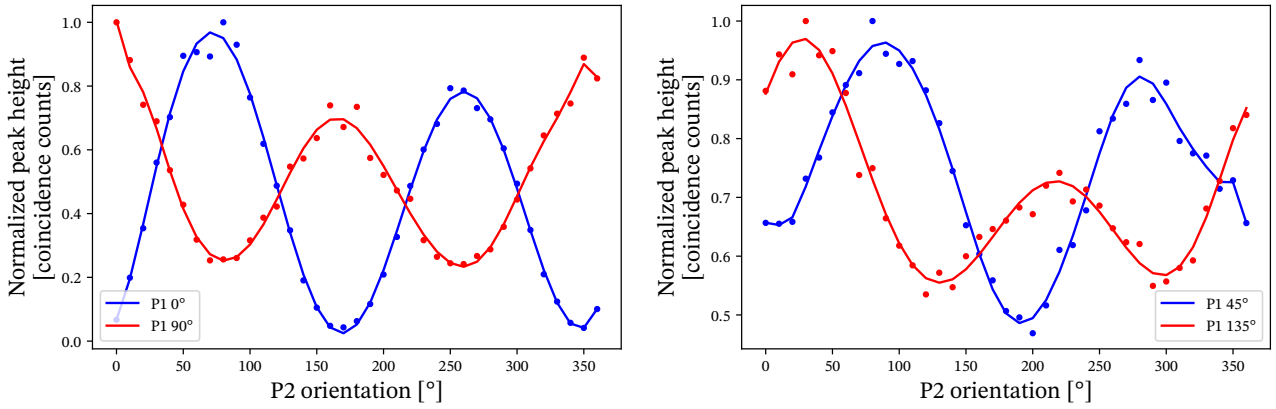
(see Fig. 37), if a pump photon traveled the Sagnac loop clockwise, the horizontally polarized down-converted photon is transmitted by the PBS and is detected by detector 1, when P1 is set horizontally. The other down-converted photon, which has a vertical polarization, is reflected by the PBS toward detector 2. The value of V_H = 86.56% therefore indicates that the SPDC process effectively generates polarization-entangled photons when the PPKTP crystal is pumped by photons propagating clockwise.

The low value of V_V now suggests that the down-conversion of photons traveling the loop in the counter-clockwise direction is not efficient, such that the correlation between the polarizations of the idler and signal photons is not strong enough to conclude to their polarization-entanglement. This weak SPDC generation rate is most likely caused by a wrong fulfillment of the quasi-phase-matching condition. Indeed, the condition is not perfectly met if the pump beam is not entering the non-linear crystal with the right angle. The down-conversion rate can thereby be diminished. Moreover, entering the crystal with an orientation different from the one intended may also lead to a different SPDC configuration than expected. If the configuration of the SPDC cones turns out to be non-collinear rather than the desired collinear configuration, the idler, signal and pump photons are not superimposed, such that the entangled photons can be found in two separate regions. As the down-converted photons are therefore spatially separated before they exit the interferometer, it becomes impossible to find an orientation of the detectors that register photons from both regions. Detecting only half of the relevant photons can then lead to a reduced entanglement quality, or even to no apparent entanglement at all.

The cause of this asymmetry will be further investigated later along with potential solutions. However, some potential causes have already been investigated and excluded. A first lead was to check that pump photons were effectively entering the non-linear crystal with a vertical polarization. To do so, it was verified that the quarter- and half-waveplates located at the beginning of the laser propagation were indeed yielding diagonally polarized photons. This was achieved with the help of a linear polarizer and a photodiode. Once the polarization of the pump photons entering the interferometer was confirmed to be diagonal, intensity measurements were performed at both output ports of the PBS to ensure a true 50/50 splitting of the rays. As the transmitted and reflected beams were measured to have the same intensity, it was concluded that the PBS effectively transmitted horizontally polarized photons and reflected the ones with a vertical polarization. The functioning of the dual-wavelength half-waveplate located inside the loop was finally verified. Measurements indicated that the pump photons were effectively vertically polarized when they entered the crystal from both directions, thereby ruling out this potential cause of the asymmetry.

The fact that many down-converted photons with a vertical polarization were detected simultaneously at the two detectors (see Fig. 44d) could be the result of a parasitic reflection of the V photons on the half-waveplate in the loop. A reflection on the waveplate would impose an optical path difference between two photons of a pair. Based on the speed of light and on the distance between the waveplate and the detectors, it was computed that the reflected photons would have a delay of 1 ns with respect to the other. This should result in a displacement of the peak of the histograms toward a delay of 1 ns (or toward 6 ns if an artificial delay is imposed on one detector). Since no such shift is observed, it was concluded that the dual-wavelength half-waveplate did not induce spurious reflections. The influence of the PPKTP crystal temperature was the final potential cause that has been investigated. Histograms were generated for different temperatures of the crystal and it appeared that the optimal configuration was indeed at the nominal temperature of 37.5 °C. Since no spurious phenomena appeared to cause the SPDC efficiency asymmetry, the issue was attributed to an imprecise alignment of the setup.

As no better-optimized alignment settings have been found, a Bell test is still conducted with the collected data to demonstrate its principle. This test relies on 16 measurements of coincidence counts [54], each corresponding to a different configuration of the linear polarizers. To obtain the data required to perform a Bell test, coincidence histograms are generated for many configurations: the reference polarizer is fixed at four orientations (horizontal, vertical, diagonal, anti-diagonal), while the second polarizer is rotated gradually in steps of 10° to cover a full 360° rotation. This procedure results in 4×36 histograms, from which the height of the peak corresponding to the simultaneous detection of correlated photons is extracted. The peak height reflects the number of coincidence events per minute triggered by photons at 810 nm, thereby illustrating a coincidence rate. These results are summarized in Figure 45.



(a) Reference polarizer in the rectilinear basis

(b) Reference polarizer in the diagonal basis

Figure 45: Polynomial fit of the normalized height of the peak reflecting the amount of 810 nm photons detected simultaneously as a function of the second polarizer orientation, when the first polarizer is taken as a reference. Dots correspond to the collected data. An artificial delay of 5 ns is imposed on the first detector. Acquisition during 1 minute with a laser output power of 4 mW. Maximum delay time of 100 ns with a bin-width of 100 ps.

Now that a complete set of data has been recorded, the true entanglement visibilities can be computed with Equation 28, instead of simply assuming that the configurations P1 at 0° with P2 at 90° and P1 at 90° with P2 at 0° yield the maximal counts of simultaneous detections:

$$V_H = 92.05\% \quad \text{and} \quad V_V = 61.08\%.$$

The same conclusions as before can be drawn. Namely, the polarizations of photons from a pair appear to be anti-correlated, with an even higher quality of polarization-entanglement of the photons propagating clockwise in the loop, as shown by the value of V_H. Visibilities can also be computed when the polarizations of the photons at the first detector are measured in the diagonal basis:

$$V_D = 36.16\% \quad \text{and} \quad V_A = 30.30\%,$$

where V_D is the entanglement visibility computed with P1 oriented at 45° and V_A when it is oriented at 135°. These low values indicate the inefficiency of the down-conversion process, occurring in at least one of the propagation directions of the photons during the pumping of the PPKTP crystal. If SPDC indeed produced polarization-entangled photons in any case, all four visibilities (V_H, V_V, V_D and V_A) should be larger than 71%.

The Bell test aims at determining the S-parameter of a system to verify whether the photons are polarization-entangled. This parameter, which violates Bell's (CHSH's) inequality when it exceeds 2, is defined as follows [115]:

$$S = |E(a,b) - E(a,b')| + |E(a',b) + E(a',b')|,$$

where a, a', b and b' correspond to different orientations of the linear polarizers. In this expression, $E(a,b)$ determines the expectation value of the joint measurement of polarizations along the directions a and b [116]. In other words, it represents the expected value of the product of the polarization measurement outcomes, when the first polarizer is oriented along a and the second along b. Therefore, $E(a,b)$ tends toward -1 when the photon polarizations measured along directions a and b are perfectly anti-correlated and toward $+1$ when they are perfectly correlated. The expectation value is given by [115]:

$$E(\alpha,\beta) = \frac{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) - N(\alpha,\beta_\perp) - N(\alpha_\perp,\beta)}{N(\alpha,\beta) + N(\alpha_\perp,\beta_\perp) + N(\alpha,\beta_\perp) + N(\alpha_\perp,\beta)},$$

where $N(\alpha,\beta)$ is the number of coincidence counts registered with P1 oriented along α and P2 along β, and where $\theta_\perp = \theta + 90°$.

