universität wien

DISSERTATION / DOCTORAL THESIS

Titel der Dissertation /Title of the Doctoral Thesis

„Single photons for quantum information: demonstration of novel quantum communication schemes and realization of a narrow-bandwidth source for interaction with atoms“

verfasst von / submitted by

Francesco Massa

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Doktor der Naturwissenschaften
(Dr. rer. nat.)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 796 605 411
Dissertationsgebiet lt. Studienblatt / field of study as it appears on the student record sheet:	Physik
Betreut von / Supervisor:	Univ.-Prof. Dr. Philip Walther

Abstract

Quantum technologies promise to revolutionize the future of information processing as they allow for applications such as perfectly secure communication and computers that are able to perform specific computational tasks faster than any classical machine. For this reason, quantum information science has come to represent one of the main research fields in nowadays physics.

Single photons, the quanta of light, are a suitable platform for encoding and processing quantum information. In particular, due to their mobility, photons are the most natural choice for quantum communication.

One of the main drawbacks of single photons is their lack of interaction, which complicates the realization of photonic "quantum transistors", necessary for quantum computation and simulation. Furthermore, in all experimental situations photons need to propagate in non-ideal material media, which therefore present a finite amount of loss. Photon loss induces errors in quantum computation protocols and hinders long-distance quantum communication.

Many research efforts in quantum photonics are therefore devoted to overcoming these problems through technological improvement. Interaction of single photons with matter - atoms, molecules or solid state systems - can provide a solution to both issues. Photon-photon interaction, in fact, can be realized by using material systems as mediators. Losses in communication, instead, can be countered by quantum repeaters. These devices are based on quantum memories that allow one to store the information carried by the photons in the internal states of matter and retrieve it at a later moment.

Yet, the research endeavors in photonic quantum information processing are not limited only to technical achievements. Important insights have also come from the investigation of novel quantum phenomena opening up new quantum protocols, which provide advantages over classical or previously designed ones.

This thesis covers both research directions and presents different kinds of experimental projects. The first two projects describe the development and implementation of novel quantum communication protocols. The third one consists in the realization of a narrow-band single-photon source for interaction with atoms.

In the first quantum communication protocol, it is experimentally demonstrated that a single photon in quantum superposition allows for the simultaneous transmission of two classical bits between two distant parties in two opposite communication directions, an impossible task in classical physics. This phenomenon is used to develop and implement a secure quantum communication protocol, in which the communication direction between the parties remains private.

In the second protocol the two parties aim to establish a secure shared cryptographic key without employing quantum resources, which are delegated to an untrusted third party, acting as a server. In this sense, this is a semi-quantum key distribution protocol. The protocol is demonstrated and the secure key rate is extracted taking into account the main experimental imperfections of the setup.

The third project is more technical. A source of photon pairs with spectral bandwidth of about 10 MHz is built and characterized. Due to this narrow bandwidth, the produced photons can be efficiently coupled to atomic hyperfine transitions. The photons are emitted at a wavelength of 780 nm, and thus are tuned to the hyperfine transitions of Rubidium D2 line. The source is based on cavity-enhanced spontaneous parametric down conversion, which is a reliable, feasible and flexible technique for narrow-bandwidth photon generation, and outperforms in brightness previous narrow-bandwidth sources at the same wavelength. This resource is meant to be used for the realization of a two-photon gate mediated by Rubidium atoms, in collaboration with external research groups.

Zusammenfassung

Quantentechnologien versprechen die Zukunft der Informationsverarbeitung zu revolutionieren, da sie Anwendungen, wie die perfekt sichere Kommunikation sowie den Bau von Computern ermöglichen, die bestimmte Rechenaufgaben schneller als jede klassische Maschine ausführen können. Aus diesem Grund ist die Quanteninformationsforschung zu einem der Hauptforschungsbereiche der heutigen Physik geworden.

Einzelne Photonen, sogenannte Lichtquanten, sind eine geeignete Plattform zum Kodieren und Verarbeiten von Quanteninformationen. Insbesondere aufgrund ihrer Mobilität sind Photonen die natürlichste Wahl für Quantenkommunikation.

Einer der Hauptnachteile von Photonen ist die fehlende Wechselwirkung zwischen ihnen, was die Realisierung von photonischen "Quantentransistoren" behindert, die für die Quantenberechnung und Quantensimulation notwendig sind. Außerdem müssen sich die Photonen, unter experimentellen Bedingungen, in nicht idealen Medien ausbreiten, was einen Lichtverlust verursachen kann. Der Verlust von Photonen führt zu Fehlern in den Quantenberechnungsprotokollen und behindert die Quantenkommunikation über große Entfernungen.

Viele Forschungsanstrengungen in der Quantenphotonik widmen sich daher der Überwindung dieser Probleme durch technologische Verbesserungen. Die Wechselwirkung einzelner Photonen mit Materie - Atomen, Molekülen oder Festkörpersystemen - kann beide Probleme lösen. Es kann sogar eine Photon-Photon-Wechselwirkung unter Verwendung von Materialsystemen als Mediatoren realisiert werden. Photonenverluste in Quantenkommunikation können durch Quanten-Repeatern ausgeglichen werden. Diese

Geräte basieren auf Quantenspeichern, die realisiert werden, indem die getragenen Informationen in den internen Zuständen der Materie gespeichert und zu einem späteren Zeitpunkt abgerufen werden können.

Die Forschungsarbeiten zur photonischen Quanteninformation beschränken sich jedoch nicht nur auf technische Errungenschaften. Wichtige Erkenntnisse stammen ebenfalls aus der Untersuchung neuartiger Quantenphänomene und -protokolle, die Vorteile gegenüber klassischen beziehungsweise früheren Quantenprotokollen bieten.

Die vorliegende Arbeit umfasst beide Forschungsrichtungen und präsentiert verschiedene experimentelle Projekte. Das erste Projekt beschreibt die Entwicklung und Implementierung zweier neuartiger Quantenkommunikationsprotokolle. Das zweite Projekt besteht in der Realisierung einer schmalbandigen Einzelphotonenquelle für die Wechselwirkung mit Atomen.

Im ersten Quantenkommunikationsprotokoll wird experimentell gezeigt, dass ein einzelnes Photon in Quantenüberlagerung die gleichzeitige Übertragung von zwei klassischen Bits zwischen zwei entfernten Parteien in zwei entgegengesetzten Kommunikationsrichtungen ermöglicht, eine in der klassischen Physik unmögliche Aufgabe. Dieses Phänomen wird verwendet, um ein sicheres Quantenkommunikationsprotokoll zu entwickeln und zu implementieren, bei dem die Kommunikationsrichtung zwischen den Parteien privat bleibt.

Im zweiten Protokoll sollen die beiden Parteien einen sicheren gemeinsamen kryptografischen Schlüssel einrichten, ohne Quantenressourcen zu verwenden, die an einen nicht vertrauenswürdigen Dritten (einen Server) delegiert werden. In diesem Sinne handelt es sich um ein Semiquantenschlüssel-Verteilungsprotokoll. Das Protokoll wird demonstriert und die sichere Schlüsselrate unter Berücksichtigung wichtiger Schwachstellen des experimentellen Aufbaus extrahiert.

Das zweite Projekt ist von rein technischer Natur. Eine Quelle von Photonenpaaren mit einer spektralen Bandbreite von etwa 10 MHz wird aufgebaut und charakterisiert. Aufgrund dieser schmalen Bandbreite, können die erzeugten Photonen effizient an atomare Hyperfeinübergänge gekoppelt werden. Die Photonen werden bei einer Wellenlänge von

780 nm emittiert und sind somit auf die Hyperfeinübergänge der Rubidium-D2-Linie abgestimmt. Die Quelle basiert auf cavity-enhanced spontaneous parametric down-conversion, die eine zuverlässige, relativ einfache und flexible Technik für die Erzeugung von Photonen mit schmaler Bandbreite darstellt und bezüglich ihrer Intensität frühere Quellen übertrifft. Diese Ressource soll zur Realisierung eines durch Rubidiumatome vermittelten Zwei-Photonen-Gates, in Zusammenarbeit mit externen Forschungsgruppen, eingesetzt werden.

Contents

Introduction

Quantum physics was one of the greatest achievements of the 20^{th} century, as it allowed scientists to describe with high precision the behaviour of matter at the smallest scale, e.g. atoms and subatomic particles, and to reveal novel important properties of radiation. The predictions of quantum physics were confirmed in a plethora of experiments involving different systems and strongly contributed to the development of technologies that are now part of our everyday life, such as lasers, silicon technology and magnetic resonance, among others. At the same time, the fascinating and counter-intuitive concepts of quantum physics challenged our interpretation of the world and triggered scientific and philosophical investigations about the nature of reality. The development of quantum theory, therefore, represented a revolution in physics, and in science in general.

A further step was made in the 1980s, when seminal works proposed to apply the ideas and methods of quantum physics to computer and information science. In particular, in 1980 Paul Benioff proposed a quantum model of a Turing machine [1] and, two years later, Richard Feynman suggested the idea of using quantum systems to efficiently simulate other quantum-physical systems [2]. These two works mark the beginning of the fields of quantum computation and simulation, which have attracted extensive interest in the last decades due to the promise of largely overpowering classical computers and simulators when performing specific tasks of high interest for fundamental and applied science, such as factorization of large numbers [3] or simulation of complex molecules [4]. In parallel, the field of quantum communication arose from the pioneering work of Bennett and Brassard in 1984, who showed how the transmission of quantum states allows two distant

parties to establish a perfectly secure cryptographic key [5], thus bringing the eternal fight between code makers and code breakers onto a more advanced level.

The final goal of these research branches is the realization of technologies going beyond the capabilities of classical information processing. Two important examples, on which many theoretical and experimental efforts are focused, are the universal quantum computer, where "universal" means that the computer is able to perform any quantum algorithm, and large-scale quantum-key-distribution networks enabling high key transmission rates over distances of thousands of kilometers. Such achievements promise to revolutionize information technology and, consequently, to deeply affect our society.

Despite the numerous efforts and the impressive technological advancement since the 1980s, practical quantum information devices overpowering their classical counterparts are still not experimentally feasible. The fundamental reason is that the necessary quantum resources for the realization of these devices are not easily generated and manipulated.

The race for the demonstration of useful quantum technologies involves many different physical systems. Each system has its own pro and cons and is more suitable for some applications than for others.

Single photons, i.e. the fundamental excitations of the electromagnetic field, present the great advantages of high mobility, as they travel at the speed of light, which makes them the preferred system for quantum communication, exactly as electromagnetic waves are the main carries of classical information over long distances. Furthermore, they exhibit low decoherence and are relatively easy to manipulate.

A significant drawback, however, is the lack of photon-photon interaction, which prevents the all-photonic realization of a "quantum transistor" and therefore represents a problem for the implementation of universal quantum computing and quantum simulation of interacting systems. This problem can be solved either by using matter systems as mediators of the interaction [6] or, alternatively, by optical schemes that exploit measurement-induced non-linear interactions and thus require a large number of independent [7] or entangled [8] photons. Unfortunately, both possibilities are technically challenging.

Another major issue is photon loss, which is particularly relevant for long-distance quantum communication. Analogously to the classical case, this issue can be addressed by (quantum) repeaters [9], which are able to amplify the transmitted photon signal so as to counter the losses and to extend the maximum communication distance. However, these device have only been demonstrated in proof-of-principle implementations, as they are based either on interaction with matter [10] or on entangled multi-photon states [11], which both require complex experimental techniques. The result is that the integration of quantum repeaters in practical quantum communication networks is beyond the current state of the art.

The research endeavor in photonic quantum information processing is two-fold. On the one hand, novel schemes for photonic quantum computation, simulation and communication are developed and demonstrated. They aim at showing new interesting advantages with respect to classical protocols and at reducing the experimental complexity of the currently existing quantum schemes. On the other hand, several efforts are devoted to the improvement of technology for generation, guiding, manipulation and detection of photons, as well as for their interface with other systems, such as atoms, molecules or solid-state systems. Both research directions are important for approaching feasible and useful applications.

Along the same line, this thesis presents two kinds of results in the field of quantum information processing with single photons. Among the three reported experimental works, two describe the proof-of-principle implementation of novel quantum communication protocols and the third illustrates the realization of a source of narrow-band single photons. Such a source is suitable for interaction of single photons with Rubidium atoms and thus for the realization of two-photon gates and quantum memories, the latter being an important component of quantum repeaters.

The thesis is structured as follows: first, in Chapter 1, the concept of single photon is defined and its application to quantum information science is elucidated, with a special focus on quantum communication. Then, the technique for photon generation that was employed in all three experimental works, spontaneous parametric down-conversion,

is explained in detail in Chapter 2. Chapters 3 and 4 describe the implementation of the quantum communication protocols, and, finally, Chapter 5 details the realized narrow-band single-photon source and its characterization.

Chapter 1

Single Photons and Their Application to Quantum Information

In this chapter, one of the fundamental concepts of quantum optics - the photon - is introduced and its application to quantum information science is discussed. The chapter starts with a description of the quantization of the electromagnetic field, which allows for the introduction of photon-number states of light. The discussion then continues with the description of single photons and their properties, with particular attention to single-photon interference, which is important for the experiments reported in this thesis. Finally, the field of quantum information science with single photons is reviewed, with a special focus on quantum communication. This serves as a contextualization of the quantum communication protocols presented in Chapters 3 and 4.

1.1 Quantization of the electromagnetic field

Quantum optics builds on classical electromagnetism. The transition between the two theories is done by replacing all classical quantities describing the electromagnetic field

with operators acting on an abstract Hilbert space. In order to describe the quantization of the electromagnetic field, it is useful to recall Maxwell's equations in vacuum:

$$\begin{aligned} \nabla \cdot \mathbf{B} &= 0 & \nabla \cdot \mathbf{E} &= 0 \\ \nabla \times \mathbf{E} &= -\frac{\partial \mathbf{B}}{\partial t} & \nabla \times \mathbf{B} &= \epsilon_0 \mu_0 \frac{\partial \mathbf{E}}{\partial t} \end{aligned} \tag{1.1}$$

where $\mathbf{E}$ and $\mathbf{B}$ are the electric and magnetic fields, respectively, and ϵ_0 and μ_0 the dielectric and magnetic constants. It is convenient to express the fields in terms of the scalar and vector potential, ϕ and $\mathbf{A}$, respectively. They are defined via the following equations:

$$\mathbf{B} = \nabla \times \mathbf{A}, \tag{1.2a}$$

$$\mathbf{E} = -\nabla\phi - \frac{\partial \mathbf{A}}{\partial t}. \tag{1.2b}$$

With these definitions, the two equations in the left column of Equations 1.1 are automatically satisfied. The remaining two may be written as:

$$\nabla(\nabla \cdot \mathbf{A}) - \nabla^2 \mathbf{A} + \frac{1}{c^2}\frac{\partial}{\partial t}\nabla\phi + \frac{1}{c^2}\frac{\partial^2 \mathbf{A}}{\partial t^2} = 0, \tag{1.3a}$$

$$\nabla^2 \phi - \nabla \cdot \frac{\partial \mathbf{A}}{\partial t} = 0, \tag{1.3b}$$

where $c = \sqrt{\epsilon_0 \mu_0}$ is the speed of light in vacuum. The potentials are not univocally defined by Equations 1.2. In fact, the pairs of potentials $\mathbf{A'}$, ϕ' and $\mathbf{A}$, ϕ, related by the following *gauge transformations*:

$$\mathbf{A} = \mathbf{A'} - \nabla\zeta, \tag{1.4a}$$

$$\phi = \phi' + \frac{\partial \zeta}{\partial t}, \tag{1.4b}$$

with ζ arbitrary function, determine the same electric and magnetic field. Since fields are observable quantities, whereas potentials are not, the two pairs in Equations 1.4 are physically equivalent. In vacuum, starting from any pair of potentials $\mathbf{A'}$ and ϕ', it is

always possible to choose ζ such that $\nabla \cdot \mathbf{A} = 0$ and $\phi = 0$, a choice called *Coulomb gauge*. Equation 1.3a then becomes:

$$\nabla^2 \mathbf{A} - \frac{1}{c^2} \frac{\partial^2 \mathbf{A}}{\partial t^2} = 0. \tag{1.5}$$

The electromagnetic field is assumed to be non-zero only in a limited region of free space, a cube of side L and volume $V_Q = L^3$, to which periodic boundary conditions are applied. This region of space is called *quantization cavity* and its volume is the *quantization volume*. The purpose of this abstraction is simplifying the procedure from the mathematical point of view. Quantization in full space can be analysed in the limit $L \to \infty$. Under these assumptions, the vector potential can be expressed in terms of plane waves:

$$\mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k},\lambda} (A_{\mathbf{k},\lambda}(t) e^{i\mathbf{k}\cdot\mathbf{r}} + c.c.), \tag{1.6}$$

where $\mathbf{e}_{\mathbf{k},\lambda}$ are unit polarization vectors and $c.c$ stands for "complex conjugate". The periodic boundary conditions determine a discrete set of valid wave vectors $\mathbf{k}$, with components $k_i = 2\pi \frac{n_i}{L}$, where n_i is an integer number and $i = x, y, z$. Due to the Coulomb gauge condition $\nabla \cdot \mathbf{A} = 0$, each $\mathbf{e}_{\mathbf{k},\lambda}$ must be perpendicular to the corresponding $\mathbf{k}$. Therefore each $\mathbf{k}$ affords only two independent polarization vectors, which can be chosen to be orthogonal. Consequently, $\mathbf{e}_{\mathbf{k},\lambda} \cdot \mathbf{e}_{\mathbf{k},\lambda'} = \delta_{\lambda,\lambda'}$, with δ representing the Kronecker delta. Each choice of $\mathbf{k}$ and λ determines a mode of the field.

Each mode must indipendently satisfy Equation 1.5, meaning that:

$$\frac{\partial^2 A_{\mathbf{k},\lambda}(t)}{\partial t^2} + \omega_k A_{\mathbf{k},\lambda}(t) = 0, \tag{1.7}$$

where $\omega_k = ck$ and $k = |\mathbf{k}|$. Equation 1.7 describes a harmonic oscillator with angular frequency ω_k. Its solution is $A_{\mathbf{k},\lambda}(t) = A_{\mathbf{k},\lambda} e^{-i\omega_k t}$, with $A_{\mathbf{k},\lambda}$ constant. The general solution of Equation 1.5 in the quantization cavity is then:

$$\mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k},\lambda} (A_{\mathbf{k},\lambda} e^{i(\mathbf{k}\cdot\mathbf{r} - \omega_k t)} + c.c.). \tag{1.8}$$

By applying Equations 1.2, the electric and magnetic field may be obtained, and consequently the expression for the electromagnetic energy in the quantization cavity:

$$H = \sum_{\mathbf{k},\lambda} \epsilon_0 V_Q \omega_k (A_{\mathbf{k},\lambda} A^*_{\mathbf{k},\lambda} + c.c.). \tag{1.9}$$

Therefore, all the relevant electromagnetic quantities can be written in terms of harmonic modes, corresponding to classical oscillators. The quantization is performed by replacing these classical oscillators with their quantum counterparts.

The Hamiltonian operator for a set of quantum oscillators is:

$$\hat{H} = \frac{1}{2} \sum_{\mathbf{k},\lambda} \hbar \omega_k (\hat{a}_{\mathbf{k},\lambda} \hat{a}^\dagger_{\mathbf{k},\lambda} + h.c.), \tag{1.10}$$

where $\hat{a}_{\mathbf{k},\lambda}$ and $\hat{a}^\dagger_{\mathbf{k},\lambda}$ are the destruction and creation operator for the oscillator characterized by $\mathbf{k}$ and λ, respectively, and $h.c.$ stands for "hermitian conjugate". The operators $\hat{a}_{\mathbf{k},\lambda}$ and $\hat{a}^\dagger_{\mathbf{k},\lambda}$ satisfy the following canonical commutation relations:

$$\left[\hat{a}_{\mathbf{k},\lambda}, \hat{a}_{\mathbf{k}',\lambda'}\right] = 0 \tag{1.11a}$$

$$\left[\hat{a}^\dagger_{\mathbf{k},\lambda}, \hat{a}^\dagger_{\mathbf{k}',\lambda'}\right] = 0 \tag{1.11b}$$

$$\left[\hat{a}_{\mathbf{k},\lambda}, \hat{a}^\dagger_{\mathbf{k}',\lambda'}\right] = \delta_{\mathbf{k},\mathbf{k}'} \delta_{\lambda,\lambda'}. \tag{1.11c}$$

A comparison between Equation 1.9 and Equation 1.10 suggests the replacement:

$$A_{\mathbf{k},\lambda} \rightarrow \sqrt{\frac{\hbar}{2\epsilon_0 V_Q \omega_k}} \hat{a}_{\mathbf{k},\lambda}. \tag{1.12}$$

Thereby, the quantum vector potential and, consequently, the electric and magnetic field

operators are:

$$\hat{\mathbf{A}}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k},\lambda} \sqrt{\frac{\hbar}{2\epsilon_0 V_Q \omega_k}} (\hat{a}_{\mathbf{k},\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + h.c.), \tag{1.13a}$$

$$\hat{\mathbf{E}}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{e}_{\mathbf{k},\lambda} \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V_Q}} (i\hat{a}_{\mathbf{k},\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + h.c.), \tag{1.13b}$$

$$\hat{\mathbf{B}}(\mathbf{r},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \mathbf{k} \times \mathbf{e}_{\mathbf{k},\lambda} \sqrt{\frac{\hbar}{2\epsilon_0 V_Q \omega_k}} (i\hat{a}_{\mathbf{k},\lambda} e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + h.c.). \tag{1.13c}$$

In typical experimental situations, the fields are not confined in a closed region of space but are described by waves travelling from sources to detectors. It is then convenient to consider one of the sides of the quantization cavity being infinite, say along the z-axis. As a consequence, the corresponding coordinate of the wave vectors $\mathbf{k}$ becomes continuous. By neglecting the transverse coordinates and by examining only fields that propagate in the positive z direction, it is possible to consider $k_z = k$. The mathematical analysis can be done equivalently using k or the frequency $\omega = ck$.

If the distance between two consecutive allowed values of k (or ω) in the confined case is $\Delta k(\Delta\omega)$, all the continuous-mode quantities may be obtained from the following substitutions [12]:

$$\sum_k \to \frac{1}{\Delta k} \int_0^\infty dk \to \frac{1}{\Delta\omega} \int_0^\infty d\omega, \tag{1.14a}$$

$$\delta_{k,k'} \to \Delta k \delta(k-k') \to \Delta\omega\delta(\omega-\omega'), \tag{1.14b}$$

$$\hat{a}_{k,\lambda} \to \sqrt{\Delta k} a_\lambda(k) \to \sqrt{\Delta\omega} a_\lambda(\omega), \tag{1.14c}$$

where δ indicates the uni-dimensional Dirac delta. From expressions 1.14, it follows that $\left[a_\lambda(\omega), a_\lambda^\dagger(\omega')\right] = \delta(\omega-\omega')\delta_{\lambda,\lambda'}$. In what follows every quantity is expressed in terms of

the frequency ω. Since $\Delta\omega = \frac{2\pi c}{L}$, the field operators in 1.13 become:

$$\hat{\mathbf{E}}(z,t) = \sum_{\lambda=1,2} \mathbf{e}_\lambda \int_0^\infty d\omega \sqrt{\frac{\hbar\omega}{4\pi\epsilon_0 c A_Q}} (i\hat{a}_\lambda(\omega) e^{-i\omega(t-z/c)} + h.c.), \tag{1.15a}$$

$$\hat{\mathbf{B}}(z,t) = -i \sum_{\lambda=1,2} \mathbf{z} \times \mathbf{e}_\lambda \int_0^\infty d\omega \sqrt{\frac{\hbar\omega}{4\pi\epsilon_0 c^3 A_Q}} (i\hat{a}_\lambda(\omega) e^{-i\omega(t-z/c)} + h.c.), \tag{1.15b}$$

where $A_Q = \frac{V_Q}{L}$ is the quantization area and $\mathbf{z}$ is the positive unit vector in the z direction.

1.2 Fock states

All the operators described in the previous section act on the state space of the electromagnetic field, which is the state space of a set of quantum harmonic oscillators.
This means that, for each mode of the field, there is a discrete set of orthonormal states $|n_{\mathbf{k},\lambda}\rangle$, with $n_{\mathbf{k},\lambda} = 0, 1, 2, ...$, for which [13]:

$$\hat{a}_{\mathbf{k},\lambda}|n_{\mathbf{k},\lambda}\rangle = \sqrt{n_{\mathbf{k},\lambda}}|n_{\mathbf{k},\lambda} - 1\rangle, \tag{1.16a}$$

$$\hat{a}^\dagger_{\mathbf{k},\lambda}|n_{\mathbf{k},\lambda}\rangle = \sqrt{n_{\mathbf{k},\lambda} + 1}|n_{\mathbf{k},\lambda} + 1\rangle. \tag{1.16b}$$

These are eigenstates of the single-mode energy operator $\hat{H}_{\mathbf{k},\lambda}$:

$$\hat{H}_{\mathbf{k},\lambda}|n_{\mathbf{k},\lambda}\rangle = \frac{1}{2}\hbar\omega_k(\hat{a}_{\mathbf{k},\lambda}\hat{a}^\dagger_{\mathbf{k},\lambda} + \hat{a}^\dagger_{\mathbf{k},\lambda}\hat{a}_{\mathbf{k},\lambda})|n_{\mathbf{k},\lambda}\rangle = (n_{\mathbf{k},\lambda} + \frac{1}{2})\hbar\omega_k|n_{\mathbf{k},\lambda}\rangle. \tag{1.17}$$

Therefore, the possible values for the energy of the field in a single mode are discrete and separated by the fixed quantity $\hbar\omega_k$. This quantity represents the energy of a *photon* in the mode $\mathbf{k}, \lambda$. Each state $|n_{\mathbf{k},\lambda}\rangle$ is associated to $n_{\mathbf{k},\lambda}$ photons in the corresponding mode. It is then possible to define a single-mode photon-number operator $\hat{n}_{\mathbf{k},\lambda} = \hat{a}^\dagger_{\mathbf{k},\lambda}\hat{a}_{\mathbf{k},\lambda}$ which commutes with $\hat{H}_{\mathbf{k},\lambda}$. The states $|n_{\mathbf{k},\lambda}\rangle$ are eigenstates of $\hat{n}_{\mathbf{k},\lambda}$ with eigenvalues $n_{\mathbf{k},\lambda}$ and are therefore called single-mode *photon-number states* or, alternatively, *Fock states*.

A Fock state of the total electromagnetic field is a product of Fock states of all

individual modes and can be described by a string of photon numbers in each mode:

$$|\{n_{\mathbf{k},\lambda}\}\rangle = |n_{\mathbf{k}_1,1}, n_{\mathbf{k}_1,2}, n_{\mathbf{k}_2,1}, n_{\mathbf{k}_2,2}, ...\rangle = \prod_{\mathbf{k},\lambda} |n_{\mathbf{k},\lambda}\rangle. \tag{1.18}$$

The ground state of the system, $|0\rangle$, also called *vacuum state*, is obtained when $n_{\mathbf{k},\lambda} = 0$ for each value of $\mathbf{k}$ and λ. Interestingly, the energy of the field in this state is not 0, as:

$$\hat{H}|0\rangle = \frac{1}{2} \sum_{\mathbf{k},\lambda} \hbar\omega_k |0\rangle. \tag{1.19}$$

The quantity $\frac{1}{2} \sum_{\mathbf{k},\lambda} \hbar\omega_k$ is called *zero-point energy* or *vacuum energy* and is infinite. This is a strange feature of the quantized electromagnetic field, which, however, does not represent a problem in practice. In fact, only variations in the electromagnetic energy are observable, which are always finite. In particular, energy differences in a given mode $\mathbf{k}, \lambda$ can only be integer multiples of $\hbar\omega_k$. A measurement device is said to detect n photons if it measures an energy difference of $n\hbar\omega_k$.

A state of the field in the cavity can be pure or mixed. The most general pure state is given by:

$$|\psi\rangle = \sum_{\{n_{\mathbf{k},\lambda}\}} c(\{n_{\mathbf{k},\lambda}\}) |\{n_{\mathbf{k},\lambda}\}\rangle, \tag{1.20}$$

where the sum is calculated over all possible sets of photon numbers and $\sum_{\{n_{\mathbf{k},\lambda}\}} |c(\{n_{\mathbf{k},\lambda}\})|^2 = 1$. If there is a probability P_i, with i going from 1 to d, that the field is in the pure state $|\psi_i\rangle$, the resulting statistical mixture is described by the density operator:

$$\hat{\rho} = \sum_{i=1}^{d} P_i |\psi_i\rangle\langle\psi_i|, \tag{1.21}$$

with $\sum_{i=1}^{d} P_i = 1$.

The eigenstates of the total number operator $\hat{n} = \sum_{\mathbf{k},\lambda} \hat{n}_{\mathbf{k},\lambda}$ with eigenvalue n are called *n-photon states*. In general they are superpositions of Fock states for which the n photons are distributed among several modes. Single-photon states ($n = 1$) are particularly

relevant for this dissertation. A general single-photon state involving m modes of the field in the cavity can be written as:

$$|\phi_1\rangle = \sum_{j=1}^{m} c_j |1_j\rangle, \tag{1.22}$$

where $|1_j\rangle$ denotes the Fock state with one photon in the mode j and 0 photons in all the other modes. Normalization imposes $\sum_j |c_j|^2 = 1$. It is then useful to define a modified creation operator $\hat{a}_\phi^\dagger$ by:

$$\hat{a}_\phi^\dagger = \sum_{j=1}^{m} c_j \hat{a}_j^\dagger, \tag{1.23}$$

where $\hat{a}_j^\dagger$ is the creation operator for the mode j. The operator $\hat{a}_\phi^\dagger$ creates a photon in the state $|\phi_1\rangle$, i.e. $\hat{a}_\phi^\dagger|0\rangle = |\phi_1\rangle$. It is easy to prove that $\left[\hat{a}_\phi, \hat{a}_\phi^\dagger\right] = 1$. By applying twice the operator $\hat{a}_\phi^\dagger$ to the vacuum state, a two-photon state is created:

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(\hat{a}_\phi^\dagger)^2|0\rangle = \sum_{j,s=1}^{m} c_j c_s |1_j\rangle|1_s\rangle. \tag{1.24}$$

This procedure can be repeated n times to create an n-photon state. All n-photon states created in this way are separable, meaning that they can be decomposed in the product of n single-photon states. Each n-photon state that does not satisfy this property is said to be *entangled*.

For instance, let us consider two wave vectors $\mathbf{k}_1$ and $\mathbf{k}_2$ having the same modulus (i.e. the same frequency) but different directions. For each $\mathbf{k}$ two polarization directions are possible, which are represented by the unit vectors $\mathbf{e}_H$ and $\mathbf{e}_V$. The following single-photon creation operators can be constructed:

$$\hat{a}_i^\dagger = \frac{1}{\sqrt{2}}(\hat{a}_{\mathbf{k}_i,H}^\dagger + \hat{a}_{\mathbf{k}_i,V}^\dagger), \tag{1.25}$$

with $i = 1, 2$. The operator $\hat{a}_i^\dagger$ creates a single photon with wavevector $\mathbf{k}_i$ in a balanced

superposition of the two different polarization modes. The state:

$$\hat{a}_1^\dagger \hat{a}_2^\dagger |0\rangle = \frac{1}{2}(|1_{\mathbf{k}_1,H}\rangle|1_{\mathbf{k}_2,H}\rangle + |1_{\mathbf{k}_1,H}\rangle|1_{\mathbf{k}_2,V}\rangle + |1_{\mathbf{k}_1,V}\rangle|1_{\mathbf{k}_2,H}\rangle + |1_{\mathbf{k}_1,V}\rangle|1_{\mathbf{k}_2,V}\rangle) \quad (1.26)$$

is a two-photon separable state. In order to show an example of an entangled state, let us only consider the terms with different polarizations in Equation 1.26. The corresponding normalized state is:

$$\frac{1}{\sqrt{2}}(|1_{\mathbf{k}_1,H}\rangle|1_{\mathbf{k}_2,V}\rangle + |1_{\mathbf{k}_1,V}\rangle|1_{\mathbf{k}_2,H}\rangle) = \frac{1}{\sqrt{2}}(\hat{a}^\dagger_{\mathbf{k}_1,H}\hat{a}^\dagger_{\mathbf{k}_2,V} + \hat{a}^\dagger_{\mathbf{k}_1,V}\hat{a}^\dagger_{\mathbf{k}_2,H})|0\rangle. \quad (1.27)$$

This state, also called *Bell state*, cannot be obtained by applying a product of single-photon creation operators to the vacuum. In such a case special correlations in polarization and wavevector arise between the two photons, which are of high importance for quantum physics [14] and have many applications in quantum information science, as discussed in Sections 1.5 and 1.6.

In the case of travelling waves along the z-axis, the set of Fock states becomes continuous. The quantum state of the field then describes an excitation with a central frequency ω_0 and a bandwidth B. If $\omega_0 >> B$, the integrals in Equations 1.15 can be evaluated between $-\infty$ and ∞ without introducing a significant error. In this approximation, it is useful to define Fourier-transformed operators:

$$a_\lambda(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} d\omega \hat{a}_\lambda(\omega) e^{-i\omega t}. \quad (1.28)$$

Again, $\left[a_\lambda(t), a_\lambda^\dagger(t')\right] = \delta(t-t')\delta_{\lambda,\lambda'}$. The continuous-mode number operator is then given by:

$$\hat{n} = \sum_{\lambda=1,2} \int_{-\infty}^{\infty} d\omega \ \hat{a}_\lambda^\dagger(\omega)\hat{a}(\omega) = \sum_{\lambda=1,2} \int_{-\infty}^{\infty} dt \ \hat{a}_\lambda^\dagger(t)\hat{a}(t). \quad (1.29)$$

If the "narrow-bandwidth" approximation cannot be applied, only the first equality in the previous equation is valid, with the integration limits going from 0 to ∞. The operator

$\hat{a}^\dagger_\lambda(t)\hat{a}(t)$ is the *photon flux* operator, $\hat{\Phi}(t)$, corresponding to the number of photons crossing the quantization area per unit time.

The action of $\hat{a}^\dagger_\lambda(\omega)$ on the vacuum state creates a single photon with polarization λ and frequency ω. Such a field excitation is of course not realistic. As mentioned before, a realistic field excitation should have a spectral structure with a central frequency and a bandwidth, like in the classical case. This corresponds to a photon-wavepacket creation operator, defined as:

$$\hat{a}^\dagger_f = \int_{-\infty}^{\infty} d\omega f(\omega)\hat{a}^\dagger(\omega), \tag{1.30}$$

where, for simplicity the polarization index is omitted. The quantity $|f(\omega)|^2$ is the normalized power spectrum of the electromagnetic excitation, which satisfies the normalization condition $\int_{-\infty}^{\infty} d\omega |f(\omega)|^2 = 1$. The action of the operator $\hat{a}^\dagger_f$ on the vacuum state creates a photon with a spectral structure that is determined by the function $f(\omega)$. The spectral properties of the field excitation are then contained in the quantum state of the field.

1.3 Single-photon interference

In the previous section, the photon was defined as the fundamental field excitation, which can occur either in a single mode or in a superposition of modes.

A single photon cannot be detected by two different measurement devices at the same time, as this would imply a splitting of its energy, which is not predicted by quantum optics. From this point of view, single photons behave like particles. However, photons are used to describe the electromagnetic field and therefore they also possess wave-like properties, expressed, for example, in single-photon interference, which will be analysed in this section. This wave-particle dualism often leads to depicting the photon as a strange particle, which can move from some point to another and be in different locations at the same time. Although not rigorous, this description permits to avoid long explanations and for this reason will be sometimes adopted in this thesis.

Single-photon interference is here discussed by examining what happens to a photon

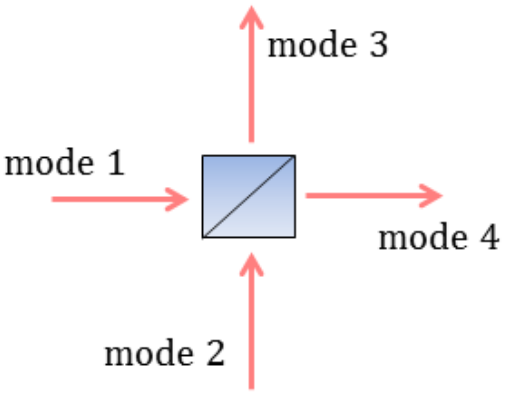


Figure 1.1: **Input and output modes of a beam splitter.** The beam splitter is an optical element with two inputs and two outputs. The input modes in the figure are labelled with indices "1" and "2", whereas the output modes with "3" and "4". The beam splitter transmits mode 1 (2) into mode 4 (3) and reflects it into mode 3(4).

in a Mach-Zehnder interferometer. A basic element of such a device is the beam splitter, which is therefore described from a quantum-optical point of view. A beam splitter reflects and transmits light impinging on one of its two inputs according to the reflection and transmission coefficients, R and T, respectively. Since reflection and transmission may induce phase shifts in the field, R and T are in general complex. Here the coefficients are assumed to be the same for both inputs of the beam splitter. If the beam splitter is lossless, the corresponding quantum operator mus be unitary. From this condition, it follows $|R|^2 + |T|^2 = 1$ and $RT^* + R^*T = 0$.

Let us consider single continuous modes of the field with a given polarization and wave vector component k along the quantization axis, as discussed in the previous sections. For simplicity the polarization index as well as the dependence of the modes on k or ω are omitted. As depicted in Figure 1.1, the beam splitter has two input modes, 1 and 2, associated to waves travelling in different directions. The corresponding destruction operators are indicated by $\hat{a}_1$ and $\hat{a}_2$, respectively. The output modes, 3 and 4 have destruction operators $\hat{a}_3$ and $\hat{a}_4$. The input-output relations for a beam splitter in classical electromagnetism are translated to analogous relations among the destruction

operators[12]:

$$\hat{a}_3 = R\hat{a}_1 + T\hat{a}_2, \tag{1.31a}$$

$$\hat{a}_4 = T\hat{a}_1 + R\hat{a}_2. \tag{1.31b}$$

The creation and destruction operators for all modes satisfy the canonical commutation relations defined in Equations 1.2. If the two input modes are independent, meaning that $\left[\hat{a}_1, \hat{a}_2^\dagger\right] = 0$, it follows that also the two output modes are independent, i.e. $\left[\hat{a}_3, \hat{a}_4^\dagger\right] = 0$. The photon-number operator in each arm is given by $\hat{n}_i = \hat{a}_i^\dagger \hat{a}_i$, with $i = 1, 2, 3, 4$. Conservation of energy implies a photon-number conservation law : $\hat{n}_1 + \hat{n}_2 = \hat{n}_3 + \hat{n}_4$.