Fitting the collected data with a polynomial curve allowed to determine coincidence counts corresponding to different combinations of the polarizers. The following angles, typically used to conduct Bell tests, are selected:

$$a = 0°,$$
$$a' = 45°,$$
$$b = 22.5°,$$
$$b' = 67.5°.$$

These measurement settings should yield the maximal value $S = 2\sqrt{2}$ if the photons are in a Bell state [115] -if they are maximally entangled.

Computing the S-parameter of the experimental source, based on the coincidence counts obtained from Figure 45, the following value is derived:

$$S = 1.091.$$

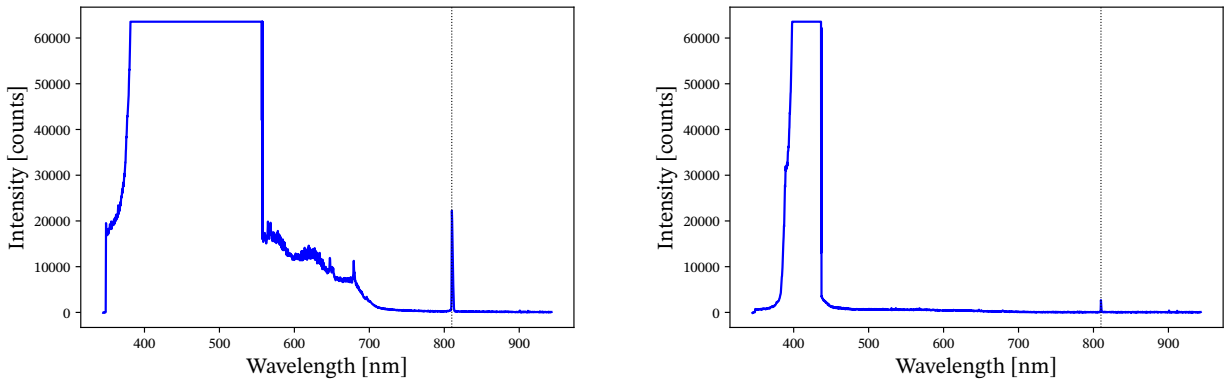
This parameter does not violate Bell's inequality as it is below the classical bound of 2. Therefore, the correlations between the polarizations of the photons can entirely be described with classical mechanics, meaning that they are not entangled. This result is potentially due to setup imperfections, like a poor alignment or decoherence induced by the optics, that reduce the strength of the correlations or to an inefficiency of the detection. The previously proposed hypothesis of an asymmetry in the SPDC conversion efficiency could also explain this low S-parameter, such that the entanglement quality of photons traveling the Sagnac loop in one direction is much lower than that of the photons rotating in the opposite direction, leading to an apparently imperfect entanglement. This hypothesis is difficult to verify in the present experiment because of the Sagnac interferometer perfect symmetry. Indeed, the isolation of the down-conversion of pump photons traveling the Sagnac loop in one direction is complex to implement without dismantling the setup.

The outcomes of the conducted visibility measurements and Bell test are not satisfying enough to conclude to a polarization-entanglement of the photon-pairs generated through SPDC. Nonetheless, there are indications that photons rotating in one direction within the Sagnac loop are indeed polarization-entangled, whereas those propagating in the opposite direction are not. The developed EPS could therefore not be used in a context of quantum key distribution, as the generation of pairs needs to be efficient in both directions to ensure the security of an entanglement-based QKD protocol. Potential sources of improvement of the setup and possible solutions will thus be investigated to seek the suitability of the entangled photon source for a QKD application (see Sec. 10.6).

10.4.3 Spectral Measurements

The final step of the source characterization is the verification of the photon wavelengths. Heating the non-linear PPKTP crystal at a temperature of 37.5 °C is supposed to enable degenerate Type-2 SPDC, such that the idler and signal photons both have a wavelength of 810 nm. However, the temperature that leads to degeneracy might be slightly inaccurate because of potential defects in the crystal or deviations of the pump beam wavelength from 405 nm. It is therefore required to verify whether the pairs generated via SPDC indeed have a wavelength of 810 nm.

To achieve this verification, successive spectral measurements are performed at both ends of the PPKTP crystal. This allows to assess that SPDC is indeed taking place and to verify that pump photons propagating in opposite directions in the crystal are being down-converted. The resulting spectra are shown in Figure 46.



(a) Clockwise pumping of the crystal

(b) Counter-clockwise pumping of the crystal

Figure 46: Intensity of the beam registered by the spectrometer as a function of the photon wavelengths, with an integration time of 1 s and the application of an electric dark count correction. The dotted black line indicates a wavelength of 810 nm. The spectrometer is first placed on one side of the crystal, such that it measures the intensity of the rays propagating clockwise in the Sagnac interferometer (a), and then on the other side of the crystal to measure the intensity of the beams propagating counter-clockwise (b).

The spectra confirm that photons at 810 nm are effectively created, as peaks at this wavelength are visible in both figures, alongside the high intensity induced by the 405 nm pump photons. Due to the high intensity of the pump beams when they exit the crystal, the spectrometer is quickly saturated. This explains the abnormal behavior of the curves around the pump wavelength. Due to the device saturation, it impossible to extract a down-conversion rate (from 405 to 810 nm photons) from these spectral data.

An asymmetry can be noticed between the height of the peaks present in Figures 46a and 46b. Indeed, when the PPKTP crystal is pumped from the left (clockwise) $\sim$ 22250 counts are registered with a wavelength of 810 nm. When it is pumped from the other direction however, only $\sim$ 2700 counts at 810 nm are recorded. This is coherent with the asymmetry between the down-conversion efficiencies of counter-propagating pump photons reported earlier. Regardless, one must note that these counts should not be trusted blindly as a collimator made of a parabolic mirror was used to focus the beams exiting the crystal into the fibered spectrometer. Therefore, a fine alignment of the collimator is required but this is not always achieved with manual manipulations. The number of counts registered by the spectrometer should thereby not be taken as a true reflection of the amount of photons effectively exiting the PPKTP crystal but rather as an indicator of the frequency of the down-conversion. Moreover, because of this potential misalignment, the time before the spectrometer reaches saturation might vary from one acquisition to the other, leading to different periods of collection and so to incomparable counts.

10.5 Limitations of the Experiment

Despite the successful implementation of the experiment, the lack of meaningful results suggested that both practical and technical constraints were limiting the source performance. This section therefore outlines the limitations that bounded the experimental work, such that potential improvements of the setup and solutions to these constraints may be determined.

As in many experimental setups, the main limitations encountered are practical as they arise from physical constraints imposed by the equipment itself. While it does not impact its capability to produce pairs of entangled-photons, the size of the Sagnac loop is subject to these limitations. Indeed, the smaller the interferometer, the more resistant it is against misalignment over time [116]. Its compactness also allows a high collection efficiency and minimizes beam clipping [55]. However, the minimal implementable size of the Sagnac interferometer is restricted by the physical constraints imposed by the spatial extension of the bulk optical elements, as well as by the need to manipulate them easily. In addition to the alignment with the mounting holes of the optical table, this is why it was chosen to work with a triangular loop measuring 12.5 cm + 17.5 cm + 12.5 cm. Although it is not the smallest interferometer that has been developed in a laboratory, its dimensions remain in the same order

of magnitude as Sagnac interferometers that have been build for entangled photon sources [57, 92, 117].

These limitations have also been observed in the focusing of laser beams at the detectors. Converging lenses have been used to focus the rays onto the active areas of the detectors, which have a diameter of 100 µm, because the single-photon detectors used in the experiment show better performance when the spot on the sensor area is small [113]. However, the only lenses available and found to be optimized at 810 nm have a short focal length of 1.2 cm. It was therefore impossible to place the detector sensor areas at the focus of the converging lenses due to the spatial extension of the lenses and their mounts but also due to the fact that the protective caps of the detectors should be easily reachable and movable. The rays are thus not perfectly focused when they arrive at the detectors, which can cause potential loss of detection performance. Additionally, the detectors are limited by their quantum efficiency which is, as expected, lower than 100%. Despite the relatively high photon detection efficiency at 810 nm (60% [113]), this results in a partial loss of the useful photons that can alter the apparent performance of the EPS.

Practical limitations also affect the focusing of the rays in the non-linear crystal. The converging lenses placed at both ends of the PPKTP crystal in the Sagnac loop enable a strong focus to enhance SPDC efficiency. Nonetheless, the choice of a two-lens configuration within the loop, with 5 cm focal lengths, resulted from a trade-off analysis, mainly driven by spatial considerations. Without these practical limits, a better configuration could have been implemented. Indeed, it is possible to optimize the focusing of a beam in a crystal, thus maximizing the conversion efficiency [108]. This is characterized by a parameter, called the beam focusing parameter, which is computed as follows:

$$\xi = \frac{L}{2z_R},$$

where L is the length of the crystal and z_R the Rayleigh range of the laser beam. With the current lens configuration in the loop, this parameter is computed to be 19.69, while the optimal focusing parameter has been determined to be $\xi = 2.84$ [108]. As the non-linear crystal is 30 mm long, the lenses should be located 18 cm from the crystal center to achieve a Rayleigh range that gives the optimal focusing parameter ξ. However, this is not feasible due to the space occupied by the mirrors, the dual-wavelength half-waveplate, the PBS and their respective mounts within the Sagnac interferometer. These spatial constraints limit the possible positions of the lenses, which explains their current positioning. Consequently, the focusing beam parameter is larger than the optimal one, so the interaction length between the crystal and the beams is short, resulting in a non-optimal conversion efficiency in the PPKTP crystal.

It was mentioned earlier that the dichroic mirrors introduced unwanted reflections in the experiment. Nevertheless, it is the case for all of the optical elements used in the setup (isolator, waveplates, mirrors, PBS, lenses, filters and polarizers). While these parasitic reflections have been used to help with the setup alignment, they represent losses of useful beam intensity. Moreover, they can interfere with the main signal, potentially leading to unwanted behaviors. In addition to these spurious beams, the optics may absorb some photons, thus inducing power losses, or even lead to their depolarization. These material limitations are complex to mitigate and impossible to avoid. They therefore must be accepted as inherent to the experimental setup and have to be accounted for during the design and the analysis of the results.

The major limitation reflected by the analysis of the results is the manual alignment of the optics, which normally require extremely precise orientations. Indeed, it has been highlighted that how the beams are focused in the PPKTP crystal and in the single-photon detectors greatly influences the SPDC efficiency and the apparent performance of the source. The optical elements that modify the propagation of the beams, like mirrors and lenses, are positioned and oriented manually, such that the alignment is imprecise and difficult to reproduce once disturbed. Therefore, although the experiment could potentially lead to promising results with a finer alignment, the current setup and alignment method inherently constrain its performance. The alignment precision was further constrained by the limited time available for experimental work.

10.6 Potential Improvements

The resources provided allowed for a good implementation of the experiment. However, some limitations could not be avoided. Potential solutions and improvements could therefore be investigated along with perspectives for future development and research. Due to time constraints, these improvements could not be carried out.

The main constraint on the performance of the current experiment is its poor alignment. A first step would be to assess the exact source of the SPDC inefficiency. To do so, a high resolution camera, or a simple photographic plate, could be used to visualize the beams exiting the non-linear crystal. It would allow to analyze the geometry of the SPDC cones and thereby determine whether the entangled photons are collinear. If they are instead in a non-collinear configuration, this could explain the inconsistent detection of entangled photons. However, the camera should be powerful enough to distinguish the faint emission of 810 nm photons that exit the crystal from the high intensity pump beam. Being able to see the shape of the cones could help with the alignment as one would have a visual support to modify the orientation of the optics that control the beam paths.

The limitations linked to the focusing of the laser beams through converging lenses could be solved by selecting other lenses, which would have more suitable focal lengths with anti-reflective coatings adapted to the work wavelengths. Indeed, with a longer focal length, the lenses placed in front of the detectors could be placed farther away, such that the active area of the sensors could coincide with their focus. This should enhance the detection efficiency. Additionally, changing the focal length of the lenses located in the Sagnac interferometer could yield a Rayleigh range that would enable the obtaining of the optimal focusing parameter ($\xi = 2.84$). As a result, the pump beams would be optimally focused inside the PPKTP crystal, therefore enhancing the SPDC efficiency.

To avoid spatial constraints linked to bulk optics, a monolithic setup could be considered. This means that all the optical elements required for the experiment are integrated in a single piece of material (often made of glass, fused silica, ceramic or even Aluminum), thereby enabling an automatic fine alignment. As a result, the angle of incidence of the beams on the PPKTP crystal would be precisely controlled, which would ensure exact fulfillment of the quasi-phase-matching condition and lead to an efficient generation of EPR pairs. On top of providing a precise alignment, a monolithic block would improve the stability of the setup and give a compact entangled photon source, therefore avoiding spatial constraints. This should enable the efficient reduction of the source dimensions, which is a key feature for the space-borne generation of entangled photons. Indeed, considering that the aim of this work is to develop an EPS that could be brought onboard a satellite, its size and weight minimization should be kept in mind when investigating further improvements. Moreover, the alignment stability provided by the monolithic block is also a great advantage against the huge vibrations the instrument has to bear during the satellite launch.

If the optics are directly manufactured with the required orientation within a solid block, there is virtually no limitation on the minimal size of the setup. As the dimensions of the source have no impact on the generation rate of photon-pairs, one might attempt to simply reduce the sizes of the different optics. However, non-linear crystals -especially the periodically poled ones- cannot be made arbitrarily small. In fact, if the non-linear crystal is too short, the interaction length between the beam and the crystal becomes insufficient, which limits the SPDC efficiency. Moreover, if the size of the whole setup is significantly reduced, the focal lengths of the lenses should also be diminished. This would result in a tighter focus of the rays in the PPKTP crystal and so in a high power density, which increases the generation rate of entangled photons. Nonetheless, if the beams are focused too close to the crystal, their angle of convergence could cause a partial clipping of the beam at the entrance of the crystal, leading to power loss and potentially parasitic reflections. Therefore, if the setup is integrated in a monolithic block, a trade-off must be made between maximizing the reduction of the EPS dimensions and maintaining its performance.

If the source were to be embedded in a spatial system, such as onboard a QKD satellite, further considerations should be taken into account. First, space-borne instruments are regularly subject to large temperature variations. The temperature of the source should thereby be actively controlled to ensure its stability, particularly around the PPKTP crystal within which SPDC occurs. Indeed, the crystal temperature modifies the length of its periodically poled domains, such that deriving from the nominal temperature modifies the quasi-phase-matching

condition and so the wavelengths of the generated photons. A heater and a thermostat would thereby be needed to ensure a stable temperature of the non-linear crystal. A thermal stability similar to the one offered by the heater currently used in the experiment ($\pm 0.1°C$) is reachable in space-borne systems [118]. This aspect should therefore not be a problem for the transposability of the source to space. If the source is made of a monolithic block, attention should be brought onto the thermal stability of the whole setup. Although the materials used for integrating space-borne sources are selected for their low coefficients of thermal expansion, active thermal control should still be implemented to prevent any alteration of the optical paths.

Space radiation should also be accounted for, if the source is to be deployed in space. Indeed, radiations might affect the optical elements by degrading their coating and thus diminishing the source performance. Therefore, space-qualified coatings should be considered rather than the common coatings of the components currently mounted in the system. Non-linear crystals are also particularly sensitive to space radiation so precautions have to be taken. Radiation can induce color center in the non-linear medium, meaning that it absorbs more light so it becomes less transparent to the laser beams. Moreover, the periodically poled domains of the PPKTP crystal could be distorted by the radiation. This would modify the quasi-phase-matching condition and so the outcome of the SPDC process, resulting in a degraded conversion efficiency. Despite the degradation of SPDC efficiency caused by space radiation, KTP crystals exhibit self-annealing properties, which means they can recover their initial state over time after being damaged by a radiation. [119]. This regeneration can be accelerated by pumping the crystal with high power laser beams. As it is better to avoid damage than recover from it, the PPKTP crystal should ideally be shielded from space radiation to ensure a safe and durable use of the EPS. Moreover, the absorption of radiation by the crystal is proportional to its length. Shorter PPKTPs are therefore preferred for space applications, although their miniaturization is inherently limited.