When there is only a single photon at input 1, the state of the field at the output is:

$$|\psi\rangle_{out} = R|1\rangle_3|0\rangle_4 + T|0\rangle_3|1\rangle_4. \tag{1.32}$$

This state is sometimes described as *single-photon entangled state*, or also as an example of *entanglement with vacuum* [15]. This notion derives from a more general definition of entanglement than that provided in Section 1.2. In general, any state of a composite system that cannot be written as a product of states of its subsystems is defined as entangled. In the case of the state $|\psi_{out}\rangle$ the two subsystems are mode 3 and mode 4, in which the state space of the electromagnetic field is spanned by $\{|n_3\rangle\}$ and $\{|n_4\rangle\}$, respectively, with $n_{3,4} = 0, 1, 2, ...$ number of photons in the corresponding mode. The state in Equation 1.32 cannot be written as a product of a Fock state for mode 3 and a Fock state for mode 4, therefore it can be considered entangled. In this sense, a beam splitter creates entanglement between its output modes.

A consequence of the structure of state $|\psi\rangle_{out}$ is that detection (lack of detection) of a photon in one of the two output arms, projects the other arm onto the vacuum state (single-photon Fock state). If, instead, a photon trap is placed in one of the two arms, so that it becomes impossible to know if that arm contains vacuum or one photon, then the other arm is projected onto a statistical mixture of states $|0\rangle$ and $|1\rangle$, with respective probabilities $|R|^2$ and $|T|^2$.

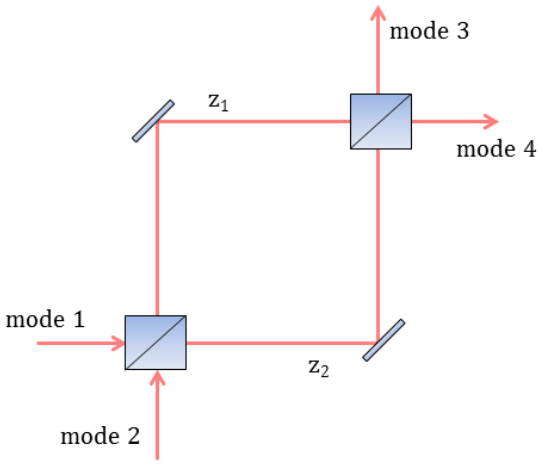


Figure 1.2: **Sketch of a Mach-Zehnder interferometer.** The Mach-Zehnder interferometer is composed of two beam splitters, which are assumed to be identical, and two mirrors. The mirrors steer the outputs of the first beam splitter to the inputs of the second beam splitter. The input modes of the interferometer are labelled "mode 1" and "mode 2"; the output modes instead "mode 3" and "mode 4". The two paths from the first to the second beam splitter have length $z1$ and $z2$, respectively.

For single-photon input, the mean photon numbers at the outputs are respectively $\langle \hat{n}_3 \rangle = |R|^2$ and $\langle \hat{n}_4 \rangle = |T|^2$. This result is similar to the classical division of electromagnetic energy at a beam splitter. The photon-number correlations at the outputs are instead fully quantum, as:

$$\langle \hat{n}_3 \hat{n}_4 \rangle = 0. \tag{1.33}$$

This results comes from the fact that a photon can be detected only in one of the two output arms, and therefore represents a signature of the particle aspect of single photons.

Let us now consider a Mach-Zehnder interferometer (MZI), as in Figure 1.2, which is composed of two consecutive beam splitters placed such that the outputs of the first one are the inputs of the second one. By assuming that the two beam splitters are identical, the following input-output relations stand:

$$\hat{a}_3 = R_{MZ} \hat{a}_1 + T_{MZ} \hat{a}_2, \tag{1.34a}$$

$$\hat{a}_4 = T_{MZ} \hat{a}_1 + R'_{MZ} \hat{a}_2, \tag{1.34b}$$

where:

$$R_{MZ} = R^2 e^{i\frac{\omega}{c}z_1} + T^2 e^{i\frac{\omega}{c}z_2}, \tag{1.35a}$$

$$R'_{MZ} = T^2 e^{i\frac{\omega}{c}z_1} + R^2 e^{i\frac{\omega}{c}z_2}, \tag{1.35b}$$

$$T_{MZ} = RT(e^{i\frac{\omega}{c}z_1} + e^{i\frac{\omega}{c}z_2}), \tag{1.35c}$$

in which ω is the frequency of the photon, and z_1 and z_2 are the lengths of the two paths from the first to the second beam splitter, respectively. The input-output relations of a MZI are therefore formally identical to those of a beam splitter but they have different coefficients, which include the phase accumulated by the photon in the propagation between the two beam splitters. Analogously to the single beam splitter:

$$|R_{MZ}|^2 + |T_{MZ}|^2 = |R'_{MZ}|^2 + |T_{MZ}|^2 = 1, \tag{1.36a}$$

$$R'_{MZ}T^*_{MZ} + T_{MZ}R^*_{MZ} = 0. \tag{1.36b}$$

The mean photon number at any of the outputs depends on the phase difference between the paths. For instance, the mean photon number at output 4 is:

$$\langle \hat{n}_4 \rangle = |T_{MZ}|^2 = 4|R|^2|T|^2 \cos^2\left[\frac{1}{2}\frac{\omega}{c}(z_1 - z_2)\right]. \tag{1.37}$$

When n identical single photons are sent consecutively to input 1 of the MZI, in the limit of large n, $n\langle \hat{n}_4 \rangle$ detections are recorded at output 4. By varying the phase difference, an interference pattern is observed, analogously to what is predicted by classical electromagnetism. This interference cannot come from interaction among different photons, as only one photon is sent to input 1 at a time. Interference therefore is an effect that involves the single quanta of light independently. The photon in the MZI therefore should be regarded as a simultaneous excitation of input, output and internal spatial modes of the interferometer, as it happens for the spatial field distribution of classical light. This is a typical wave-like feature, which, together with the particle features discussed above, shows the dual nature of single photons. Any attempt to

"localize" the photon destroys interference, according to the *which-path principle*.

The previous analysis will now be extended to multi-mode light, where the multiple modes are characterized by different frequencies ω. Assuming a narrow-band excitation, the dependence of the beam splitter coefficients on ω can be neglected. Relations 1.31 then are also valid for the Fourier-transformed operators $\hat{a}_i(t)$, with $i = 1, 2, 3, 4$. The dependence of the acquired phase between the two beam splitters on frequency, instead, cannot be neglected, and is incorporated in the Fourier-transformed operators. For instance, the operator $\hat{a}_4(t)$ for a MZI is given by:

$$\hat{a}_4(t) = RT\hat{a}_1(t - \frac{z_1}{c}) + RT\hat{a}_1(t - \frac{z_2}{c}) + T^2\hat{a}_2(t - \frac{z_1}{c}) + R^2\hat{a}_2(t - \frac{z_2}{c}). \tag{1.38}$$

If a photon-wavepacket characterized by the function $f(\omega)$ is considered at input 1, the expectation value of the photon flux at output 4 is:

$$\langle\hat{\Phi}_4(t)\rangle = |R|^2|T|^2|f(t - \frac{z_1}{c}) + f(t - \frac{z_2}{c})|^2, \tag{1.39}$$

where $f(t)$ is the Fourier transform of $f(\omega)$.
From the previous expression it is clear that single-photon interference cannot occur if the quantity $\frac{z_2 - z_1}{c}$ is far larger than the time bandwidth of the function $f(t)$. In this case, in fact, the two wavepackets described by $f(t - \frac{z_1}{c})$ and $f(t - \frac{z_2}{c})$ do not overlap. Even though this effect is predicted by classical electromagnetism for a multi-mode input field, a quantum-mechanical interpretation is also possible. If the path difference is large, in fact, the two pulse contributions are fully distinguishable in time and therefore, by recording the arrival time at the detector, it is possible to tell which way the photon travelled. According to the which-path principle, this suppresses interference.

1.4 Photons and qubits

Single-photon states of light play an important role in quantum information science, as it will be discussed in detail in the next sections. For this discussion, however, some basic

concepts are needed, which are reviewed below.

The fundamental unit of digital information is the *bit*. It is a representation of a binary digit, assuming a logical value of either "0" or "1". A bit can be physically realized by any classical system that has two stable states, such as the two possible directions of magnetic moment in a medium or two voltage levels in a circuit. Analogously, the basic unit of quantum information is the quantum bit, or *qubit*. Any quantum system with a bi-dimensional Hilbert space may be used to encode a qubit, like, for instance, the spin-$\frac{1}{2}$ of a particle. Two possible states of a qubit are $|0\rangle$ and $|1\rangle$, which form an orthonormal basis of the qubit Hilbert space, known as *computational basis*. But, in contrast to a classical bit, a qubit can be in any superposition $|\psi\rangle$ of these two states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.40}$$

where α and β are complex numbers satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. Due to this relation between the coefficients, Equation 1.40 may be re-written as:

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle), \tag{1.41}$$

with γ, θ and ϕ real numbers. The phase factor $e^{i\gamma}$ represents a global phase with no observable effect and can therefore be neglected. From Equation 1.41 it follows that each state of a qubit can be univocally associated to a point on a sphere of unit radius, called *Bloch sphere* (see Figure 1.3).

In order to describe a qubit, then, one needs to provide two real quantities. This implies that a qubit contains an infinite amount of information, which is necessary for its full characterization. In practice, however, this information is not accessible unless an infinite number of measurements is performed.

Measuring the state $|\psi\rangle$ of a qubit in an orthonormal basis results into two possible outcomes, meaning that the measurement can provide only one (classical) bit of information. By measuring a qubit of the form in Equation 1.40 in the computational basis, the result "0" is obtained with probability $|\alpha|^2$ and the result "1" with probability $|\beta|^2$. In

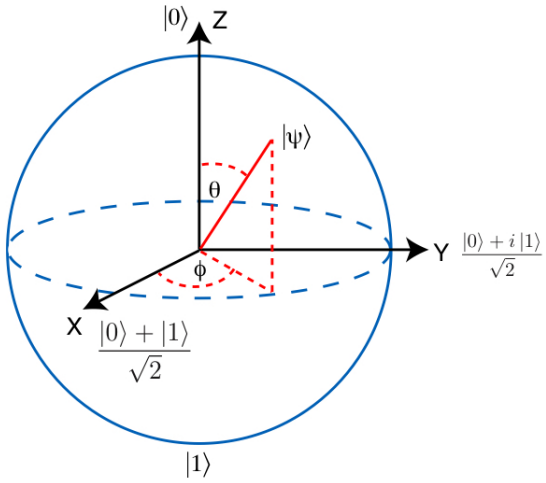


Figure 1.3: **Bloch sphere.** Each pure state of a qubit can be associated to a point on the surface of the Bloch sphere. The two poles of the sphere on the z axis correspond to the states $|0\rangle$ and $|1\rangle$, respectively. The parameters θ and ϕ in Equation 1.41 are the spherical coordinates of the point corresponding to $|\psi\rangle$.

both cases, the superposition collapses onto a state of the computational basis after the measurement. In order to fully determine α and β, one needs to perform measurements in three different orthonormal bases on an infinite number of identically prepared qubits. This solves the apparent paradox of the infinite amount of information.

A logic gate is an operation on bits that provides an output state after an input state is given, thus converting information from one form to another. In the classical case, only four single-bit gates are possible. On the contrary, there are infinite single-qubit gates, which correspond to unitary operators acting on the qubit Hilbert space. Each possible state of a qubit may be written as a vector matrix of the coefficients in the chosen basis. The basis vectors are then $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively. In this formalism, single-qubit gates are expressed as 2×2 matrices. For example, a very common single-qubit gate is the Hadamard gate, H:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1.42}$$

which converts the states $|0\rangle$ and $|1\rangle$ into the balanced superpositions $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$,

respectively. The states $|+\rangle$ and $|-\rangle$ form another orthonormal basis.

In general, the Hilbert space of a system of N qubits is given by the tensor product of the single-qubit Hilbert spaces and has dimension 2^N. For instance, the generic state of two qubits can be written as:

$$\psi = \alpha_{00}|00\rangle + \alpha_{10}|10\rangle + \alpha_{01}|01\rangle + \alpha_{11}|11\rangle, \tag{1.43}$$

with $\sum_{ij} |\alpha_{ij}|^2 = 1$. Multiple qubit states can be grouped in separable and entangled, as already discussed in sections 1.2 and 1.3. A gate operating on N qubits is a unitary operator in the corresponding Hilbert space and can therefore be represented as a $2^N \times 2^N$ matrix. An example is given by the controlled-not (CNOT) gate, U_{CNOT}:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.44}$$

The two qubits on which U_{CNOT} acts are traditionally called *control* and *target* qubit, respectively. In the computational basis the CNOT gate acts as follows: it flips the target qubit if the control qubit is $|1\rangle$, leaves it unaltered if the control qubit is $|0\rangle$; the control qubit instead is always left unaltered. This gate is particularly relevant, as it can be shown that any multi-qubit gate can be decomposed in CNOT and single-qubit gates. In this sense the CNOT gate is universal [16].

A crucial property of qubits is that they cannot be cloned. The no-cloning theorem of quantum mechanics [17] states that it is not possible to create an identical copy of an arbitrary unknown state. A cloning device, therefore, might work perfectly for some states but necessarily gives approximate results for other states. This phenomenon has important consequences in the field of quantum information, as explained in the next sections.

Qubits can be encoded by using several degrees of freedom of different quantum

systems, such as, among others, magnetic flux, charge and phase of superconducting circuits [18], energy levels and nuclear spins of atoms [19] or trapped ions [20] and single photons [21]. Photons offer many degrees of freedom for qubit encoding: spatial or temporal, frequency, polarization, orbital angular momentum or photon number in a given mode. Photonic qubits are mobile, easy to generate and exhibit low decoherence because of their lack of interaction with the external environment. Single-qubit gates are also relatively easy to realize. As an example, let us consider the case in which a qubit is encoded in the spatial degree of freedom of a single photon, which can be in two spatial modes a and b. The computational basis states are then defined as $|0\rangle = |1\rangle_a|0\rangle_b$ and $|1\rangle = |0\rangle_a|1\rangle_b$. Here, $|0\rangle$ ($|1\rangle$) represents the state in which there is one photon in mode a (b) and no photon mode b (a). In this encoding system, also called *dual-rail* encoding, all single-qubit gates can be performed with linear optical elements. For instance, the Hadamard gate is realized by a simple 50:50 beam-splitter, as it can be deduced from Equation 1.32.

The main disadvantage of photonic qubits is that light does not interact with itself. Consequently, quantum gates requiring interaction among qubits, like the CNOT gate, are not easily realized. These gates are based on optical non-linear effects, which are usually very weak at low field intensities [22]. Non-linearities at single-photon level can be obtained in atoms [23, 24, 25, 26, 27] or quantum dots [28], but these systems are technically complicated and their performance as quantum gates is still not optimal. However, some methods have been proposed to realize two-qubit gates without requiring non-linearity, as discussed in the next section.

1.5 Photonic quantum computation and simulation

Quantum computation consists in the design and realization of algorithms employing qubits and quantum-mechanical operations. In the past decades, a few relevant quantum algorithms have been developed. These algorithms require fewer computational steps than any known classical algorithm to solve some specific problems and therefore can

lead to significantly faster computation. Important examples are Shor's algorithm [3] and Grover's algorithm [29]. Shor's algorithm allows one to factorize a prime number with an exponentially lower number of steps with respect to the best known classical algorithm. Grover's algorithm, also called *quantum search algorithm*, achieves a quadratic improvement in the task of searching for a specific element in an unordered database. These results triggered many research efforts for the realization of quantum computers.

The most studied quantum computing architectures are the *quantum circuit model* (QCM) and the *measurement-based quantum computation* (MBQC). In QCM, computation is performed by a sequence of quantum gates and qubits are typically initialized in one of the computational basis states, analogously to classical schemes. MBQC requires highly-entangled initial states, called *graph* or *stabilizer* states, on which single-qubit measurements are performed. At each step of the computation, the measurement basis depends on the previous measurement outcomes. The sequence of measurements then determines the executed algorithm. These two architectures are equivalent in terms of computational power but require different resources and have different properties.

Single photons may be used both for QCM and MBQC. The principal problem represented by QCM with photonic qubits is the realization of two-qubit gates, as explained in the previous section. A solution was provided by Knill, Laflamme and Milburn, who proposed a scheme to perform universal quantum computation with linear optical elements only [7]. The basic idea is that effective non-linear photon-to-photon interactions, and therefore two-qubit gates, can be obtained probabilistically via projective measurements. Ancillary photons are needed to increase the success probability of each gate. The amount of necessary resources does not scale exponentially with the number of gates, but in practice is still too high to be considered feasible in the near future.

A more suitable architecture for photonic quantum computing is MBQC. In this case, two-qubit gates can be directly realized with linear optics, even though generation of the necessary entangled multi-photon resource state still represents a major technical challenge.

To date, the main factor preventing the realization of scalable photonic quantum

computation is represented by the low performance of photon sources. In principle, they need to deterministically provide indistinguishable Fock states at high rates, which may then be manipulated to create graph states for MBQC.

Currently, the most common photon sources in quantum information laboratories are those based on second- and third-order non-linear effects in dielectric materials (see Chapter 2). They are flexible, robust, relatively easy to operate and can satisfy all the requirements for an ideal photon source except for deterministic emission, as they are based on stochastic processes. They can be made (near-) deterministic by using multiplexing techniques, at the price of reducing the average emission rate or, alternatively, increasing the necessary number of emitters [30, 31].

Alternatively, in the last years some solid state photon sources have proved to be very promising [32]. Among them, InAs/GaAs quantum dots have shown the best performance [33, 34] as single-photon emitters. They can produce photons with high purity and a reasonable level of indistinguishability, which is a key requirement for quantum interference. On the other hand, they are less flexible, require cryogenic temperatures to be operated and are still not tunable enough to allow the generation of identical photons from different emitters. A great potential advantage of solid state sources, however, is that they are in principle able to directly generate large entangled states [35, 36].

Besides the problems with the sources, noise constitutes another major technical issue. It was shown, in fact, that scalable quantum computation is possible only if the probability of error per qubit per gate is kept below a given threshold, which depends on the architecture and the implemented error-correction codes. Currently, even the most optimistic threshold values are too low to be experimentally realized [37, 38].

Finally, most MBQC photonic quantum computation schemes are based on adaptive measurements [39], which require fast optical switches and detectors, with operation frequencies of $\gtrsim 10$ GHz. The realization of such devices, which should also be integrable in the current quantum computation systems, still represents a technical challenge.

Because of all these difficulties, the construction of a photonic quantum computer

simultaneously processing millions of qubits can only be a long-term goal. However, there are highly interesting intermediate steps on the way to this final result. In fact, already with a few tens of qubits, it is possible to perform computational tasks that cannot be run on ordinary computers [40]. These tasks typically involve the simulation of microscopic systems, whose analysis is particularly hard due to the large number of parameters required to describe a quantum state. Indeed it is natural to think that quantum systems can be simulated by other quantum systems: this is the basic idea of quantum simulation.

In general, quantum simulation can be very useful in exploring properties of complicated molecules, and therefore holds the promise to produce great advancements in chemistry [41]. To date, there have been several proof-of-principle experiments in quantum simulation, among which photonic architectures played an important role [42, 43]. The realization of simulations that are not executable on current computers is likely to happen in a near future.

1.6 Quantum communication

Quantum communication is the transmission of a quantum state from a point of space to another. Because of their mobility, photons are the main tool for this application, exactly as electromagnetic waves are used for classical communication. There are several forms of quantum communication, which differ in purposes, features, and requirements.

An important category of quantum communication protocols aims at reducing the amount of information to be transmitted to or between different parties in order to perform a shared computational task. The development and analysis of these protocols constitutes the field of *quantum communication complexity*. To date, several quantum schemes have been proposed to solve distributed computation problems more efficiently than classical algorithms [44, 45, 46, 47, 48, 49, 50, 51]. Proof-of-principle demonstrations of some of these theoretical proposals have also been realized [52, 53, 54, 55, 56].

A related but different question concerns the possibility of using quantum states

to optimize the physical resources that are necessary to transfer a given amount of information. This is the case of *dense coding*, which allows to transfer two bits of information between two parties by sending only one qubit, with the assumption that the parties pre-share an entangled state [57, 58, 59]. This can be seen as the opposite of *quantum teleportation*, in which a single qubit state is transferred by communicating two bits of information, still with the assumption that the parties already have an entangled state [60, 61, 62, 63].

The most studied quantum communication protocols are the cryptographic ones, which allow for information-theoretic secure transmission of classical bits between two parties. This means that the transmitted strings of bits cannot be eavesdropped, independently of the resources of the eavesdropper. For instance, the parties can use quantum states to share a secure cryptographic key and then use it for classical encrypted communication. This technique is called *quantum key distribution* (QKD). In case the message to be communicated is directly encoded and transferred by means of quantum systems, the parties are said to perform *quantum secure direct communication* (QSDC). These two categories of protocols are analysed in further detail below. The analysis is limited to protocols in the discrete-variable regime.

1.6.1 Quantum Key Distribution

A cryptographic key is a string of classical bits that allows for encryption and/or decryption of a message, which thus becomes hidden. Despite the large number of proposed and implemented schemes, the only provably secure cryptographic system known to date is the *one-time pad* [64, 65]. In this system, the secret message is encrypted by adding (modulo 2) each bit to a randomly generated key bit, whereas the decryption consists in bit-by-bit subtraction of the key from the encrypted message. In order to obtain unconditional security, the key must be used only once, hence the name of the system. Therefore, the parties involved in the communication need to share as many keys as the messages that are transferred, each key being a long, random sequence of bits. A crucial question is then how to securely distribute the keys.

QKD is a way to solve the key distribution problem, which, at least in principle, completes the one-time pad protocol and thus allows for unconditionally secure communication. In practice, due to the imperfections of the employed devices, unconditional security is actually never reached. Yet, QKD provides a security advantage with respect to the currently used cryptographic techniques, which all rely on computational problems that are hard to solve in reasonable time for a potential eavesdropper and thus could be broken by advances in classical and quantum computation [66].

In a typical QKD scheme, two parties, conventionally called Alice and Bob, aim at establishing a shared random sequence of bits, the key. To this purpose, they send and receive quantum states through a quantum channel, which may also include intermediate nodes. The quantum channel is assumed to be unsafe, meaning that is fully accessible and modifiable by potential eavesdroppers. By manipulation and measurement of the transferred qubits, Alice and Bob establish a *raw key*, i.e. they share two strongly correlated but not identical, and only partially secret, strings of bits.

After this phase, they use a classical channel to perform an interactive post-processing protocol, which allows them to distil two identical and completely secret copies of the key. In order for QKD to be secure, the classical channel must be authenticated, meaning that Alice and Bob identify themselves and the messages they send cannot be modified, even though they may be read by a third party. This authentication requires a cryptographic system as well, and consequently a key. QKD therefore allows two parties who already share a secret key to extend it, in principle infinitely. For this reason, rather than quantum key distribution it would be more precise to talk about quantum key growing.

Basic QKD protocols

In this section, some fundamental QKD protocols are presented. They constitute the basis of most implementations realized to date and a reference for alternative protocols.

The first QKD scheme was proposed by Bennett and Brassard in 1984 and therefore is called BB84 [5]. In this protocol, which is outlined in Figure 1.4, one of the parties, say Alice, randomly prepares and sends qubits to the other, Bob, in two different orthonormal

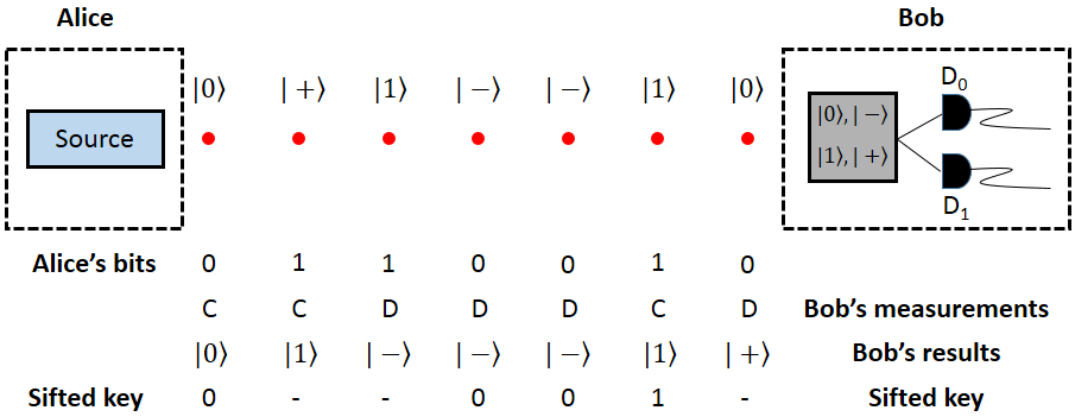


Figure 1.4: **BB84 protocol.** Alice sends a sequence of single photons to Bob that are prepared at random in the states of the computational basis (C), $|0\rangle$ and $|1\rangle$, or diagonal basis (D), $|+\rangle$ and $|-\rangle$. Bob performs for each photon a measurement in one of the two bases, selected at random, i.e. he uses a device that steers the photon to either D_0 or D_1 according to the basis state. The figure shows possible results obtained by Bob for a given sequence of bits encoded by Alice and measurement bases selected by Bob. The corresponding sifted key bits are also shown. In case Alice's preparation basis and Bob's measurement basis do not coincide, no sifted key bit is established.

bases such that the scalar product between states of different bases is always $\frac{1}{2}$. For instance, the two bases can be the computational basis $\{|0\rangle, |1\rangle\}$ and the diagonal basis, $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. The two states of each basis are associated to the classical bits 0 and 1, respectively (for example $|0\rangle, |-\rangle \rightarrow 0$ and $|1\rangle, |+\rangle \rightarrow 1$).

Bob measures each received qubit in one of the two bases, selected at random, and registers a raw-key bit according to the result of the measurement. When Bob's measurement basis coincides with Alice's preparation basis, Bob correctly receives the key bit prepared by Alice, otherwise Bob records the wrong key bit half of the time. Therefore, the two strings corresponding to the sent and received raw key are not identical, as they differ for one quarter of the bits.

After the raw-key transfer is over, Alice and Bob communicate through the authenticated classical channel their basis choice for each qubit, but not the prepared state (for Alice) or the measurement outcome (for Bob). They then discard all the bit digits corresponding to different basis choices. This procedure is called *sifting*. Ideally, after sifting, Alice's and Bob's key should be identical, but errors can arise due to experimental

imperfections or the action of an eavesdropper. Alice and Bob then publicly reveal part of the key to evaluate the so-called *quantum bit error rate* (QBER), defined as the percentage of different bits in the two sifted-key strings. Assuming that all the errors in the key are due to eavesdropping, the two parties can calculate the maximum amount of information that is leaked out to the eavesdropper.

The last step of the protocol is the application of classical algorithms for error correction and for reducing the amount of information transferred to the eavesdropper, a process that is called *privacy amplification* [67]. The resulting key is free from errors and fully secret, given that Bob receives more information than the eavesdropper, which can be checked from the QBER. If that is not the case, no secret key can be established and the sifted key is discarded.
Variations of the BB84 protocol using two states [68] and six states [69, 70] instead of four have also been proposed.

A different approach to QKD was presented in 1991 by Arthur Eckert, who developed a protocol based on entangled states, known as E91 protocol [71]. This scheme requires Alice and Bob to share, for each iteration of the protocol, a singlet state of two spin-$\frac{1}{2}$ particles, $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\downarrow\rangle_B - |\downarrow\rangle_A|\uparrow\rangle_B)$, where $|\uparrow\rangle$ and $|\downarrow\rangle$ denote the two eigenstates of the spin component along the z-axis, whereas the subscripts A and B stand for Alice and Bob, respectively. This state may be generated by one of the parties or, alternatively, provided by an external server, which can be untrusted.

Each of the parties randomly measures the spin component along one of three possible directions in the $x-y$ plane, characterized by azimuthal angles $\Phi = 0$, $\frac{\pi}{4}$ and $\frac{\pi}{2}$ for Alice, and $\Phi = \frac{\pi}{4}$, $\frac{\pi}{2}$ and $\frac{3}{4}\pi$ for Bob. The measurement of the spin component along one of such directions corresponds to a measurement in the basis $\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + e^{i\Phi}|\downarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - e^{i\Phi}|\downarrow\rangle)\}$.

After the measurement phase, Alice and Bob communicate their measurement choices through the authenticated channel and divide the iterations in two groups, according to whether they chose the same spin component (group 1) or not (group 2). For the iterations of group 2, they reveal the outcome of the measurements and use them to check for eavesdropping. The state $|\psi^-\rangle$, in fact, presents unique spin correlations that

change if the protocol is disturbed by an eavesdropper. A test of these correlations is called a *Bell test* [14, 72]. Analogously, when the state is provided by an external server, the Bell test is used to check the honesty of the server. A dishonest server, in fact, may send to the parties a state different from $|\psi^-\rangle$ in order to extract some information on the key.

After verification, Alice and Bob use the iterations of group 1 to establish the shared key, as, whenever they measure the same component of the spin (which occurs about $\frac{2}{9}$ of the time), the measurement results are perfectly anti-correlated, but random.

Analogously to the BB84 protocol, the parties evaluate the QBER on a sub-set of the key and, from that, they bound the maximum amount of information obtained by the eavesdropper. Error correction and privacy amplification algorithms complete the protocol. Note that for the protocol the two parties can use any of the four possible Bell states: $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\downarrow\rangle_B \pm |\downarrow\rangle_A|\uparrow\rangle_B)$, $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_A|\uparrow\rangle_B \pm |\downarrow\rangle_A|\downarrow\rangle_B)$. Furthermore, they can use any degree of freedom, not necessarily spin, for the qubit realization.

In 1992 Bennett, Brassard and Mermin, inspired by the E91 protocol, proposed a simpler scheme, the BBM92 protocol, in which Alice and Bob perform measurements in only two bases, those corresponding to $\Phi = 0$ and $\Phi = \frac{\pi}{2}$ [73] (see Figure 1.5). In this case, Alice and Bob only keep the iterations in which they performed the same measurement, and sacrifice a large sub-set (more than half) of them to verify the correlation of the measurement outcomes. If the correlations are as expected, they infer absence of eavesdropping and honesty of the server. The iterations for which the outcomes were not revealed are used for key generation. This protocol was shown to be equivalent to BB84.

Since the development of these first protocols, much progress has been done in QKD, both theoretically and experimentally [74, 75, 76]. The BB84 protocol, due to its simplicity, still represents the basis of many implementations, although the basic scheme has been modified to face all the theoretical and experimental challenges that arose in the last decades, as it will be discussed in the next sections.

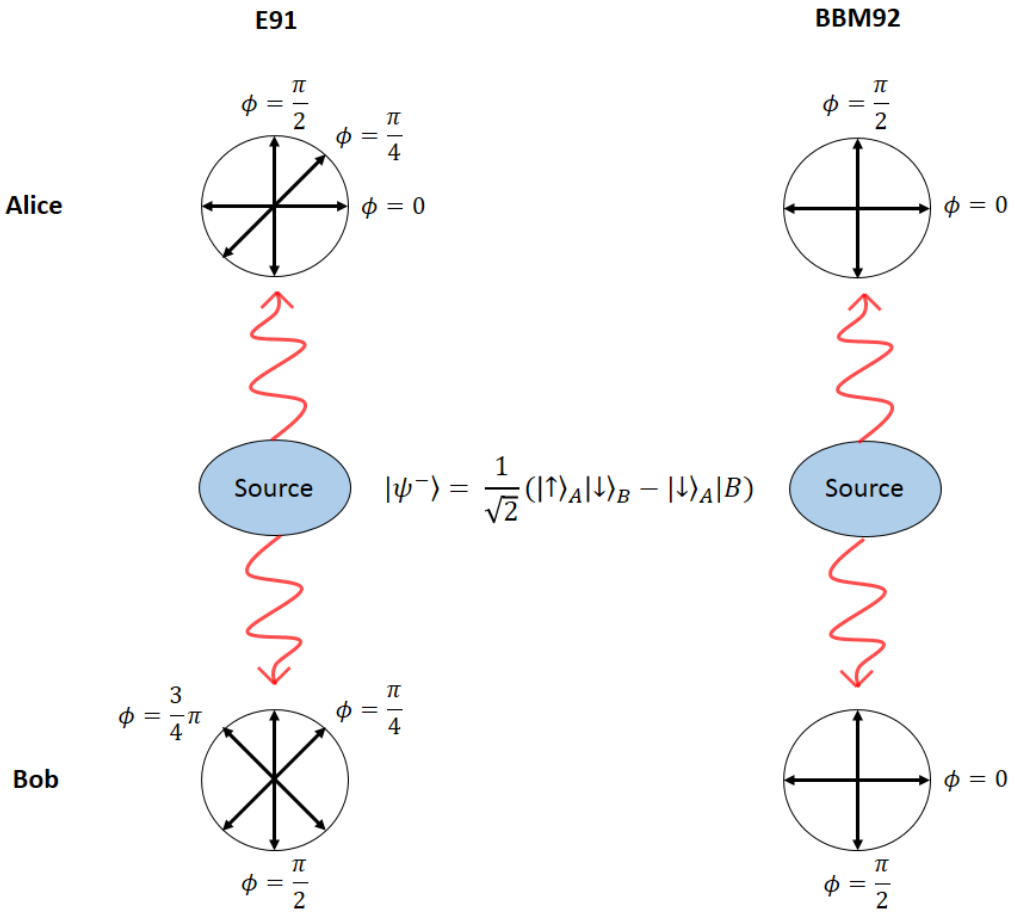


Figure 1.5: **E91 vs BBM92 protocols.** In both protocols, Alice and Bob share a maximally-entangled two-particle state, which here is assumed to be the singlet state $|\psi^-\rangle$. The states $|\uparrow\rangle$ and $|\downarrow\rangle$ represent the two eigenstates of the spin component along the z axis. In the E91 protocol, sketched on the left, each of the parties performs measurements along three different spin components in the x-y plane (where the x axis corresponds to $\Phi = 0$). Two of the components are the same for Alice and Bob, while the third is different. The parties use the iterations in which they measured along the same component for key generation and the other iterations for a Bell test, which is used to verify eavesdropping and honesty of the state provider, in the case that the state is not generated by one of the parties. In the BBM92 protocol, outlined on the right, the two parties perform measurements along the same two spin components and use part of the iterations to verify for eavesdropping and provider honesty. The remaining ones are used for sharing the key.

From the first experimental realization, showing QKD over a distance of 32.5 cm in free-space [77], technology has reached a level allowing for satellite-based QKD over distances of thousands of kilometers [78, 79, 80]. Regarding entanglement-based QKD, after the first proof-of-principle realizations [81, 82, 83], experiments covering a record distance of over 100 km in fibers were reported [84, 85]. Furthermore, protocols exploiting entanglement in higher dimensions have been developed and successfully implemented [86, 87, 88, 89, 90, 91, 92]. These protocols attract attention from the quantum cryptography community due to the possibility of transferring a high number of bits per photon.

Hacking techniques

In the ideal scenario of perfect devices, the possible attacks performed by a potential eavesdropper, Eve, are grouped in three categories: individual, collective and coherent attacks. In individual attacks, Eve acts on each qubit sent through the quantum communication channel separately and independently. In the case of collective attacks, Eve still interacts independently with each qubit exchanged by Alice and Bob but she does it by using one or more independent ancillary qubits. At any point in time, she can then perform a joint measurement on all the ancillas. Finally, coherent attacks are those in which Eve prepares an entangled state of ancillary qubits to be interacted with the qubits of the channel before being measured jointly. An information-theoretic (perfect) secure protocol must be proven secure against all these possible attacks, which has been done for the BB84 protocol and its entanglement-based version, BBM92 [93, 94, 95]. These security proofs also extend to the E91 protocol. Statistical effects due to the finite size of the key should also be taken into account for practical applications [96].

Intuitively, the security of QKD is based on the fact that any attempt of measuring a qubit alters it in a way that is detectable by the communication parties. At the same time, the no-cloning theorem prevents Eve from copying the transmitted qubits and acting on the copies without disturbing the original qubits. From the amount of alteration, Alice and Bob quantify the maximum amount of information leaked to a third party and apply techniques for its arbitrary reduction.

As an example, the simplest individual attack in the BB84 protocol - the intercept-resend attack - is considered. For this attack Eve measures each transferred qubit at random in one of the two possible preparation bases and sends to Bob another qubit, which is prepared according to the measurement outcome. Whenever Eve's measurement basis and Alice's preparation basis do not coincide, which happens in 50% of the cases, Bob receives the wrong qubit. This leads to an error in half of the useful cases for key generation, thus determining a QBER of 25% in the sifted key. If Bob detects such a large error, an intercept-resend attack is deduced and the key is discarded.

Even though the basic QKD protocols can be proven perfectly secure in the ideal case, imperfections in the actually employed devices make other attacks possible and thus complicate the security proofs. Any QKD set-up is composed of three parts: the source, the quantum channel and the detection system. Even in the ideal case, Eve is free to access and alter the quantum channel as she wishes, so attacks based on device imperfections focus on the source or the detectors.

The main attack at the source level is the photon-number-splitting (PNS) attack [97, 98]. This attack exploits the fact that the source can emit multiple copies of the same qubit. In the language of single-photon sources, this means that the source emits multi-photon components. For practical reasons, the most used photon sources for QKD are phase-randomized attenuated lasers, as they are cheaper and simpler to use than actual single-photon sources. They produce a state that can be described, for security analysis, by the following density operator:

$$\hat{\rho} = \sum_{n=1}^{\infty} P(n)|n\rangle\langle n|, \tag{1.45}$$

where $|n\rangle$ is the n-photon Fock state in a given mode and $P(n) = e^{-\mu}\frac{\mu^n}{n!}$ is the Poisson distribution in photon number with average μ. Security of most QKD protocols, including BB84, is granted only for the single-photon component, therefore, typically, μ is set to be lower than 1. Nevertheless, the multi-photon components may still be significant, thus providing a tool for Eve to extract information on the key, as it is described below, with

reference to a BB84 protocol in which Alice sends photons to Bob.

In a PNS attack, Eve performs a quantum non-demolition measurement [99, 100] on each quantum signal sent by Alice. With this measurement Eve can infer the photon number of the signal without destroying photons. If she obtains $n = 1$, she blocks the signal, otherwise she splits it in two parts, keeps one of the parts for herself and sends the other one to Bob. In order to compensate for the introduced losses, Eve can increase the channel transmission, t, defined as the probability that a single photon leaving Alice's laboratory reaches Bob. Full compensation is possible only if $t < p_m$, where p_m is the probability of multi-photon pulses. In this case, Eve obtains a copy of each qubit received by Bob and, therefore, she can extract the full key after the information on the bases is revealed during the sifting process. If $t > p_m$, instead, Eve is forced to let some single-photon pulses reach Bob, in order to stay undetected. Hence, she can obtain only partial information on the key. The parameter p_m therefore sets a lower bound to the channel transmission, which limits the maximum distance for secure QKD.

Bob could, in principle, counter the described PNS attack by measuring the photon-number statistics of the received pulses and comparing them with the expected specifications of the source specifications, provided by Alice, also taking into account the channel losses. Unfortunately, this countermeasure can be neutralized by more sophisticated PNS attacks, in which Eve blocks or releases the pulses sent by Alice such that the photon-number statistics are preserved [101]. Luckily, a solution to this problem was found in the decoy-state methods, which will be described in the next section.

A more dangerous class of attacks involves the detectors. The increased danger comes from the fact that while Alice and Bob can somehow control what they emit, they are forced to let signals from the outside reach their detection stages. These signals could be used to change their devices in a way that is advantageous for eavesdropping. Among the proposed attacks, the most powerful one is the detector-blinding attack [102], which was also successfully demonstrated on some practical types of QKD sytems [103].

This attack exploits the fact that the typical detectors used in QKD, InGaAs/InP avalanche photo-diodes (APD), can be switched by bright laser light between their two

possible mode of operations - linear mode and geiger mode [104]. For QKD the APDs are operated in geiger mode, meaning that they produce a macroscopic current when hit by a single photon. When this current exceeds a certain threshold value I_{th}, set by the read-out electronics, a "click", i.e. a single-photon detection, is recorded. The attack consists in "blinding" the detectors by sending a strong laser pulse, which makes them switch to linear mode. In this regime, the detectors just provide a current that is proportional to the input optical power. The threshold current I_{th} then sets a threshold input optical power, P_{th}, above which a click is recorded.

After blinding Bob's detectors, Eve can perform an intercept-resend attack where, instead of sending single photons to Bob, she sends bright pulses with power P such that P is above P_{th}, but $\frac{P}{2}$ is not. Consequently, when Bob measures in a different basis than Eve's, the pulse is split in two pulses of half power and does not produce a single-photon detection. All Bob's detections, therefore, correspond to cases in which he chooses the same basis as Eve, who can obtain full information on the key without increasing the QBER.

There are several strategies to counter detection-based attacks. For instance, the detection systems can be modified such that they are no longer vulnerable to one or more given attacks. The drawback of this method is that the devices need to be continuously upgraded as new attacks are discovered. Another possibility is including detector imperfections in the security analysis of QKD protocols so as to calculate the maximum amount of secure-key rate that is achievable. Modelling the detectors' behaviour however is quite challenging due to the many possible effects that are involved. Furthermore, in some cases, it is not possible for Alice and Bob to establish a secure key.

A more effective solution is to design new QKD protocols in which no assumption on the detectors is made. With such schemes, in principle, the detectors can even be controlled by the eavesdropper. This is the basic assumption of measurement-device-independent (MDI) QKD, which will be described after the next section.

Decoy-state method

The decoy-state method is an effective technique to detect and counter any PNS attack [105, 106, 107, 108]. The starting point for the development of this method is the consideration that a PNS attack causes an abnormally higher channel transmission probability, or *yield*, for pulses containing more than one photon, than for single-photon pulses. Alice and Bob can then test the photon-number-dependent yields of the channel to detect potential PNS attacks.

In order to do that, Alice must use at least two different kinds of pulses, which are sent at random: signal pulses, used for transmitting the key digits, and decoy pulses, with different photon-number statistics, used for verification. Except for the different statistics, the two categories of pulses must be completely identical so that Eve cannot know whether a given measured photon number, n, comes from a signal or a decoy pulse. This means that, even assuming the presence of an eavesdropper, the yield, y_n, and the error rate, e_n, for a pulse with photon number n, do not depend on which distribution the pulse belongs to. In the verification phase, Alice reveals the position of the signal and decoy states so that the channel yields can be characterized and a potential PNS attack can be detected.

Decoy states may be generated by modulating the intensity of a single laser or, alternatively, by using different lasers. Both techniques determine the generation of pulses with different Poisson distributions, $P_\mu(n)$, with different values of μ. The overall yeld and error rate for each decoy distribution are then, respectively:

$$Y_\mu = \sum_{n=0}^{\infty} P_\mu(n) y_n \tag{1.46}$$

$$\mathrm{QBER}_\mu = \frac{1}{Y_\mu} \sum_{n=0}^{\infty} P_\mu(n) e_n y_n, \tag{1.47}$$

from which the quantities y_n and e_n can be extracted. In general, even in the case of an attempted attack, Alice and Bob might still be able to establish a secret key. In order to decide if that is the case and to calculate the secret key rate, they need to estimate the

single-photon yield, y_1 and error rate, e_1, which can be obtained from Equations 1.46. In practice, a good estimation is already possible with three values of μ, one for signal and two for decoy states [107, 108].

The decoy-state technique allowed for an extension of the maximum distance at which QKD can be performed, even when using an imperfect source. From the experimental point of view, after the theoretical development of the decoy-state technique, several implementations have been realized [109, 110, 111, 112]. Nowadays, this concept represents a standard technique for QKD. Decoy-state QKD was demonstrated over 1200 km in free-space satellite-based communication, using polarization encoding and reaching a secure key rate of 1.1 kbit/s [79]. In fiber, a record distance of 421 km was covered, with time-bin encoding and a secure key rate of 6.5 bits/s [113]. Over a shorter fiber distance of 45 km, within Tokyo metropolitan area, a record secure key rate of 304.0 kbits/s was reported using phase encoding [114].

Measurement-device-independent (MDI) QKD

The most practical solution to attacks at detection is the MDI-QKD protocol, developed by Lo and collaborators in 2012 [115]. In this scheme, Alice and Bob do not perform any detection, which is delegated to an untrusted third party, Charlie. However, the protocol assumes that the sources of quantum states are trusted and do not present loopholes.

In MDI-QKD, each party generates at random one of the four possible BB84 states and sends it to Charlie. Charlie, if honest, performs a Bell-state measurement on the global state received by Alice and Bob, which consists in a simultaneous projection onto the four Bell states used for the E91 protocol, $|\psi^{\pm}\rangle$ and $|\phi^{\pm}\rangle$. The protocol is described in terms of polarization. The two bases for encoding the BB84 states are then those of linear polarizations $\{|H\rangle, |V\rangle\}$ and $\{|D\rangle, |A\rangle\}$, where D and A stand for "diagonal" and "anti-diagonal", and indicate polarization directions rotated counterclockwise by $\frac{\pi}{4}$ and$\frac{3}{4}\pi$ with respect to $|H\rangle$, respectively. Here, $|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, indicate single-photon states in the polarization mode corresponding to the letters.

The protocol does not require Charlie to perform a complete Bell-state measurement,

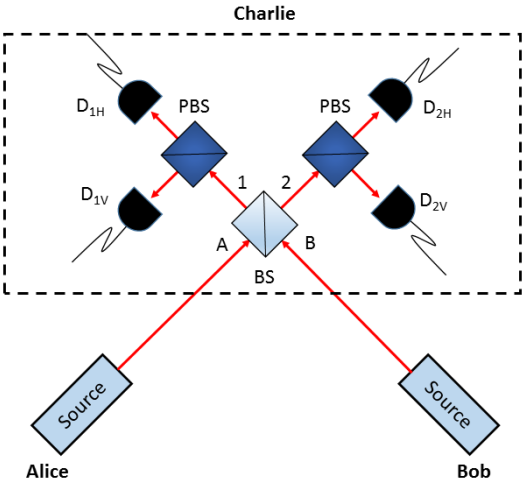


Figure 1.6: **Setup for MDI-QKD.** Alice and Bob send single-photon pulses, potentially together with decoy states, to an untrusted party, Charlie, who is the only party performing detection. Alice and Bob prepare each BB84 states at random and Charlie implements a partial Bell-state measurement, capable of distinguishing $|\psi^-\rangle$ from $|\psi^+\rangle$. The pulses sent by Alice and Bob reach a beam splitter (BS), which maps the state $|\psi^+\rangle$ into $\frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_1 - |H\rangle_2|V\rangle_2)$ and the state $|\psi^-\rangle$ into $\frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$, where 1 and 2 are the spatial modes at the outputs of the beam splitter, respectively. The polarizing beam splitter (PBS) at each output transmits the horizontal polarization and reflects the vertical one, therefore $|\psi^+\rangle$ determines a coincidence between D_{1H} and D_{1V} or between D_{2H} and D_{2V}. By contrast, $|\phi^-\rangle$ can only give coincidences between D_{1H} and D_{2V} or between D_{1V} and D_{2H}. The other two Bell states are converted by the beam splitter to states where both photons always have the same polarization and therefore do not yield coincidences.

i.e. a measurement that can distinguish each Bell state from any other. Only distinction between the states $|\psi^+\rangle$ and $|\psi^-\rangle$ is needed, which can be performed with linear optics using the setup in Figure 1.6. The state $|\psi^+\rangle$ determines a coincidence between detectors D_{1H} and D_{1V} or between D_{2H} and D_{2V}, whereas $|\psi^-\rangle$ makes detectors D_{1H} and D_{2V} or D_{2H} and D_{1V} click simultaneously. By contrast, the states $|\phi^+\rangle$ and $|\phi^-\rangle$ do not cause any coincidence detection.

Each product of BB84 states produced by Alice and Bob can be written in terms of the four Bell states, as these constitute a basis of the four-dimensional space associated to the polarization of the two photons. When Alice and Bob both choose to use the H-V basis, coincidences arise only if they generate different states, as only the states $|H\rangle_A|V\rangle_B$ and $|V\rangle_A|H\rangle_B$ contain $|\psi^+\rangle$ and $|\psi^-\rangle$. In the diagonal basis, instead, the states $|D\rangle_A|D\rangle_B$ and $|A\rangle_A|A\rangle_B$ contain $|\psi^+\rangle$, while $|D\rangle_A|A\rangle_B$ and $|A\rangle_A|D\rangle_B$ contain

$|\psi^-\rangle$. Therefore, based on which pair of detectors gives a coincidence, the parties can deduce whether they encoded identical or different states. If the parties choose different bases, the different encoded states are not distinguishable.

After performing the (partial) Bell-state measurement, Charlie announces the detection outcome. Alice and Bob, after the communication phase, declare their choices of bases and only keep the iterations where coincidence events were recorded and they chose the same basis. Using the information on which detectors fired, they can establish the correlation between the encoded states and, consequently, they can share a sifted key. As usual, they estimate the QBER on a sub-set of the key for detecting eavesdropping and verifying Charlie's honesty.

The decoy-state method may be applied to make the protocol secure against PNS attacks. In this case, the fact that the detectors are not controlled by Alice and Bob complicates the security analysis. Nevertheless, this analysis was conducted and several decoy-state techniques for MDI-QKD have been proposed [76].

Experimentally, MDI-QKD presents an additional challenge with respect to the other schemes discussed so far: the two states produced by Alice and Bob have to interfere[1] at Charlie's station and, therefore, the corresponding photons have to be indistinguishable, except for polarization. In particular, they need to arrive simultaneously at Charlie's beam splitter, which could be particularly challenging when applied to long distances. Stabilization techniques for the length of the two paths between Alice and Charlie, and Bob and Charlie, must therefore be enforced.

The feasibility of MDI-QKD was shown in 2013 by several groups [116, 117, 118, 119]. After those first demonstrations, effort has been put in extending the distance covered by the protocols and in increasing the key rate. To date, a maximum distance of 404 km was achieved in fiber using time-bin encoding, with a secret key rate of 3.2×10^{-4} bits/s [120]. The highest reported key rate over long distance communication was 2.2×10^3 bits/s over 102 km of fiber, with polarization encoding [121]. Finally, a real-world MDI-QKD

[1]The interference mentioned here is a two-photon interference and not the single-photon interference described in Section 1.3

network with three users and one untrusted relay was implemented in the city of Hefei in China [122].

Technological challenges

Even though great progress has been made in the field of QKD since its original proposal, the realization of a full, ideally world-wide, QKD network that can be used in everyday life still represents a challenge. It has been proven that, without intermediate nodes, the secure key rate shared by Alice and Bob is proportional to the transmittance of the channel between them [123]. As the transmittance of optical fibers scales exponentially with the distance, this strongly limits the maximum distance at which QKD can be performed.

In classical optical communication, the problem of losses in optical fibers is solved by using repeaters, which amplify the signal at intermediate nodes. In principle, this concept can be applied also to quantum communication, but in this case the realization of a repeater is far more complicated. A quantum repeater typically uses a combination of entanglement swapping and purification in order to transport an entangled state through long distance [9, 10]. In order to be effective, these schemes need to use quantum memories, which typically require interactions between light and matter. Significant improvements in the realization of light-matter hybrid systems would therefore allow for the realization of a large-scale quantum network [124]. However, at the current technological stage the performance of quantum memories is still limited both in terms of storage time and fidelity of the retrieved state, which prevents the practical implementation of quantum repeaters [125]. As an alternative, all-optical quantum repeaters have been proposed [11], but they require large multi-photon entangled states, whose preparation is challenging, as discussed already for MBQC.

A promising route to extend the distance covered by QKD is satellite communication. Above a given height in the atmosphere, in fact, optical absorption is practically zero. This allows to distribute keys between parties that are thousands of kilometers distant on Earth, by using a satellite as a relay [79, 80]. This kind of configuration is also

particularly suitable for MDI-QKD.

Besides extension of distance, another technological challenge consists in the realization of compact and cheap devices for QKD, which can be practically and economically convenient. The most natural solution is the employment of integrated devices, some of which have already been demonstrated [126, 127, 128].

Important insights may also come from theoretical research. On the one hand, an improved security analysis of the current protocols may result into higher secure key rates, even without technological improvements; on the other hand, new protocols might result in better performance or simpler setups, as it will be discussed in the next two sections .

Twin-field QKD

A way to overcome the fundamental rate-distance limit of repeaterless QKD is twin-field (TF) QKD, which was proposed in 2018 by Lucamarini et al. [129]. The inventors of this protocol showed a quadratic improvement in the secure key rate, which is found to be proportional to the square root of the channel transmittance between Alice and Bob. The scheme is an example of MDI-QKD, based on single-photon interference and consequently single-photon detection, instead of coincidence detection, which is the reason for the quadratic improvement. A comparison of the rate-distance dependence for the main QKD schemes developed so far can be found in Figure 1.7.

In TF-QKD, Alice and Bob both use phase-randomized dim laser pulses as sources, together with decoy states. The parties apply two additional phases, ϕ_b and ϕ_k, which can only be 0 or π and are selected at random. The value of the phase ϕ_b corresponds to the basis choice of the BB84 protocol, while the value of ϕ_k determines the key bit. The pulses are sent to a third party, Charlie, who interferes them at a beam splitter and records single-photon detections at detectors D_0 and D_1 (see Figure 1.8). Charlie publicly declares the detection result for each pulse. In the verification phase, Alice and Bob declare for each pulse both the random phases applied to the pulses and the two phases ϕ_b. According to which detector clicked, Alice and Bob can deduce the parity of

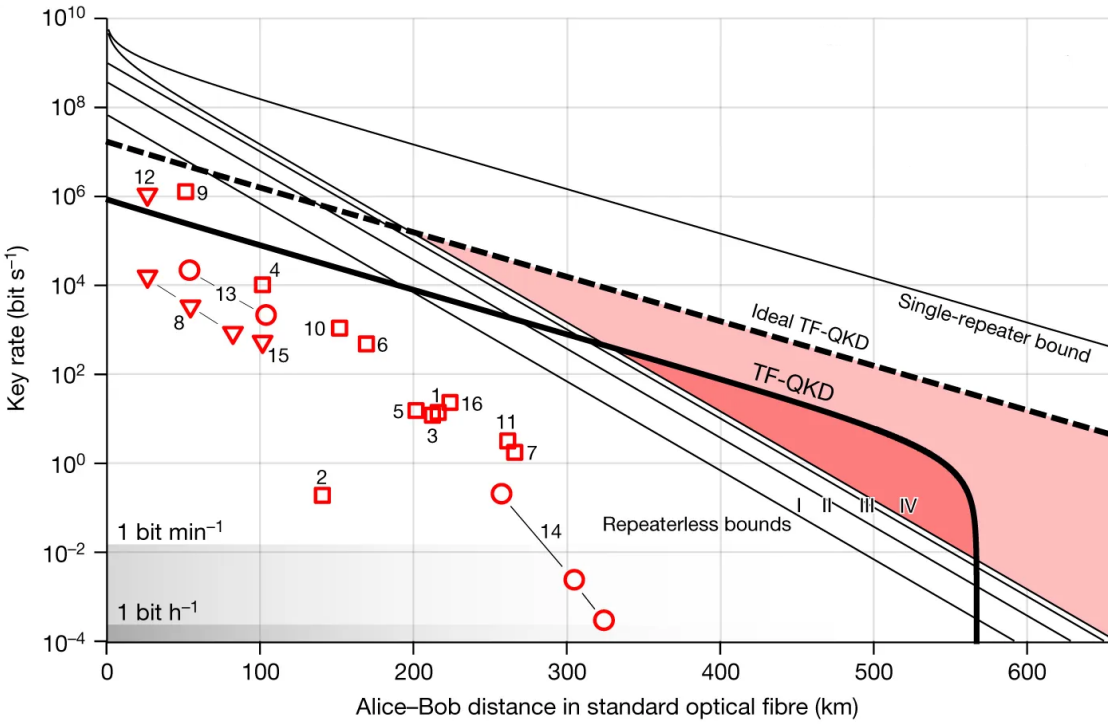


Figure 1.7: **Theoretical bounds and experimental results for QKD in fiber.** The solid lines indicate the theoretical bounds for different QKD schemes, where I indicates decoy-state MDI-QKD, II general decoy-state QKD, III single-photon QKD and IV the theoretical bound found in [123]. It is clear that ideal TF-QKD surpasses all these bounds at large distances, approaching the single-repeater bound. Imperfect QKD instead surpasses the repeaterless bounds only for a specific range of distances. The experimental results are shown with symbols and are numbered in chronological order. The figure is adopted from [129].

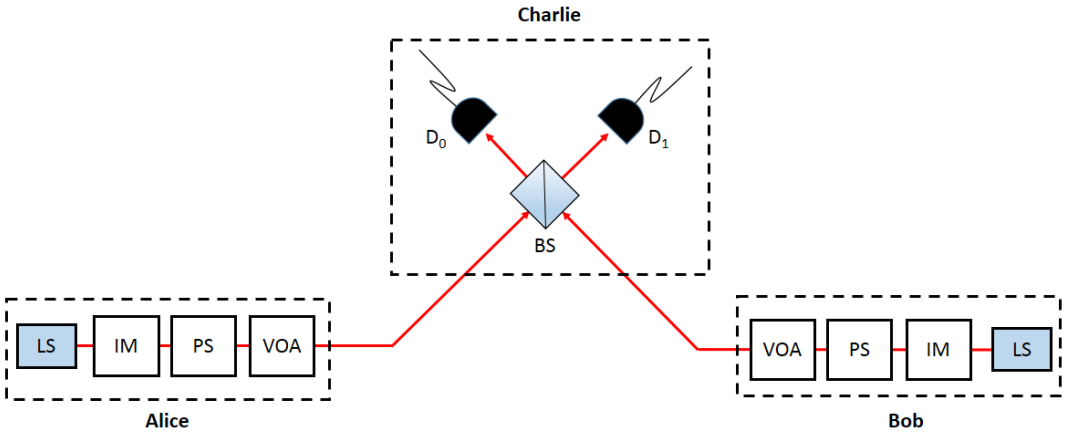


Figure 1.8: **Sketch of TF-QKD scheme.** Alice and Bob both have a light source (LS), which is typically a laser, an intensity modulator (IM), a phase shifter (PS) and a variable optical attenuator (VOA). The intensity modulator is used to randomly variate the average photon number in the light signal for the decoy-state method. The phase shifter is used to apply the random phases as well as the phases ϕ_b and ϕ_k. The variable optical attenuator is used to switch at random between dim and bright pulses. The bright pulses are used to actively stabilize the interferometric paths.

the encoded bits and, consequently, establish a shared key.

Technically, the main challenge of the protocol is that single-photon interference requires phase stability between the paths connecting Alice to Charlie and Bob to Charlie, respectively. This can be achieved with active stabilization performed by Charlie, using bright pulses (classical regime), which are sent at random by the two users.

Variations of the basic protocol have been proposed and analysed in the asymptotic-key regime [130, 131, 132, 133] and some experiments proving the feasibility of the concept have been realized [134, 135, 136, 137]. Recently, a TF-QKD protocol was implemented over 509 km of optical fiber [138], showing a secure key rate of 1.79×10^{-8} bits/s, which surpasses the repeaterless bound in [123].

Semi-classical QKD

All the QKD protocols discussed up to now assume that both parties Alice and Bob are "quantum" in nature. This means that both parties are allowed to prepare and/or measure single-photon states (or laser light attenuated to single-photon level) in at least two bases. In fact, if both parties are restricted to classical communication, unconditional security

is impossible to achieve for the key distribution problem. A natural question then arises, namely "how quantum" must a protocol actually be to obtain unconditional security? This question, besides its fundamental interest, may have practical consequences, as the quantum nature of the parties sets stricter technological requirements than classical communication.

To help study this, the semi-quantum model of cryptography was introduced in 2007 by Boyer et al. [139]. In this model, one party, say Bob, is restricted to operations on qubits that have a classical counterpart, such as preparation or measurement in a single basis. By contrast, Alice is quantum, i.e. she is only limited by the laws of physics. The Boyer protocol requires Alice and Bob to share a two-way quantum communication channel. Alice sends Bob N qubits that are randomly prepared in the four BB84 states. For each qubit, Bob can choose between two actions: measuring the qubit in the computational basis and re-sending it in the same state he found, or reflecting the qubit without any modification.
Bob sends the first qubit after receiving the last qubit from Alice, without altering the qubits order. Consequently, Alice measures the qubits from Bob in the same basis in which she prepared them.

After the communication is over, Alice reveals the bases she chose and Bob declares his actions. They obtain the sifted key from the cases in which Alice prepared a qubit in the computational basis and Bob measured. The cases in which Bob reflected the qubit are used to detect the presence of eavesdroppers, while the cases in which Alice prepared a qubit in the diagonal basis are discarded. Finally, as usual, Alice and Bob check the QBER on a sub-set of the key and apply error correction and privacy amplification algorithms. This protocol was proven to be *robust*, meaning that Alice and Bob can always detect the attempts of the eavesdropping to obtain the key.

Most SQKD protocols up to this point have been theoretical in nature. In fact, on the one hand they often require devices that are still far from actual realization, such as quantum memories with long storage time; on the other hand they typically assume perfect qubit channels, i.e., for instance, no photon loss and multi-photon emission are

permitted for their security to be valid [140, 141, 142].

A few SQKD protocols facing these problems were proposed recently [143, 144], although no full proof of security was provided. meaning that their key rates and noise tolerances are still unknown. Indeed, up to this point, all information theoretic security proofs of SQKD protocols have required perfect qubits as an assumption. Furthermore, they have always been conducted in the asymptotic-key regime.

In 2015, a new semi-quantum protocol, referred to as a a mediated SQKD protocol, was introduced [145], which allows two "classical" users to establish a shared secret key with one another, using the help of a quantum server who must prepare, and later measure, quantum bits. This quantum server does not need to be trusted, and in fact could be an all-powerful adversary. For each iteration of the protocol, the server prepares and sends to the parties the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$, where A and B stand for Alice and Bob. The two parties decide at random whether to reflect back the received qubit or to measure it in the computational basis $\{|0\rangle, |1\rangle\}$.

The server performs a Bell measurement on the returned qubits and publicly declares the result, in particular "1" if the two-qubit state is found to be in $|\phi^+\rangle$ or"-1" in the case of $|\phi^-\rangle$. In absence of noise or eavesdropping, the results $|\psi^\pm\rangle$ are not possible. After the quantum communication phase, Alice and Bob share their choices (reflection or measurement) over an authenticated classical channel. They use the iterations in which they both reflected the qubit for detecting eavesdropping and server dishonesty, as, in those cases, the server should always declare "1". For key generation, they only keep the cases in which they both measured and the server declared "-1". This choice turns to be important for security, which was proven, but again, only for the perfect-qubit scenario in the asymptotic-key regime.

The original mediated SQKD protocol and its subsequent variations [146, 147] require the generation, manipulation and measurement of entangled states, which often represents a technical challenge. Furthermore, in all of them, Alice and Bob need to be able to generate quantum states in the computational basis, which, from the experimental point of view, translates into generation of single photons. This means that, in practice, the

parties must effectively provide quantum resources.

1.6.2 Quantum secure direct communication (QSDC)

Quantum secure direct communication (QSDC) unifies in one single technique QKD and the subsequent encrypted classical communication. The goal of two parties performing QSDC is not sharing a random sequence of bits but directly transferring a classical meaningful message, which is encoded in quantum states.

In this case, however, it is harder to attain perfect security, as, contrary to QKD, the parties cannot discard the message, or a part of it, if they realize that information has leaked out to an eavesdropper. This complicates the design and implementation of QSDC protocols. Furthermore, the practical advantages of QSDC over QKD followed by classical communication are not fully clear. Nevertheless, QSDC is an interesting intellectual problem and the methods developed in this field can be beneficial for quantum communication in general, including QKD.

The first QSDC protocol was proposed by Boström and Felbinger in 2002 [148]. In this scheme, the message receiver, say Bob, prepares the two-photon Bell state $|\psi^+\rangle$ for each iteration of the protocol and transmits one of the photons to the sender, Alice. Alice randomly switches between two modes: message mode, with probability $1-c$, and control mode, with probability c. In the message mode, Alice performs one of the two unitaries U_0 and U_1 on the received qubit, according to the message bit she wants to encode, and returns the photon to Bob, who performs a Bell measurement to read out the encoded bit. Here U_0 is the identity, which leaves the qubit and the global state $|\psi^+\rangle$ unaltered, while U_1 adds a π-phase to $|1\rangle$ and leaves $|0\rangle$ unchanged, thus transforming the state $|\psi^+\rangle$ into $|\psi^-\rangle$.

In the control mode, Alice measures her qubit in the computational basis $\{|0\rangle, |1\rangle\}$ and communicates the result to Bob over an authenticated classical channel. Bob, then performs the same measurements and check if the two results are compatible. This mode is used to detect the presence of eavesdroppers. This scheme, also known as "ping-pong protocol", was shown to be quasi-secure, meaning that the information leakage about

the message is not zero but asymptotically tends to zero as c is increased.

After the original proposal, several researchers showed that the ping-pong protocol is vulnerable to attacks in case of losses or noise in the quantum channel between Alice and Bob [149, 150, 151]. For this reason, some improvements were proposed. In particular, Cai and Li [152] suggested to use two measurement bases instead of one in the control mode, to attain security also in presence of losses and noise, and four operators instead of two in the message mode in order to double the transmission capacity. Lucamarini and Mancini [153] replaced the Bell states with simple BB84 states sent by Bob to Alice and back. In this scheme, the two operators U_0 and U_1 become the identity and the bit flip in both bases, respectively. The Bell state measurement performed by Bob is replaced by a measurement in the same basis used for preparation and, in the control mode, Alice not only measures in two bases but sends to Bob a BB84 state according to the result of the measurement. In this way, the authors show that the protocol is quasi-secure also in the case of losses and noise, and perfectly secure if used for QKD.

The first fully secure QSDC protocols, the two-step protocol and the quantum one-time-pad protocol (also known as DL04) were presented by Deng, Long and collaborators in 2003 and 2004, respectively [154, 155]. In both protocols security is ensured by a procedure that is composed of two stages. In the first stage, one party distributes quantum states to the other and, after that, both parties verify whether eavesdropping occurred. In the second stage, the message is encoded and transferred by using the states distributed in the first stage. If the distributed states were not eavesdropped during the first stage, then the message is secure.

For instance, in the two-step protocol, Alice prepares a sequence of identical Bell pairs and sends one photon of each pair to Bob. After Bob receives all the photons, the two parties randomly select some pairs and perform measurements to detect eavesdropping. This is the first stage. If no eavesdropping is detected, it means that Alice and Bob safely share several copies of a Bell state. At this point Alice encodes message bits in the photons she kept and sends them to Bob. Even if now an eavesdropper acts on the channel between Alice and Bob, no information on the message can be extracted from a

single photon that is part of a Bell pair. Alice may anyway randomly place some check bits for additional eavesdropping detection and error checking.

The DL04 protocol adopts a similar procedure, but now, during the fist stage, the receiver, Bob, sends BB84 states to Alice, who randomly performs measurements in two bases on some of them, for verification purposes. If the verification is successful, she encodes information in the remaining states and sends them back to Bob. Generalizations of these schemes in higher dimensions were also proposed [106, 156, 157].

These protocols are not easily implementable, as they need quantum memories with long storage times. However, some proof-of-principle implementations of the two-step and the DL04 protocol were realized [158, 159, 160]. In particular, the experiment in [159] used an atomic quantum memory to show the basic stages of the two-step protocol, while in [158, 160] long fibers were used as memories. These realizations show that the experimental requirements for QSDC still represent a challenge, preventing this technique to be used for practical applications.

Chapter 2

Generation of Single Photons Through Spontaneous Parametric Down-conversion

The technique used for single-photon generation in all the works comprising this Ph.D. project, and described in the next chapters, is spontaneous parametric down-conversion (SPDC). SPDC is a non-linear optical process occurring in non-centrosymmetric crystals, which is largely used in quantum optics experiment. This chapter aims to give a general picture of SPDC, and it is structured as follows. At first, some basic concepts of second-order non-linear optics are introduced, then, SPDC is explained in detail, both in single-pass and resonant configuration. In the end of the chapter, some methods for temporal and spectral characterization of SPDC-based single-photon sources involving quantum correlation functions are described. The present chapter serves in particular as theoretical background for Chapter 5, which describes the realization and characterization of a narrow-band SPDC-based single-photon source.

2.1 Non-linear optical processes

Maxwell's equation in a source-free dielectric medium involve four fields, the electric field **E**, the magnetic field **H**, the electric flux density **D** and the magnetic flux density **B**. **D** and **B** include the response of the medium, according to the following relations:

$$\mathbf{D} = \epsilon_0 \mathbf{E} + \mathbf{P} \tag{2.1a}$$

$$\mathbf{B} = \mu_0 \mathbf{H} + \mathbf{M}, \tag{2.1b}$$

where **P** and **M** are the polarization and the magnetization density of the medium, defined as the average spatial density of total electric and magnetic dipole moment induced by **E** and **H**, respectively. The fields **P** and **M** in turn depend on **E** and **H** via expressions that are known as *constitutive relations*. In the following discussion, only non-magnetic media are considered, for which $\mathbf{M} = 0$ and **P** is a function of the electric field only.

For applied electric fields that are small compared to the inter-atomic fields in the medium, the function $\mathbf{P}(\mathbf{E})$ can be expanded in Taylor series around $\mathbf{E} = 0$, thus obtaining, in the general case of an anisotropic medium:

$$P_i = \epsilon_0(\chi_{ij}E_j + \chi^{(2)}_{ijk}E_jE_k + \chi^{(3)}_{ijkl}E_jE_kE_l + ...), \tag{2.2}$$

where the subscripts indicate the vectorial components of the fields and summation over repeated indices is assumed. The tensor $\chi^{(n)}$ is called *n-th order non-linear susceptibility* and, in general, depends on spatial and temporal coordinates. In most cases, however, this dependence can be neglected. Let us consider for simplicity the case of an isotropic medium, where **P** and **E** are parallel. Equation 2.2 becomes:

$$\mathbf{P} = \epsilon_0(\chi\mathbf{E} + \chi^{(2)}\mathbf{E}^2 + \chi^{(3)}\mathbf{E}^3 + ...). \tag{2.3}$$

The terms in the series decrease in magnitude as the corresponding non-linear order

increases, meaning that in most situations the sum can be truncated after the first few addends. As this chapter aims to examine second-order non-linear effects, the sum is truncated after the $\chi^{(2)}$-term. This kind of non-linearity vanishes in centrosymmetric media, where $\chi^{(2)} = 0$. By separating the linear and non-linear contributions to $\mathbf{P}$, Equation 2.3 may be re-written as:

$$\mathbf{P} = \epsilon_0 \chi \mathbf{E} + \epsilon_0 \chi^{(2)} \mathbf{E}^2 = \mathbf{P}_L(\mathbf{E}) + \mathbf{P}_{NL}(\mathbf{E}), \tag{2.4}$$

from which the equation governing the propagation of the field in the medium can be derived [161]:

$$\nabla^2 \mathbf{E} - \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2} = \mu_0 \frac{\partial^2 \mathbf{P}_{NL}(\mathbf{E})}{\partial t^2}, \tag{2.5}$$

where $c = \frac{c_0}{n}$, with $c_0 = (\sqrt{\epsilon_0 \mu_0})^{-1}$ speed of light in vacuum and $n = \sqrt{1 + \chi}$ refractive index of the medium. Equation 2.5 can be interpreted as a wave equation with a field-dependent source, which is determined by the non-linear polarization. This differential equation is at the core of non-linear optics.

In order to provide an intuitive picture of second-order non-linear processes, Equation 2.5 can be analysed in the framework of scattering theory. In this framework, an external field $\mathbf{E}_0$ is incident on a finite non-linear medium, such as a non-linear crystal. The non-linear polarization induced by $\mathbf{E}_0$, $\mathbf{P}_{NL}(\mathbf{E}_0)$, behaves as a radiating source for a secondary field, which, together with $\mathbf{E}_0$, determines the field $\mathbf{E}_1$. The field $\mathbf{E}_1$ in turn produces a non-linear polarization $\mathbf{P}_{NL}(\mathbf{E}_1)$, which is used to calculate the field $\mathbf{E}_2$ and so on, iteratively. If the external field is weak enough, the procedure can be stopped at the first iteration (first Born approximation [162]). By analysing $\mathbf{P}_{NL}(\mathbf{E}_0)$ then, all processes that take place in the crystal can be deduced. From this point on, the dependence of $\mathbf{P}_{NL}$ on $\mathbf{E}_0$ will be omitted for simplicity. Furthermore, the input field will be assumed to have only one one vectorial component so that the analysis can be done in terms of scalar quantities.

Let us consider a monochromatic wave incident on the crystal so that $E_0 = \mathrm{Re}(Ae^{-i\omega_0 t})$,

where A is a complex quantity. Then:

$$P_{NL} = \frac{\epsilon_0 \chi^{(2)}}{2}|A|^2 + \frac{\epsilon_0 \chi^{(2)}}{2}\mathrm{Re}(A^2 e^{-2i\omega_0 t}) = P_{NL}(0) + P_{NL}(2\omega_0). \tag{2.6}$$

The non-linear polarization is composed of two terms: a DC term, called *optical rectification* term, and a term at frequency $2\omega_0$, which radiates a wave at double the input frequency. This process is called *second harmonic generation* (SHG). Equation 2.6 shows that the term $P_{NL}(2\omega_0)$, and consequently the generated second harmonic field, is proportional to the square of the amplitude of the input field. This means that the second harmonic intensity, $I(2\omega_0)$ is proportional to the square of the input field intensity. It can be also shown that $I(2\omega_0)$ is proportional to the square of the length of the crystal [163]. Second harmonic generation is a well-known process at the core of many non-linear optical devices.

In the case of an external field comprising two monochromatic waves at frequencies ω_1 and ω_2, meaning that $E_0 = Re(A_1 e^{-i\omega_1 t)} + A_2 e^{-i\omega_2 t)})$, the non-linear polarization is a sum of the following terms:

$$P_{NL}(0) = \frac{\epsilon_0 \chi^{(2)}}{2}(|A_1|^2 + |A_2|^2), \tag{2.7a}$$

$$P_{NL}(2\omega_1) = \frac{\epsilon_0 \chi^{(2)}}{2} Re(A_1^2 e^{-2i\omega_1 t}), \tag{2.7b}$$

$$P_{NL}(2\omega_2) = \frac{\epsilon_0 \chi^{(2)}}{2} Re(A_2^2 e^{-2i\omega_2 t}), \tag{2.7c}$$

$$P_{NL}(\omega_+) = \epsilon_0 \chi^{(2)} Re(A_1 A_2 e^{-i(\omega_1+\omega_2)t}), \tag{2.7d}$$

$$P_{NL}(\omega_-) = \epsilon_0 \chi^{(2)} Re(A_1 A_2^* e^{-i(\omega_1-\omega_2)t}). \tag{2.7e}$$

The first term is again a DC optical rectification term, which is followed by two second harmonic terms at double the incident frequencies. But this time two new terms appear: $P_{NL}(\omega_+)$, which oscillates at the sum frequency $\omega_1 + \omega_2$, and $P_{NL}(\omega_-)$, at the difference frequency $\omega_1 - \omega_2$. . The corresponding processes are called *frequency up-conversion* or *sum frequency generation* (SFG) and *frequency down-conversion* or *difference frequency*

generation (DFG), respectively. The non-linear interaction between optical waves therefore induces a frequency mixing. By going beyond the first Born approximation, it is clear that the generated SFG and DFG waves can interact with either of the two input fields to produce radiation at the frequency of the other one. The second-order non-linearity of the crystal therefore allows for mutual interaction among three waves at different frequencies: this process is called *three-wave mixing*.

Let us then consider the interaction of three monochromatic plane waves with wave vectors $\mathbf{k}_1$, $\mathbf{k}_2$ and $\mathbf{k}_3$, respectively. In order for the three-wave mixing process to be efficient, additional spatial and temporal phase-matching conditions must be satisfied, so as to avoid destructive interference effects. By assuming $\omega_3 > \omega_{1,2}$, the phase-matching conditions are:

$$\omega_3 = \omega_1 + \omega_2, \tag{2.8a}$$

$$\mathbf{k}_3 = \mathbf{k}_1 + \mathbf{k}_2. \tag{2.8b}$$

When waves 1 and 2 are used as inputs, wave 3 is generated through frequency up-conversion. If wave 3 is one of the two inputs, a frequency down-conversion takes place. Normally, only one process among those described by equations 2.7 is permitted by the phase-matching conditions 2.8.

SHG can be regarded as a special case of frequency up-conversion where $\omega_1 = \omega_2$. Excluding SHG, equations of classical electromagnetism do not permit three-wave mixing processes with a single input wave. However, quantum theory predicts the possibility of a frequency down-conversion process for which only wave 3 is impinging onto the crystal. This phenomenon is at the heart of the single-photon sources commonly used in quantum optics experiments and will be described in Section 2.2.

2.1.1 Phase-matching techniques

In order to discuss how phase matching can be achieved in three-wave mixing processes, let us consider for simplicity the case where all the waves are collinear. Equations 2.8

then become:

$$\omega_3 = \omega_1 + \omega_2, \tag{2.9a}$$

$$n_3\omega_3 = n_1\omega_1 + n_2\omega_2 \tag{2.9b}$$

where n_i is the medium refractive index for wave i. In general, n_1, n_2 and n_3 are different because of dispersion, therefore the two phase-matching equations are independent.

Uusally, second-order non-linear crystals, such as beta barium borate (BBO), lithium triborate (LBO), lithium niobate (LN) or potassium titanyl phosphate (KTP), are birefringent. This means that the refractive indices n_1, n_2, n_3 are generally dependent on the polarization of the corresponding waves and the angles between their propagation directions and the crystal optical axes. These additional degrees of freedom can be tuned so as to simultaneously satisfy equations 2.9.