The last improvement to the experimental entangled photon source, aimed at enhancing its suitability for space-based QKD, would be its connection with other subsystems to enable the integration in a larger platform, such as a satellite. The source should indeed be able to direct the entangled photons it produces toward a transmitter which would allow quantum communication with ground stations. Depending on the QKD protocol implemented, the nature of the connection between the EPS and the transmitter might vary: it can consist of fiber coupling, beam collimators, ... In any case, this interface should ideally be lossless and should imperatively preserve the polarization of the photons it transmits to ensure a good implementation of the entanglement-based protocol.

If the improvements listed at the top of this section enabled good performance of the source with high SPDC efficiency, characterizing the EPS should be done before considering a space application. To do so, visibility measurements and a Bell test should be conducted again, with the aim of obtaining visibilities higher than 71% and a S-parameter greater than 2, to confirm the polarization-entanglement of the down-converted photons. On top of these tests, several characterization methods might be used to evaluate the SPDC efficiency and the quality of the entanglement of the photons. For example, a Hong-Ou-Mandel two-photon interference test [120] might be performed to verify the entanglement quality of the photons via their temporal synchronization. In this test, two photons from an EPR pair are sent simultaneously at the entrance ports of a beam splitter. Due to a special effect, called the Hong-Ou-Mandel effect, both photons are expected to exit the beam splitter through the same port if they are entangled and arrive in a perfect time overlap. This test can also be used to determine the bandwidth of the idler and signal beams, and so to identify the indistinguishability of the down-converted photons. Another method is the quantum state tomography, which aims at recreating the quantum state of a system based on a set of measurements. In the context of a source of polarization-entangled photons, these measurements correspond to polarization correlations [121]. The fidelity between the quantum state of the system, reconstructed through tomography, and an ideal entangled state reflects the degree of entanglement of the system: the higher the fidelity, the higher the entanglement quality.

Part IV
Conclusions

11 Conclusion

This thesis provided an overview of the development of a source of polarization-entangled photons, alongside its potential application for space QKD. Different technical concepts were first introduced: fundamental principles of quantum mechanics, such as the entanglement of particles, quantum key distribution and spontaneous parametric down-conversion among others. These provided the foundations for understanding the relevance of the examples presented afterwards in a state of the art. Indeed, different types of entangled photon sources were discussed, depending on their architecture, on the type of entanglement they produced and how they generated entangled-photon pairs. Multiple examples of QKD satellites were reviewed to assess the current state of the field. A particular attention was brought to the Chinese *Micius* satellite, which successfully demonstrated space-borne quantum communication technologies.

The entangled photon source tested onboard this satellite allowed for the exchange of a cryptographic key over a distance of 1120 km via the BBM92 entanglement-based protocol. This proof of concept inspired many to develop space-based quantum technologies, able to communicate with terrestrial infrastructures to create a global quantum communication network. Therefore, this work took great inspiration from this mission to implement a laser source of entangled-photons pairs. The experimental setup has been described in details, covering both the characteristics of the optical elements used in the experiment and the computations made to design it. Additionally, short theoretical reminders about the functioning of some optics were provided.

This part of the thesis also allowed to fully grasp the point of the experiment configuration. Indeed, the Sagnac interferometer, located at the heart of the setup, and the non-linear PPKTP crystal enable the generation of polarization-entangled photon pairs. This is achieved by pumping the crystal -from both directions- with a 405 nm laser beam that is down-converted, via SPDC, in two photons of equal energy: the idler and signal photons, both with a wavelength of 810 nm. Due to the degeneracy of the SPDC process and to the collinearity of the down-converted photons, these are indistinguishable as they exit the non-linear crystal. Moreover, the perfect symmetry of the Sagnac interferometer allows photons to propagate in opposite directions along identical paths. This results in these photons to remain indistinguishable as they exit the loop, such that their polarization cannot be determined unless it is measured. This key feature of the polarization Sagnac interferometer (PSI) makes it a configuration of choice for entangled photon sources in QKD applications.

Two single-photon detectors were used to analyze the generation of photons of the EPS. By placing one detector in the trajectory of photons exiting the Sagnac loop from each port of the PBS and by correlating their detections, it was possible to determine whether the source generated pairs of entangled photons. Histograms showing coincidence counts between detection events at the two detectors allowed to confirm that photons were effectively emitted simultaneously by the source, thus hinting toward the entanglement of their timing. Moreover, spectrometric measurements were performed to assess the wavelengths of the down-converted photons. This proved the energy-entanglement of the idler and signal photons as they were both determined to have a wavelength of 810 nm. The last step of the EPS characterization was to verify the polarization-entanglement of the lower-energy photons. The check has first been effectuated with visibility measurements. These indicated that only one configuration of the tests yielded a good polarization-entanglement of the photons. The visibility computed in this configuration was more than satisfactory, $\sim 92\%$ being much larger than 71%, it illustrated a good entanglement quality. However the asymmetry of the results suggested that the higher-energy photons were effectively down-converted in only one pumping direction of the crystal. This showed that, despite the successful generation of entangled photons, the implementation and alignment of the setup were not optimal, thereby significantly limiting the SPDC efficiency and the polarization-entanglement of the photons.

In the last sections of this paper, possible causes to the malfunctioning of the experiment were outlined. They were followed by potential solutions as well as necessary improvements to the source to make it suitable

for a space-based QKD applications. Indeed, diverse considerations related to the space environment, such as strong variations of temperature and space radiation, would have to be accounted for. Moreover, the connection of the EPS with a transmitter should be studied to enable the implementation of an entanglement-based QKD protocol.

This project represents one of the first groundworks for the development of experimental QKD systems at CSL. Despite the lack of fully satisfactory results, the experiment outcomes suggested that, with further refinements and punctual improvements, the performance of the developed laser source of polarization-entangled photons could be enhanced and thereby make it compatible with space-based QKD applications.

12 Perspectives

While potential short-term improvements have been presented, this work also opens the path to broader, long-term perspectives that could greatly improve the experiment and expand its objectives.

For instance, the performance of the setup could be significantly improved by resorting to an automated alignment procedure. Using feedback systems and electronically controlled optics would enable a constant monitoring of the trajectory of the beams and allow for real-time correction of the orientation of the optics. Therefore, the source would not only benefit from a fine alignment but also from the ability to be re-aligned in case a disturbance alters the setup. Implementing such automation would require a modeling of the optical paths within the experiment and identifying the key parameters to control. An algorithm could then be developed to ensure correct beam propagation through the setup and efficient pumping of the non-linear crystal.

The entangled photon source could see its flexibility improved by including more complex technologies, like an aperiodically poled KTP crystal, that allow to tune the wavelengths of the down-converted photons. Combining such technologies with broadband optics could make the source more variable and adapted to other wavelengths, transforming it into a more tunable instrument. This flexibility could be further expanded by using the setup to exploit other types of photonic entanglement.

In the long-term, modifications can be made to the setup to ensure its compatibility with space platforms. While some considerations have been outlined, broader adjustments remain possible. Indeed, one could think about the miniaturization of the EPS and its integration onto a photonic chip, making it compatible with smaller satellites like CubeSats or even nanosatellites. Beyond size and weight constraints, the source would need to be connected with other subsystems of the satellite, such as a transmitter, and it should include additional features. To enable a precise transmission of the entangled photons emitted by the EPS, components like a beacon laser and a pointing system should be included in the source. These are aspects that need to be thoroughly studied and tested to validate the source suitability for space-based quantum communication.

Finally, the natural next step after demonstrating the well-functioning of the experiment in a laboratory would be to test its performance in real-world conditions. The generation rate of pairs of polarization-entangled photons should be tested in an environment that is not perfectly controlled. This would assess whether the source would be ready for realistic free-space transmissions. Moreover, its compatibility with entanglement-based QKD protocols should also be verified by integrating the EPS in a complete quantum communication system.

In summary, this thesis established an experimental foundation for the generation of pairs of polarization-entangled photons and presented the key aspects that need to be investigated for adapting the source to space-based QKD applications.

References

[1] C.-Y. Lu et al. “Micius quantum experiments in space”. In: *Reviews of Modern Physics* 94.3 (2022). DOI: 10.1103/RevModPhys.94.035001.

[2] European Union. *Quantum Communication Infrastructure (EuroQCI)*. Consulted on 2025-06-02. 2025. URL: https://hadea.ec.europa.eu/programmes/connecting-europe-facility/about/quantum-communication-infrastructure-euroqci_en.

[3] European Union. *IRIS² | Secure Connectivity*. Consulted on 2025-06-02. 2024. URL: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en.

[4] European Space Agency. *Eagle-1*. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1. Consulted on 2025-05-29. Sept. 2022.

[5] European Space Agency. *Secure Communication via Quantum Cryptography*. Consulted on 2025-06-02. 2024. URL: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Secure_communication_via_quantum_cryptography.

[6] European Space Agency. *Caramuel – GEO QKD Hosted Payload (Phase A)*. Consulted on 2025-06-02. 2025. URL: https://connectivity.esa.int/projects/caramuel.

[7] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: public key distribution and coin tossing”. In: *International conference on Computers, Systems and Signal Processing*. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84 1 (Dec. 1984), pp. 176–179. DOI: 10.1016/j.tcs.2014.05.025.

[8] Ramona Wolf. *Quantum Key Distribution: An Introduction with Exercises*. en. Vol. 988. Lecture Notes in Physics. Cham: Springer International Publishing, 2021. DOI: 10.1007/978-3-030-73991-1.

[9] A. Einstein, B. Podolsky, and N. Rosen. “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” In: *Physical Review* 47 (May 1935). Publisher: American Physical Society, pp. 777–780. DOI: 10.1103/PhysRev.47.777.

[10] J. S. Bell. “On the Einstein Podolsky Rosen paradox*”. en. In: *Physics* 1 (Nov. 1964). Publisher: Physics Publishing Co., pp. 195–200.

[11] John F. Clauser et al. “Proposed Experiment to Test Local Hidden-Variable Theories”. In: *Physical Review Letters* 23.15 (Oct. 1969). Publisher: American Physical Society, pp. 880–884. DOI: 10.1103/PhysRevLett.23.880.

[12] Stuart J. Freedman and John F. Clauser. “Experimental Test of Local Hidden-Variable Theories”. en. In: *Physical Review Letters* 28.14 (Apr. 1972), pp. 938–941. DOI: 10.1103/PhysRevLett.28.938.

[13] Alain Aspect, Philippe Grangier, and Gérard Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment* : A New Violation of Bell’s Inequalities”. en. In: *Physical Review Letters* 49.2 (July 1982), pp. 91–94. DOI: 10.1103/PhysRevLett.49.91.

[14] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Physical Review Letters* 67.6 (Aug. 1991). Publisher: American Physical Society, pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[15] C. H. Bennett and G. Brassard. “Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working]”. In: *SIGACT News* 20.4 (Nov. 1989), pp. 78–80. DOI: 10.1145/74074.74087.

[16] Eli Biham et al. *A Proof of the Security of Quantum Key Distribution*. Dec. 1999. DOI: 10.48550/arXiv.quant-ph/9912053.

[17] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. In: *Physical Review Letters* 85.2 (July 2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441.

[18] Nicolas Gisin et al. “Quantum cryptography”. In: *Reviews of Modern Physics* 74.1 (Mar. 2002). Publisher: American Physical Society, pp. 145–195. DOI: 10.1103/RevModPhys.74.145.

[19] PostQuantum. *Entanglement-Based QKD Protocols: E91 and BBM92*. Consulted on 2025-05-30. Apr. 2020.

[20] Charles H. Bennett, Gilles Brassard, and N. David Mermin. “Quantum cryptography without Bell’s theorem”. en. In: *Physical Review Letters* 68.5 (Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557.

[21] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. en. In: *Nature* 299.5886 (Oct. 1982). Publisher: Nature Publishing Group, pp. 802–803. DOI: 10.1038/299802a0.

[22] D. Dieks. “Communication by EPR devices”. en. In: *Physics Letters A* 92.6 (Nov. 1982), pp. 271–272. DOI: 10.1016/0375-9601(82)90084-6.

[23] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. “Privacy Amplification by Public Discussion”. In: *SIAM Journal on Computing* 17.2 (Apr. 1988). Publisher: Society for Industrial and Applied Mathematics, pp. 210–229. DOI: 10.1137/0217014.

[24] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-Device-Independent Quantum Key Distribution”. In: *Physical Review Letters* 108.13 (Mar. 2012). Publisher: American Physical Society, p. 130503. DOI: 10.1103/PhysRevLett.108.130503.

[25] Peter Schartner and Stefan Rass. “Quantum key distribution and Denial-of-Service: Using strengthened classical cryptography as a fallback option”. In: *2010 International Computer Symposium (ICS2010)* (Dec. 2010), pp. 131–136. DOI: 10.1109/COMPSYM.2010.5685533.

[26] Renato Renner and Ramona Wolf. *The debate over QKD: A rebuttal to the NSA’s objections*. en. July 2023. DOI: 10.48550/arXiv.2307.15116.

[27] Zhao Yi. *Quantum Cryptography in Real-life Applications: Assumptions and Security*. 2009.

[28] Mark Fox. “Quantum Optics: An Introduction”. In: Oxford University Press, 2006. Chap. 2, pp. 8–24.

[29] François Sanchez. “Optique non-linéaire - Cours et problèmes résolus”. fr. In: Éditions Ellipses, 1999. Chap. 3, pp. 51–55.

[30] Felix Bussieres. “Intrication temporelle et communication quantique”. fr. PhD thesis. Ecole Polytechnique de Montréal, 2009.

[31] Christophe Couteau. “Spontaneous parametric down-conversion”. In: *Contemporary Physics* 59.3 (July 2018). Publisher: Taylor & Francis, pp. 291–304. DOI: 10.1080/00107514.2018.1488463.

[32] Hee Jung Lee et al. “Generation of bright visible photon pairs using a periodically poled stoichiometric lithium tantalate crystal”. en. In: *Optics Express* 23.11 (June 2015), p. 14203. DOI: 10.1364/OE.23.014203.

[33] Matthias Bock et al. “Highly efficient heralded single-photon source for telecom wavelengths based on a PPLN waveguide”. en. In: *Optics Express* 24.21 (Oct. 2016), p. 23992. DOI: 10.1364/OE.24.023992.

[34] Robert W. Boyd. *Nonlinear optics*. en. Fourth edition. London: Elsevier, AP Academic Press, 2020. DOI: 10.1016/C2015-0-05510-1.

[35] W. Sellmeier. “Ueber die durch die Aetherschwingungen erregten Mitschwingungen der Körpertheilchen und deren Rückwirkung auf die ersteren, besonders zur Erklärung der Dispersion und ihrer Anomalien”. de. In: *Annalen der Physik* 223.11 (Jan. 1872), pp. 386–403. DOI: 10.1002/andp.18722231105.

[36] Gorachand Ghosh. “Sellmeier coefficients and dispersion of thermo-optic coefficients for some optical glasses”. en. In: *Applied Optics* 36.7 (Mar. 1997), p. 1540. DOI: 10.1364/AO.36.001540.

[37] Maria Chekhova and Peter Banzer. *Polarization of Light: In Classical, Quantum, and Nonlinear Optics*. De Gruyter, Mar. 2021. DOI: 10.1515/9783110668025.

[38] Ziqi Zeng et al. “Controllable transitions among phase-matching conditions in a single nonlinear crystal”. EN. In: *Chinese Optics Letters* 22.2 (Feb. 2024), p. 021901. DOI: 10.3788/COL202422.021901.

[39] Paul G. Kwiat et al. “Ultrabright source of polarization-entangled photons”. In: *Physical Review A* 60.2 (Aug. 1999). Publisher: American Physical Society, R773–R776. DOI: 10.1103/PhysRevA.60.R773.

[40] Peter E. Powers and Joseph W. Haus. *Fundamentals of nonlinear optics*. en. Second edition. Boca Raton: CRC Press, Taylor & Francis Group, 2017.