Birefringent crystals are grouped in uniaxial and biaxial. In uniaxial crystals, the refractive index n_e for light polarized along one of the crystal axes, often indicated as the *optical axis*, is different from the refractive index n_o along the other two axes. The two indices n_e and n_o are called *extraordinary* and *ordinary* index, respectively. One of the most used uniaxial crystals is BBO, which is a negative crystal, where "negative" means that $n_e < n_o$, with normal dispersion, i.e. $n_{e,o}(\omega_i) > n_{e,o}(\omega_j)$ if $\omega_i > \omega_j$. Biaxial crystals, such as KTP, instead, have a different refractive index for each crystal axis. In general, a light beam propagating in a birefringent crystal at an arbitrary direction, $\mathbf{k}$, presents two polarization modes with refractive indices depending on $\mathbf{k}$. In the case of a uniaxial crystal, the propagation direction is identified by the angle θ between $\mathbf{k}$ and the optical axis. In this situation, one polarization mode is perpendicular to the optical axis and experiences the ordinary index n_o, while the other polarization mode has a non-zero component along the optical axis and an (extraordinary) refractive index that depends on θ, $n_e(\theta)$. The index $n_e\theta$ reduces to n_e for $\theta = 90°$.

Let us consider the case of three-wave mixing in a BBO crystal, with the three waves propagating at an angle θ with respect to the optical axis. Two phase-matching

configurations are possible: 1) *type-I phase matching*, where wave 1 and wave 2 have the same polarization, in this case ordinary. It follows that wave 3 is extraordinarily polarized. 2) *Type-II phase matching*, for which wave 1 and wave 2 are orthogonally polarized. Wave 3 must then be ordinarily polarized. The phase-matching Equation 2.9b in the two cases reads:

$$\textbf{Type I} \rightarrow n_e(\omega_3, \theta)\omega_3 = n_o(\omega_1)\omega_1 + n_o(\omega_2)\omega_2, \tag{2.10a}$$

$$\textbf{Type II} \rightarrow n_e(\omega_3, \theta)\omega_3 = n_e(\omega_1, \theta)\omega_1 + n_o(\omega_2)\omega_2. \tag{2.10b}$$

By tuning θ it is possible to achieve phase matching for a large range of frequencies. For different crystals, the allowed combinations of polarizations may be different. For example, in the case of type-I phase matching in a positive uniaxial crystal with normal dispersion, wave 3 must be ordinarily polarized. The described phase-matching technique is also called *critical phase matching*, due to its sensitivity to the alignment of the involved light beams. A major problem of this technique is that when $\theta \neq 90°$, the intensity distribution of any extraordinary beam propagating in the birefringent crystal drifts away from the direction of the wave vector. This phenomenon, called *spatial walk-off* [164], limits the effective length along which the different waves interact, thus reducing the efficiency of the process. Furthermore, the three interacting waves must have different polarizations, meaning that only non-diagonal components of the second-order non-linear susceptibility tensor $\chi^{(2)}_{ijk}$ play a role in the process. These components are usually smaller than the diagonal ones.

A technique that overcomes these issues is *quasi-phase matching* (QPM). The basic idea of QPM is compensating the phase mismatch between the interacting waves via a periodic spatial modulation of the non-linear susceptibility. In fact, the mismatch $\Delta\mathbf{k} = \mathbf{k}_3 - \mathbf{k}_2 - \mathbf{k}_1$ is fully compensated if $\chi^{(2)} = C\sin(\Delta\mathbf{k} \cdot \mathbf{r})$, where C is a constant

[163]. The phase-matching conditions then become:

$$\omega_3 = \omega_1 + \omega_2, \tag{2.11a}$$

$$\mathbf{k}_3 = \mathbf{k}_1 + \mathbf{k}_2 + \mathbf{G}, \tag{2.11b}$$

where $\mathbf{G}$ is the wave vector associated to the modulation of the non-linear susceptibility. Practically, it is hard to produce a continuous harmonic variation of the properties of a medium, whereas simpler periodic structures are more feasible. In general, any periodic function can be expanded in Fourier series, that is as a sum of harmonic terms of the form $C_m \sin(\mathbf{G}_m \cdot \mathbf{r})$, with $m = (m_1, m_2, m_3)$ and m_i integer for $i = 1, 2, 3$. Then, quasi-phase matching is achieved if $\Delta\mathbf{k} = \mathbf{G}_m$ for a given value of m of the Fourier series. The other harmonic components do not contribute to the non-linear conversion, as they do not determine any compensation of the phase mismatch. A non-harmonic periodic structure, however, results into a reduced effective non-linear susceptibility, thus leading to a decrease in the efficiency of the non-linear process. Nevertheless, the absence of spatial walk-off and the possibility to exploit larger components of the tensor $\chi^{(2)}_{ijk}$ make this technique preferable to critical phase matching in many situations.

Let us focus on collinear QPM. The simplest periodic structure in this case corresponds to a medium whose non-linear susceptibility is periodically reversed in sign along one coordinate axis, say z. If the modulation period is Λ, the non-linear susceptibility can be expanded in Fourier series as $\sum_{l=-\infty}^{+\infty} G_l \sin(G_l z)$, with $G_l = l\frac{2\pi}{\Lambda}$ and l integer number. For QPM, it must be $\Delta k = l\frac{2\pi}{\Lambda}$ for some l. The choice $l = 1$ leads to the highest effective non-linear susceptibility and, in fact, is the most common one [163]. Equations 2.9 become:

$$\omega_3 = \omega_1 + \omega_2 \tag{2.12a}$$

$$n_3\omega_3 = n_1\omega_1 + n_2\omega_2 + \frac{2\pi c_0}{\Lambda}. \tag{2.12b}$$

Here nothing is assumed about the polarization and the direction of incidence of the

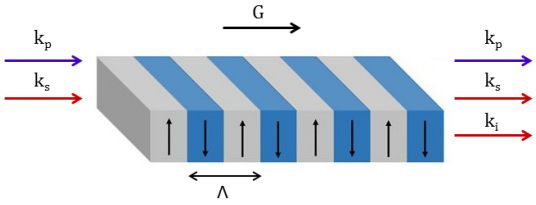


Figure 2.1: **QPM with a periodically-poled crystal.** QPM can be realized by periodically reversing the polarization vector in a ferroelectric non-linear crystal, thus obtaining a periodic inversion of the non-linear susceptibility $\chi^{(2)}$. In the figure, collinear parametric down-conversion is shown, for which $k_p = k_s + k_i + G$, where $G = \frac{2\pi}{\Lambda}$ is the compensation term provided by the periodic structure.

three waves, since QPM may be achieved for almost any combination of these variables by suitably choosing the period Λ. Typically, in quasi-phase-matched processes the three waves are polarized along the optical axes of the crystal. In addition to type-I and type-II processes, a *type-0* process is also possible, for which all the waves have the same polarization and the non-linear susceptibility is larger. This shows the higher versatility of QPM with respect to critical phase matching.

The main technique for the fabrication of the described periodic structure is called *periodic poling* (PP) and is applied to ferroelectric media, such as KTP and LN [165]. It consists in periodically reversing the direction of the permanent spontaneously-formed electric polarization of the medium by exposing it to an electric field. Typical poling periods are of the order of μm. An example of poled crystal in a collinear QPM configuration is shown in Figure 2.1.

2.2 Spontaneous parametric down-conversion

Spontaneous parametric down-conversion (SPDC) is the second-order non-linear process for which an input photon, the *pump* photon, at frequency ω_p, is converted into two photons at lower frequencies ω_s and ω_i, traditionally called *signal* and *idler* photon, respectively. SPDC can be interpreted as an ordinary down-conversion process where the signal and idler fields are seeded by the quantum fluctuations of vacuum, rather than by classical macroscopic fields. As such, it requires a quantum-mechanical treatment.

In this section, the expression of the quantum state produced by SPDC will be derived and its properties described. For simplicity, the analysis will be restricted to a collinear SPDC process in which the three interacting fields are linearly polarized plane waves. The three wave vectors are assumed to be parallel to the z-axis; consequently the three directions of polarization are along either the x- or y-axis. The non-linear medium is a crystal of length L.

In the interaction picture, the state of the signal and idler fields at time t, $|\psi(t)\rangle$ is given by:

$$|\psi(t)\rangle = \hat{T} e^{\frac{1}{i\hbar}\int_0^t \hat{H}_I(t')dt'} |\psi(0)\rangle, \tag{2.13}$$

where $\hat{H}_I$ is the interaction hamiltonian and $\hat{T}$ is the time-ordering operator [13]. At time $t = 0$, no generation has occurred yet, therefore $|\psi(0)\rangle = |0\rangle$, where $|0\rangle$ is the vacuum state. If the interaction strength is small, the exponential function can be expanded in Taylor series, of which only the first two terms are considered, thus obtaining:

$$|\psi(t)\rangle \approx \left(1 + \frac{1}{i\hbar}\int_0^t dt' \hat{H}_I(t') - \frac{1}{2\hbar^2}\int_0^t dt' \int_0^t dt'' \hat{H}_I(t')\hat{H}_I(t'')\right)|0\rangle. \tag{2.14}$$

The addends in the previous expression are the first three terms of the Dyson series associated to the quantum evolution operator [13]. The interaction energy in a generic three-wave mixing process is given by [166]:

$$U_I = \frac{1}{2}\int_V dV \mathbf{P}_{NL} \cdot \mathbf{E} = \frac{1}{2}\epsilon_0 \int_V dV \sum_{j,k=1}^{3} \chi^{(2)}_{ijk} E_i E_j E_k, \tag{2.15}$$

where V is the interaction volume. For the process under consideration, the sum in 2.15 reduces to only one term comprising the three scalar components of the interacting fields:

$$U_I = \frac{1}{2}\epsilon_0 d_{eff} \int_V dV E_p E_s E_i, \tag{2.16}$$

in which the subscripts p, s and i indicate pump, signal and idler, respectively, and the quantity d_{eff} encloses the elements of the $\chi^{(2)}$ tensor. From expression 2.16, the form of

the operator $\hat{H}_I$ can be deduced:

$$\hat{H}_I = \frac{1}{2}\epsilon_0 d_{eff} \int_V dV \hat{E}_p^{(+)} \hat{E}_s^{(-)} \hat{E}_i^{(-)} + h.c, \tag{2.17}$$

where, according to equations 1.15, $\hat{E}_\mu^{(+)}$ and $\hat{E}_\mu^{(-)}$ are given by:

$$\hat{E}_\mu^{(+)} = i \int_0^\infty d\omega_\mu A_\mu(\mu) \hat{a}_\mu(\omega_\mu) e^{i(k_\mu(\omega_\mu)z - \omega_\mu t)}, \tag{2.18a}$$

$$\hat{E}_\mu^{(-)} = -i \int_0^\infty d\omega_\mu A_\mu(\mu) \hat{a}_\mu^\dagger(\omega_\mu) e^{-i(k_\mu(\omega_\mu)z - \omega_\mu t)}, \tag{2.18b}$$

with $A_\mu(\omega_\mu) = \sqrt{\frac{\hbar\omega_\mu}{4\pi c\epsilon_0 n(\omega_\mu) A_Q}}$ and $\mu = p, s, i$. Assuming that the pump field comes from a laser above threshold, its quantum properties can be neglected and the corresponding operator be replaced by a classical field:

$$\hat{E}_p^{(+)} \to E_p = A_p \int_0^\infty d\omega_p \alpha(\omega_p) e^{i(k_p(\omega_p)z - \omega_p t)}. \tag{2.19}$$

Normally, the time interval between two consecutive photon emissions for an SPDC-based single-photon source is far longer than the time interval in which the three fields interact.It is then legitimate to assume that the final state is measured long after the interaction is over. Furthermore, there is no reason why the system should keep a memory of the initial time, which then can be taken to be $-\infty$. These two considerations allow one to extend the time integration limits in Equation 2.14 to infinity. In formulas:

$$\int_0^t dt' \hat{H}_I(t')|0\rangle \to \int_{-\infty}^\infty dt' \hat{H}_I(t')|0\rangle. \tag{2.20}$$

After performing the volume and time integrals, it is obtained [166]:

$$\int_{-\infty}^\infty dt' \hat{H}_I(t')|0\rangle = \tag{2.21}$$
$$= -2V\epsilon_0 d_{eff} A_p \int_0^\infty d\omega_s \int_0^\infty d\omega_i A_s(\omega_s) A_i(\omega_i) \alpha(\omega_s + \omega_i) \phi(\omega_s, \omega_i) \hat{a}_s^\dagger(\omega_s) \hat{a}_i^\dagger(\omega_i)|0\rangle,$$

where

$$\phi(\omega_s, \omega_i) = e^{i\frac{\Delta k(\omega_s,\omega_i)l}{2}} \text{sinc}(\frac{\Delta k(\omega_s, \omega_i)L}{2}) \tag{2.22}$$

and $\Delta k(\omega_s, \omega_i) = k_p(\omega_s + \omega_i) - k_s(\omega_s) - k_i(\omega_i)$.

By defining the function $\Phi(\omega_s, \omega_i)$ as:

$$\Phi(\omega_s, \omega_i) = \frac{A_s(\omega_s)A_i(\omega_i)\alpha(\omega_s + \omega_i)\phi(\omega_s, \omega_i)}{\sqrt{N}}, \tag{2.23}$$

in which

$$N = \int_0^\infty d\omega_s \int_0^\infty d\omega_i |A_s(\omega_s)A_i(\omega_i)\alpha(\omega_s + \omega_i)\phi(\omega_s, \omega_i)|^2, \tag{2.24}$$

and by exploiting equations 2.21, 2.22 and 2.23, the state in 2.14 can be re-written as:

$$|\psi\rangle \approx (1 - \frac{|\eta|^2}{2})|0\rangle + \eta|\Phi_1\rangle + \eta^2|\Phi_2\rangle, \tag{2.25}$$

where:

$$|\Phi_1\rangle = \int_0^\infty d\omega_s \int_0^\infty d\omega_i \Phi(\omega_s, \omega_i)\hat{a}_s^\dagger(\omega_s)\hat{a}_i^\dagger(\omega_i)|0\rangle, \tag{2.26}$$

$$|\Phi_2\rangle = \frac{1}{2}\int_0^\infty d\omega_s \int_0^\infty d\omega_i \int_0^\infty d\omega_s' \int_0^\infty d\omega_i' \Phi(\omega_s, \omega_i)\Phi(\omega_s', \omega_i')\hat{a}_s^\dagger(\omega_s)\hat{a}_i^\dagger(\omega_i)\hat{a}_s^\dagger(\omega_s')\hat{a}_i^\dagger(\omega_i')|0\rangle, \tag{2.27}$$

and

$$\eta = \frac{2i\sqrt{N}V\epsilon_0 d_{eff}A_p}{\hbar}. \tag{2.28}$$

This state comprises three terms, related to vacuum, two-photon and four-photon emission, respectively. Note that the expansion of the evolution operator is truncated. The full series, in fact, would also include a six-photon term, an eight-photon term and so on.

The quantity $|\eta|^2$ represents the probability P_1 that a pump photon is down-converted to a signal-idler pair. Analogously, $|\eta|^4$ is the probability P_2 that two pairs are created simultaneously from two pump photons. P_1 and P_2 are proportional to the first and second power of the pump intensity, respectively, meaning that the ratio P_2/P_1 is linear

in the pump power. This is true for all ratios P_n/P_{n-1}.

If signal and idler photons are spatially separated and one of the two fields, say idler, is detected, two cases are possible, according to whether the detector can resolve different photon numbers or not. If the detector is number-resolving and a given photon number n is found for the idler, the signal is consequently projected onto the Fock state associated to n. This occurs with probability P_n. By only keeping the cases in which the detection result is $n = 1$, therefore, a perfect single-photon state is obtained in the signal mode. In most experimental situations, however, detectors are not number-resolving, therefore they can only distinguish between vacuum and a Fock state with $n \neq 0$, without determining the value of n. In this case, a detection at the idler projects the signal onto a mixed state of Fock states with different photon numbers. At low pump power, for which $P_2 << P_1$, this mixture can be approximated to a single-photon state. A successful photon detection in the idler mode, therefore, *heralds* a single photon in the signal mode. This heralding process effectively makes the non-linear crystal a single-photon emitter. Without heralding, both signal and idler fields would be in a quantum superposition of different photon numbers, with thermal statistics.

The spectral properties of the emitted photons are determined by the function $\Phi(\omega_s, \omega_i)$, known as *joint spectral amplitude*. The quantity $|\Phi(\omega_s, \omega_i)|^2$ is called *joint spectral intensity* and provides the probability that, given the creation of a photon pair, the signal is emitted at frequency ω_s and the idler at frequency ω_i. $\Phi(\omega_s, \omega_i)$ comprises four terms that are analysed below. $A_s(\omega_s)$ and $A_i(\omega_i)$ derive from the quantization of the electric field and are generally slowly-varying functions of the frequency. The function $\alpha(\omega_s + \omega_i)$ is the pump envelope from Equation 2.19, where ω_p was replaced by $\omega_s + \omega_i$, due to phase-matching condition 2.8a, which ensures conservation of energy. The last term, $\phi(\omega_s, \omega_i)$, is called *phase-matching function* and is determined by the properties of the non-linear crystal. As $\phi(\omega_s, \omega_i)$ contains a sinc function, its modulus has a peak for $\Delta k(\omega_s, \omega_i) = 0$, meaning that photons satisfying this condition have the highest probability to be generated. This corresponds to phase-matching Equation 2.8b, related to momentum conservation. The sinc function has a finite width in Δk (see

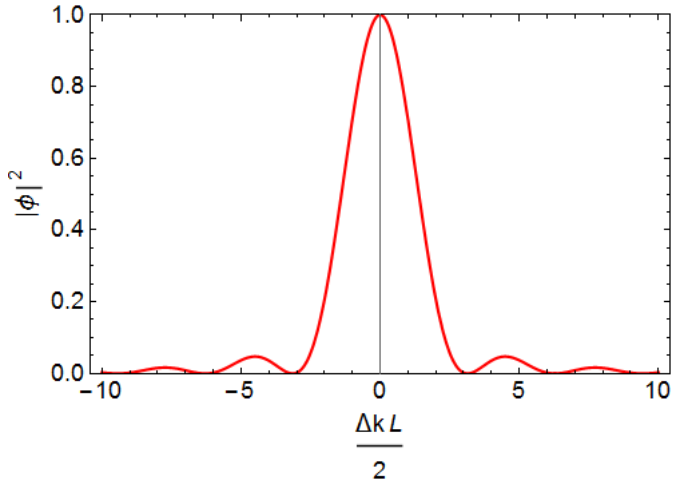


Figure 2.2: **Phase-matching profile.** The quantity $|\phi(\omega_s, \omega_i)|^2$ is plotted with respect to the quantity $\frac{\Delta k(\omega_s,\omega_i)L}{2}$. The resulting profile is a $sinc^2$-function centred at 0. The function reaches half of the peak value for $|\Delta k(\omega_s, \omega_i)|L = 2.78$.

Figure 2.2), which allows for some phase mismatch among the three fields. This reflects the quantum uncertainty in Δk due to the spatial confinement of the fields in the crystal.

If the pump field is approximated as a monochromatic wave at frequency $2\omega_0$, then $\alpha(\omega_s + \omega_i) = \delta(2\omega_0)$. This results in perfect correlation between the frequencies of signal and idler photons. If a signal photon is emitted at frequency ω_s, the corresponding idler frequency is $2\omega_0 - \omega_s$. In general, the degree of frequency correlation depends on the product $\alpha(\omega_s + \omega_i)\phi(\omega_s, \omega_i)$. Frequency correlations result into entanglement in the frequency degree of freedom. By engineering pump envelope and phase-matching function, it is possible to remove these correlations and to obtain a separable joint spectral amplitude, meaning $\Phi(\omega_s, \omega_i) = \xi_1(\omega_s)\xi_2(\omega_i)$ [167].

The bandwidth of the emitted photons depends on the pump bandwidth as well as the properties of the phase-matching function, and can be calculated from the marginal frequency distributions of signal and idler, defined as $f_{s(i)} = \int_0^\infty d\omega_{i(s)} |\Phi(\omega_s, \omega_i)|^2$.
In the approximation of a monochromatic pump, a more insightful expression can be obtained. Let us assume perfect phase matching for signal and idler frequencies ω_{s_0} and ω_{i_0} so that $\omega_p = \omega_{s_0} + \omega_{i_0}$ and $\Delta k(\omega_{s_0}, \omega_{i_0}) = 0$. Δk may then be expanded in series

around zero, till the first order:

$$\Delta k(\omega_s, \omega_i) \approx \frac{\partial \Delta k(\omega_s, \omega_i)}{\partial \omega_s}|_{\omega_{s_0}, \omega_{i_0}}(\omega_s - \omega_{s_0}) + \frac{\partial \Delta k(\omega_s, \omega_i)}{\partial \omega_i}|_{\omega_{s_0}, \omega_{i_0}}(\omega_i - \omega_{i_0}). \quad (2.29)$$

Because of conservation of energy $\omega_s - \omega_{s_0} = -(\omega_i - \omega_{i_0}) = \Delta\omega$. Therefore:

$$\Delta k(\omega_s, \omega_i) \approx \frac{1}{c_0}(n_{g_i}(\omega_{s_0}, \omega_{i_0}) - n_{g_s}(\omega_{s_0}, \omega_{i_0}))\Delta\omega, \quad (2.30)$$

where n_{g_i} and n_{g_s} are the signal and idler group indices, respectively. Since the power spectrum of the photons is proportional to the function $\text{sinc}^2(\frac{\Delta kL}{2})$, the corresponding frequency bandwidth (full width half maximum) is obtained from the condition $|\Delta k| = \frac{5.56}{L}$:

$$\Delta\omega_{FWHM} = 5.56\frac{c_0}{L|n_{g_s}(\omega_{s_0}, \omega_{i_0}) - n_{g_i}(\omega_{s_0}, \omega_{i_0})|}. \quad (2.31)$$

Degeneracy in signal and idler therefore provides large photon bandwidths, in the monochromatic pump approximation. This approximation can be applied to a pump laser with a spectral bandwidth that is far narrower than the width of the phase-matching function.

2.3 Cavity-enhanced SPDC

As seen in Equation 2.31, the photon bandwidth for a monochromatic pump depends on the length of the crystal and on the difference between the group indices for signal and idler. The tunability of these parameters, however, is quite limited: in particular the crystal length cannot be increased too much due to fabrication and practicality constraints. The result is that the typical spectral bandwidth obtained in SPDC experiments ranges from about 100 GHz to some THz [168]. The bandwidth can be reduced by orders of magnitude via cavity-enhanced SPDC (CE-SPDC), in which the non-linear process takes place inside an optical resonator. In this section this process will be analysed in more detail. Before doing that some basic concepts of optical resonators will be recalled.

2.3.1 Optical resonators

An optical resonator, or cavity, is a device that makes light propagate along a closed path. For instance light can be guided in a closed loop or forced to bounce between two or more (partially) reflective surfaces. Such a device can be used in many ways, for instance as a filter, a frequency reference, an enhancement device for non-linear processes, among others, and constitutes a fundamental element of lasers [169]. When an electromagnetic field is confined in a region of space, Maxwell's equations allow for discrete solutions for the electromagnetic field, which are called *cavity (or resonator) modes*. They correspond to waves that reproduce themselves after a round trip in the cavity.

Let us consider the case of a resonator composed of two mirrors with perfect reflectivity, separated by a distance d. A fundamental requirement for a wave to be a cavity mode is that the phase shift corresponding to a single round trip is an integer multiple of 2π. This condition on the phase shift determines the frequencies that are allowed to propagate in the resonator: $\nu_q = q\frac{c}{2d}$, where c is the speed of light in the medium between the mirrors and q is an integer. The frequency modes of the cavity are called *longitudinal modes*. The separation between ν_q and ν_{q+1} defines the *free spectral range* (FSR) , which is equal to $\frac{c}{2d}$. The resonance frequencies ν_q correspond to monochromatic solutions of the wave equation in the cavity with the boundary condition that the field is 0 at the mirrors. This frequency selection can be explained in terms of interference. In fact, if the round-trip phase shift for a given monochromatic wave in the cavity is not a multiple of 2π, the field at any point of the resonator is given by a sum of infinite terms with different phase, corresponding to different numbers of round trips. As these terms have equal magnitude, the field is suppressed due to fully destructive interference.

If the mirrors are not perfect the condition on the phase shift relaxes, because the sum providing the field in the resonator is this time composed of an infinite number of terms with geometrically decreasing magnitude, as part of the energy is lost at each bounce at the mirrors. In this case, the longitudinal modes of the cavity are not strictly monochromatic but present a finite bandwidth $\Delta\nu$. The ratio between the FSR and the bandwidth of the modes is determined by a parameter of the resonator, $\mathcal{F}$, which is

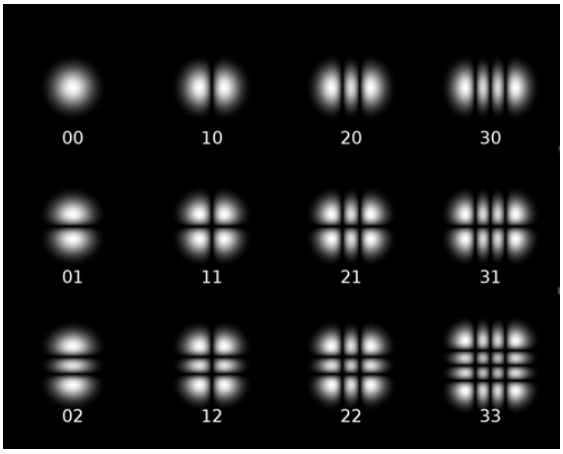


Figure 2.3: **Intensity distribution of Hermite-Gauss modes.** Each mode is characterized by two integer numbers l and m, which determine the spatial properties of the related intensity distribution. For instance the numbers of nodes in the horizontal and vertical direction are l and m, respectively. The fundamental mode, also called TEM_{00} is obtained for $l = m = 0$.

called *finesse*. The finesse is connected to loss in the cavity by the following expression:

$$\mathcal{F} = \frac{\pi \sqrt[4]{\rho}}{1 - \sqrt{\rho}}, \tag{2.32}$$

in which ρ is the round-trip power transmission of the resonator. With this definition of the finesse, it results: $\mathcal{F} \approx \frac{FSR}{\Delta\nu}$, where the approximation is valid in the low-loss regime. Roughly speaking, the finesse can be interpreted as the average number of times a photon travels a round trip of the resonator before leaving the cavity or being lost.

Besides the longitudinal modes, a resonator has also *transverse modes*. They are related to the spatial distribution of the field in a plane perpendicular to the cavity axis and depend on the cavity geometric properties. For a cavity with two spherical mirrors, the transverse modes are described by Hermite-Gauss functions, which are characterized by two integer numbers l and m (see Figure 2.3). These modes are indicated by TEM_{lm}, which is an acronym for "transverse electro-magnetic". The fundamental mode TEM_{00} is the ordinary Gaussian beam. A mode of the cavity then is fully described by three numbers: q, l and m, where q determines the longitudinal mode, and l, m determine its transverse spatial distribution. Because of the phase properties of Gaussian modes, the

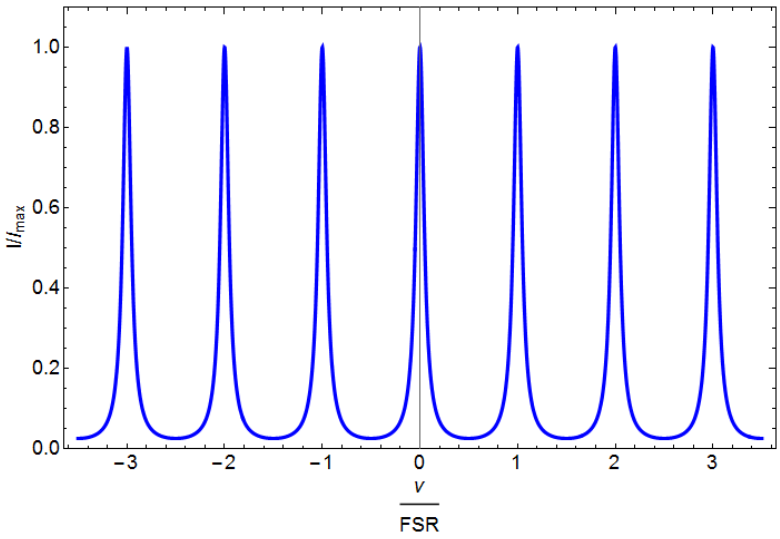


Figure 2.4: **Frequency dependence of intra-cavity intensity.** The cavity spectrum is composed of a set of peaks separated by a FSR. The shape of the peaks is Lorentzian, wit a bandwidth approximately given, in the low-loss regime, by $\frac{FSR}{\mathcal{F}}$.

frequency of a mode also depends on l, m. In particular, the resonance frequencies are given by:

$$\nu_{q,l,m} = q\text{FSR} + (l + m + 1)\frac{\Delta\zeta\,\text{FSR}}{\pi}, \tag{2.33}$$

where $\Delta\zeta$ is the difference in Gouy phase between the mirrors [163].

The frequency dependence of the field intensity inside the resonator for the fundamental mode in the low-loss regime is given by the function:

$$I_r(\nu) = \frac{I_{max}}{1 + (\frac{2\mathcal{F}}{\pi}\sin(\frac{\pi\nu}{\text{FSR}}))^2}, \tag{2.34}$$

with $I_{max} = \frac{I_0}{(1-\sqrt{\rho})^2}$ and I_0 the intensity entering the cavity. The maximum intensity is reached when ν is a resonance frequency whereas the minimum is obtained at the midpoints between two consecutive frequency modes. The frequency spectrum of the light inside the resonator is therefore a sequence of peaks separated by the FSR, as shown in Figure 2.4. By multiplying $I_r(\nu)$ by the transmittance of the output mirror the transmitted intensity is obtained, which consequently also has a comb-like structure. In the case of no internal losses, and if the transmittivity of the input and output mirrors

are equal, all the resonant light incident on the resonator is transmitted. Because of conservation of energy, each transmission peak corresponds to a reflection minimum and vice versa. For this reason, a resonator can be used as a frequency filter.

2.3.2 Parametric down-conversion in a cavity

If a parametric down-conversion process takes place inside an optical resonator, the resulting device takes the name of optical parametric oscillator (OPO). In an OPO, at least one of the down-converted fields is reflected by the cavity mirrors and therefore travels many times in the non-linear medium. This causes an enhancement of the SPDC process due to the extension of the interaction length among the involved fields.

An OPO can work in different regimes of operation, according to how high the SPDC pump power is with respect to the *threshold* power, defined as the pump power for which the gain of the non-linear process equals the cavity round-trip loss for the generated fields. Three regimes of operation are possible: 1) *well above threshold*, where a stable classical oscillation can be sustained and the OPO basically produces coherent light, like a laser, with the advantage that the emission frequencies are highly tunable; 2) *below/around threshold*, used for the generation of non-classical macroscopic fields, such as bright squeezed vacuum [170]; 3) *far below threshold*, for CE-SPDC. In the latter regime, the cavity has the function of an *active filter* for the single photons. The SPDC emission, in fact, is constrained to occur in the cavity modes only, which can easily have a spectral bandwidth as narrow as $1 - 10$ MHz. The enhancement effect due to multiple reflections in the cavity results into far higher single-photon rates, when compared to the case of passive filtering at the same bandwidth [171, 172]. The following discussion will be limited to this regime of operation, as it is the only relevant one for the experimental work described in this thesis.

According to how many different fields are simultaneously resonant in the cavity, the OPO can be *singly, doubly or triply resonant*. Single-resonance condition is attained when only one of the generated fields, either signal or idler, is resonant to the cavity or when they are both resonant but indistinguishable, like in the case of degenerate and collinear

type-I SPDC. When signal and idler are distinguishable and both resonant to the cavity, the OPO is doubly resonant. Triple-resonance condition means that the generated fields and the pump are all simultaneously resonant. The more fields are resonant, the lower the OPO threshold is. Here and throughout the thesis, only double-resonance condition will be considered. For such a case, the threshold power is given by [173]

$$P_{th} = \frac{2c_0\epsilon_0 n_p n_s n_i \lambda_s \lambda_i A}{2\mathcal{F}_s \mathcal{F}_i (2\chi^{(2)} L)^2}, \tag{2.35}$$

where the subscripts p, s and i indicate pump, signal and idler, respectively, c_0 denotes the speed of light in vacuum, ϵ_0 the dielectric constant of vacuum, λ the wavelength, $\mathcal{F}$ the cavity finesse, and n, L, A and $\chi^{(2)}$ are the refractive index, the length, the illuminated area and the second-order susceptibility of the non-linear medium, respectively.

Let us consider the case of cavity-enhanced collinear type-II SPDC. The analysis of this process will be conducted by using the formalism of Section 2.2 and by assuming that emission occurs only in the fundamental Gaussian mode so that higher-order transverse modes can be neglected. The SPDC state can then be written in the form 2.25, with a modified joint spectral amplitude,$\Phi_R(\omega_s, \omega_i)$, which takes into account the presence of the cavity. In order to obtain this result, it is enough to replace the phase-matching function $\phi(\omega_s, \omega_i)$ in Equation 2.22 with $\phi_R(\omega_s, \omega_i)$, defined as [174]:

$$\phi_R(\omega_s, \omega_i) = f_s(\omega_s) f_i(\omega_i) \phi(\omega_s, \omega_i), \tag{2.36}$$

with f_s and f_i functions describing the cavity modes. In particular:

$$f_{s,i}(\omega_{s,i}) = \frac{\sqrt{(1 - R_{1s,i}(1 - R_{2s,i})(1 - L_{s,i})}}{1 - \sqrt{R_{1s,i} R_{2s,i}}(1 - L_{s,i}) e^{i\zeta(\omega_{s,i})}}, \tag{2.37}$$

where $R_{1s,i}$, $R_{2s,i}$ and $L_{s,i}$ are the input (1) and output (2) mirror reflectivity and the internal loss in the cavity (from mirror 1 to 2) for signal and idler, respectively. The quantity $\zeta(\omega_{s,i})$ is the round-trip phase shift, which depends on the signal/idler frequency. The joint spectral intensity is proportional to $|\phi_R(\omega_s, \omega_i)|^2 = |f_s(\omega_s)|^2 |f_i(\omega_i)|^2 |\phi(\omega_s, \omega_i)|^2$.

From Equation 2.37, it results:

$$|f_{s,i}(\omega_{s,i})|^2 = \frac{(1-R_{1s,i})(1-R_{2s,i})(1-L_{s,i})}{1+(\frac{2\mathcal{F}}{\pi}sin^2(\frac{\zeta(\omega_{s,i})}{2}))^2}, \tag{2.38}$$

which is of the same form as 2.34. It is then clear that the emission can only happen in the modes of the cavity that fall within the phase-matching function.

With respect to the non-resonant case, the spectral brightness of the process, defined as the number of generated photons per unit time, pump power and photon bandwidth is enhanced by a factor M, given by:

$$M = \frac{\int_0^\infty d\omega_s \int_0^\infty d\omega_i |\Phi(\omega_s,\omega_i)|^2}{\int_0^\infty d\omega_s \int_0^\infty d\omega_i |\Phi_R(\omega_s,\omega_i)|^2}. \tag{2.39}$$

It can be shown that M is proportional to $\mathcal{F}_s\mathcal{F}_i\eta_s\eta_i$ [174], where $\mathcal{F}_{s,i}$ is the finesse for signal/idler and $\eta_{s,i}$ is the escape probability. This quantity is defined as the probability that a generated photon leaves the cavity, which can be expressed as:

$$\eta_{s,i} = \frac{1-R_{2s,i}}{1-R_{1s,i}R_{2s,i}(1-L_{s,i})^2} = \frac{1-R_{2s,i}}{1-\rho_{s,i}}. \tag{2.40}$$

In case $R_{1s,i} = 1$ and $L_{s,i} = 0$, $\eta_{s,i} = 1$. The enhancement factor is then roughly proportional to the finesse squared, assuming comparable values of $\mathcal{F}$ for signal and idler. Increasing the finesse of the resonator therefore determines a quadratic increase in the spectral brightness. If, however, for a given level of loss in the crystal, the finesse is increased by choosing mirrors with higher reflectivity, the enhancement factor does not increase quadratically. In this case, in fact, the escape probability is reduced, as it can be seen from Equation 2.40. For each value of the internal loss, L, therefore, there is an optimal value of the finesse for which the spectral brightness is maximum.

In a doubly resonant OPO, the FSR for the signal field, FSR_s is different from that of the idler field, FSR_i. For this reason, corresponding longitudinal modes of signal and idler, i.e. modes that are paired by the phase-matching conditions, are simultaneously resonant only at certain frequencies. This concept is depicted in Figure 2.5, where the overlap

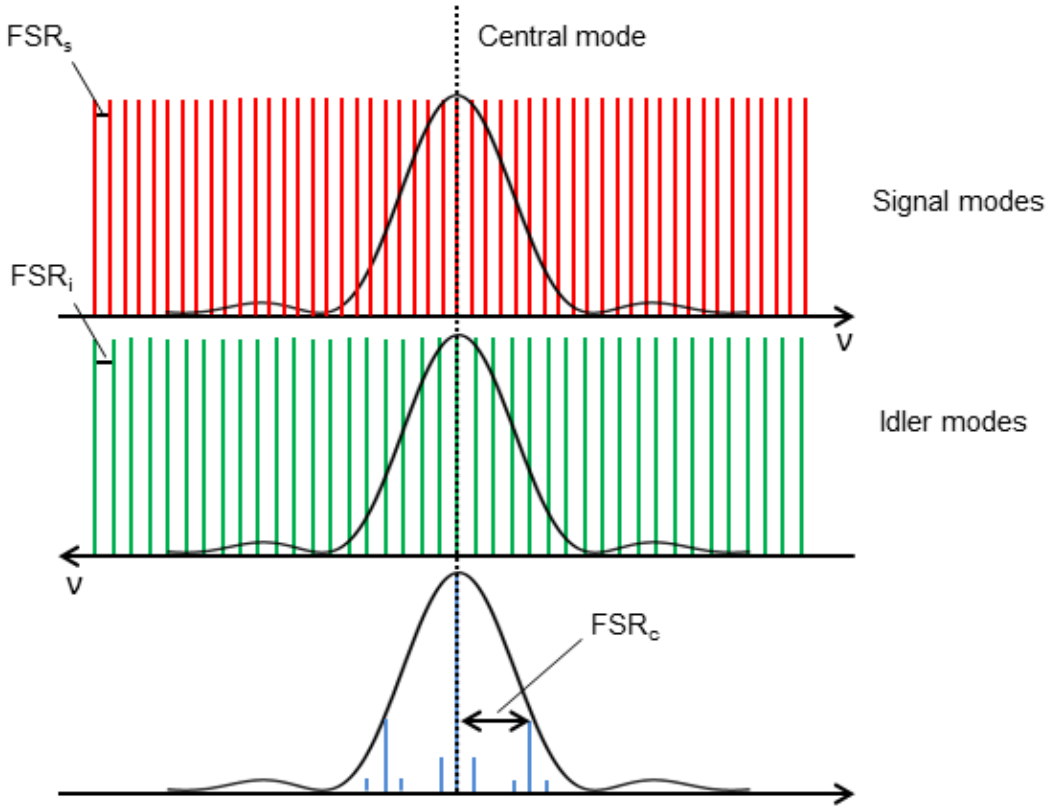


Figure 2.5: **Cluster effect in a double-resonant OPO.** The longitudinal modes for signal (idler) are shown in red (green) in the case of degenerate type-II phase matching. The two arrows indicate the direction in which frequency increases. For maximum SPDC gain, the simultaneous resonance of signal and idler should occur at the frequency for which the SPDC gain (black solid curve) is maximum, as depicted in the figure. The overlap condition is periodic, but because of the difference in free spectral range of signal and idler, the modes that are next to the fully overlapping ones coincide only partially. This leads to a spectrum that is made of clusters of modes, separated by FSR$_c$ (blue lines). In each cluster, a bright central mode is surrounded by weaker neighboring modes. The main mode of the central cluster corresponds to degenerate emission, while the other modes to non-degenerate emission. In this latter case, when the signal is emitted in one of the side modes the cluster is emitted in the conjugate one such that signal and idler frequencies always sum up to the pump frequency.

of signal and idler modes indicates their simultaneous resonance. If two modes fully overlap, their adjacent modes do it only partially. The full-overlap condition occurs again after a certain number of free spectral ranges, N_c, for which $N_c\,\mathrm{FSR}_- = (N_c - 1)\,\mathrm{FSR}_+$, where FSR_- and FSR_+ indicat, the smaller and the larger value between FSR_s and FSR_i, respectively. The output spectrum is thus composed of *clusters* of modes, separated by a cluster free spectral range, FSR_c, given by:

$$\mathrm{FSR}_c = N_c\mathrm{FSR}_- = \frac{\mathrm{FSR}_-\mathrm{FSR}_+}{\mathrm{FSR}_+ - \mathrm{FSR}_-} = \frac{\mathrm{FSR}_s\mathrm{FSR}_i}{|\mathrm{FSR}_s - \mathrm{FSR}_i|}. \tag{2.41}$$

This has an effect on the enhancement factor, which becomes also proportional to the cluster separation FSR_c. The phenomenon of clustering is particularly relevant for this thesis work, as discussed in Chapter 5.

2.4 Correlation functions in SPDC

A useful way to characterize SPDC-based single-photon sources consists of measuring the correlation functions for the SPDC output state. These measurements are relatively simple with respect to other methods and provide insights about the spectral and temporal structure of the generated photons. Usually, three types of correlation functions are measured: the *signal-idler cross-correlation function*, the *second-order signal-signal* or *idler-idler auto-correlation function* and the *second-order heralded auto-correlation function*. These quantities will be described in this section.

2.4.1 Signal-idler cross-correlation function

The signal-idler cross-correlation function at times t_1 and t_2 is defined as:

$$G_{si}(t_1, t_2) = \langle \hat{E}_s^{\,(-)}(t_1)\hat{E}_i^{\,(-)}(t_2)\hat{E}_i^{\,(+)}(t_2)\hat{E}_s^{\,(+)}(t_1)\rangle, \tag{2.42}$$

where the brackets indicate expectation value. $G_{si}(t_1, t_2)$ represents the probability of detecting a signal photon at time t_1 and an idler photon at time t_2 with ideal detectors,

i.e. detectors with 100 % detection efficiency and zero time jitter. The field operators are evaluated at the detectors location. The cross-correlation function is strictly connected to the joint spectral intensity via two-dimensional inverse Fourier transform. It can be shown, in fact, that $G_{si}(t_1, t_2)$ is proportional to $|\int_0^\infty d\omega_s d\omega_i \Phi(\omega_s, \omega_i) e^{-i\omega_s t_1} e^{-i\omega_i t_2}|^2$ [166]. Expression 2.42 may be re-written in terms of the variables t and τ, where $t = t_1$ and $\tau = t_2 - t_1$. In most situations, only the dependence on τ is relevant for extracting information on the source. In particular, if the pump field is stationary, $G_{si}(t, \tau)$ is independent of t, which can then be omitted. In this case, therefore, the cross-correlation function can be measured by simply recording the coincidence counts between signal and idler photons at different delays.

As in SPDC the signal and idler photons are produced together, the cross-correlation function has a peak at $\tau = 0$, assuming no delay between signal and idler is introduced after photon generation. At large delays, i.e. for $|\tau| \to \infty$, instead, the signal and idler detections are fully uncorrelated and therefore the quantum average in expression 2.42 factorizes in two independent terms:

$$G_{si}(\tau \to \infty) = \langle \hat{E}_s^{(-)}(0) \hat{E}_s^{(+)}(0) \rangle \langle \hat{E}_i^{(-)}(\tau) \hat{E}_i^{(+)}(\tau) \rangle. \tag{2.43}$$

This implies that $G_{si}(0) >> G_{si}(\infty)$. The FWHM of the function $G_{si}(\tau)$ defines the *correlation time*, τ_c, which is related to the bandwidth of the signal and idler photons. In case the two photons have the same bandwidth, as for degenerate type-I SPDC, τ_c is simply proportional to the inverse of the photon bandwidth. For single-pass SPDC processes, τ_c is typically of the order of $1 - 10$ ps [168]. Since the time resolution of the available single-photon detectors is in the best case a few ps [175, 176], this means that the cross-correlation function cannot be resolved in time and τ_c cannot be experimentally evaluated. In these conditions, any measurement of the coincidence counts only provides a characterization of the detectors jitter. However, for resonant SPDC the bandwidth of the emitted photons is far narrower and consequently τ_c reaches values in the range of $10 - 100$ ns [171, 172]. It is therefore possible to resolve $G_{si}(\tau)$ and extract the correlation

time.

Let us then consider a double-resonant CE-SPDC process pumped by a CW laser beam that is approximated as a monochromatic wave. Signal and idler fields are both assumed to be emitted in a single longitudinal mode of the cavity, described by the Lorentzian function $f(\omega_{s,i}) \propto ((\omega_{s,i} - \omega_{s_0,i_0}) + i\gamma_{s,i})^{-1}$. Under these assumptions, the joint spectral amplitude, Φ_R, is a function of the frequency difference $\delta\omega = \omega_s - \omega_{s_0} = \omega_{i_0} - \omega_i$ only. Consequently, the cross-correlation function is proportional to the square modulus of the one-dimensional inverse Fourier transform of Φ_R, which is a double exponential decay:

$$G_{si}(\tau) \propto u(\tau)e^{-2\gamma_s\tau} + u(-\tau)e^{2\gamma_i\tau}, \tag{2.44}$$

where $u(\tau)$ is the step function. In the multi-mode case $G_{si}(\tau)$ has a comb structure that is modulated by the single-mode cross-correlation function [177]. However, typically the comb structure is experimentally not resolvable due to the detector jitter. In general $\gamma_s \neq \gamma_i$, therefore the correlation decay rate is different for positive and negative values of τ. Based on Equation 2.44, the time constants $\tau_\mu = \frac{1}{2\gamma_\mu} = \frac{1}{2\pi\Delta\nu_\mu}$ can be defined, with $\Delta\nu_\mu$ frequency bandwidth and $\mu = s, i$. Consequently, the correlation time is given by $\tau_c = \log 2\,(\tau_s + \tau_i)$.
By defining an average time constant $\overline{\tau} = \frac{\tau_s+\tau_i}{2}$ and an average bandwidth $\overline{\Delta\nu} = \frac{1}{2\pi\overline{\tau}}$, the following relation can be found $\overline{\Delta\nu} = \frac{\log 2}{\pi\tau_c}$. In the case that signal and idler have the same bandwidth, the average bandwidth and the signal/idler photon bandwidth also coincide.

2.4.2 Second-order auto-correlation function

Other important quantities that are useful for the characterization of SPDC-based single-photon sources are the signal-signal and idler-idler auto-correlation functions. They provide information on the statistics of the signal and idler fields, respectively. In general, the normalized n-th order auto-correlation function for the field μ at times $t_1, ..., t_{2n}$ is

defined as[178]:

$$g_{\mu}^{(n)}(t_1, t_2, ..., t_n, t_{n+1}, ..., t_{2n}) = \frac{\langle \hat{E_{\mu}}^{(-)}(t_1)...\hat{E_{\mu}}^{(-)}(t_n)\hat{E_{\mu}}^{(+)}(t_{n+1})\hat{E_{\mu}}^{(+)}(t_{2n})\rangle}{(\langle \hat{E_{\mu}}^{(-)}(t_1)\hat{E_{\mu}}^{(+)}(t_1)\rangle ... \langle \hat{E_{\mu}}^{(-)}(t_{2n})\hat{E_{\mu}}^{(+)}(t_{2n})\rangle)^{1/2}}. \tag{2.45}$$

In what follows, the second order auto-correlation function at times t and $t+\tau$ will be analysed in detail. This is given by:

$$g_{\mu}^{(2)}(t, \tau) = \frac{\langle \hat{E_{\mu}}^{(-))}(t)\hat{E_{\mu}}^{(-)}(t+\tau)\hat{E_{\mu}}^{(+)}(t+\tau)\hat{E_{\mu}}^{(+)}(t)\rangle}{\langle \hat{E_{\mu}}^{(-)}(t)\hat{E_{\mu}}^{(+)}(t)\rangle \langle \hat{E_{\mu}}^{(-)}(t+\tau)\hat{E_{\mu}}^{(+)}(t+\tau)\rangle}. \tag{2.46}$$

Analogously to expression 2.42, $g_{\mu}^{(2)}(t, \tau)$ constitutes the probability of detecting a photon at time t and another photon at time $t+\tau$ in the same mode μ (signal or idler), normalized to the probability of two independent single detections at t and $t+\tau$. Throughout this section, the function in 2.4.2 will be assumed to depend only on τ.

The value of the second-order auto-correlation function for $\tau = 0$ is related to the photon-number statistics of the SPDC state. In particular, it can be shown that $g_s^{(2)}(0) = g_i^{(2)}(0) = 2$, which is a typical feature of thermal light [166]. In this case, the second-order auto-correlation function can be expressed in terms of the first-order auto-correlation function:

$$g_{\mu}^{(2)}(\tau) = 1 + \left| \frac{\langle \hat{E_{\mu}}^{(-)}(t)\hat{E_{\mu}}^{(+)}(t+\tau)\rangle}{\langle \hat{E_{\mu}}^{(-)}(t)\hat{E_{\mu}}^{(+)}(t)\rangle} \right|^2 = 1 + |g_{\mu}^{(1)}(\tau)|^2. \tag{2.47}$$

The term $|g_{\mu}^{(1)}(\tau)|^2$ in 2.47 is proportional to [1] $\int_0^{\infty} d\omega_{\mu} d\omega_{\hat{\mu}} |\Phi(\omega_{\mu}, \omega_{\hat{\mu}})|^2 e^{-\omega_{\mu}\tau}$[166]. This means that, once the joint spectral intensity is known, the second-order auto-correlation function can also be calculated.

The auto-correlation measurement is usually performed by inserting a 50/50 beam-splitter in the signal (or idler) arm and by detecting the photon coincidences at the two output ports of the beam splitter at different delays. In case of single-pass SPDC, the

[1] if the pump field is non stationary this is true only for the *time-averaged* first-order auto-correlation function

temporal profile of $g^{(2)}(\tau)$ typically cannot be resolved, because of the low time resolution of the available single-photon detectors. The same happens for the peak value $g^{(2)}(0)$: the only accessible quantity is an averaged value over the detector time jitter, which in general is not 2. However, this apparent drawback turns out to be a resource for the characterization of the modal structure of the emitted photons.

In the case of doubly resonant CE-SPDC, under the same assumptions made in Section 2.4.1, one obtains, for both signal and idler:

$$g^{(2)}(\tau) = \begin{cases} 1 + |\frac{1}{\gamma_i - \gamma_s} e^{-0.5(\gamma_i+\gamma_s)|\tau|}(\gamma_i e^{0.5(\gamma_i+\gamma_s)|\tau|} - \gamma_s e^{-0.5(\gamma_i+\gamma_s)|\tau|})|^2 & \gamma_s \neq \gamma_i, \\ 1 + |e^{-\gamma_s|\tau|}(1 + \gamma_s|\tau|)|^2 & \gamma_s = \gamma_i. \end{cases}$$

The above equation provides the auto-correlation function in the case that signal and idler are emitted into a single longitudinal cavity mode. In the multi-mode case, interference fringes below the single-mode envelope appear, which are usually non-resolvable by the employed detection systems. Expression 2.4.2 can be approximated as a simpler Lorentzian:

$$g^{(2)}(\tau) = 1 + \frac{1}{1 + (\frac{1}{2}(\gamma_s + \gamma_i)\tau)^2}. \tag{2.48}$$

Note that, unlike cross-correlation, the auto-correlation peak is symmetric, independent of signal and idler decay rates. The FWHM of the peak is given by the *auto-correlation time* $T_{ac} = \frac{4}{\gamma_s+\gamma_i}$. By assuming $\gamma_s \approx \gamma_i$, one obtains $T_{ac} \approx \frac{2}{\log 2}\tau_c$, meaning that the auto-correlation time is about 3 times larger than the correlation time. This result implies that the two-photon component in the signal/idler fields, related to the product of two joint spectral amplitudes, are associated to a narrower frequency bandwidth than the one-photon component, which includes a single joint spectral amplitude.

In general, it is not possible to measure the exact value of the auto-correlation function at a given time delay τ_0, but only the average quantity:

$$g^{(2)}_{meas}(\tau_0) = \frac{1}{2t_d} \int_{\tau_0 - t_d}^{\tau_0 + t_d} g^{(2)}(\tau) d\tau, \tag{2.49}$$

where t_d is the detector time jitter. This becomes particularly relevant for $\tau_0 = 0$. In

fact, the measured value of $g^{(2)}(0)$ depends on how many longitudinal modes are involved in the averaging, as t_d usually covers many periods of mode beating. In particular [174]:

$$g^{(2)}_{meas}(0) \approx 1 + \frac{1}{N}, \tag{2.50}$$

where N is the average number of emitted longitudinal modes, obtained by considering all the modes equally excited. The reader should note that in the case of ideal detectors, with no jitter, the auto-correlation measurement would always provide $g^{(2)}(0) = 2$.

2.4.3 Heralded second-order auto-correlation function

The measurement of the second-order auto-correlation function at $\tau = 0$ for a source producing a genuine single-photon Fock state, gives the result 0. The reason is evident: since only one photon is excited, it is impossible to detect a coincidence at zero delay at the output ports of the beam-splitter, at least in theory, as this would imply the presence of two photons. In principle any ideal single-photon source should satisfy this condition. However, in the case of SPDC-based single-photon sources $g^{(2)}(0) = 2$. SPDC, in fact, approximates genuine single-photon generation only if heralding is performed and the pump power is low so that multi-photon emission can be neglected. The heralded second-order auto-correlation function for an SPDC process in the low-pump-power regime is then expected to mimic that of a Fock state. This quantity is defined as:

$$g^{(2)}_{\mu h}(t+\tau|t) = \frac{\langle \hat{E_\mu}^{(-)}(t)\hat{E_\mu}^{(-)}(t+\tau)\hat{E_\mu}^{(+)}(t+\tau)\hat{E_\mu}^{(+)}(t)\rangle_{pm}}{\langle \hat{E_\mu}^{(-)}(t)\hat{E_\mu}^{(+)}(t)\rangle_{pm}\langle \hat{E_\mu}^{(-)}(t+\tau)\hat{E_\mu}^{(+)}(t+\tau)\rangle_{pm}}, \tag{2.51}$$

where $\mu = s, i$ and the average is evaluated on the post-selected state after detection of a photon in the complementary mode $\hat{\mu}$. The function in Equation 2.51 expresses the correlation between the simultaneous detection of a signal and idler photon at t and the further detection of a signal or idler (according to whether $\mu = s$ or $\mu = i$, respectively) photon at time $t + \tau$. This quantity is measured in the same way as the non-heralded auto-correlation, with the only difference that the signal detections are now heralded by

an idler photon, or vice versa.

Assuming the dependence on t can be neglected, $g^{(2)}_{\mu h}(\tau)$ can be expressed as [179]

$$g^{(2)}_{\mu h}(\tau) = \frac{P_{\mu\mu\hat{\mu}}(\tau)R(0)}{P_{\mu\hat{\mu}(\tau)}P_{\mu\hat{\mu}}(0)}, \tag{2.52}$$

where $P_{\mu\mu\hat{\mu}}$ and $P_{\mu\hat{\mu}}$ are the probabilities of a double and triple coincidence detection between the fields μ and $\hat{\mu}$, respectively and $R(0)$ is the non-normalized first-order correlation function at zero delay, which is assumed to be the same for signal and idler. $R(0)$ is proportional to the single-detection probability for signal and idler. However, the actually measured correlation function, for instance for $\mu = s$, is:

$$g^{(2)}_{sh}(\tau) = \frac{N_{ssi}(\tau)R_0}{N_{si}(\tau)N_{si}(0)}, \tag{2.53}$$

where R_0 is the single-detection rate for the signal and the other terms are the coincidence rates corresponding to the probabilities in 2.52. All these quantities are averaged over the detector jitter τ_d and the coincidence rates include an additional average over the coincidence window, τ_{coinc}.

The function $g^{(2)}_{sh}(\tau)$ tends to 1 for large delays and decreases as $\tau \to 0$. The value $g^{(2)}_{sh}(0)$ quantifies multi-photon emission from the source, which decreases by decreasing the pump power. In regime of low pump power and short coincidence windows, that is for $R_0\tau_{coinc} << 1$, due to the averaging over jitter and coincidence windows, $g^{(2)}_{sh}(0)$ can be approximated as $R_0\tau_{coinc}$ [179]. Measuring the heralded second-order correlation function at zero delay, therefore, allows one to confirm that the source operates in low-gain regime and can be approximated to a real single-photon source, but cannot provide a fully quantitative indication of how good this approximation is [180].

Chapter 3

Experimental Two-Way Communication with One Photon

In this chapter, the first part of the experimental work comprising the Ph.D. project presented in this thesis is described. This work aims to experimentally demonstrate two-way communication between two distant parties who can only exchange a single quantum particle once. Such a task, based on quantum superposition, is impossible with classical particles, as both parties would either need to exchange the same particle more than once or simultaneously use more particles simultaneously.

The scheme for two-way communication with one particle (TWCOP) was proposed in 2018 by Del Santo and Dakić [181], and experimentally demonstrated for the first time in this Ph.D. project, during which furthermore a novel anonymous and secure direct communication protocol based on TWCOP was designed and implemented.

The chapter is structured as follows: first, TWCOP and the related anonymous and secure protocol are explained; then, the setup for the implementation of the experiments is described, and finally the experimental results are discussed.

This Chapter is entirely taken from the article "Experimental two-way communication with one photon" by Francesco Massa et al., published in *Advanced Quantum Technologies* in 2019. Some modifications are applied for readability improvement.

3.1 Two-way communication with one particle

In order to explain TWCOP, let us consider a communication game in which a referee assigns two random input bits, x and y, to two distant communication parties, Alice and Bob, respectively. After receiving the bits, they are allowed to exchange one particle. The time necessary for the exchange to be completed is indicated by τ, which then represents the interval between the time at which the particle leaves Alice's or Bob's location and the time at which it is detected. The time τ is assumed to be shorter than the time required for a physical object to travel the distance between Alice and Bob more than once. When the exchange is completed, the referee asks Alice and Bob to reveal two output bits, a and b - they win the game if they both guess correctly the value of the other player's input (i.e. if $a = y$ and $b = x$). This game can be considered a variation of the well-known "Guess Your Neighbour's Input" (GYNI) game [182].

Under the constraint that the parties can only exchange one classical particle within the time window τ, only two possible causal relations between the variables x, y, a, and b, are possible: either x influences a and b while y influences b only (corresponding to a one-way communication from Alice to Bob), or y influences a and b while x influences a only (one-way communication from Bob to Alice), as illustrated in Figure 3.1. Accordingly, the joint probability distribution $p(ab|xy)$ results in a classical mixture of the two one-way signalling distributions. This imposes a maximal probability value of $1/2$ of winning the game [183].

The situation is different if the parties are allowed to share a quantum particle, which is assumed here to be a single photon. The photon, in fact, can be prepared in a coherent superposition:

$$|\psi_{in}\rangle = \frac{1}{\sqrt{2}}(\widehat{a}^{\dagger} + \widehat{b}^{\dagger})|0\rangle, \tag{3.1}$$

where $\widehat{a}^{\dagger}$ and $\widehat{b}^{\dagger}$ are the photon creation operators at Alice's and Bob's locations, respectively, and $|0\rangle$ is the vacuum state. Alice and Bob can then encode the bits x and y in

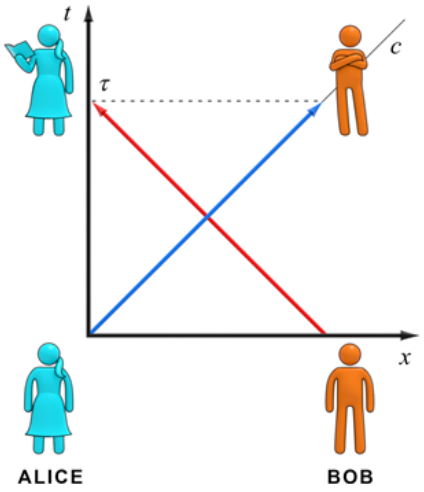


Figure 3.1: **Communication between two distant parties with a classical particle.** A single carrier travelling with finite speed, bound by the speed of light, c, can transmit information either from Alice to Bob (blue arrow) or from Bob to Alice (red arrow), if the time τ allowed for the communication is shorter than the time the carrier takes to travel the distance between Alice and Bob multiple times.

the phase of the photon, thus obtaining the state:

$$|\psi_{encode}\rangle = \frac{1}{\sqrt{2}}((-1)^x\ \widehat{a}^\dagger + (-1)^y\ \widehat{b}^\dagger)|0\rangle. \tag{3.2}$$

If a 50/50 beam splitter is placed at the centre of the path between Alice and Bob (see Figure 3.2), due to single-photon interference, the final state of the photon is:

$$|\psi_{fin}\rangle = \begin{cases} \widehat{a}^\dagger|0\rangle, & \text{if } x=0 \text{ and } y=0, \\ \widehat{b}^\dagger|0\rangle, & \text{if } x=0 \text{ and } y=1, \\ -\widehat{b}^\dagger|0\rangle, & \text{if } x=1 \text{ and } y=0, \\ -\widehat{a}^\dagger|0\rangle, & \text{if } x=1 \text{ and } y=1. \end{cases} \tag{3.3}$$

This means that, by checking whether they detect the particle or not, Alice and Bob can infer the parity, r, of x and y. This piece of information, combined with the knowledge of their input bits, allows them to win the game with probability 1, thus demonstrating genuine two-way communication.

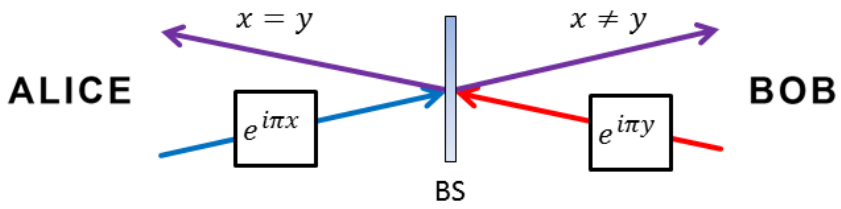


Figure 3.2: **Scheme of two-way communication with a quantum particle.** Alice and Bob, who share a single photon in superposition, encode the bits to be transferred, x and y, in the phase of the photon and send the photon to a beam splitter (BS). The photon travels to Alice or Bob after the beam splitter based on the parity of the encoded bits. In this way each party obtains the value of the bit encoded by the other one, and two-way communication is performed. The superposition state of the photon thus corresponds to a superposition of the communication directions.

3.2 Application of TWCOP for anonymous communication

The described scheme of TWCOP can be used as a primitive for a secure two-party quantum communication protocol that bestows anonymity upon the direction of communication between Alice and Bob. This is achieved by converting the two-way scheme to a direct messaging system in which only a single party transmits a message at a time and the other transmits random bits.

The basic assumption of the protocol is that Alice and Bob share a quantum channel and many copies of the required superposition state, $|\psi_{in}\rangle$, which is known to be a powerful recourse for secure communication [184]. Such states could be supplied on demand via a trusted server, assuming the channel between the server and Alice, and the server and Bob are secure from potential eavesdroppers. Alternatively, these superposition states could, in theory, be produced and stored by the two parties when they meet and then used at a later time. Prior to the protocol, each state $|\psi_{in}\rangle$ is labelled with index i.

For the i-th round of communication, the parties encode the classical bits x_i and y_i in the state $|\psi_{encode}\rangle_i = \frac{1}{\sqrt{2}}((-1)^{x_i}\ \widehat{a}^\dagger + (-1)^{y_i}\ \widehat{b}^\dagger)\,|0\rangle$. Both send their parts of the state $|\psi_{encode}\rangle_i$ via the quantum channel and detect any returning photon. Detection of a photon reveals the parity bit $r_i = x_i \oplus y_i$ to each party.

Assuming Alice wishes to send an M-bit message $\{X_1, \ldots, X_M\}$ to Bob, the protocol

may be described by the following sequence of steps:

1. **Decline communication.** If no message is to be sent, Alice and Bob select the bits x_i and y_i uniformly at random.

2. **Declaration of the communication direction.** Alice initializes the communication by setting $x_i = 1$ for d iterations of the protocol, where d is chosen to be sufficiently large as to be sufficiently improbable to occur by chance. Detection of d repeated $x_i = 1$ results by Bob indicates that Alice intends to send a message. Should Bob simultaneously declare his intention to communicate, the protocol is aborted.

3. **Transmission of the message.** Alice sets $x_i = X_i$, for i going from 1 to M. Bob may or may not detect a photon, thus obtaining the parity value $r_i = y_i \oplus X_i$, from which the bit X_i can be deduced.

4. **Declaration of the end of the message.** To end the message transmission, Alice sends $x_i = 0$ for d iterations of the protocol. Alice and Bob return to step 1.

The scheme is fully secure against a potential eavesdropper, Eve, acting on the quantum channel between Alice and Bob, as interception of a photon between the two parties can at most reveal the parity between x_i and y_i given by the position of the photon after the interference at the central beam splitter. In fact, the four possible states of $|\psi_{encode}\rangle$ form two pairs that are identical under global phases, which cannot be observed via measurement on single photons. As each bit y_i is chosen uniformly at random, the parity bit contains no information on x_i, provided that y_i is unknown, and thus leaks no information on Alice's message bit X_i. Bob's input thus acts as a random one-time pad. As communication is two-way, pad bits y_i are also obtained by Alice, and as such the scheme is anonymous in the direction of the message and the pad.

If Eve intercepts and replaces the resource state $|\psi_{in}\rangle$ before it is received by the parties, a man-in-the-middle attack may be successfully performed. Eve could, in fact, prepare two single-photon superposition states and implement the TWCOP scheme

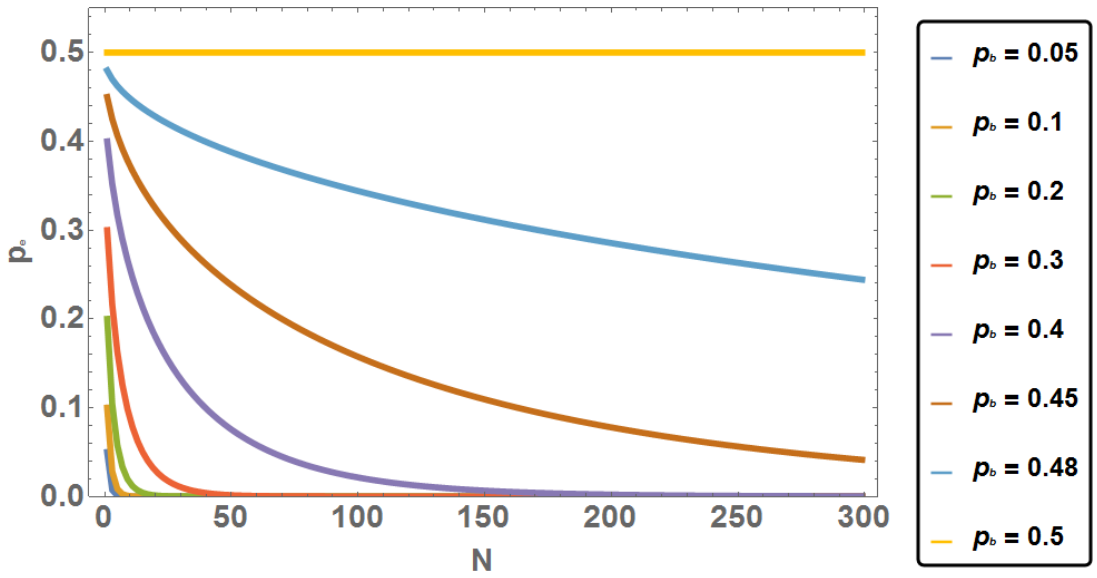


Figure 3.3: **Error correction performance.** The plot shows the error probability per bit after applying majority-voting error correction, p_e, with respect to the number of encodings of each bit, N. This dependence is shown for different values of the error probability per bit for the uncorrected protocol, p_b. The slope of the curve reduces as p_b approaches 0.5.

separately with Alice and Bob. In this way she can obtain full information on the encoded bits. This possibility is, however, excluded by the assumption that Alice and Bob share many copies of the state $|\psi_{in}\rangle$ prior to the beginning of the protocol.

The protocol as described above is not resistant to photon loss. Loss caused by an erasure channel may result in no photon being detected by Bob when required, causing a single bit error in the received message. Additional errors may be caused by imperfections in the experimental setup, such as dephasing or non-optimal interference visibility. However, errors can be overcome, without compromising security, by adding redundancy to the protocol.

The simplest strategy for this purpose consists of repeating the encoding of each message bit N times, with N being odd, and performing majority voting, meaning that the result occurring at least $\frac{N+1}{2}$ times is chosen. If the probability of error per bit of the

basic protocol is p_b, the probability of error per bit after error correction, p_e, is given by:

$$p_e = \sum_{k=\frac{N+1}{2}}^{N} \binom{N}{k} p_b^k (1-p_b)^{N-k}. \tag{3.4}$$

In Figure 3.3 the behaviour of p_e with respect to N is shown for different values of p_b. It is clear that the higher p_b is, the slower p_e goes to 0 when increasing the number of repetitions. When $p_b = 0.5$, p_e is independent of N, and for $p_b > 0.5$ the majority-voting procedure only worsens the overall probability of success. The transfer of many copies of the same bit pair does not jeopardize the security of the protocol. In fact, Eve can only obtain the (same) parity bit every time, which does not reveal any information about the encoded bits.

3.3 Experimental setup

3.3.1 The single-photon source

The photon source used for the experimental implementation of the TWCOP scheme and the related anonymous communication protocol is based on SPDC in a Sagnac configuration [185].

Laser light at 394.5 nm (Toptica Blue Mode, fiber-coupled maximum power: 23 mW, bandwidth: < 0.1 nm) impinges on a dual-wavelength polarizing beam splitter (DPBS), after its polarization is set to diagonal. Here, "dual-wavelength" means that the device works in the same way both at 394.5 nm and at 789 nm. The DPBS then splits the original input beam into two equally intense output beams, which travel along the two possible propagation directions (clockwise and counterclockwise) of a Sagnac interferometer, composed of the DPBS and two mirrors (M) (see Figure 3.4). The interferometer contains a 20-mm-long PPKTP crystal, phase-matched for type-II degenerate and collinear SPDC at ambient temperature. The crystal, therefore, emits photon pairs at 789 nm in the polarization state $|H\rangle_s|V\rangle_i$, when pumped with horizontally-polarized light at 394.5 nm. A dual-wavelength half-wave plate (DHWP) is placed in the interferometer such that the

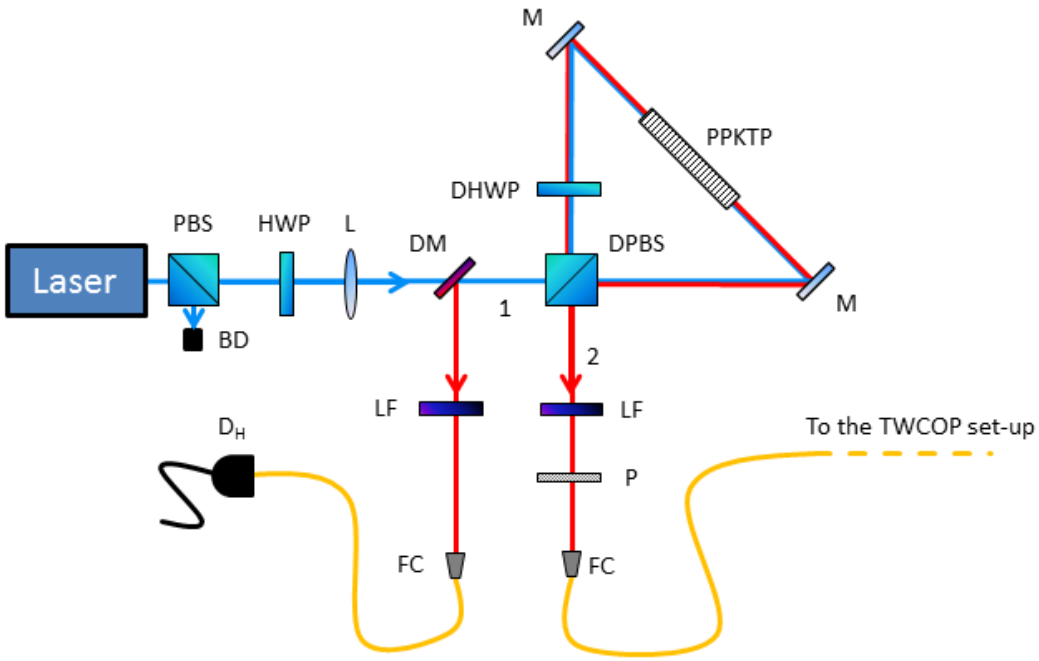


Figure 3.4: **Scheme of the single-photon source.** A laser at 394.5 nm is diagonally polarized after passing through a polarizing beam splitter (PBS) and a half-wave plate (HWP) (with a beam dump (BD) collecting the rejected light from the PBS) and focused by a lens (L) onto a PPKTP crystal (Raicol Crystals). The crystal is placed in a Sagnac loop, which is realized using a dual-wavelength polarizing beam splitter (DPBS), a dual-wavelength half-wave plate (DHWP) and two mirrors (M). A type-II degenerate SPDC process takes place in the crystal, which thus converts a pump photon at 394.5 nm into two photons at 789 nm with orthogonal polarizations. As photons are produced along both propagation directions of the pump beam in the interferometer, the photonic state at the outputs 1 and 2 of the PBS is entangled. After filtering out the pump by means of a dichroic mirror (DM) and two long-pass filters (LF), the generated photons are coupled into single-mode fibers through two fiber couplers (FC): one of the photons is sent to the setup for the implementation of TWCOP and the other is sent directly to a detector (D_H) to herald the presence of its twin. The use of a polarizer (P) ensures that a defined polarization state is produced.

two counter-propagating beams at 397 nm are both horizontally polarized when they impinge on the PPKTP. This allows for photon generation in both propagation directions of the Sagnac loop.

The generated photons reach the DPBS and exit the interferometer to the output modes 1 and 2. The photons propagating clockwise and counterclockwise produce the output states $|H\rangle_1|V\rangle_2$ and $|V\rangle_1|H\rangle_2$, respectively. As these possibilities are coherently superposed, the resulting emitted state, $|\psi\rangle$, is entangled: $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2)$, where the minus sign accounts for the phase shift between reflected and transmitted outputs of the beam splitter. Note that, due to the presence of the DHWP, the signal photons always exit to output 1, whereas idler photons always go to output 2. This preserves the entanglement even in the case of non-degenerate emission or frequency correlations between signal and idler photons. However, entanglement is not needed for the experiments described in this chapter, which instead require a defined polarization state. For this reason, a polarizer (P) selects only the term $|V\rangle_1|H\rangle_2$ of the state $|\psi\rangle$. After the pump is filtered out, the generated photons are coupled to single-mode fibers - one of them directly connected to detector D_H (avalanche photo-diode, Excelitas SPCM AQRH-13) to herald the other one, which is sent to the TWCOP setup.

At 7 mW of pump power, the source provides about 3×10^4 coincidences/s between D_H and the detectors in the TWCOP setup. The corresponding heralded second-order correlation function at zero delay is measured to be $g_h^{(2)}(0) = 0.004 \pm 0.010$, meaning that, to a good level of approximation, the source emits single photons. This value was obtained from Equation 2.53 by counting single detections, two- and three-fold coincidences for 3 minutes. According to Equation 2.31 and assuming the pump monochromatic, the bandwidth of the emitted photons is calculated to be: $\Delta\omega_{FWHM} = 700$ GHz, corresponding to a coherence time of 9 ps and a coherence length of 3 mm.

3.3.2 The TWCOP setup

The TWCOP setup is basically a Mach-Zehnder interferometer, as depicted in Figure 3.6. A heralded single photon is made to impinge on a 50/50 beam splitter, BS_1, which

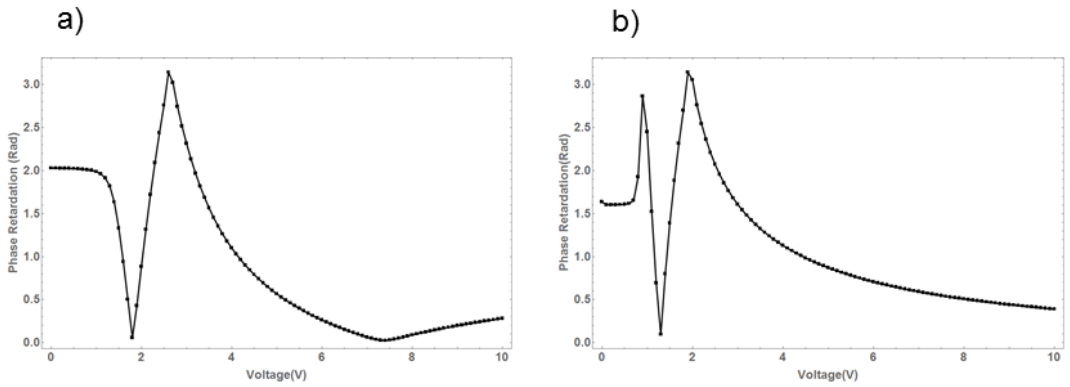


Figure 3.5: **Characterization of the liquid-crystal phase shifters.** The characterization is performed with laser light. The phase shifter to be characterized is rotated by 45° with respect to the horizontal direction, and a polarizer is placed right after the device. The light transmitted through the polarizer is monitored while varying the voltage applied to the phase shifter. The plots report the dependence of the phase retardation between the two axes of the liquid crystals with respect to the voltage for LC_A (a) and LC_B (b). The two devices are operated at the minimum (0 phase) and the maximum (π phase) of the curves.

puts the photon in a superposition of Alice's and Bob's locations. Alice and Bob each encode their bits in the phase of the photon by means of a liquid-crystal phase shifter, LC_A (from Meadowlark Optics) for Alice and LC_B (Thorlabs LCC1221-B) for Bob. The slow axes of the two phase shifters are aligned to the photon polarization, which is set to horizontal. The refractive index along these axes depends on the voltage applied to the liquid crystal, meaning that the applied phase shift is tunable. Prior to the experiment, the dependence of the phase shift on the applied voltage is characterized, and the values of the voltage necessary to obtain 0 and π phase shifts, corresponding to the bits 0 and 1, repspectively, are found (see Figure3.5). The rise time from 0 to π phase is observed to be about 5 ms for LC_A and about 40 ms for LC_B, while the fall times are about 20 ms and 0.5 ms, respectively. For this reason, a buffer of 50 ms is set before encoding each bit pair, in order to avoid errors due to imperfect phase setting. After encoding, each party uses a mirror, M_A for Alice and M_B for Bob, to steer the photon to a second beam splitter, BS_2. Due to interference, the state of the photon after BS_2 is $|\psi_{fin}\rangle$. The photon is then sent back to Alice (Bob) by means of an additional mirror, M_1 (M_2), and detected by an avalanche photo-diode (Excelitas SPCM AQRH-13), D_A (D_B).