[41] Shigeki Takeuchi. “Beamlike twin-photon generation by use of type II parametric downconversion”. en. In: *Optics Letters* 26.11 (June 2001), p. 843. DOI: 10.1364/OL.26.000843.

[42] Marco Fiorentino, Christopher E. Kuklewicz, and Franco N. C. Wong. “Source of polarization entanglement in a single periodically poled KTiOPO4 crystal with overlapping emission cones”. en. In: *Optics Express* 13.1 (2005), p. 127. DOI: 10.1364/OPEX.13.000127.

[43] Franz X. Kärtner and Tobias Herr. *Nonlinear Optics - Lecture Notes, Chapter 4*. https://ufox.cfel.de/teaching/winter_semester_2021_2022/. Lecture notes from the Winter Semester 2021/22 course at CFEL, University of Hamburg. Oct. 2021.

[44] Alexander Mamrashev et al. “Optical Properties of KTP Crystals and Their Potential for Terahertz Generation”. en. In: *Crystals* 8.8 (July 2018), p. 8. DOI: 10.3390/cryst8080310.

[45] Chao Zhang et al. “Spontaneous Parametric Down-Conversion Sources for Multiphoton Experiments”. en. In: *Advanced Quantum Technologies* 4.5 (2021), p. 2000132. DOI: 10.1002/qute.202000132.

[46] Orazio Svelto et al. “Lasers and Coherent Light Sources”. en. In: *Springer Handbook of Lasers and Optics*. Ed. by Frank Träger. New York, NY: Springer, 2007, pp. 583–936. DOI: 10.1007/978-0-387-30420-5_11.

[47] Sidney A. Self. “Focusing of spherical Gaussian beams”. en. In: *Applied Optics* 22.5 (Mar. 1983), p. 658. DOI: 10.1364/AO.22.000658.

[48] Dominik Maximilian Soliman. “Augmented microscopy: Development and application of high-resolution optoacoustic and multimodal imaging techniques for label-free biological observation”. de. PhD thesis. Technischen Universität München, 2016.

[49] Edmund Optics. *Beam Quality and Strehl Ratio*. en. https://www.edmundoptics.com/knowledge-center/application-notes/lasers/beam-quality-and-strehl-ratio/. Consulted on 2025-04-24.

[50] Lucas Hofer. *M^2 Measurement*. en. https://dataray.com/blog/m-measurement. Consulted on 2025-04-18. 2016.

[51] Shojiro Nemoto. “Waist shift of a Gaussian beam by plane dielectric interfaces”. en. In: *Applied Optics* 27.9 (May 1988), p. 1833. DOI: 10.1364/AO.27.001833.

[52] Georges Sagnac. “L’éther lumineux démontré par l’effet du vent relatif d’éther dans un interféromètre en rotation uniforme.” fr. In: *Comptes rendus hebdomadaires des séances de l’Académie des sciences* 157 (1913).

[53] B Culshaw. “The optical fibre Sagnac interferometer: an overview of its principles and applications”. en. In: *Measurement Science and Technology* 17.1 (Jan. 2006), R1–R16. DOI: 10.1088/0957-0233/17/1/R01.

[54] A. Motazedifard et al. “Nonlocal realism tests and quantum state tomography in Sagnac-based type-II polarization-entanglement SPDC-source”. In: *Heliyon* 7.6 (2021). DOI: 10.1016/j.heliyon.2021.e07384.

[55] Taehyun Kim, Marco Fiorentino, and Franco N. C. Wong. “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”. In: *Physical Review A* 73.1 (Jan. 2006). Publisher: American Physical Society, p. 012316. DOI: 10.1103/PhysRevA.73.012316.

[56] Rui-Bo Jin et al. “Pulsed Sagnac polarization-entangled photon source with a PPKTP crystal at telecom wavelength”. EN. In: *Optics Express* 22.10 (May 2014). Publisher: Optica Publishing Group, pp. 11498–11507. DOI: 10.1364/OE.22.011498.

[57] Heonoh Kim, Osung Kwon, and Han Seb Moon. “Pulsed Sagnac source of polarization-entangled photon pairs in telecommunication band”. en. In: *Scientific Reports* 9.1 (Mar. 2019). Publisher: Nature Publishing Group, p. 5031. DOI: 10.1038/s41598-019-41633-z.

[58] M. V. Jabir and G. K. Samanta. “Robust, high brightness, degenerate entangled photon source at room temperature”. en. In: *Scientific Reports* 7.1 (Oct. 2017). Publisher: Nature Publishing Group, p. 12613. DOI: 10.1038/s41598-017-12709-5.

[59] S. Tanzilli et al. “PPLN Waveguide for Quantum Communication”. In: *The European Physical Journal D - Atomic, Molecular and Optical Physics* 18.2 (Feb. 2002), pp. 155–160. DOI: 10.1140/epjd/e20020019.

[60] Shalom EO. *BBO Crystals supporting the research of quantum entanglements*. https://www.shalomeo.com/BBO-Crystals-SPDC-Shalomeo.html. Consulted on 2025-05-27.

[61] Thorlabs, Inc. *BBO Crystals for Spontaneous Parametric Down-Conversion (SPDC)*. https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=16384. Consulted on 2025-05-27. 2024.

[62] Joshua W. Silverstone et al. “Silicon Quantum Photonics”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 22.6 (Nov. 2016), pp. 390–402. DOI: 10.1109/JSTQE.2016.2573218.

[63] Hiroki Takesue and Kyo Inoue. “Generation of polarization entangled photon pairs and violation of Bell’s inequality using spontaneous four-wave mixing in fiber loop”. en. In: *Physical Review A* 70.3 (Sept. 2004), p. 031802. DOI: 10.1103/PhysRevA.70.031802.

[64] Mallory Pickett. “Quantum Dots Serve Entangled Photons on Demand”. In: *Physics* 11 (2018), p. 82.

[65] Jonathan R. A. Müller et al. “Active reset of a radiative cascade for entangled-photon generation beyond the continuous-driving limit”. In: *Physical Review Research* 2.4 (Nov. 2020). Publisher: American Physical Society, p. 043292. DOI: 10.1103/PhysRevResearch.2.043292.

[66] S. E. Harris, M. K. Oshman, and R. L. Byer. “Observation of Tunable Optical Parametric Fluorescence”. In: *Physical Review Letters* 18.18 (May 1967). Publisher: American Physical Society, pp. 732–734. DOI: 10.1103/PhysRevLett.18.732.

[67] W. Tittel et al. “Quantum Cryptography Using Entangled Photons in Energy-Time Bell States”. In: *Physical Review Letters* 84.20 (May 2000). Publisher: American Physical Society, pp. 4737–4740. DOI: 10.1103/PhysRevLett.84.4737.

[68] Yuan Qian and Zhao Sheng-mei. “Quantum key distribution based on Orbital Angular Momentum”. In: *2010 IEEE 12th International Conference on Communication Technology*. Nov. 2010, pp. 1228–1231. DOI: 10.1109/ICCT.2010.5689105.

[69] X. Yan et al. “Decoherence of orbital angular momentum tangled photons in non-Kolmogorov turbulence”. eng. In: *Journal of the Optical Society of America. A, Optics, Image Science, and Vision* 33.9 (Sept. 2016), pp. 1831–1835. DOI: 10.1364/JOSAA.33.001831.

[70] Filippus S. Roux. *Decoherence of orbital angular momentum entanglement in a turbulent atmosphere*. Sept. 2010. DOI: 10.48550/arXiv.1009.1956.

[71] T. Jennewein et al. “Quantum cryptography with entangled photons”. In: *Physical Review Letters* 84.20 (2000), pp. 4729–4732. DOI: 10.1103/PhysRevLett.84.4729.

[72] Gregoire Ribordy et al. “Long distance entanglement based quantum key distribution”. In: *Physical Review A* 63.1 (Dec. 2000), p. 012309. DOI: 10.1103/PhysRevA.63.012309.

[73] Giuseppe Vallone et al. “Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons”. en. In: *Physical Review Letters* 113.6 (Aug. 2014), p. 060503. DOI: 10.1103/PhysRevLett.113.060503.