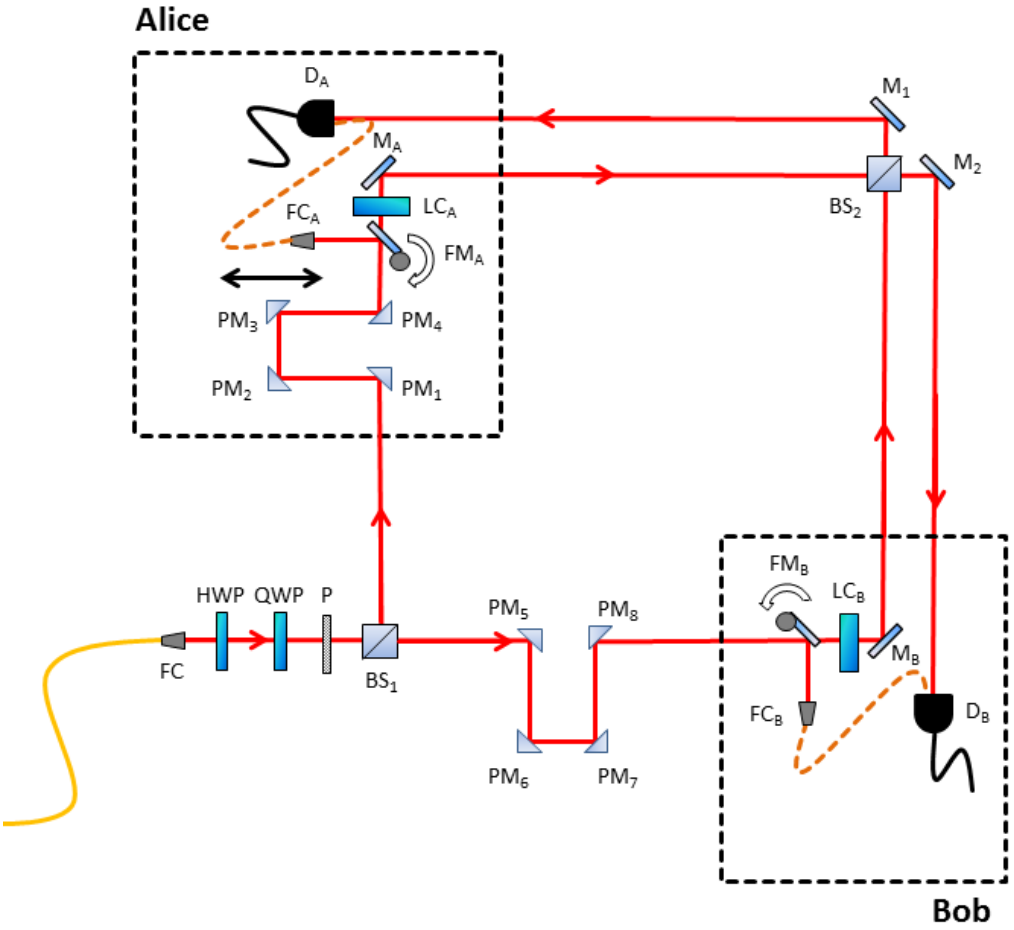


Figure 3.6: **Interferometer for the demonstration of two-way communication with a single photon.** The "laboratories" of Alice and Bob are delimited by the dashed black lines. The photon coming from the source in Figure 3.4 is collimated by a fiber coupler (FC), and its polarization is set to horizontal by means of a quarter-wave plate (QWP), a half-wave plate (HWP) and a polarizer (P). Then, the photon enters a Mach-Zehnder interferometer, whose basic elements are the 50/50 beam splitters BS_1 and BS_2 and the mirrors M_A and M_B. The liquid-crystal phase shifters LC_A and LC_B are used for phase encoding, whereas the flip mirrors FM_A and FM_B, when flipped up, are used to steer light to the fiber couplers FC_A and FC_B and the related multi-mode fibers for the measurement of the photon's arrival-time distributions at the users. When this measurement is not performed, the flip mirrors are flipped down and the fibers are disconnected from the detectors, D_A and D_B, which then work in free space. In this configuration, after interference at BS_2 the photon is sent back to Alice or Bob by mirrors M_1 and M_2, where it is detected. The photon path is indicated by the solid red lines. A trombone delay line composed of prism mirrors PM_1, PM_2, PM_3, PM_4 is inserted into one arm of the interferometer, within Alice's laboratory. This is used to finely tune the difference between the two interferometric paths such that they are equal within the photon coherence length (3 mm). The path difference can be tuned by ± 20 mm with micrometer resolution. A fixed trombone (prism mirrors PM_5, PM_6, PM_7, PM_8) is inserted into the other arm to compensate for the additional travel distance introduced by the delay line. A piezo actuator (travel range: 2 μm) in the trombone delay line allows Alice to actively stabilize the phase of the interferometer when needed.

The interferometer is passively stabilized by means of thermal and vibrational isolation so that the phase between the two arms is stable for about one minute. After this time, the phase can be re-set by means of a piezo actuator mounted on a trombone delay line composed of four prism mirrors (PM_1, PM_2, PM_3, PM_4), which may be used to delay one arm with respect to the other and therefore to change the interference visibility. The piezo is re-set every 25 s to ensure high phase stability in the interferometer.

The distance between M_A and BS_2 is (106 ± 1) cm, whereas the distance between M_B and BS_2 is (119 ± 1) cm. The minimum distance between the regions occupied by Alice and Bob is (156 ± 1) cm, corresponding to the distance between the sides of the liquid-crystal phase shifters. This means that the time employed by the photon to travel from mirror M_A or M_B to the detectors, is shorter than the time it would take to travel the minimum distance between Alice and Bob twice.

A direct verification of this inequality requires the photon's arrival-time distribution at Alice and Bob to be recorded, as described in the next section. To this purpose, two flip mirrors, FM_A and FM_B, are placed at a distance of (10.0 ± 0.5) cm from M_A and M_B, respectively. When FM_A and FM_B are flipped up, they steer the photon to two fiber couplers, FC_A and FC_B, connected to two 2 m-long multi-mode fibers, respectively. The distance between the flip mirrors and the couplers is also (10.0 ± 0.5) cm. In this way, the photon takes the same amount of time to travel from FM_A (FM_B) to FC_A(FC_B) when FM_A (FM_B) is flipped up, as it does to go from FM_A (FM_B) to M_A (M_B) when FM_A (FM_B) is flipped down. For the recording of the arrival time distribution at Alice and Bob, the flip mirrors are flipped up, and the multi-mode fibers are connected to the detectors D_A and D_B. Otherwise, FM_A and FM_B are flipped down, and the two detectors work in free-space configuration.

3.4 Demonstration of two-way signalling with one photon

The probability of winning the communication game described in Section 3.1 is estimated by using a random sequence of 100 input bit pairs, one every 0.5 s.

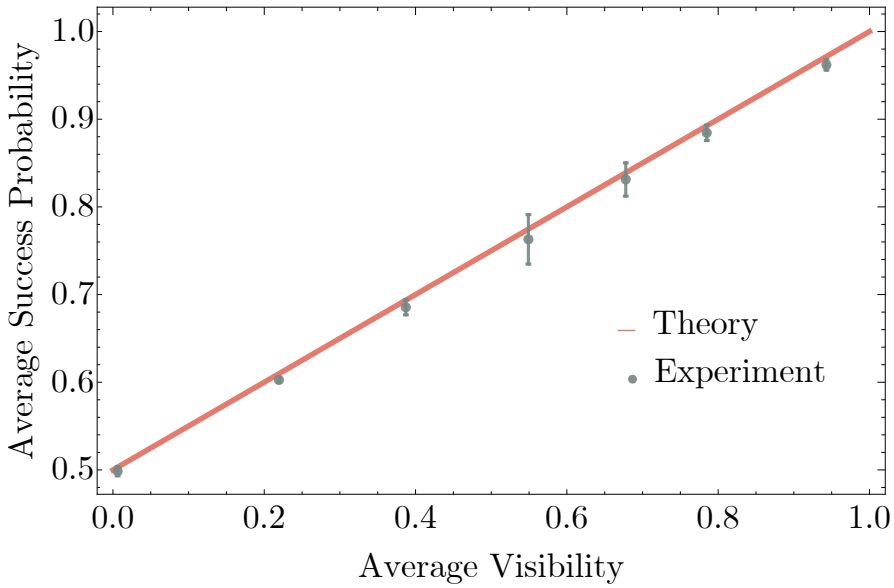


Figure 3.7: **Success probability vs interferometric visibility.** The plot shows the dependence of the probability of winning the game on the quality of the single-photon interference at BS_2, quantified by the average interferometric visibility. The visibility is varied by delaying one interferometric path with respect to the other in the trombone delay lin. At zero visibility, the two photon wave-packets travelling in the two arms no longer overlap at the final beam splitter, and interference is completely suppressed. The equation for the red theoretical curve is $y = 0.5(x + 1)$. The error of each probability is the standard error of the mean, obtained from the statistical variation over the sequence of input bits. For each point in the plot, a different random input sequence of 100 bit pairs is generated.

In this time interval, an average number of photon detections of about 15×10^3 is registered among the two detectors D_A and D_B. All detections are in coincidence between D_A or D_B and the heralding detector D_H. The success probability is computed by counting how many detections occur at the "right" detector for each input bit pair with respect to the total number of detections, and then by averaging this ratio over the input sequence. Figure 3.7 shows the measured success probability for different values of the interferometric visibility, which is averaged over the two output ports. The visibility at each port is defined as $(N_{MAX} - N_{MIN})/(N_{MAX} + N_{MIN})$, where N_{MAX} and N_{MIN} are the maximum and minimum number of detections at that port, respectively, obtained while varying the interferometric phase. The success probability surpasses the classical limit as soon as the visibility is greater than zero. For the maximally achieved visibility of 0.941 ± 0.007, a maximal success probability of 0.961 ± 0.006 is observed.

Initial Reception	Final Detection	Delay (ns)
Alice	Alice	7.1 ± 0.4
Alice	Bob	8.2 ± 0.4
Bob	Alice	7.5 ± 0.3
Bob	Bob	8.5 ± 0.4
Reference time: (10.1 ± 0.1) ns		

Table 3.1: **Time-measurement results.** The four possible delays between the initial reception and the final detection of the photon at Alice or Bob are shown in the table. They are compared to the time the photon would take to travel twice the minimum distance between the two parties, roughly equal to the diagonal of the interferometer, at the speed of light in vacuum (reference value). For each delay, the measurements are taken by unblocking only the corresponding path and recording the arrival-time statistical distributions for reception and final detection. The uncertainty of each time interval is obtained from the standard deviations of the two associated arrival-time distributions, dominated by the time jitter of the detectors. The uncertainty of the reference value is not statistical but comes from the uncertainty of the measurement of the minimum distance between Alice and Bob.

At zero visibility the success probability is 0.498 ± 0.006, compatible with the maximally achievable value in the classical case (0.5). At this point, the effect of the quantum superposition is totally nullified.

In order to prove that each photon cannot be exchanged more than once between the two parties, the delay between two events - the reception of the photon before the encoding and the final detection after the second beam splitter - is measured. Actually, there are four delays to be measured, according to whether the initial reception and the final detection of the photon are considered at Alice or Bob. The delays are slightly different due to the fact that the implemented interferometer is rectangular. The results of these measurements are shown in Table 3.1. It can be seen that, in all the cases, the time τ necessary for the photon exchange to be completed is shorter than the time the photon would take to travel the minimum distance between Alice and Bob twice (reference time) by more than three standard deviations. This sets a probability of less than 1% that the photon travels back and forth between Alice and Bob.

The procedure for the measurement of the delays reported in Table 3.1 is described as follows. Let us call Δt_{AB} the time a photon takes to travel from mirror $\mathrm{M_A}$ to detector $\mathrm{D_B}$ along the arms of the interferometer. Analogously, Δt_{AA}, Δt_{BA}, Δt_{BB} are the times the photon takes to go from $\mathrm{M_A}$ to $\mathrm{D_A}$, from $\mathrm{M_B}$ to $\mathrm{D_A}$ and from $\mathrm{M_B}$ to $\mathrm{D_B}$, respectively.

The measurement procedure for Δt_{AB} is summarized in the following steps:

1. All the possible paths for the photon are blocked except for the path going from M_A to D_B.

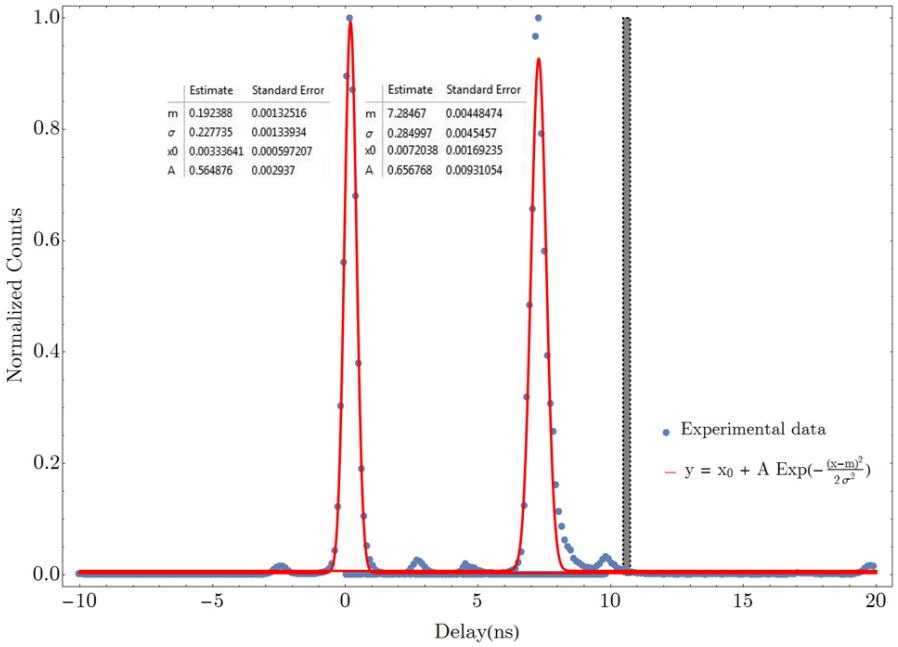
2. The delay between the detection of the heralding photon and the detection of its twin photon at D_B is recorded for a large number of emitted photon pairs. In this way, the arrival-time distribution for the final detection at D_B is acquired, where the arrival times are referred to the heralding detection, used as a trigger. The arrival times are measured by means of a time-tagging module (RoithnerLaserTechnik TTM8000).

3. The flip mirror FM_A is flipped up, and the multi-mode fiber of coupler FC_A is connected to detector D_B. The arrival-time distribution at M_A is acquired, as performed in Point 2, and is corrected for the delay introduced by the fiber.

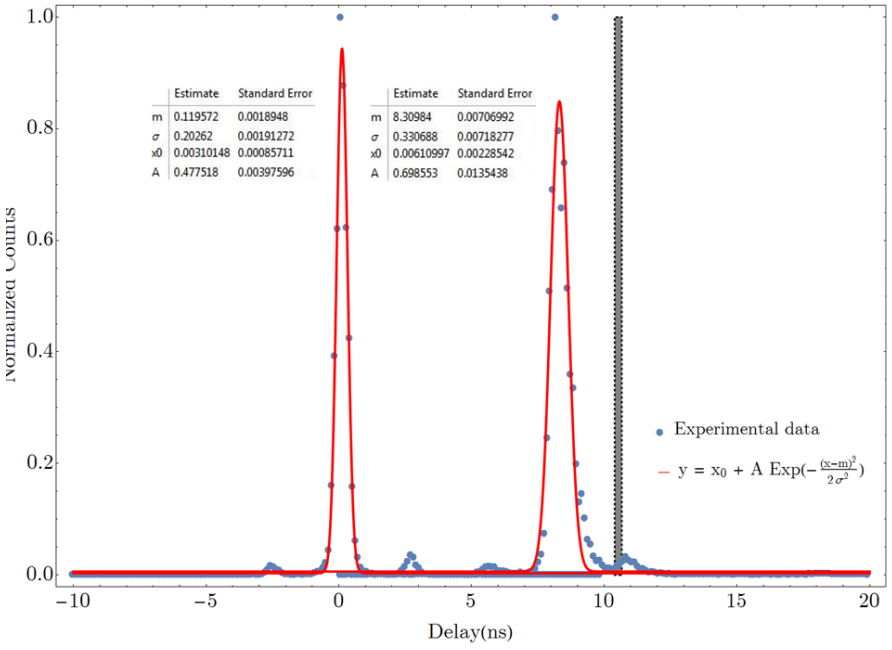
4. The two arrival-time distributions are fitted with Gaussian functions in order to find their mean values and standard deviations.

5. The quantity Δt_{AB} is calculated as the difference between the mean values of the two distributions. Since the detections take place at the same detector with the same time-tagging module, the difference is not affected by further electronic delays. The error of Δt_{AB} is the sum in quadrature of the standard deviations of the two arrival-time distributions.

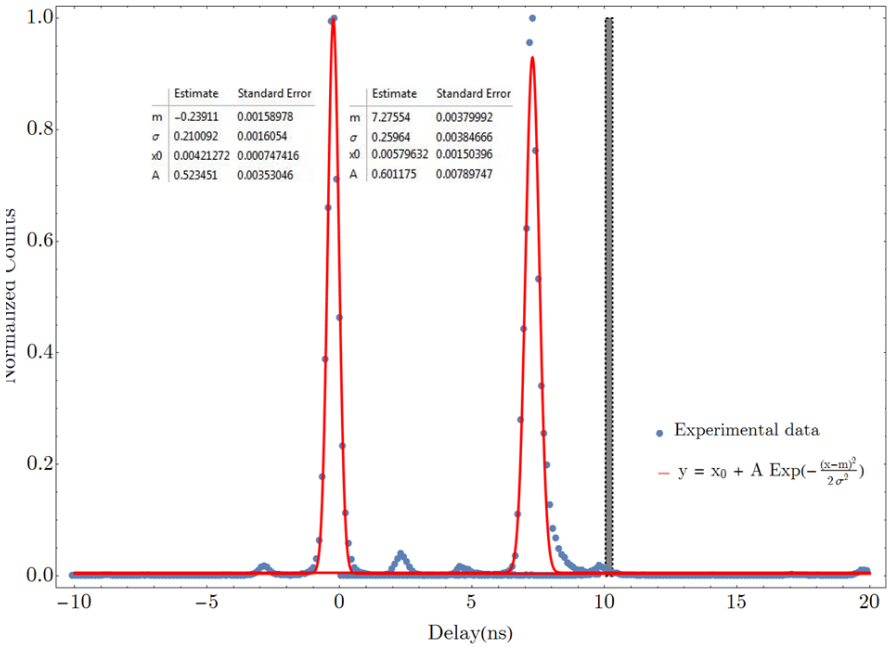
For the measurement of Δt_{AA}, Δt_{BA} and Δt_{BB} the procedure is analogous. In order to correct the delays introduced by the fibers, their lengths are measured with a fiber-meter. A length of (2.080 ± 0.004) m is obtained for the fiber connected to FC_A, and of (2.088 ± 0.004) m for the fiber connected to FC_B. The refractive index of the core, made of pure silica, is taken from literature [186]. The errors of the fiber lengths and refractive index are negligible with respect to the standard deviations of the arrival-time distributions. Figure 3.8 shows the acquired arrival-time distributions, together with the related Gaussian fits.


Estimate Standard Error
m 0.192388 0.00132516
σ 0.227735 0.00133934
x0 0.00333641 0.000597207
A 0.564876 0.002937
Estimate Standard Error
m 7.28467 0.00448474
σ 0.284997 0.0045457
x0 0.0072038 0.00169235
A 0.656768 0.00931054
Normalized Counts
Delay(ns)
Experimental data
y = x0 + A Exp(−(x−m)²/2σ²)

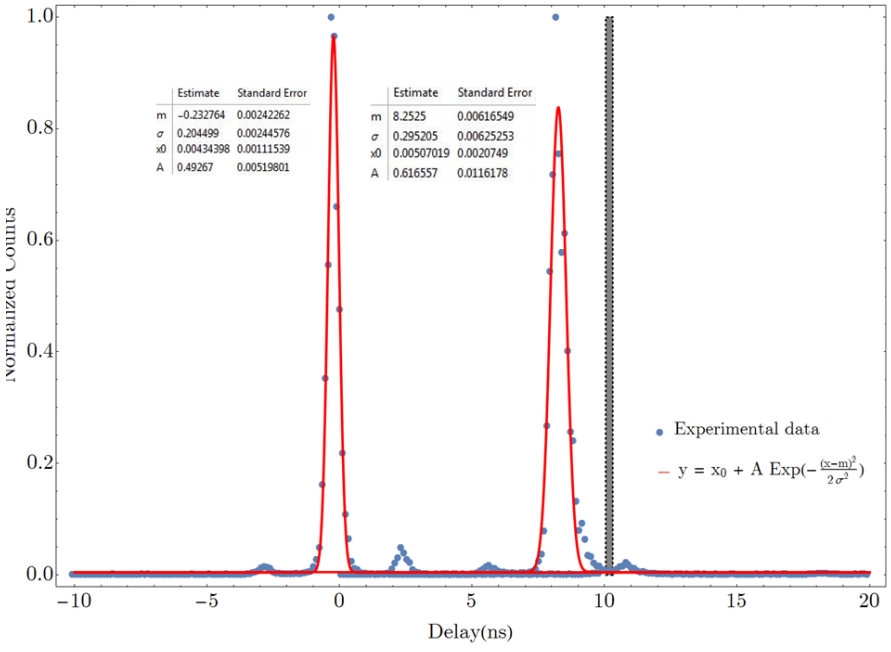
(a)


Estimate Standard Error
m 0.119572 0.0018948
σ 0.20262 0.00191272
x0 0.00310148 0.00085711
A 0.477518 0.00397596
Estimate Standard Error
m 8.30984 0.00706992
σ 0.330688 0.00718277
x0 0.00610997 0.00228542
A 0.698553 0.0135438
Normalized Counts
Delay(ns)
Experimental data
y = x0 + A Exp(−(x−m)²/2σ²)

(b)



(c)



(d)

Figure 3.8: **Arrival-time distributions.** The figures are related to the four possible time intervals Δt_{AA} (a), Δt_{AB} (b), Δt_{BA} (c) and Δt_{BB} (d). The arrival times at M_A or M_B (peaks on the left), after correcting for the fiber delay, and those at the final detectors D_A or D_B (peaks on the right) are reported on the x-axes. These times are expressed as delays with respect to the heralding photon detection. The two peaks in each figure are fitted with Gaussian functions (solid lines). The parameters of the fits are shown to the left of the corresponding peak. The black vertical bars indicate the time windows at which the photons would arrive at D_A or D_B if they travel the minimum distance between Alice and Bob twice.

In the plots, two secondary peaks for each main peak are observed, which are compatible with optical reflections in the setup. The counts composing the secondary peaks are approximately 5% of those in the corresponding main peaks. In the implementation of the communication game, therefore, a coincidence window of 1 ns is set so that the coincidences corresponding to the secondary peaks are not considered in the measurements.

It can be observed that the arrival-time distributions at D_A and D_B are slightly asymmetric. This might be due to the fact that the photons, in the free-space detection case, hit the edge of the active area of the photo-diode, thus producing some capacitive effect in the resulting electrical signal.

The employed detectors have a typical jitter time (standard deviation) of 0.149 ns (data from the manufacturer). Since each peak is obtained by coincidence detection between two APDs, a standard deviation of 0.210 ns is expected when only the effect of the jitter is considered. This value is compatible with those obtained for fiber-coupled detection, but is significantly lower than those obtained in the case of free-space detection. This mismatch is again ascribed to the imperfect alignment of the beam in the case of free-space detection.

3.5 Implementation of the TWCOP-based communication protocol

As the single-photon source in Figure 3.4 is probabilistic, a variation of the anonymous communication protocol detailed in Section 3.2 is implemented. In this variation, a communication interval of 0.5 s is set for each pair of bits x_i and y_i, and the source emission rate is reduced so as to have an average of approximately three detection events per communication interval. Here, the sum of the detections recorded by Alice and Bob is considered. If Alice (Bob) receives one or more photons during a given communication interval, she (he) infers that $r_i = 0$ $(= 1)$, and $r_i = 1$ $(= 0)$ otherwise. The emission rate is reduced by attenuating the pump laser with a rotating neutral density filter. Every 50

input bit pairs, the filter is rotated back such that the maximum emission rate is restored and the interferometric phase can be set to 0 by the piezo actuator in Alice's laboratory.

With this variation, the protocol becomes more robust to photon loss and experimental imperfections, as explained below. In each communication interval the source emits n_e photons at different times, of which n are detected. The photon statistics are assumed to be Poissonian. Within this assumption, the probability that Alice and Bob together detect n photons is:

$$\mathrm{p}(n) = e^{-m}\frac{m^n}{n!}, \tag{3.5}$$

with m average number of detections. An error occurs in any of the following cases: 1) no photon is detected at all, 2) both Alice and Bob detect photons, 3) all photons travel to the wrong output. In case 1 Alice (Bob) always infers a value of "1"("0") for the parity bit, r_i. The two values are swapped in case 2. Since the parity bit is random, this produces an error in the message bit transmission 50% of the time. In case 3 the wrong message bit is transferred 100% of the time. This results in the following probability of error per bit, p_b:

$$\mathrm{p}_b = \frac{\mathrm{p}(0)}{2} + \frac{\mathrm{p}_{AB}}{2} + \mathrm{p}_{aw}, \tag{3.6}$$

where $\mathrm{p}(0)$, p_{AB} and p_{aw} are the probabilities of cases 1, 2 and 3, respectively. The probabilities p_{AB} and p_{aw} may be written as:

$$\mathrm{p}_{AB} = \sum_{n=2}^{\infty}\mathrm{p}(n)\sum_{k=1}^{\infty}\binom{n}{k}(1-\mathrm{p}_s)^k\mathrm{p}_s^{n-k} = \tag{3.7}$$

$$= 1 + \mathrm{p}(0) - \sum_{n=0}^{\infty}\mathrm{p}(n)\mathrm{p}_s^n - \sum_{n=0}^{\infty}\mathrm{p}(n)(1-\mathrm{p}_s)^n,$$

$$\mathrm{p}_{aw} = \sum_{n=1}^{\infty}\mathrm{p}(n)(1-\mathrm{p}_s)^n = \tag{3.8}$$

$$= \sum_{n=0}^{\infty}\mathrm{p}(n)(1-\mathrm{p}_s)^n - \mathrm{p}(0),$$

where p_s is the probability of a single detection at the right output. After substituting the last two equations in Equation 3.6, a simple expression for p_b is obtained:

$$\mathrm{p}_b = \frac{1}{2}(1 + e^{-m\mathrm{p}_s} - e^{-m(1-\mathrm{p}_s)}). \tag{3.9}$$

This expression tends to $\frac{1}{2}$ for $m \to 0$, when the term $\frac{\mathrm{p}(0)}{2}$ becomes dominant, and for $m \to \infty$, when the main contribution to p_b is given by p_{AB}. In between these two regimes, p_b has a minimum at:

$$m_{opt_m} = \frac{1}{2\mathrm{p}_s - 1} log(\frac{\mathrm{p}_s}{1 - p_s}). \tag{3.10}$$

In certain situations, one might wish to optimize the probability that both Alice's and Bob's bits are correctly transferred. An error in the bit-pair transmission occurs whenever no photon is detected at all, or at least one photon in the encoding interval exits from the "wrong" port of BS_2. If p_w is the probability of the latter case, the probability of error in the bit-pair transfer, $\mathrm{p}_{b_{pair}}$, is:

$$\mathrm{p}_{b_{pair}} = \mathrm{p}(0) + \mathrm{p}_w \tag{3.11}$$

By replacing $\mathrm{p}(0)$ and p_w with their explicit expressions, the previous equation becomes:

$$\begin{aligned} \mathrm{p}_{b_{pair}} = \mathrm{p}(0) + \sum_{n=1}^{\infty} \mathrm{p}(n)(1 - \mathrm{p}_s^n) = \\ = 1 + e^{-m} - e^{-m(1-\mathrm{p}_s)}. \end{aligned} \tag{3.12}$$

This expression tends to 1 for $m \to 0$ and $m \to \infty$, and has a minimum for:

$$m_{opt_p} = -\frac{log(1 - \mathrm{p}_s)}{\mathrm{p}_s}. \tag{3.13}$$

Note that the difference between m_{opt_m} and m_{opt_p} tends to 0 as p_s tends to 1. Since the value of p_s at maximum visibility is approximately 0.96, m_{opt_m} and m_{opt_p} are both

around 3. This justifies the choice of the average number of detections per interval.

Several random sequences of 100 random input bit pairs are used to evaluate the probability that a given message bit is correctly transferred, $\mathrm{p}_c = 1 - \mathrm{p}_b$, which results as $\mathrm{p}_c = 0.88 \pm 0.01$. Correspondingly, the values $m = 3.34 \pm 0.06$ and $\mathrm{p}_s = 0.0935 \pm 0.008$ are found. From these two values, a theoretical probability $\mathrm{p}_{c_{th}} = 0.88 \pm 0.01$ can be calculated. This value is perfectly compatible with the experimental one. Note that, for $\mathrm{p}_s = 0.0935$, $m_{opt_m} = 3.06$ and the corresponding maximum value of p_c is $\mathrm{p}_{c_{max}} = 0.881$. Under the same experimental conditions, the probability $\mathrm{p}_{c_{pair}} = 1 - \mathrm{p}_{b_{pair}}$ is measured to be $\mathrm{p}_{c_{pair}} = 0.75 \pm 0.02$.

As $\mathrm{p}_b < 0.5$, a majority-voting error correction procedure can be implemented. This is performed for both $N = 3$ and $N = 5$ repetitions per message bit. The probability of correct bit transfer is measured to be $\mathrm{p}_c = 0.93 \pm 0.02$ and $\mathrm{p}_c = 1.00 \setminus -0.01$ in the two cases, respectively. The corresponding theoretical values are $\mathrm{p}_{c_{th}} = 0.969 \pm 0.004$ and $\mathrm{p}_{c_{th}} = 0.995 \pm 0.001$. All the experimental values are within 2 standard deviations from the corresponding theoretical expectation, thus confirming the validity of the assumed Poissonian model. An example in which Alice sends a 10×10 pixels image in black and white, corresponding to 100 bits, and Bob sends a sequence of 100 random bits is illustrated in Figure 3.9.

The described variation of the protocol with a probabilistic source does not compromise its security, at least in the case of the resource state being $|\psi_{in}\rangle$, for the same reason reported in Section 3.2 with regard to error correction. In the case that the resource state differs from $|\psi_{in}\rangle$, in general, the protocol might not be secure. If so, the amount of information obtained by Eve is increased due to error correction and the use of a probabilistic source with different numbers of emissions per communication interval. However, a large category of states leads to perfect security. In particular, for a given total number of photon n, perfect security is attained for any state of the form:

$$|\psi_{in}^{gen}\rangle = \sum_{k=0}^{n} \alpha_k (\hat{a}^\dagger)^k (\hat{b}^\dagger)^{n-k} |0\rangle, \tag{3.14}$$

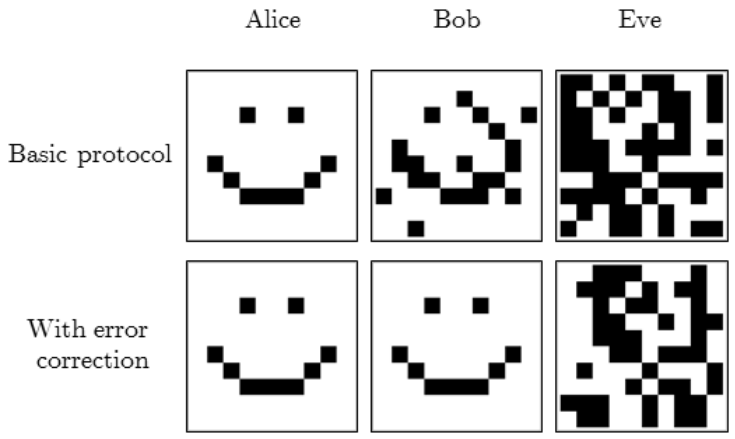


Figure 3.9: **Example of anonymous communication.** An example in which Alice sends a message in the form of a figure, and Bob a random sequence with the same length, is presented. The three columns report,from left to right, the figure sent by Alice, the one received by Bob, and the parity of the bits sent by Alice and Bob (the only piece of information an eavesdropper, Eve, can obtain from the superposition state). Two cases are shown: the basic protocol, where each bit pair is sent once with an average 88% probability of success and the error-corrected protocol, where each bit pair is sent five times, with an average 100% probability of success.

where $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are the photon creation operators in Alice's and Bob's spatial modes, and α_k are complex coefficients. In fact, after phase encoding, the state $|\psi_{in}^{gen}\rangle$ becomes:

$$|\psi_{in}^{gen}\rangle = \sum_{k=0}^{n} \alpha_k e^{i\pi kx} (\hat{a}^\dagger)^k e^{i\pi(n-k)y} (\hat{b}^\dagger)^{n-k} |0\rangle = \tag{3.15}$$
$$= e^{i\pi ny} \sum_{k=0}^{n} \alpha_k e^{i\pi k(x-y)} (\hat{a}^\dagger)^k (\hat{b}^\dagger)^{n-k} |0\rangle.$$

Beside the unmeasurable global phase, the state only contains the quantity $x - y$, which corresponds to the parity bit r, as $e^{i\pi k(x-y)} = e^{i\pi kr}$. Eve, therefore, can only obtain the parity bit but not the single bits x and y. Of course, even though the eavesdropper cannot obtain any information on the message bits, deviation from the resource state $|\psi_{in}\rangle$ leads to an increased error probability per message bit. If $n = 1$, the expression in 3.14 includes a single-photon unbalanced superposition state and superposition states with a bias phase between the two interferometric arms of the Mach-Zehnder. These states can be generated due to imperfections in the beam splitters, loss along the interferometric paths

or fluctuating phase between the two arms. If $n > 1$, the state $|\psi_{in}^{gen}\rangle$ expresses the state created by BS_1 when a Fock state $|n\rangle$ is sent to its input.

Perfect security is also extended to states represented by the density matrix:

$$\rho_{in} = \sum_{l=1}^{M} |\psi_{in}^{gen}\rangle_{l\,l}\langle\psi_{in}^{gen}|, \tag{3.16}$$

where $|\psi_{in}^{gen}\rangle_l$ is any state of the form described by Equation 3.14 for any n. The reason for that is that the global phase, containing information on the single bits, is not measurable for each of the $|\psi_{in}^{gen}\rangle_l$, and therefore is also not measurable for their statistical mixture, as there is no phase coherence between the different terms of the sum in Equation 3.16. This is exactly the state that is sent to Alice and Bob in the case of an SPDC-based source with a significant multi-photon emission, if the heralding detection is not number resolving. On the contrary, a quantum superposition of terms with different values of n is not secure. The typical example is coherent laser light for which, in principle, it is possible to read the global phase, if the eavesdropper shares a phase reference with the server.

The anonymity of the protocol is a direct consequence of its security, since Eve cannot tell which of the parties is transmitting the message and which one random bits if she cannot obtain the encoded bits.

3.5.1 Comparison to other quantum communication protocols

The described protocol can be considered an example of QSDC (see Section 1.6.2). The main differences from other QSDC protocols are that the direction of the communication is hidden from an external eavesdropper, i.e. the communication is anonymous, and the resource state involves only a single photon in superposition, exchanged only once between the two parties; while other protocols involve entangled states and/or ping-pong communication [152, 153, 154, 155].

The main drawback of the TWCOP-based protocol is the assumption that the resource state $|\psi_{in}\rangle$ is pre-shared between the parties, or is provided by a trusted server with secure

channels connecting the server to the parties. This sets strict limitations on the protocol applicability, which are generally not present in other QSDC schemes. Nevertheless, there are some situations in which the protocol could be applied. For example, in mobile networks some repeaters connected to a central server need to exchange information in order to make mobile communication possible [187]. This protocol offers secure and anonymous communication between the repeaters, given that the channels to and from the server are secure. As each bit is carried by one photon that is exchanged only once, it is possible to save resources, in particular, energy (number of photons) and time. Although error correction requires more photons to be exchanged per transferred bit, each iteration of the protocol still requires only one photon, and therefore, it might be advantageous compared to other protocols with the same level of redundancy.

Alternatively, the parties may perform resource state verification, which, however, would require an authenticated classical channel between them and the use of more complicated quantum devices. In order to ensure that the communication is secure, in fact, Alice and Bob have to first verify a random subset of the ensemble of states they share and then, if the verification is successful, transfer the bits. In order to do that, they need quantum memories, like in all QSDC protocols developed so far (see Section 1.6.2). Unfortunately, quantum memories are still not advanced enough to allow for such an application [125].

The TWCOP-based scheme can be converted to a QKD protocol if Alice also sends random bits instead of a meaningful message. In this case, the verification requirements for the state are relaxed, as this can be done after all the bits are transferred. For each iteration of the protocol, each party should decide at random whether to perform a measurement on the received photon, with probability p_{meas}, or encode and transfer one bit, with probability $\mathrm{p}_{comm} = 1 - \mathrm{p}_{meas}$. Then, the probability of bit transfer for both parties is p_{comm}^2. This QKD protocol presents many analogies with TF-QKD (see Section 1.6.1). The advantage with respect to TF-QKD is that only one light source is needed, as the users do not generate any quantum state. Furthermore, the protocol is based on single photons and not coherent states. Therefore the decoy-state method explained in

Section 1.6.1 is not required. A disadvantage is that, as the parties need to receive the photon from the server and then send it again to each other, the distance travelled by the photon is larger than that in TF-QKD, and therefore, the dependence of the secure key rate on the overall transmission of all quantum channels employed is definitely worse, even though an exact calculation has not been yet performed. Both schemes share the same technical difficulty in terms of phase stability of the interferometric paths necessary for the implementation, which becomes more and more challenging as the size of the interferometer to be stabilized increases. The phase fluctuations for TF-QKD in fact were characterized to be 2.4 rad/ms and 6.0 rad/ms (standard deviation) in a 100 km-arm and 500 km-arm fiber interferometer, respectively [129]. These fluctuations would induce high error rates in the TWCOP-based protocol as well, which cannot be corrected by the error correction schemes described in the previous sections. Nevertheless, the phase noise can be reduced by suitable stabilization techniques. Active stabilization in a fiber-based single-photon interferometer with 6 km-long arms has shown a residual phase fluctuation of 0.06 rad [188], even though only in laboratory environment. The same technique can be applied to the TWCOP-based protocol, but it is not clear how this would perform in real-world conditions and what is the maximum interferometer size to which it can be applied.