[74] Mario Krenn et al. “Twisted light transmission over 143 km”. In: *Proceedings of the National Academy of Sciences* 113.48 (Nov. 2016). Publisher: Proceedings of the National Academy of Sciences, pp. 13648–13653. DOI: 10.1073/pnas.1612023113.

[75] Davide Grassani et al. *A micrometer-scale integrated silicon source of time-energy entangled photons*. Sept. 2014. DOI: 10.48550/arXiv.1409.4881.

[76] Robert Bedingtori et al. "Small photon entangling quantum systems (SPEQS) enabling space based quantum key distribution (QKD): 66th International Astronautical Congress 2015: Space - The Gateway for Mankind's Future, IAC 2015". In: *66th International Astronautical Congress 2015, IAC 2015*. Proceedings of the International Astronautical Congress, IAC (2015), pp. 3623–3628.

[77] Lukas Knips et al. "QUBE – Towards Quantum Key Distribution with Small Satellites". en. In: *Quantum 2.0 Conference and Exhibition*. Boston, MA: Optica Publishing Group, 2022, QTh3A.6. DOI: 10.1364/QUANTUM.2022.QTh3A.6.

[78] Claire Autebert et al. "Multi-user quantum key distribution with entangled photons from an AlGaAs chip". In: *Quantum Science and Technology* 1.1 (Dec. 2016), 01LT02. DOI: 10.1088/2058-9565/1/1/01LT02.

[79] Trevor J. Steiner et al. *Continuous Entanglement Distribution from an AlGaAs-on-Insulator Microcomb for Quantum Communications*. Oct. 2023. DOI: 10.48550/arXiv.2310.14112.

[80] Cuo Wu et al. "Room-temperature on-chip orbital angular momentum single-photon sources". In: *Science Advances* 8.2 (2022), eabk3075. DOI: 10.1126/sciadv.abk3075.

[81] Faraz Najafi et al. "On-Chip Detection of Entangled Photons by Scalable Integration of Single-Photon Detectors". In: *Nature Communications* 6.1 (Jan. 2015), p. 5873. DOI: 10.1038/ncomms6873.

[82] Hatam Mahmudlu et al. "Fully on-chip photonic turnkey quantum source for entangled qubit/qudit state generation". en. In: *Nature Photonics* 17.6 (June 2023). Publisher: Nature Publishing Group, pp. 518–524. DOI: 10.1038/s41566-023-01193-1.

[83] P A Hiskett et al. "Long-distance quantum key distribution in optical fibre". en. In: *New Journal of Physics* 8.9 (Sept. 2006), p. 193. DOI: 10.1088/1367-2630/8/9/193.

[84] Alberto Boaron et al. "Secure quantum key distribution over 421 km of optical fiber". In: *Physical Review Letters* 121.19 (Nov. 2018), p. 190502. DOI: 10.1103/PhysRevLett.121.190502.

[85] Qiang Zhang et al. "Large scale quantum key distribution: challenges and solutions". In: *Optics Express* 26.18 (Sept. 2018), p. 24260. DOI: 10.1364/OE.26.024260.

[86] M Stanley et al. "Recent Progress in Quantum Key Distribution Network Deployments and Standards". en. In: *Journal of Physics: Conference Series* 2416.1 (Dec. 2022), p. 012001. DOI: 10.1088/1742-6596/2416/1/012001.

[87] Stefanie Häusler et al. "Evaluation of integration concepts of Optical Ground Stations for satellite-based Quantum Key Distribution into a quantum network". In: *2023 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. Oct. 2023, pp. 209–216. DOI: 10.1109/ICSOS59710.2023.10491230.

[88] P Villoresi et al. "Experimental verification of the feasibility of a quantum channel between space and Earth". en. In: *New Journal of Physics* 10.3 (Mar. 2008), p. 033038. DOI: 10.1088/1367-2630/10/3/033038.

[89] Sheng-Kai Liao et al. "Satellite-to-ground quantum key distribution". en. In: *Nature* 549.7670 (Sept. 2017), pp. 43–47. DOI: 10.1038/nature23655.

[90] Richard J Hughes et al. "Practical free-space quantum key distribution over 10 km in daylight and at night". en. In: *New Journal of Physics* 4.1 (July 2002), p. 43. DOI: 10.1088/1367-2630/4/1/343.

[91] Sheng-Kai Liao et al. "Satellite-Relayed Intercontinental Quantum Network". In: *Physical Review Letters* 120.3 (Jan. 2018). Publisher: American Physical Society, p. 030501. DOI: 10.1103/PhysRevLett.120.030501.

[92] Juan Yin et al. "Satellite-based entanglement distribution over 1200 kilometers". en. In: *Science* 356.6343 (June 2017), pp. 1140–1144. DOI: 10.1126/science.aan3211.

[93] Juan Yin et al. “Entanglement-based secure quantum cryptography over 1,120 kilometres”. eng. In: *Nature* 582.7813 (June 2020), pp. 501–505. DOI: 10.1038/s41586-020-2401-y.

[94] Charles H. Bennett et al. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. In: *Physical Review Letters* 70.13 (Mar. 1993). Publisher: American Physical Society, pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895.

[95] Ji-Gang Ren et al. “Ground-to-satellite quantum teleportation”. eng. In: *Nature* 549.7670 (Sept. 2017), pp. 70–73. DOI: 10.1038/nature23675.

[96] SpeQtral. *SpooQy-1 CubeSat Mission*. https://www.nanosats.eu/sat/spooqy-1. Consulted on 2025-05-29. Singapore, Apr. 2019.

[97] Yang Li et al. “Microsatellite-based real-time quantum key distribution”. en. In: *Nature* 640.8057 (Apr. 2025). Publisher: Nature Publishing Group, pp. 47–54. DOI: 10.1038/s41586-025-08739-z.

[98] German Aerospace Center (DLR). *QUBE-II - Quantum Key Distribution with CubeSat*. https://www.dlr.de/en/kn/research-transfer/projects/qkd-quantum-technology-for-secure-communication/qube-ii-quantum-key-distribution-with-cubesat. Consulted on 2025-05-29. Weßling, Germany, Jan. 2025.

[99] Thomas Jennewein et al. *QEYSSat 2.0 – White Paper on Satellite-based Quantum Communication Missions in Canada*. Jan. 2024. DOI: 10.48550/arXiv.2306.02481.

[100] Inc. Coherent. *OBIS LX SF - Single Frequency Narrow Linewidth Lasers Datasheet*. https://www.coherent.com/content/dam/coherent/site/en/resources/datasheet/lasers/obis-lx-sf-ds.pdf. Consulted on 2025-03-05.

[101] Raicol Crystals. *PPKTP Crystal Selection Guide*. Consulted on 2025-05-25. n.d.

[102] Youn-Chang Jeong, Kang-Hee Hong, and Yoon-Ho Kim. “Bright source of polarization-entangled photons using a PPKTP pumped by a broadband multi-mode diode laser”. EN. In: *Optics Express* 24.2 (Jan. 2016). Publisher: Optica Publishing Group, pp. 1165–1174. DOI: 10.1364/OE.24.001165.

[103] Thorlabs. *IO-3D-405-PBS Free-Space Optical Isolator, 405 nm, Ø2.7 mm Max Beam, 1.5 W Max*. https://www.thorlabs.com/thorproduct.cfm?partnumber=IO-3D-405-PBS. Consulted on 2025-04-23.

[104] MKS Instruments, Newport. *Introduction to Waveplates*. https://www.newport.com/n/introduction-to-waveplates. Consulted on 2025-05-17.

[105] Svenska LaserFabriken. *PPKTP Crystals*. https://www.laserfabriken.com/ppktp/. Consulted on 2025-02-24. 2025.

[106] Kiyoshi Kato and Eiko Takaoka. “Sellmeier and thermo-optic dispersion formulas for KTP”. EN. In: *Applied Optics* 41.24 (Aug. 2002). Publisher: Optica Publishing Group, pp. 5040–5044. DOI: 10.1364/AO.41.005040.

[107] Shai Emanueli and Ady Arie. “Temperature-Dependent Dispersion Equations for KTiOPO4 and KTiOAsO4”. en. In: *Applied Optics* 42.33 (2003), p. 6661. DOI: 10.1364/AO.42.006661.

[108] G. D. Boyd and D. A. Kleinman. “Parametric Interaction of Focused Gaussian Light Beams”. en. In: *Journal of Applied Physics* 39.8 (July 1968), pp. 3597–3639. DOI: 10.1063/1.1656831.

[109] GaussianBeam Project. *GaussianBeam: Gaussian Optics Simulator*. 2008.

[110] S. Meraner et al. “Approaching the tsirelson bound with a sagnac source of polarization-entangled photons”. In: *SciPost Physics* 10.1 (2021). DOI: 10.21468/SCIPOSTPHYS.10.1.017.

[111] Thorlabs. *DMSP490: Protective Silver Coated Mirrors*. https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9240&pn=DMSP490. Consulted on 2025-03-11. 2018.

[112] RP Photonics. *Avalanche Photodiodes*. https://www.rp-photonics.com/avalanche_photodiodes.html. Consulted on 2025-06-01.

[113] Thorlabs. *SPDMH2 - Single-Photon Detector Module, FC/PC*. https://www.thorlabs.com/thorproduct.cfm?partnumber=SPDMH2. Consulted on 2025-02-15.

[114] ID Quantique. *ID1000 Time Controller*. https://www.idquantique.com/quantum-detection-systems/products/id1000-time-controller/. Consulted on 2025-05-07. 2024.

[115] Ali Motazedifard, Seyed Ahmad Madani, and N. S. Vayaghan. "Measurement of entropy and quantum coherence properties of two type-I entangled photonic qubits". en. In: *Optical and Quantum Electronics* 53.7 (July 2021), p. 378. DOI: 10.1007/s11082-021-03067-8.

[116] Vasile-Laurentiu Dosan et al. "Construction and characterization of a Sagnac-based entangled-photon source". en. In: *Romanian Reports in Physics* 74 (2022), p. 119. DOI: 10.48550/arXiv.2208.10140.

[117] Neng Cai et al. "Broadband-laser-diode pumped periodically poled potassium titanyl phosphate-Sagnac polarization-entangled photon source". EN. In: *JOSA B* 39.1 (Jan. 2022). Publisher: Optica Publishing Group, pp. 77–82. DOI: 10.1364/JOSAB.437808.

[118] Leijie Jiang et al. "High-precision and wide-range temperature measurement and control system of satellite-borne calibration blackbody". In: *Measurement* 231 (May 2024), p. 114591. DOI: 10.1016/j.measurement.2024.114591.

[119] Hossain A. Abdeldayem et al. *Contamination and Radiation Effects on Nonlinear Crystals for Space Laser Systems*. July 2005.

[120] C. K. Hong, Z. Y. Ou, and L. Mandel. "Measurement of subpicosecond time intervals between two photons by interference". en. In: *Physical Review Letters* 59.18 (Nov. 1987), pp. 2044–2046. DOI: 10.1103/PhysRevLett.59.2044.

[121] Daniel F. V. James et al. "Measurement of qubits". In: *Physical Review A* 64.5 (Nov. 2001). Publisher: American Physical Society, p. 052312. DOI: 10.1103/PhysRevA.64.052312.

A Optical Components References

A.1 Optical Table and Breadboard

Figure 47: RS4000 Top performance optical table with six precision tuned dampers, from Newport.

https://www.newport.com/g/optical-tables

Figure 48: Industrial grade 3.4 mm skin honeycomb optical breadboard, from Newport.

https://www.newport.com/f/ig-3.4-mm-skin-honeycomb-core-breadboards

A.2 Laser Source

Figure 49: Laser OBIS LX 405 nm 40 mW, single mode, single frequency narrow linewidth, from Coherent.

https://www.coherent.com/content/dam/coherent/site/en/resources/datasheet/lasers/obis-lx-sf-ds.pdf

A.3 Optical Isolator

Figure 50: IO-3D-405-PBS - Free-space isolator, optimized for 405 nm, max beam diameter of 2.7 mm, max input power of 1.5 W, from Thorlabs.

https://www.thorlabs.com/thorproduct.cfm?partnumber=IO-3D-405-PBS

A.4 Quarter-Waveplate

Air-spaced 0th order quarter-waveplate, optimized for 405 nm, 15.0 mm diameter, 1" mounted, from Newlight photonics.
https://www.newlightphotonics.com/Waveplates/Air-Spaced-0th-Order-Waveplates

A.5 Half-Waveplate

Figure 51: Achromatic half-waveplate 10RP52-1B made in Quartz-MgF_2, 25.4 mm diameter, optimized for the range 400-700 nm, from Newport.

https://www.newport.com/n/introduction-to-waveplates

A.6 Mirror Outside the Sagnac Loop

Figure 52: UV aluminum mirror 20D20AL.2, Borofloat, 50.8 mm diameter, λ/10 surface flatness, optimized for the 250-600 nm range, from Newport.

https://www.newport.com/p/20D20AL.2

A.7 Dichroic Mirror

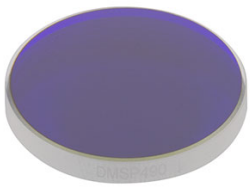


Figure 53: Shortpass dichroic mirror DMSP490, 1" diameter, 490 nm cutoff wavelength, from Thorlabs.

https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9240&pn=DMSP490

A.8 Polarizing Beam Splitter Cube

Figure 54: Polarizing beam splitter cube PBS0025-405/810, size 25.4x25.4x25.4mm, spectral range: dual wavelength @ 405 and 810 nm, from Newlight photonics.

https://www.newlightphotonics.com/index.php?route=product/search&search=PBS0025-405%2F810

A.9 Dual Wavelength Half-Waveplate

Dual wavelength half-waveplate, @810nm + @405nm, diameter of 15mm, 1" mounted, from Newlight photonics.
https://www.newlightphotonics.com/Waveplates/Dual-Wavelength-Waveplates

A.10 Mirror Inside the Sagnac Loop

Figure 55: Dielectric mirror 10Q620BB.HR2, high reflector, 25.4 mm diameter, 0-50° angle of incidence, optimized for the range 350-1100 nm, from Newport.

https://www.newport.com/p/10Q620BB.HR2

A.11 Converging Lens Inside the Loop

Figure 56: LA1131-AB - N-BK7 Plano-convex lens, 1" diameter, focal length f = 50 mm, anti-reflective coating for 400 - 1100 nm, from Thorlabs.

`https://www.thorlabs.com/thorproduct.cfm?partnumber=LA1131-AB`

A.12 Periodically Poled KTP Non-Linear Crystal

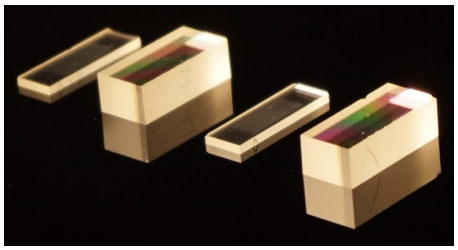


Figure 57: PPKTP crystal, from Svenska LaserFabriken. The crystal on the left of the figure corresponds to the dimensions of the one used in the experiment.

`https://www.laserfabriken.com/ppktp/`

A.13 Long-Pass Filter

Figure 58: FELH0600 Longpass filter, 25.0 mm diameter, cut-on wavelength: 600 nm, from Thorlabs.

`https://www.thorlabs.com/thorproduct.cfm?partnumber=FELH0600`

A.14 Converging Lens Outside the Sagnac Loop

Figure 59: Converging lens #64-580, 12.7 mm diameter, effective focal length of 12.70 mm, NIR coated, molded acrylic aspheric lens, from Edmund optics.

`https://www.edmundoptics.eu/p/127mm-dia-f-1-nir-coated-molded-acrylic-aspheric-lens/19292/`

A.15 Single-Photon Detector

Figure 60: SPDMH2 - Single-photon detection module, optimized detection for the 400 - 1000 nm range, 100 µm diameter of active area, 100 hz dark count rate, from Thorlabs.

`https://www.thorlabs.com/thorproduct.cfm?partnumber=SPDMH2`

A.16 Time Controller

Figure 61: ID1000 Time controller series, all-in-one time-tagging, coincidence correlation and delay/pulse generation, from ID Quantique.

`https://www.idquantique.com/quantum-detection-systems/products/id1000-time-controller/`