The achieved transmission rate, without error correction is 2 bits/s, over a distance of about 1.5 m. New developments in the realization of single-photon fast switches [189], low-jitter and high-efficiency single-photon detectors [190], and deterministic single-photon sources [191] can dramatically improve these values.

3.6 Summary of the results

In the experimental work described in this chapter, the following contributions have been made:

- It was experimentally demonstrated, for the first time, that a single quantum particle in superposition (a photon) allows for two-way communication between distant

parties, following the theoretical proposal in [181]. The performed measurements exclude the possibility that the particle travels back and forth between the parties or that more than one particle are exchanged simultaneously.

- Based on the aforementioned two-way communication scheme, a novel anonymous and secure quantum communication protocol was developed and implemented. The basic assumption for security is that the parties share many copies of a single-photon superposition state. The proof-of-principle implementation achieves a rate of 2 bits/s over a distance in free space of 1.5 m.

- A suitable error correction scheme for the protocol based on a probabilistic single-photon source, in combination with bit redundancy and majority voting, was developed and analysed.

Chapter 4

A novel mediated SQKD protocol based on interaction-free measurements

The second project described in this thesis is the development and implementation of a novel mediated SQKD protocol, in which the two users, Alice and Bob, do not need to perform any quantum-mechanical operation nor generate quantum states, and therefore are considered "classical". The quantum resources are provided by an external untrusted server, which is required to prepare single photons in superposition and send them to the parties. Contrary to the previously proposed SQKD protocols (see Chapter 1), the quantum resources necessary for the key distribution task are feasible within current technology.

The following sections illustrate this work, first by describing the protocol and the experimental setup used for its implementation, then by explaining the adopted methods for security analysis and finally by presenting the obtained experimental results, which mainly consist in computing the secret key rate for the implemented protocol.

The protocol was developed in collaboration with the quantum information theory group of Prof. Paulo Mateus in Lisbon and experimentally implemented in Vienna, which

represents to date the first experimental demonstration of a mediated SQKD protocol. This sets a milestone in SQKD and paves the way for the practical realization of QKD protocols to be used in situations where the resources of the users are necessarily limited.

This chapter is an adaptation of the preprint "Experimental quantum cryptography with classical users" by Francesco Massa et al., posted on arXiv under the identification number *1908.01780*, from which therefore large portions of text and all figures are taken.

4.1 The protocol

The protocol involves three parties: two classical users, or clients, Alice and Bob, whose aim is to exchange a secret cryptographic key, and a quantum server, which provides the quantum resources for this purpose. Furthermore, Alice and Bob are able to communicate through a classical authenticated channel, while the server can send unauthenticated classical messages to the users. The scheme consists of a key-generation step and a verification step. In the former, the two parties exchange quantum signals with the server with the purpose of establishing a shared raw key, in the latter, after the exchange is over, the parties communicate to verify the server honesty and the absence of eavesdroppers.

A sketch of the scheme is depicted in Figure 4.1. In the key-generation phase, the server sends to Alice and Bob a single photon in a balanced superposition of their respective locations, i.e. in the resource state of Equation 3.1. Each user can independently choose to perform two actions: "detect" (D) or "reflect" (R). In the former case, the photon travels to a detector controlled by the user, in the latter, the photon is sent back to one of the two inputs of a balanced beam splitter controlled by the server, at whose outputs two detectors, D_0 and D_1, are placed. When both clients choose to reflect, single-photon interference occurs at the beam splitter, with the relative phase of the two interfering photon amplitudes tuned such that only detector D_0 can click. However, in the ideal case of perfect detection efficiency, when only one of the clients chooses to measure the photon and does not detect any, the photon collapses into the other client's location. This corresponds to performing an interaction-free measurement [192, 193, 194], which

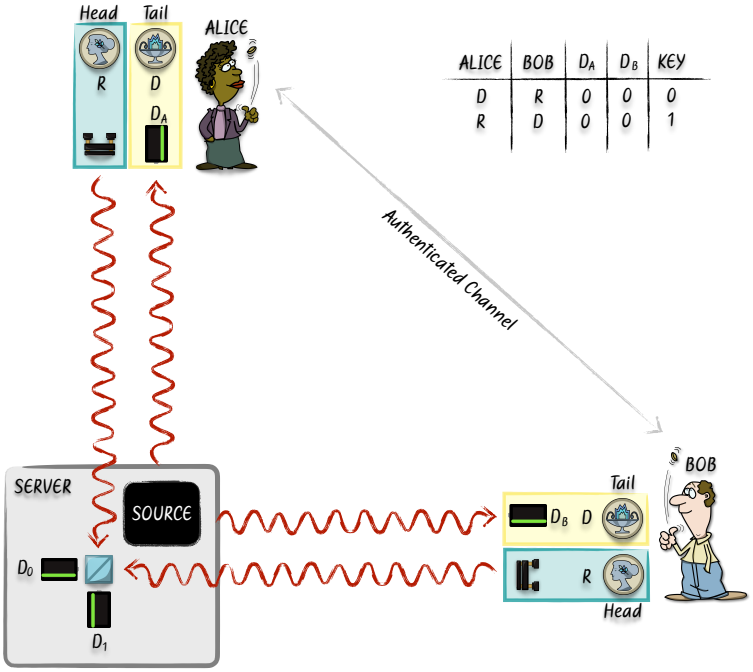


Figure 4.1: **Scheme of the protocol.** Two parties, Alice and Bob, share a single-photon superposition state distributed by a server. For each iteration of the protocol, Alice and Bob flip a coin to randomly decide whether sending the photon to the detector D_A and D_B, respectively, or reflecting it back to the server. The server controls two detectors, D_0 and D_1 and a beam splitter, at which single-photon interference occurs when both parties chose to reflect. In this case, only detector D_0 can click. A click at D_1 means that one of the parties decided to detect the photon and his or her detector did not click. Consequently, a key digit is generated according to the table in the figure. Alice and Bob communicate through an authenticated channel to verify the honesty of the server and the absence of eavesdroppers.

suppresses single-photon interference at the server and allows both detectors D_0 and D_1 to click with non-zero probability. A click at detector D_1, therefore, enables each user to deduce the action of the other one, thus allowing for the establishment of a shared secret-key digit.

The detailed steps of the key-generation phase are described below.

1) The server sends single photons in superposition to the users at predetermined regular intervals. Each interval constitutes a single round of the protocol.

2) For each round, Alice and Bob randomly choose between the two actions R and D. This choice determines the user's key bit in the following way: Alice stores a key bit

0 if she chooses to detect, and 1 if she reflects. Bob's actions are complementary: he stores 0 for "reflection", and 1 for "measurement".

3) The server measures the photon coming from Alice/Bob and announces the following results: "0", if detector D_0 clicks, "1", if detector D_1 clicks, "v", if no detector clicks, and "m", if more than one click is observed. The latter two cases can arise due to experimental imperfections or the action of an adversary.

4) Alice and Bob only keep the key bit if the message received from the server is "1" and they did not detect a photon, thus obtaining the raw key.

Let N be the total number of iterations. At the end of each iteration, the server announces the result, and each user compares it with their own action. If the server announces "1", and a client either reflected, or measured vacuum, then the client's action is said to be "consistent" with the server's result, and no information is sent to the other client. Otherwise, the user detecting inconsistency announces it to the other one and the corresponding round is discarded.

When the server announces "1" and both users' actions are consistent with such outcome, then a raw-key digit is generated. The probability of such case is indicated by $p(1)$. If the server announces "1" and both parties reflected or both measured vacuum, an error in the key occurs. Note that, unlike the majority of QKD protocols, no use of the authenticated channel is necessary for raw-key generation.

Alice and Bob choose each action (R or D) independently at random, with probability 1/2. Thus, the iterations in which the key can potentially be generated (associated to the choices RD and DR) occur with probability 1/2. In these cases, ideally, there is a probability of 1/2 that the photon collapses in the spatial mode associated to the user that chooses to reflect. Finally, the reflected photon has at best a further probability of 1/2 to reach detector D_1. Therefore, $p(1)$ is at best 1/8, which can be reduced by experimental imperfections, eavesdropping or the action of an adversarial server.

For the rest of $(1 - p(1))N$ iterations, the users exchange the information of their actions and detection results. This information is used for verification purposes. In

particular, by checking the statistics of detection in the *DD* case, Alice and Bob can verify if the received state matches the resource state that the server is supposed to send. This state, in principle, can also have a vacuum and a multi-photon component. The former is due to loss in the quantum channels connecting the server and the users, the latter is due to imperfections in the photon source. In practice, after a characterization of the channels and of the source, but prior to the start of the protocol, the server can declare the probability of sending vacuum, one or more photons. If the users do not verify these values, they assume eavesdropping and/or a dishonest server, and, consequently, discard the key. Additionally, Alice and Bob can use the shared information to test the behaviour of the server after they choose their actions, i.e. whether he uses a balanced beam splitter with balanced detectors and honestly declares the detections at D_0 and D_1. Again, if the test reveals inconsistencies, it means that either the server is cheating, or that an eavesdropper is disturbing the communication.

Note that it is enough that only one user, say Alice, performs the verification with the information received from the other. This allows for a reduction of the communication complexity. In addition to his action choices and results for the $(1 - p(1))N$ iterations, Bob will also send the messages announced by the server over all the iterations. Alice will proceed with the verification procedure only if all of Bob's messages match with hers.

The users can exchange full information on their actions for a randomly chosen fraction τ of N_{raw} iterations to perform a direct estimation of the probability of exchanging a key digit, p_{key} and the probability of error in the key, p_{err}. Alternatively, Alice can use the information received from Bob during the verification phase to evaluate p_{key} and p_{err} without the need to discard any key digit (see Section 4.4).

4.2 Experimental setup

The experimental setup for the implementation of the protocol is depicted in Figure 4.2. After setting its polarization to horizontal (parallel to the optical table) a single photon is sent to a beam splitter that creates the superposition between Alice's and Bob's locations.

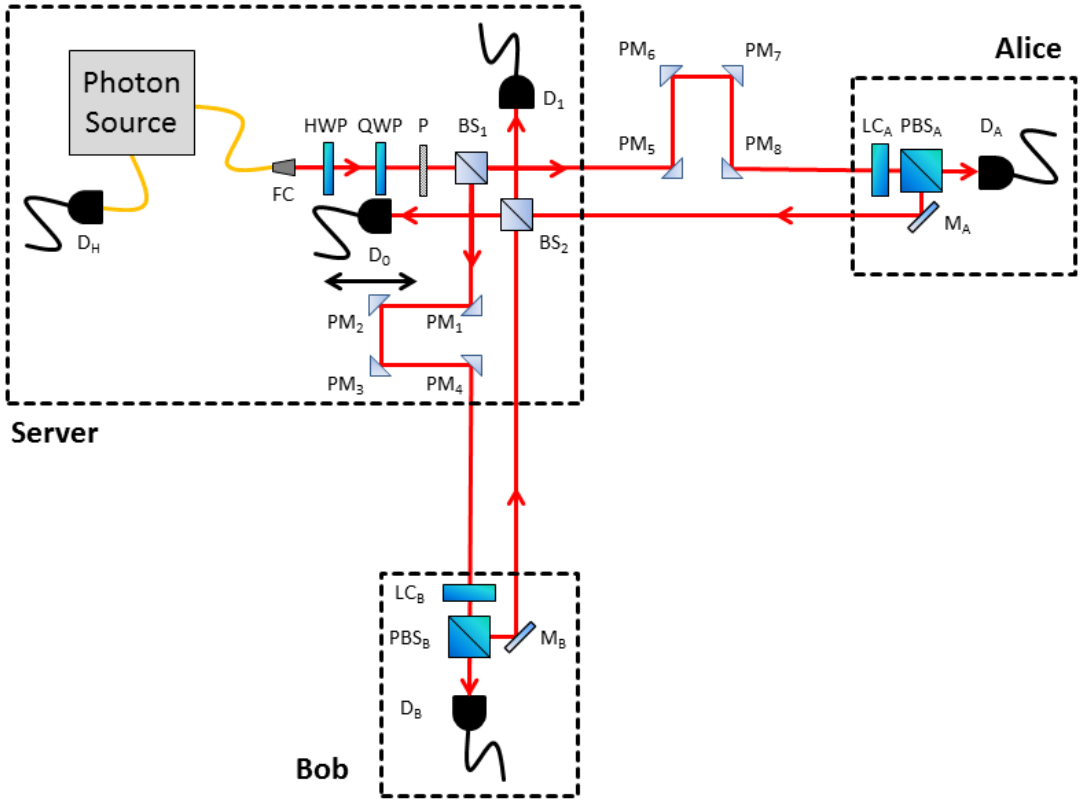


Figure 4.2: **Setup for the implementation of the protocol.** The regions of space occupied by Alice, Bob and the server are delimited by dashed black lines. The path of the photons is indicated by red lines. The server uses a heralded single-photon source and a beam splitter (BS_1) to produce the superposition state that is sent to Alice and Bob. Each of the parties employs a liquid crystal phase shifter (LC) and a polarizing beam splitter (PBS) to randomly switch between "detection" and "reflection". The server collects the reflected photons at a second beam splitter (BS_2), where single-photon interference takes place when both parties choose "reflection". The server records the detections at the detectors D_0 and D_1 and announces the results to the parties via a classical channel. The initial half-wave plate, quarter-wave plate and polarizers are used to set the photon polarization to horizontal. A trombone delay line (prism mirrors PM_1, PM_2, PM_3, PM_4), accompanied by a fixed trombone (PM_5, PM_6, PM_7, PM_8) is used to obtain full overlap at BS_2 of the two photon amplitudes travelling the interferometer. A piezo actuator is mounted on the trombone delay line for active phase stabilization every 100 s.

Each of the parties controls a switch composed of a liquid-crystal cell (same models as described in Chapter 3) at 45° with respect to horizontal and a polarizing beam splitter. The phase retardation between the two axes of the phase shifter can be switched between 0 and π by means of a voltage signal. Consequently, the photon polarization is rotated by 0° or 90°, respectively. In the former case, the photon is steered to a fiber-coupled avalanche photo-diode (APD) for detection, D_A for Alice or D_B for Bob, otherwise it is reflected by the PBS and travels back to the server. The photons going back to the server impinge on a second beam-splitter, at whose outputs two fiber-coupled APDs, D_0 and D_1, are placed (all the APDs are Excelitas SPCM AQRH-13). The setup, therefore, implements a folded Mach-Zehnder interferometer.

The phase between the two arms of the interferometer is set such that detector D_0 clicks whenever Alice and Bob both decide to reflect back the photon. The interferometer is passively stabilized so that the phase is constant for about 100 s. After this time, the server re-sets the phase to the initial value by means of a piezo actuator that is mounted on a trombone delay line. The trombone delay line is used to finely tune the difference between the two interferometric paths so that the two photon amplitudes in the interferometer overlap at the second beam splitter.

The single photons are provided by the source described in Section 3.3.1. The source produces photon pairs, with a photon of each pair heralding the presence of its twin in the inteferometer. All the detections considered in this chapter are therefore in coincidence with the heralding detector D_H.

The server sets intervals of 0.5 s in which Alice and Bob can decide to either measure or reflect the photons. At the end of each interval, the server announces "0", "1", "v" or "m", according to the number of clicks at its detectors.

The probabilistic nature of the source implies that, in each interval, multiple non-simultaneous single-photon emissions can occur. In some intervals, therefore, the total number of detections results higher than one. By attenuating the pump power, the output rate of the source is reduced so that the total average number of detections among the four detectors of the setup is about 0.2 per interval, in order to lower the

probability of multi-photon emission. Given this detection rate and a measured detection efficiency of 58% at each detector (68% detector efficiency, 85% fiber-coupling efficiency), the probability of more than two non-simultaneous single-photon emissions within one interval is considered negligible. With this assumption, the average number of emissions per interval is calculated to be 0.35.

During the phase stabilization stage, occurring every 100 s, the server increases the source pump power so that about 10^4 photons are detected per communication interval. Alternatively, the server might use strong laser pulses. During this process, the parties must always reflect the received photons.

4.3 Security Analysis

4.3.1 Assumptions and Notation

Let N be the total number of rounds of the protocol and p(1) be the probability of the server announcing "1" when no party received a click upon detection. Then $N_{raw} = \mathrm{p}(1)N$ rounds are potentially used for key generation. Alice and Bob may choose to use a subset of the raw key of size μ to directly estimate the QBER and, consequently, the secure key rate. The portion of the raw key remaining after the parameter-estimation step is the sifted key, of the length $N_{sift} = N_{raw} - \mu$. Let the random variables $\mathcal{R}_A$ and $\mathcal{R}_B$ denote Alice's and Bob's respective sifted keys. Completing the sifting stage, however, does not guarantee the following requirements for the shared key to be a perfectly secure secret key:

(i) Alice and Bob share exactly the same uniformly distributed key. The parameter-estimation step only sets the degree of the correlation between Alice's and Bob's random variables $\mathcal{R}_A$ and $\mathcal{R}_B$ of the sifted key.

(ii) The shared key is completely uncorrelated with Eve (including the server). Again, the parameter-estimation step only gives upper limits to the correlation with Eve.

Both problems are treated classically, as they are applied to classical random variables.

Problem (i) is solved using standard error correction techniques (often called information reconciliation), which turn $\mathcal{R}_A$ and $\mathcal{R}_B$ into $\tilde{X}_A$ and $\tilde{X}_B$ such that $\tilde{X}_A = \tilde{X}_B$. Problem (ii) is solved by further applying privacy amplification techniques, resulting in random variables $X_A = X_B$ uncorrelated with Eve, giving the final secret key of length N_{sec}.

The security of the protocol is proved under the assumption that anything outside of Alice's and Bob's private laboratories, including the quantum server, is completely untrusted. The security level of the key shared between Alice and Bob is given by the parameter ϵ, which quantifies the deviation of the key $X_A = X_B$ from a perfectly secure key [195]. The security criterion requires ϵ to tend to zero as the number of rounds N tends to infinity, thus obtaining perfectly secret key in the asymptotic scenario. One can compute the sifted key rate as $r' = \lim_{N\to\infty} N_{sec}/N_{sif} = S(A|C) - S(A|B)$, where S indicates the conditional Von Neumann entropy, and A, B and C stand for Alice, Bob and Charlie, a third party, which can be the server or an eavesdropper. In other words, the sifted key rate is given by the difference between the amount of information that leaks from Alice to a third party and the amount of information that is transferred from Alice to Bob. The quantity $S(A|B)$ can be easily computed using the probabilities $p_{i,j}$ of Alice and Bob establishing the raw-key bit values i and j, respectively. Further, the secret key rate is defined as $r = N_{sec}/N = r'(N_{sift}/N)$, which is the same as the sifted key rate in the asymptotic regime, as the number μ, albeit big, is still finite, and therefore $N_{sif} = N - \mu \approx N$, for $N \to \infty$.

In the realistic case of limited resources, however, where Alice and Bob can exchange only a finite number of key digits, imperfect parameters must be taken into account. Let us then denote ϵ_{PE} as a given error tolerance for the parameter estimation and define $\delta(\epsilon_{PE})$ as the confidence interval associated to ϵ_{PE}. This means that the probability that the observed parameters distance more than δ from the actual values is ϵ_{PE}. Furthermore, let ϵ be the desired security of the final secret key, and ϵ_{EC} be the maximal probability that error correction fails, i.e. that the two sequences of bits X_A and X_B do not coincide. All of these are given by the users. Then, after μ rounds being wasted for direct parameter

estimation, it can be shown that [195]:

$$r \geq \frac{\mathrm{p}(1)N - \mu}{N}\left(S(A|C) - \frac{\mathtt{leak}_{EC} + \Delta}{\mathrm{p}(1)N - \mu}\right), \tag{4.1}$$

where

$$\Delta = 2\log_2\left(\frac{1}{2(\epsilon - \epsilon_{EC} - \epsilon')}\right) + 7\sqrt{(\mathrm{p}(1)N - \mu)\log_2(2/(\epsilon' - \epsilon_{PE}))}, \tag{4.2}$$

and ϵ' is arbitrary, meaning that it is chosen by the user to maximize the expression but bound by $\epsilon - \epsilon_{EC} > \epsilon' > \epsilon_{PE} \geq 0$. In the above expression, $S(A|C)$ is minimized over all observable statistics within the given confidence interval. The value $\mathtt{leak}_{EC}$ represents the number of (classical) bits exchanged between Alice and Bob during error correction. It is possible to take $\mathtt{leak}_{EC}/(\mathrm{p}(1)N - \mu) = (1.2)h(Q)$ [195], with h binary Shannon entropy and $Q = \mathrm{p}_{err}/\mathrm{p}(1)$, with p_{err} the probability to generate opposite key bits during the entire protocol. Note that μ is also a function of ϵ_{PE}, since in order to obtain higher precision on the parameters, a higher number of key digits needs to be sacrificed.

In order to compute the secret key rate described above, one needs to compute $S(A|C)$. Before proceeding with this computation, let us first define some useful terminology. Let us denote the Hilbert spaces corresponding to Alice's and Bob's equipment as:

$$\begin{aligned}\mathcal{H}_A &= \mathrm{span}\{|D_c\rangle_A, |D_v\rangle_A, |D_\ell\rangle_A, |D'_\ell\rangle_A, |D'_c\rangle_A, |R\rangle_A\},\\ \mathcal{H}_B &= \mathrm{span}\{|D_c\rangle_B, |D_v\rangle_B, |D_\ell\rangle_B, |D'_\ell\rangle_B, |D'_c\rangle_B, |R\rangle_B\},\end{aligned} \tag{4.3}$$

respectively. Here, $|D_c\rangle$ and $|D_v\rangle$ denote the states of a detector, the first corresponding to the case of a photon causing a click, and the second corresponding to the case when there were no photons, resulting in a no-click. The detectors' state corresponding to the case when an incoming photon was lost is denoted as $|D_\ell\rangle$. The state $|D'_\ell\rangle$ corresponds to a loss, while $|D'_c\rangle$ to a click of the photon at a later time $t' > t$ when two non-simultaneous photons were emitted by the source at times t and t'. Finally, $|R\rangle$ denotes the state of a reflecting mirror. Note that $|D_c\rangle$ and $|D'_c\rangle$, are not distinguishable between each other,

since in the realized implementation, Alice and Bob do not keep track of the detection times. The same occurs for the three states, $|D_v\rangle$, $|D'_\ell\rangle$ and $|D'_\ell\rangle$, as Alice and Bob are not able to distinguish whether a detector did not click because there were no photons present, or they were lost.

The server's Hilbert space $\mathcal{H}_S = \text{span}\{|0\rangle_S, |1\rangle_S, |v\rangle_S, |m\rangle_S\}$ consists of macroscopic orthogonal states modeling classical messages "0", "1", "v" (vacuum) and "m" (multiple clicks), respectively. Additionally, the server can use an ancilla system, denoted by C and spanned by the Hilbert space $\mathcal{H}_C$, and entangle it with the photons sent to Alice and Bob to extract information on the exchanged key.

Let us assume Alice tosses a fair coin to decide whether she will detect or reflect the photon, and set the initial state of the apparatus accordingly, resulting in a statistical mixture of the two states, $|D_v\rangle_A$ and $|R\rangle_A$, and analogously for Bob. Without loss of generality, the coin states can always be included into the macroscopic description of the apparatus states such that the purified initial state of Alice's apparatus is

$$|\phi_0\rangle_A = \frac{1}{\sqrt{2}}\big(|D_v\rangle_A + |R\rangle_A\big), \tag{4.4}$$

and analogously for Bob, making their joint state as

$$|\phi_0\rangle_{AB} = \frac{1}{2}\Big(|D_v,R\rangle_{AB} + |R,D_v\rangle_{AB} + |D_v,D_v\rangle_{AB} + |R,R\rangle_{AB}\Big). \tag{4.5}$$

Note that due to possible imperfect single-photon sources, and the presence of adversaries, the number of photons present is not necessarily fixed to be one. Thus, a number basis will be used to describe the photonic states. The overall Fock space of the photons in Alice's and Bob's arms will be decomposed as:

$$\mathcal{F}_f = \text{span}\{|0,0\rangle_f, |1,0\rangle_f, |0,1\rangle_f, |2,0\rangle_f, |1,1'\rangle_f, |1',1\rangle_f, |0,2\rangle_f\} \oplus \mathcal{F}_f^k, \tag{4.6}$$

where $|0,0\rangle_f \equiv |v\rangle_f$ represents the vacuum state, $|1,0\rangle_f$ ($|0,1\rangle_f$) represents the state with a single photon in Alice's (Bob's) arm and no photon in Bob's (Alice's) arm,

whereas $|2,0\rangle_f$, and $|0,2\rangle_f$, are associated to two non-simultaneous photons in Alice' and Bob's arms, respectively. The states $|1,1'\rangle_f$ and $|1',1\rangle_f$ represent the case of two non-simultaneous photons with the first one going to Alice while the second to Bob and vice-versa, respectively. $\mathcal{F}_f^k$ denotes the sub-space corresponding to the multi-photon case of $k > 2$ photons.

4.3.2 Extraction of the secret key

The security analysis is conducted by considering a probabilistic source, which emits vacuum state with probability p_0, a single photon with probability p_1, and two non-simultaneous photons with probability p_2, within a communication interval of duration T. The state produced by the source is then:

$$|\phi_0\rangle_f = \sqrt{\mathrm{p}_0}\,|v\rangle_f + \sqrt{\frac{\mathrm{p}_1}{T}}\int_0^T \hat{a}^\dagger(t)\,|v\rangle_f\,\mathrm{d}t + \frac{\sqrt{\mathrm{p}_2}}{T}\int_0^T\int_0^T \left(\frac{\hat{a}^\dagger(t)\hat{a}^\dagger(t')}{\sqrt{2}}\,|v\rangle_f\right)\mathrm{d}t\;\mathrm{d}t', \quad (4.7)$$

where $\hat{a}^\dagger(t)$ and $\hat{a}^\dagger(t')$ represent photon creation at times t and $t' > t$, respectively. The probability to emit higher numbers of photons is considered negligible and therefore not included in the analysis, i.e., $\mathrm{p}_0 + \mathrm{p}_1 + \mathrm{p}_2 \approx 1$.
However, instead of the above initial photon state, the untrusted server can prepare the following photonic state, entangled with the ancilla,

$$|\phi_0\rangle_{fC} \;=\; \sqrt{\mathrm{p}_0}\,|v\rangle_f\,|d_v\rangle_C + \sqrt{\mathrm{p}_1}\,|1\rangle_f\,|d_1\rangle_C + \sqrt{\mathrm{p}_2}\,|2\rangle_f\,|d_2\rangle_C\,, \quad (4.8)$$

where $|v\rangle_f$ is the photon vacuum state, $|1\rangle_f = \hat{a}^\dagger(t)\,|v\rangle_f$, $|2\rangle_f = \hat{a}^\dagger(t)\hat{a}^\dagger(t')\,|v\rangle_f$, and the ancilla states are $|d_i\rangle_C \in \mathcal{H}_C$. After passing through the first 50/50 beam splitter of the interferometer, the above state becomes:

$$\begin{aligned}|\phi_0\rangle_{fC} = &\sqrt{\mathrm{p}_0}\,|v\rangle_f\,|d_v\rangle_C + \sqrt{\frac{\mathrm{p}_1}{2}}\left(|1,0\rangle_f + |0,1\rangle_f\right)|d_1\rangle_C + \\ &+\frac{\sqrt{\mathrm{p}_2}}{2}\left(|2,0\rangle_f + |1,1'\rangle_f + |1',1\rangle_f + |0,2\rangle_f\right)|d_2\rangle_C\,.\end{aligned} \quad (4.9)$$

Upon possible further action of the adversary, the above state evolves to the normalized state:

$$|\phi_0\rangle_{fC} \longrightarrow \sum_{\substack{a,b\geq 0 \\ a+b\leq 2}} |a,b\rangle_f \, |c_{a,b}\rangle_C \tag{4.10}$$

where $|c_{a,b}\rangle_C \in \mathcal{H}_C$ (not necessarily orthogonal, nor normalized states) are associated to the cases when there are a and b photons entering Alice's and Bob's arms, respectively. Nevertheless, the states $|c_{a,b}\rangle_C$ are arbitrary and contain any number of photons. Therefore, the overall state before the photon(s) enter Alice's and Bob's laboratories is:

$$|\phi_0\rangle_{ABfC} = |\phi_0\rangle_{AB} \otimes |\phi_0\rangle_{fC} \, . \tag{4.11}$$

Let us denote Alice's and Bob's respective detectors' efficiencies as p_d^A and p_d^B, with $\mathrm{p}_\ell^A = 1 - \mathrm{p}_d^A$ and $\mathrm{p}_\ell^B = 1 - \mathrm{p}_d^B$. The individual actions (say, for Alice) in the practical scenario are:

$$\begin{gathered} |D_v\rangle \, |0\rangle \to |D_v\rangle \, |0\rangle \, , \\ |D_v\rangle \, |1\rangle \to \left(\sqrt{\mathrm{p}_\ell^A} \, |D_\ell\rangle + \sqrt{\mathrm{p}_d^A} \, |D_c\rangle \right) |0\rangle \, , \\ |D_v\rangle \, |2\rangle \to \left(\mathrm{p}_\ell^A \, |D_\ell D'_\ell\rangle + \sqrt{\mathrm{p}_\ell^A \mathrm{p}_d^A} \, |D_c D'_\ell\rangle + \sqrt{\mathrm{p}_\ell^A \mathrm{p}_d^A} \, |D_\ell D'_c\rangle + \mathrm{p}_d^A \, |D_c D'_c\rangle \right) |0\rangle \, , \\ |R\rangle \, |0\rangle \to |R\rangle \, |0\rangle \, ; |R\rangle \, |1\rangle \to |R\rangle \, |1\rangle \, ; |R\rangle \, |2\rangle \to |R\rangle \, |2\rangle \, , \end{gathered} \tag{4.12}$$

where primed and unprimed states of the apparatuses correspond to times t' and t, respectively. Therefore, upon applying the operator U_1, given in terms of Alice's and Bob's local actions described by (4.12), the state $|\phi_1\rangle_{ABfC} = U_1 \, |\phi_0\rangle_{ABfC}$ is obtained.

Following this, the adversary will apply a quantum operator to the returning photon state, whose action is defined as:

$$\mathcal{I} \, |a', b'\rangle_f \, |c_{a,b}\rangle_C = |0\rangle_S \, |e^{a,b}_{a',b'}\rangle_C + |1\rangle_S \, |f^{a,b}_{a',b'}\rangle_C + |v\rangle_S \, |g^{a,b}_{a',b'}\rangle_C + |m\rangle_S \, |h^{a,b}_{a',b'}\rangle_C \, , \tag{4.13}$$

where states $|e^{a,b}_{a',b'}\rangle_C , |f^{a,b}_{a',b'}\rangle_C , |g^{a,b}_{a',b'}\rangle_C , |h^{a,b}_{a',b'}\rangle_C \in \mathcal{H}_C$ are again not necessarily normal-

ized, nor orthogonal. Note that, due to the action of U_1, the photon numbers a, b are no longer correlated to $a', b' \in \{0, 1, 2\}$; nevertheless, the inequality $a' + b' \leq 2$ still holds.

Only the the key-generation rounds are of interest for the computation of the secret key rate, therefore only the events, in which the server announces "1" and neither Alice nor Bob receives a click will be here considered. Hence, by omitting $|1\rangle_S$, the final density operator (without the off-diagonal terms) of the system ABC is:

$$\begin{aligned}\rho_{ABC} = \frac{1}{\mathcal{N}} \Big[& |D_v,R\rangle_{AB}\langle D_v,R| \otimes |k_{0,0}\rangle_C\langle k_{0,0}| + |R,D_v\rangle_{AB}\langle R,D_v| \otimes |k_{1,1}\rangle_C\langle k_{1,1}| + \\ & + |D_\ell,R\rangle_{AB}\langle D_\ell,R| \otimes |k^1_{0,0}\rangle_C\langle k^1_{0,0}| + |R,D_\ell\rangle_{AB}\langle R,D_\ell| \otimes |k^1_{1,1}\rangle_C\langle k^1_{1,1}| + \\ & + |D'_\ell,R\rangle_{AB}\langle D'_\ell,R| \otimes |k^2_{0,0}\rangle_C\langle k^2_{0,0}| + |R,D'_\ell\rangle_{AB}\langle R,D'_\ell| \otimes |k^2_{1,1}\rangle_C\langle k^2_{1,1}| + \\ & + |D_\ell D'_\ell,R\rangle_{AB}\langle D_\ell D'_\ell,R| \otimes |k^3_{0,0}\rangle_C\langle k^3_{0,0}| + |R,D_\ell D'_\ell\rangle_{AB}\langle R,D_\ell D'_\ell| \otimes |k^3_{1,1}\rangle_C\langle k^3_{1,1}| + \\ & + |D_v,D_v\rangle_{AB}\langle D_v,D_v| \otimes |k_{0,1}\rangle_C\langle k_{0,1}| + |R,R\rangle_{AB}\langle R,R| \otimes |k_{1,0}\rangle_C\langle k_{1,0}| + \\ & + |D_\ell,D_v\rangle_{AB}\langle D_\ell,D_v| \otimes |k^1_{0,1}\rangle_C\langle k^1_{0,1}| + |D_v,D_\ell\rangle_{AB}\langle D_v,D_\ell| \otimes |k^2_{0,1}\rangle_C\langle k^2_{0,1}| + \\ & + |D_\ell,D'_\ell\rangle_{AB}\langle D_\ell,D'_\ell| \otimes |k^3_{0,1}\rangle_C\langle k^3_{0,1}| + |D'_\ell,D_\ell\rangle_{AB}\langle D'_\ell,D_\ell| \otimes |k^4_{0,1}\rangle_C\langle k^4_{0,1}| + \\ & + |D_\ell D'_\ell,D_v\rangle_{AB}\langle D_\ell D'_\ell,D_v| \otimes |k^5_{0,1}\rangle_C\langle k^5_{0,1}| + |D_v,D_\ell D'_\ell\rangle_{AB}\langle D_v,D_\ell D'_\ell| \otimes |k^6_{0,1}\rangle_C\langle k^6_{0,1}| \Big]. \end{aligned} \tag{4.14}$$

The states $|k_{i,j}\rangle_C$ are associated to the cases when Alice establishes the value i and Bob

j as a key bit, and are given by:

$$
\begin{aligned}
|k_{0,0}\rangle &= \frac{1}{2}\left[|f^{0,0}_{0,0}\rangle + |f^{0,1}_{0,1}\rangle + |f^{0,2}_{0,2}\rangle\right], & |k_{1,1}\rangle &= \frac{1}{2}\left[|f^{0,0}_{0,0}\rangle + |f^{1,0}_{1,0}\rangle + |f^{2,0}_{2,0}\rangle\right], \\
|k^1_{0,0}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\left[|f^{1,0}_{0,0}\rangle + |f^{1,1}_{0,1}\rangle\right], & |k^1_{1,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\left[|f^{0,1}_{0,0}\rangle + |f^{1,1}_{1,0}\rangle\right], \\
|k^2_{0,0}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\,|f^{1',1}_{0,1}\rangle, & |k^2_{1,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\,|f^{1,1'}_{1,0}\rangle, \\
|k^3_{0,0}\rangle &= \frac{1}{2}\mathrm{p}^A_\ell\,|f^{2,0}_{0,0}\rangle, & |k^3_{1,1}\rangle &= \frac{1}{2}\mathrm{p}^B_\ell\,|f^{0,2}_{0,0}\rangle, \\
|k_{0,1}\rangle &= \frac{1}{2}\,|f^{0,0}_{0,0}\rangle, & |k_{1,0}\rangle &= \frac{1}{2}\big[\,|f^{0,0}_{0,0}\rangle + |f^{1,0}_{1,0}\rangle + |f^{0,1}_{0,1}\rangle + |f^{2,0}_{2,0}\rangle + \\
& & & \quad + |f^{1,1'}_{1,1'}\rangle + |f^{1',1}_{1',1}\rangle + |f^{0,2}_{0,2}\rangle\,\big], \\
|k^1_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell}\,|f^{1,0}_{0,0}\rangle, & |k^4_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell\,\mathrm{p}^B_\ell}\,|f^{1',1}_{0,0}\rangle, \\
|k^2_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^B_\ell}\,|f^{0,1}_{0,0}\rangle, & |k^5_{0,1}\rangle &= \frac{1}{2}\mathrm{p}^A_\ell\,|f^{2,0}_{0,0}\rangle, \\
|k^3_{0,1}\rangle &= \frac{1}{2}\sqrt{\mathrm{p}^A_\ell\,\mathrm{p}^B_\ell}\,|f^{1,1'}_{0,0}\rangle, & |k^6_{0,1}\rangle &= \frac{1}{2}\mathrm{p}^B_\ell\,|f^{0,2}_{0,0}\rangle.
\end{aligned}
\tag{4.15}
$$

The normalization constant $\mathcal{N}$ is the probability to obtain the result "1", when there were no clicks at the agents' detectors, expressed as:

$$
\begin{aligned}
\mathcal{N} = {} & \langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle + \\
& + \langle k^1_{1,1}|k^1_{1,1}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle + \langle k_{0,1}|k_{0,1}\rangle + \langle k^1_{0,1}|k^1_{0,1}\rangle + \\
& + \langle k^2_{0,1}|k^2_{0,1}\rangle + \langle k^3_{0,1}|k^3_{0,1}\rangle + \langle k^4_{0,1}|k^4_{0,1}\rangle + \langle k^5_{0,1}|k^5_{0,1}\rangle + \langle k^6_{0,1}|k^6_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle\,.
\end{aligned}
\tag{4.16}
$$

In Equation (4.14), the state $|D_v,R\rangle\langle D_v,R|$ describes Alice detecting without a click and Bob reflecting, and is associated to a shared key bit of 0. However, $|D_\ell,R\rangle\langle D_\ell,R|$, $|D'_\ell,R\rangle\langle D'_\ell,R|$ and $|D_\ell D'_\ell,R\rangle\langle D_\ell D'_\ell,R|$ also correspond to a shared key bit of 0, and are a consequence of Alice's imperfect detector and multi-photon events. Similarly, $|R,D_v\rangle\langle R,D_v|$, $|R,D_\ell\rangle\langle R,D_\ell|$, $|R,D'_\ell\rangle\langle R,D'_\ell|$ and $|R,D_\ell D'_\ell\rangle\langle R,D_\ell D'_\ell|$ are associated to a key bit 1. The remaining states correspond to errors, i.e., the cases when the two users

establish opposite key bit values. From the definitions of k_{ij} and $\mathcal{N}$:

$$\frac{\langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle}{\mathcal{N}} = \mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R|1). \tag{4.17}$$

Here, $\mathrm{p}(\mathcal{P}|\mathcal{C})$ denotes the conditional probability that the proposition $\mathcal{P}$ holds (in the above case, Alice detects and observes no clicks, while Bob reflects), given that the condition $\mathcal{C}$ is satisfied (in the above case, the server announces "1"). Therefore, using the notation $\langle k_{i,j}|k_{i,j}\rangle = \mathrm{p}_{i,j}$; $\langle k^m_{i,j}|k^m_{i,j}\rangle = \mathrm{p}^m_{i,j}$, the probability to share a key digit is given by:

$$\begin{aligned}
\mathrm{p}_{key} =& \langle k_{0,0}|k_{0,0}\rangle + \langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^3_{0,0}|k^3_{0,0}\rangle + \\
&+ \langle k_{1,1}|k_{1,1}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle = \\
&= \mathrm{p}_{0,0} + \mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} + \mathrm{p}^3_{0,0} + \mathrm{p}_{1,1} + \mathrm{p}^1_{1,1} + \mathrm{p}^2_{1,1} + \mathrm{p}^3_{1,1} = \\
&= \tilde{\mathrm{p}}_{0,0} + \tilde{\mathrm{p}}_{1,1} = \\
&= \mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;1) + \mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;1),
\end{aligned} \tag{4.18}$$

where $\mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;1)$ represents the joint probability of the following event: Alice detects vacuum, Bob reflects, and the server announces the result "1"; and analogously for the other term. Note that, for simplicity, the symbol ";" is used to denote logical AND between two propositions, instead of introducing the additional parenthesis for the first one and the standard symbol $\wedge$. The probability of error in the raw key is

given by:

$$\begin{aligned}
\mathrm{p}_{err} &= \langle k_{0,1}|k_{0,1}\rangle + \langle k^1_{0,1}|k^1_{0,1}\rangle + \langle k^2_{0,1}|k^2_{0,1}\rangle + \langle k^3_{0,1}|k^3_{0,1}\rangle + \\
&+ \langle k^4_{0,1}|k^4_{0,1}\rangle + \langle k^5_{0,1}|k^5_{0,1}\rangle + \langle k^6_{0,1}|k^6_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle = \\
&= \mathrm{p}_{0,1} + \mathrm{p}^1_{0,1} + \mathrm{p}^2_{0,1} + \mathrm{p}^3_{0,1} + \mathrm{p}^4_{0,1} + \mathrm{p}^5_{0,1} + \mathrm{p}^6_{0,1} + \mathrm{p}_{1,0} = \\
&= \tilde{\mathrm{p}}_{0,1} + \tilde{\mathrm{p}}_{1,0} = \\
&= \mathrm{p}(D_v, D_v \vee D_\ell, D_v \vee D_v, D_\ell \vee D_\ell, D'_\ell \vee D'_\ell, D_\ell \vee D_v, D_\ell D'_\ell \vee D'_\ell D_\ell, D_v\,; 1) + \mathrm{p}(RR\,; 1),
\end{aligned} \tag{4.19}$$

where $\mathrm{p}(D_v, D_v \vee D_\ell, D_v \vee D_v, D_\ell \vee D_\ell, D'_\ell \vee D'_\ell, D_\ell \vee D_v, D_\ell D'_\ell \vee D'_\ell D_\ell, D_v\,; 1)$ represents the joint probability of the event: Alice and Bob both detect vacuum, and the server announces the result "1"; and analogously for the other term. The probabilities $\tilde{\mathrm{p}}_{i,j}$ can be directly observed from the experiment.

To obtain the secret key rate, the following bound is considered [196]:

$$\begin{aligned}
S(A|C) \;\geq\; & \frac{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k_{0,0}|k_{0,0}\rangle}{\langle k_{0,0}|k_{0,0}\rangle + \langle k_{1,1}|k_{1,1}\rangle} \right] - h(\lambda_0) \right) + \\
& + \frac{\langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^1_{0,0}|k^1_{0,0}\rangle}{\langle k^1_{0,0}|k^1_{0,0}\rangle + \langle k^1_{1,1}|k^1_{1,1}\rangle} \right] - h(\lambda_1) \right) + \\
& + \frac{\langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^2_{0,0}|k^2_{0,0}\rangle}{\langle k^2_{0,0}|k^2_{0,0}\rangle + \langle k^2_{1,1}|k^2_{1,1}\rangle} \right] - h(\lambda_2) \right) + \\
& + \frac{\langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k^3_{0,0}|k^3_{0,0}\rangle}{\langle k^3_{0,0}|k^3_{0,0}\rangle + \langle k^3_{1,1}|k^3_{1,1}\rangle} \right] - h(\lambda_3) \right) + \\
& + \frac{\langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle}{\mathcal{N}} \left(h\left[\frac{\langle k_{0,1}|k_{0,1}\rangle}{\langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle} \right] - h(\lambda_4) \right),
\end{aligned} \tag{4.20}$$

where h is the binary Shannon entropy, and:

$$\lambda_i = \frac{1}{2} \left(1 + \frac{\sqrt{(\langle k^i_{0,0}|k^i_{0,0}\rangle - \langle k^i_{1,1}|k^i_{1,1}\rangle)^2 + 4\mathrm{Re}^2\,\langle k^i_{0,0}|k^i_{1,1}\rangle}}{\langle k^i_{0,0}|k^i_{0,0}\rangle + \langle k^i_{1,1}|k^i_{1,1}\rangle} \right). \tag{4.21}$$

The first four terms in $S(A|C)$ correspond to the key digits shared between Alice and

Bob, while the last term corresponds to errors in the key. However, the lower bound on $S(A|C)$ is estimated by considering only the first term since its contribution to the entropy is far larger than that of any of the other terms.

From expression (4.21) for λ_0, it is clear that minimizing $S(A|C)$ essentially means minimizing $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$. Therefore, in addition to different probabilities obtained from the experiment, it is also necessary to estimate $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$, which is done here by computing the lower bound for $\mathrm{Re}^2\,\langle k_{0,0}|k_{1,1}\rangle$, i.e., for $|\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle\,|$. By using the following notation for simplification:

$$|x\rangle = |f^{1,0}_{1,0}\rangle + |f^{2,0}_{2,0}\rangle\,; \quad |y\rangle = |f^{0,1}_{0,1}\rangle + |f^{0,2}_{0,2}\rangle\,, \quad |z\rangle = |f^{1,1'}_{1,1'}\rangle + |f^{1',1}_{1',1}\rangle\,, \tag{4.22}$$

$\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ can be obtained as:

$$\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle = \frac{1}{4}\left[\langle f^{0,0}_{0,0}|f^{0,0}_{0,0}\rangle + \mathrm{Re}\,\langle x|f^{0,0}_{0,0}\rangle + \mathrm{Re}\,\langle f^{0,0}_{0,0}|y\rangle + \mathrm{Re}\,\langle x|y\rangle\right]. \tag{4.23}$$

At this point, by defining $\langle k_{1,0}|k_{1,0}\rangle = \mathcal{Q}/4$ and considering $\langle f^{0,0}_{0,0}|f^{0,0}_{0,0}\rangle = 4\,\langle k_{0,1}|k_{0,1}\rangle = 4\mathrm{p}_{0,1}$, one can write:

$$\langle k_{0,0}|k_{1,1}\rangle = \frac{\mathcal{Q}}{8} + \frac{\mathrm{p}_{0,1}}{2} - \frac{1}{8}\left[\langle x|x\rangle + \langle y|y\rangle + \langle z|z\rangle\right] - \frac{1}{4}\left[\langle x|z\rangle + \langle y|z\rangle + \langle f^{0,0}_{0,0}|z\rangle\right]. \tag{4.24}$$

Considering that $\langle x|z\rangle = |\,\langle x|z\rangle\,|e^{\varphi_{x,z}}$, it follows:

$$\mathrm{Re}\,\langle x|z\rangle = |\,\langle x|z\rangle\,|\cos\varphi_{x,y} = ||\,|x\rangle\,|| \cdot ||\,|z\rangle\,|| \cdot |\cos\chi_{x,z}|\cos\varphi_{x,z} = \sqrt{\langle x|x\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{x,z}, \tag{4.25}$$

where $\chi_{x,z}$ denotes the angle between $|x\rangle$ and $|z\rangle$ and $\cos\theta_{x,z} \equiv |\cos\chi_{x,z}|\cos\varphi_{x,z}$, and analogously for $\mathrm{Re}\,\langle y|z\rangle$ and so on.

Therefore, the final expression for $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ is:

$$\begin{aligned}\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle \;=\; & \frac{\mathcal{Q}}{8} + \frac{\mathrm{p}_{0,1}}{2} - \frac{1}{8}\left[\langle x|x\rangle + \langle y|y\rangle + \langle z|z\rangle\right] - \frac{1}{4}\left[\sqrt{\langle f^{0,0}_{0,0}|f^{0,0}_{0,0}\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{f,z}\right] + \\ & - \frac{1}{4}\left[\sqrt{\langle x|x\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{x,z} + \sqrt{\langle y|y\rangle}\sqrt{\langle z|z\rangle}\cos\theta_{y,z}\right].\end{aligned} \tag{4.26}$$

To evaluate $\langle x|x\rangle$ and $\langle y|y\rangle$, Equation (4.15) can be exploited, thus obtaining:

$$\begin{aligned}\langle k_{1,1}|k_{1,1}\rangle &= \frac{1}{4}\left[\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \langle x|x\rangle + 2\mathrm{Re}\,\langle f_{0,0}^{0,0}|x\rangle\right] \\ \langle k_{0,0}|k_{0,0}\rangle &= \frac{1}{4}\left[\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle + \langle y|y\rangle + 2\mathrm{Re}\,\langle f_{0,0}^{0,0}|y\rangle\right].\end{aligned} \tag{4.27}$$

Note that $\langle f_{0,0}^{0,0}|f_{0,0}^{0,0}\rangle = 4\,\langle k_{0,1}|k_{0,1}\rangle = 4\mathrm{p}_{0,1}, \langle k_{0,0}|k_{0,0}\rangle = \mathrm{p}_{0,0}$ and $\langle k_{1,1}|k_{1,1}\rangle = \mathrm{p}_{1,1}$. Therefore, solving the quadratic equations from (4.27), the following positive roots of $\sqrt{\langle x|x\rangle}$ and $\sqrt{\langle y|y\rangle}$ are extracted:

$$\begin{aligned}\sqrt{\langle x|x\rangle} &= 2\left[-\sqrt{\mathrm{p}_{0,1}}\cos\theta_{x,f} + \sqrt{\mathrm{p}_{1,1} - (1 - \cos^2\theta_{x,f})\,\mathrm{p}_{0,1}}\right], \\ \sqrt{\langle y|y\rangle} &= 2\left[-\sqrt{\mathrm{p}_{0,1}}\cos\theta_{y,f} + \sqrt{\mathrm{p}_{0,0} - (1 - \cos^2\theta_{y,f})\,\mathrm{p}_{0,1}}\right].\end{aligned} \tag{4.28}$$

Analogously, for $\langle z|z\rangle$:

$$\begin{aligned}\langle z|z\rangle + \underbrace{2\left[\sqrt{\langle x|x\rangle}\,\cos\,\theta_{x,z} + \sqrt{\langle y|y\rangle}\,\cos\,\theta_{y,z} + 2\sqrt{\mathrm{p}_{0,1}}\,\cos\,\theta_{f,z}\right]}_{\beta}\sqrt{\langle z|z\rangle} + \\ + 4\left[\mathrm{p}_{0,1} - \mathrm{p}_{1,0}\right] + \Big[\langle x|x\rangle + \langle y|y\rangle + 2\sqrt{\langle x|x\rangle}\sqrt{\langle y|y\rangle}\,\cos\,\theta_{x,y}\Big] \\ \underbrace{+ 4\sqrt{\mathrm{p}_{0,1}}\left[\sqrt{\langle x|x\rangle}\,\cos\,\theta_{x,f} + \sqrt{\langle y|y\rangle}\,\cos\,\theta_{y,f}\right]}_{\gamma} = 0,\end{aligned} \tag{4.29}$$

where $\cos\theta_{x,z} \equiv |\cos\chi_{x,z}|\cos\varphi_{x,z}$ and analogously for $\cos\theta_{y,z}$, $\cos\theta_{f,z}$, etc. Again, solving the above quadratic equation, the positive root of $\sqrt{\langle z|z\rangle}$ can be obtained. The lower bound for $\mathrm{Re}\,\langle k_{0,0}|k_{1,1}\rangle$ is estimated by minimizing with respect all the angles defined in the above expressions.

4.4 Parameter Estimation

In order to compute $S(A|C)$ in Equation (4.20) and eventually obtain the secret key rate of Equation (4.1), the probabilities $\mathrm{p}_{0,0}, \mathrm{p}_{1,1}$ and $\mathrm{p}_{0,1}$ need to be computed. Below, two methods of estimation are discussed: direct estimation, where Alice and Bob use part of

the key to obtain the required probabilities, and indirect estimation, where only rounds that do not lead to key generation are used.

4.4.1 Direct estimation

In case of direct estimation, a fraction μ of the total N_{raw} key-generation rounds is used to directly compute the relevant probabilities. However, since Alice's and Bob's detectors are imperfect, they cannot compute $\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1)$ and $\mathrm{p}_{1,1} = \mathrm{p}(R,D_v\,;1)$ directly, as they cannot differentiate the event D_v,R from the events D_ℓ,R, D'_ℓ,R and $D_\ell D'_\ell,R$, and analogously for R,D_v. However, the users can obtain $\tilde{\mathrm{p}}_{0,0}$ and $\tilde{\mathrm{p}}_{1,1}$ directly, which, combined to the estimation of $\mathrm{p}^1_{0,0} = \langle k^1_{0,0}|k^1_{0,0}\rangle$, $\mathrm{p}^2_{0,0} = \langle k^2_{0,0}|k^2_{0,0}\rangle$ and $\mathrm{p}^3_{0,0} = \langle k^3_{0,0}|k^3_{0,0}\rangle$, eventually provides $\mathrm{p}_{0,0}$. From Equation (4.15) one has:

$$\begin{aligned}
\mathrm{p}^1_{0,0} &= \mathrm{p}(D_\ell,R\,;1) = \frac{\mathrm{p}_\ell^A}{4}\left(||\,|f^{1,0}_{0,0}\rangle + |f^{1,1'}_{0,1'}\rangle\,||^2\right),\\
\mathrm{p}^2_{0,0} &= \mathrm{p}(D'_\ell,R\,;1) = \frac{\mathrm{p}_\ell^A}{4}\,\langle f^{1',1}_{0,1}|f^{1',1}_{0,1}\rangle\,,\\
\mathrm{p}^3_{0,0} &= \mathrm{p}(D_\ell D'_\ell,R\,;1) = \frac{\mathrm{p}_\ell^{A^2}}{4}\,\langle f^{2,0}_{0,0}|f^{2,0}_{0,0}\rangle\,.
\end{aligned} \tag{4.30}$$

The above probabilities can be estimated by looking at the events corresponding to the detector clicks, using the expressions:

$$\begin{aligned}
\mathrm{p}(D_c,R\,;1) &= \frac{\mathrm{p}_d^A}{4}\left(||\,|f^{1,0}_{0,0}\rangle + |f^{1,1'}_{0,1'}\rangle\,||^2\right),\\
\mathrm{p}(D'_c,R\,;1) &= \frac{\mathrm{p}_d^A}{4}\,\langle f^{1',1}_{0,1}|f^{1',1}_{0,1}\rangle\,,\\
\mathrm{p}(D_cD'_c,R\,;1) &= \frac{\mathrm{p}_d^{A^2}}{4}\,\langle f^{2,0}_{0,0}|f^{2,0}_{0,0}\rangle\,.
\end{aligned} \tag{4.31}$$

In fact, $\left(\mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0}\right)$ and $\mathrm{p}^3_{0,0}$ can be written as:

$$\begin{aligned}
\mathrm{p}^1_{0,0} + \mathrm{p}^2_{0,0} &= \left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\mathrm{p}(D_c,R\vee D'_c,R\,;1),\\
\mathrm{p}^3_{0,0} &= \left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\mathrm{p}(D_cD'_c,R\,;1),
\end{aligned} \tag{4.32}$$

where $\mathrm{p}(D_c D'_c,R\,;1)$ is obtained using the rounds when Alice gets double clicks in her detector. The probability $\mathrm{p}(D_c,R\vee D'_c,R\,;1)$ is computed from the following expression:

$$\mathrm{p}(D_c,R\vee D'_c,R;1)=\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R;1)-\mathrm{p}(D_\ell D'_c,R;1)-\mathrm{p}(D_c D'_\ell,R;1), \tag{4.33}$$

considering that $\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R\,;1)$, corresponding to a single click in Alice's detector, can be obtained directly and that:

$$\mathrm{p}(D_\ell D'_c,R\,;1)=\frac{\mathrm{p}_\ell^A\mathrm{p}_d^A}{4}\,\langle f_{0,0}^{2,0}|f_{0,0}^{2,0}\rangle=\mathrm{p}(D_c D'_\ell,R\,;1). \tag{4.34}$$

Therefore, the required probabilities $\mathrm{p}_{0,0}$ and $\mathrm{p}_{1,1}$ are:

$$\begin{aligned}\mathrm{p}_{0,0}&=\tilde{\mathrm{p}}_{0,0}-\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R\,;1)+\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\mathrm{p}(D_c D'_c,R\,;1),\\ \mathrm{p}_{1,1}&=\tilde{\mathrm{p}}_{1,1}-\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell\,;1)+\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2\mathrm{p}(D_c D'_c,R\,;1).\end{aligned} \tag{4.35}$$

Additionally, to compute $\mathrm{p}_{0,1}$, relation $\mathrm{p}_{0,1}=\tilde{\mathrm{p}}_{0,1}-\mathrm{p}_{0,1}^1-\mathrm{p}_{0,1}^2-\mathrm{p}_{0,1}^3-\mathrm{p}_{0,1}^4-\mathrm{p}_{0,1}^5-\mathrm{p}_{0,1}^6$ is used. Again, applying straightforward algebra:

$$\begin{aligned}\mathrm{p}_{0,1}=\;&\tilde{\mathrm{p}}_{0,1}-\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\mathrm{p}(D_c,D_v\vee D_c,D'_\ell\vee D'_c,D_\ell\vee D_c D'_\ell,D_v\vee D_\ell D'_c,D_v\,;1)+\\ &-\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)\mathrm{p}(D_v,D_c\vee D_\ell,D'_c\vee D'_\ell,D_c\vee D_v,D_c D'_\ell\vee D_v,D_\ell D'_c\,;1)+\\ &-3\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\mathrm{p}(D_c D'_c,D_v\,;1)-3\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2\mathrm{p}(D_v,D_c D'_c\,;1)+\\ &-3\left(\frac{\mathrm{p}_\ell^A\,\mathrm{p}_\ell^B}{\mathrm{p}_d^A\,\mathrm{p}_d^B}\right)\mathrm{p}(D_c,D'_c\vee D'_c,D_c\,;1).\end{aligned} \tag{4.36}$$

4.4.2 Indirect estimation

To avoid wasting the rounds used for key-generation, the remaining rounds (when "0","v" or "m" was announced or "1" was announced with click(s) at Alice's and Bob's detectors)

can be used for parameter estimation. For these cases, Alice and Bob can communicate over an authenticated channel to convey their respective action choices and resulting states to each other. In fact:

$$\mathrm{p}_{0,0} = \mathrm{p}(D_v,R\,;1) = \mathrm{p}(D_v,R) - \mathrm{p}(D_v,R\,;0) - \mathrm{p}(D_v,R\,;v) - \mathrm{p}(D_v,R\,;m), \tag{4.37}$$

where:

$$\begin{aligned}\mathrm{p}(D_v,R) \;=\; & \mathrm{p}(D,R) - \mathrm{p}(D_\ell,R) - \mathrm{p}(D'_\ell,R) - \mathrm{p}(D_c,R) + \\ & -\;\mathrm{p}(D'_c,R) - \mathrm{p}(D_\ell D'_\ell,R) - \mathrm{p}(D_c D'_\ell,R) - \mathrm{p}(D_\ell D'_c,R) - \mathrm{p}(D_c D'_c,R).\end{aligned} \tag{4.38}$$

Note that $\mathrm{p}(D,R)$ is the probability of Alice choosing to detect and Bob to reflect. Since Alice and Bob choose their actions at random, ideally $\mathrm{p}(D,D) = \mathrm{p}(D,R) = \mathrm{p}(R,D) = \mathrm{p}(R,R) = 1/4$. However, considering the finite sample size and the inefficiency of switching between the two actions, Alice and Bob do not take these probabilities to be $1/4$ but compute them considering only the non-useful rounds.

By combining Equations 4.37 and 4.38, one has:

$$\begin{aligned}\mathrm{p}_{0,0} \;=\; & \mathrm{p}(D,R) - \mathrm{p}(D_\ell,R) - \mathrm{p}(D'_\ell,R) - \mathrm{p}(D_c,R) - \mathrm{p}(D'_c,R) - \mathrm{p}(D_\ell D'_\ell,R) - \mathrm{p}(D_c D'_\ell,R) + \\ & -\;\mathrm{p}(D_\ell D'_c,R) - \mathrm{p}(D_c D'_c,R) - \mathrm{p}(D_v,R\,;0) - \mathrm{p}(D_v,R\,;v) - \mathrm{p}(D_v,R\,;m).\end{aligned} \tag{4.39}$$

Note that Alice and Bob cannot directly compute all the quantities from the above expression. For instance, the probability $\mathrm{p}(D_v,R\,;0)$ is not directly observable. However, this quantity can be obtained indirectly from $\mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;0)$, according to the following expression:

$$\begin{aligned}\mathrm{p}(D_v,R\,;0) \;=\; & \mathrm{p}(D_v,R \vee D_\ell,R \vee D'_\ell,R \vee D_\ell D'_\ell,R\,;0) + \\ & -\;\mathrm{p}(D_\ell,R\,;0) - \mathrm{p}(D'_\ell,R\,;0) - \mathrm{p}(D_\ell D'_\ell,R\,;0).\end{aligned} \tag{4.40}$$

Analogous procedures can be adopted for $\mathrm{p}(D_\ell,R\,;0)$, $\mathrm{p}(D'_\ell,R\,;0)$ and $\mathrm{p}(D_c D'_\ell,R\,;0)$, etc.

The final expressions for $\mathrm{p}_{0,0}$ and $\mathrm{p}_{1,1}$, in terms of directly observable probabilities, are then:

$$\begin{aligned}
\mathrm{p}_{0,0} \;=\; & \mathrm{p}(D,R) - \mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R) - \mathrm{p}(D_c D'_c,R) + \\
& - \mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;0) + \mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;v) + \\
& - \mathrm{p}(D_v,R\vee D_\ell,R\vee D'_\ell,R\vee D_\ell D'_\ell,R\,;m) + \\
& + \left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)\big[\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R\,;0) + \\
& + \;\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R\,;v) + \\
& + \;\mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R\,;m) + \\
& - \mathrm{p}(D_c,R\vee D'_c,R\vee D_\ell D'_c,R\vee D_c D'_\ell,R)\big] - \left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2\big[\mathrm{p}(D_c D'_c,R\,;0) + \\
& + \mathrm{p}(D_c D'_c,R\,;v) + \mathrm{p}(D_c D'_c,R,m) - \mathrm{p}(D_c D'_c,R)\big],
\end{aligned} \tag{4.41}$$

$$\begin{aligned}
\mathrm{p}_{1,1} \;=\; & \mathrm{p}(R,D) - \mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell) - \mathrm{p}(R,D_c D'_c) + \\
& - \mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;0) - \mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;v) + \\
& - \mathrm{p}(R,D_v\vee R,D_\ell\vee R,D'_\ell\vee R,D_\ell D'_\ell\,;m) + \\
& + \left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)\big[\mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell\,;0) + \\
& + \mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell\,;v) + \\
& + \mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell\,;m) + \\
& - \mathrm{p}(R,D_c\vee R,D'_c\vee R,D_\ell D'_c\vee R,D_c D'_\ell)\big] - \left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2\big[\mathrm{p}(R,D_c D'_c\,;0) + \\
& + \;\mathrm{p}(R,D_c D'_c\,;v) + \mathrm{p}(R,D_c D'_c\,;m) - \mathrm{p}(R,D_c D'_c)\big].
\end{aligned} \tag{4.42}$$

Analogously:

$$\tilde{\mathrm{p}}_{1,0} = \mathrm{p}(R,R\,;1) = \mathrm{p}(RR) - \mathrm{p}(R,R\,;0) - \mathrm{p}(R,R\,;v) - \mathrm{p}(R,R\,;m), \tag{4.43}$$

and:

$$\begin{aligned}
\mathrm{p}_{0,1} &= \mathrm{p}(1) - \tilde{\mathrm{p}}_{0,0} - \tilde{\mathrm{p}}_{1,1} - \tilde{\mathrm{p}}_{1,0} + \\
&- \left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right) \mathrm{p}(D_c, D_v \vee D_c, D'_\ell \vee D'_c, D_\ell \vee D_c D'_\ell, D_v \vee D_\ell D'_c, D_v\,; 1) + \\
&- \left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right) \mathrm{p}(D_v, D_c \vee D_\ell, D'_c \vee D'_\ell, D_c \vee D_v, D_c D'_\ell \vee D_v, D_\ell D'_c\,; 1) + \\
&- 3\left(\frac{\mathrm{p}_\ell^A}{\mathrm{p}_d^A}\right)^2 \mathrm{p}(D_c D'_c, D_v\,; 1) - 3\left(\frac{\mathrm{p}_\ell^B}{\mathrm{p}_d^B}\right)^2 \mathrm{p}(D_v, D_c D'_c\,; 1) + \\
&- 3\left(\frac{\mathrm{p}_\ell^A\, \mathrm{p}_\ell^B}{\mathrm{p}_d^A\, \mathrm{p}_d^B}\right) \mathrm{p}(D_c, D'_c \vee D'_c, D_c\,; 1).
\end{aligned} \tag{4.44}$$

Note that, to compute $\mathrm{p}_{key} = \tilde{\mathrm{p}}_{00} + \tilde{\mathrm{p}}_{11}$ using the indirect method, one has:

$$\begin{aligned}
\tilde{\mathrm{p}}_{0,0} &= \mathrm{p}(D,R) - \mathrm{p}(D_c, R \vee D'_c, R \vee D_\ell D'_c, R \vee D_c D'_\ell, R) - \mathrm{p}(D_c D'_c, R) + \\
&- \mathrm{p}(D_v, R \vee D_\ell, R \vee D'_\ell, R \vee D_\ell D'_\ell, R\,; 0) + \\
&- \mathrm{p}(D_v, R \vee D_\ell, R \vee D'_\ell, R \vee D_\ell D'_\ell, R\,; v) - \mathrm{p}(D_v, R \vee D_\ell, R \vee D'_\ell, R \vee D_\ell D'_\ell, R\,; m),
\end{aligned} \tag{4.45}$$

$$\begin{aligned}
\tilde{\mathrm{p}}_{1,1} &= \mathrm{p}(R,D) - \mathrm{p}(R, D_c \vee R, D'_c \vee R, D_\ell D'_c \vee R, D_c D'_\ell) - \mathrm{p}(R, D_c D'_c) + \\
&- \mathrm{p}(R, D_v \vee R, D_\ell \vee R, D'_\ell \vee R, D_\ell D'_\ell\,; 0) + \\
&- \mathrm{p}(R, D_v \vee R, D_\ell \vee R, D'_\ell \vee R, D_\ell D'_\ell\,; v) - \mathrm{p}(R, D_v \vee R, D_\ell \vee R, D'_\ell \vee R, D_\ell D'_\ell\,; m).
\end{aligned} \tag{4.46}$$

4.5 Experimental Results

The experimental probabilities p_{key} and p_{err}, computed both directly and indirectly, are reported in Table 4.1. Direct estimation is performed both over the full data set of 10^5 iterations and over a subset with 10^4 iterations. The indirect estimation is performed using all the iterations that do not lead to key generation, over the full data set. The probabilities computed with the different methods are all consistent within experimental errors, which are higher in the case of indirect estimation, due to the higher number of measured quantities, each with its error, necessary for the computation. On the other

	Direct Method (full dataset)	Direct Method (subset)	Indirect Method (full dataset)
p_{key}	$1.55(3) \times 10^{-2}$	$1.5(1) \times 10^{-2}$	$1.5(3) \times 10^{-2}$
p_{err}	$7.5(8) \times 10^{-4}$	$5(2) \times 10^{-4}$	$3(3) \times 10^{-3}$

Table 4.1: **Evaluation of key generation and error rates**. The probabilities of raw-key generation, p_{key} and error on a key digit, p_{err}, respectively, are shown per round (in our case an interval of 0.5 s). p_{key} and p_{err} are evaluated in three different ways: direct estimation over the full data set, direct estimation over a randomly chosen subset of 10^4 rounds and indirect estimation. The latter allows the parties to avoid the loss of key digits, at a price of higher uncertainty of the estimated values, which are calculated from several experimentally obtained quantities, each with its error. In the table, the numbers in parentheses are the errors on the last digits, obtained with the assumption of Poissonian uncertainty of the counts.

hand, in the case of direct estimation, the uncertainty of the final probabilities depends on the size μ of the considered sub-sample. The choice of which method to use, therefore, depends on the experimental situation and the length of the raw key.

The full data set is used to directly estimate the probabilities of Equations 4.35 and 4.36, and consequently the secure key rate, r, which is plotted with respect to the number of iterations, N in Figure 4.3.

The measured probabilities necessary for the estimation of r are found to be: $p_{0,0} = (7.3 \pm 0.3) \times 10^{-3}$, $p_{1,1} = (5.5 \pm 0.3) \times 10^{-3}$, $p_{0,1} = (1.1 \pm 0.9) \times 10^{-4}$ and $p_{1,0} = (5.1 \pm 0.7) \times 10^{-4}$. The security parameter is taken to be $\epsilon = 10^{-5}$, while a probability of error for information reconciliation of $\epsilon_{EC} = 10^{-10}$ is assumed. The optimization value ϵ' is set to $\epsilon' = 10^{-7}$ and the tolerance on parameter estimation to $\epsilon_{PE} = 10^{-11}$. Given the experimental errors, a confidence interval of $\delta = 10^{-4}$ is considered. The calculated secret key rate corresponds to the minimum lower bound of the entropy $S(A|C)$ (see Equation (4.20)) over the confidence interval of the experimental probabilities. This minimum occurs for the highest value of the error probability p_{err} and the lowest of p_{key}, and therefore represents the worst possible key rate within the considered experimental uncertainty. Note that these results are lower bounds and, therefore, the actual key rate could be significantly higher. Indeed, to compute these lower bounds the strong sub-additivity of von Neumann entropy is exploited, by actually discarding several components of the entropy function (components which would only have increased Eve's uncertainty). Such

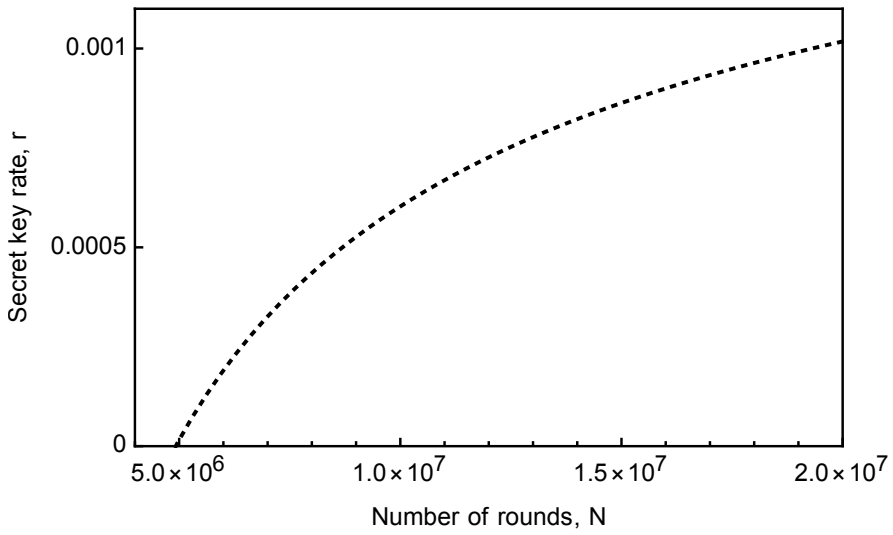


Figure 4.3: **Secret key rate, r, vs number of rounds,** N. For the estimation it is assumed $\epsilon = 10^{-5}$, $\epsilon_{EC} = 10^{-10}$, $\epsilon_{PE} = 10^{-11}$, $\delta = 10^{-4}$, $\epsilon' = 10^{-7}$. The key rate becomes positive after about 5×10^6 iterations and tends to an asymptotic value of about 0.001.

a method gives a worst-case computation.

One of the reasons why the secure key rate is low with respect to other QKD protocols (see Section 1.6.1) is that, given the average number of photons per interval of 0.35, vacuum is sent to Alice and Bob in most iterations. Further reasons are the non-simultaneous two-photon emission from the source, due to its probabilistic nature and the errors induced by phase fluctuations in the interferometer. Deterministic single-photon sources and fast switches would solve all these problems but phase stability, which is definitely an issue for scaling the protocols to large distances. Regarding this last point, the same considerations as in Section 3.5.1 are valid.

In terms of loss, the dependence of the secure key rate on detection efficiency of Alice's and Bob's detectors, p_d^A and p_d^B, assumed to be the same, is studied. The only quantity depending on p_d^A and p_d^B is p(1), which corresponds to the normalization constant $\mathcal{N}$ of Equation 4.16. By explicitly expressing this dependence in terms of the loss probabilities

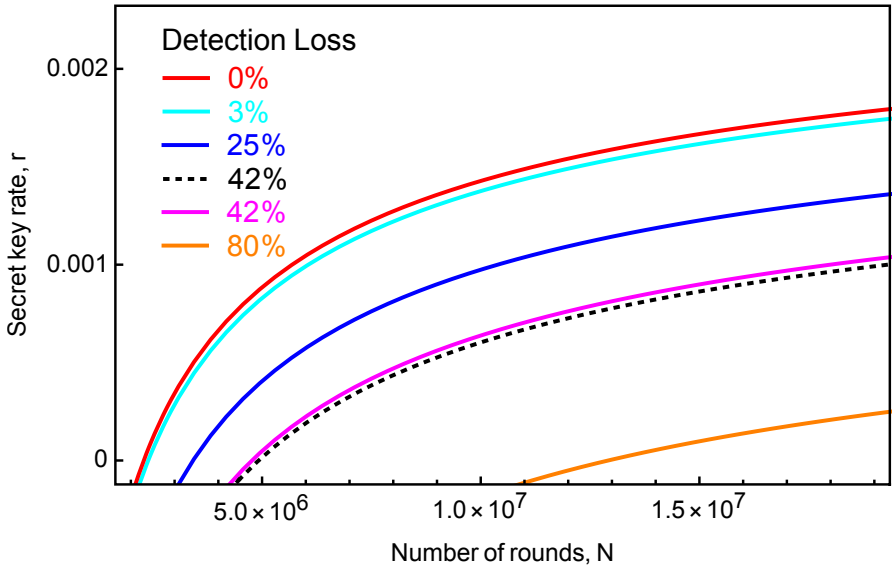


Figure 4.4: **Secret key rate vs number of rounds, for different values of detection loss**. The black dashed curve refers to the experimental implementation, corresponding to a detection loss of 42% for each Alice and Bob. The red, cyan, blue, magenta and orange curves represent the calculated results for a detection loss of $0, 3, 25, 42$ and 80%, respectively. If the detection loss increases, the number of rounds for which r becomes positive also increases, while the asymptotic secret key rate decreases.

$\mathrm{p}_\ell^A = 1 - \mathrm{p}_d^A$ and $\mathrm{p}_\ell^B = 1 - \mathrm{p}_d^B$, one obtains:

$$\begin{aligned}\mathcal{N}(\tilde{\mathrm{p}}_\ell^A, \tilde{\mathrm{p}}_\ell^B) =& \langle k_{0,0}|k_{0,0}\rangle + \sqrt{\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}}\left(\langle k_{0,0}^1|k_{0,0}^1\rangle + \langle k_{0,0}^2|k_{0,0}^2\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)\langle k_{0,0}^3|k_{0,0}^3\rangle + \\ &+ \langle k_{1,1}|k_{1,1}\rangle + \sqrt{\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}}\left(\langle k_{1,1}^1|k_{1,1}^1\rangle + \langle k_{1,1}^2|k_{1,1}^2\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)\langle k_{1,1}^3|k_{1,1}^3\rangle + \\ &+ \langle k_{0,1}|k_{0,1}\rangle + \langle k_{1,0}|k_{1,0}\rangle + \sqrt{\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}}\langle k_{0,1}^1|k_{0,1}^1\rangle + \sqrt{\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}}\langle k_{0,1}^2|k_{0,1}^2\rangle + \\ &+ \sqrt{\frac{\tilde{\mathrm{p}}_\ell^A\,\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^A\,\mathrm{p}_\ell^B}}\left(\langle k_{0,1}^3|k_{0,1}^3\rangle + \langle k_{0,1}^4|k_{0,1}^4\rangle\right) + \left(\frac{\tilde{\mathrm{p}}_\ell^A}{\mathrm{p}_\ell^A}\right)\langle k_{0,1}^5|k_{0,1}^5\rangle + \left(\frac{\tilde{\mathrm{p}}_\ell^B}{\mathrm{p}_\ell^B}\right)\langle k_{0,1}^6|k_{0,1}^6\rangle + \\ &= \mathrm{p}(1)(\tilde{\mathrm{p}}_\ell^A, \tilde{\mathrm{p}}_\ell^B).\end{aligned} \tag{4.47}$$

Moreover, $\mathrm{p}_{err} = \mathrm{p}(1) - \mathrm{p}_{key}$ is also modified accordingly, to be used in computing $Q = \mathrm{p}_{err}/\mathrm{p}(1)$ to obtain the secret key rate (4.1). This allows one to compute the secure key rate for different values of detection loss, as shown in Figure 4.4.

4.6 Summary of the results

In this Chapter the following results were presented:

- A mediated SQKD protocol was developed, which only requires the users to detect the presence of a photon in their respective laboratories. A quantum, not necessarily honest, server provides the parties single photons in superposition.
- The protocol is implemented by using a folded Mach-Zehnder interferometer and a probabilistic photon source, which can emit in each communication interval 0, 1 or 2 non-simultaneous photons.
- The secure key rate of the implemented protocol is computed in the finite key-scenario, taking into account experimental imperfections, in particular detection loss at the users' detectors and multi-photon emission from the source. This represents the first security analysis of a SQKD protocol in realistic experimental condition and in the finite-key regime.
- For a detection loss of 42% for both users and an average emission rate of 0.35 photons per communication interval (0.5 s), the secure key rate becomes positive after about 5×10^6 iterations and tends to an asymptotic value of about 0.001.

Chapter 5

Realization of a Narrow-Bandwidth Single-Photon Source Tuned to Rubidium D2 Line

This chapter presents the third experimental project included in the present Ph.D. dissertation. The project consists in the demonstration of a source of narrow-band (about 10 MHz spectral bandwidth) single photons that are tuned to Rubidium (Rb) D2 line (780 nm) and can be efficiently coupled to Rb hyperfine transitions (having a natural linewidth of a few MHz). The source is based on degenerate CE-SPDC. The degeneracy in frequency allows for the realization of light-matter hybrid systems in which more photons interact with the same Rb atom. This is necessary for multi-photon gates or quantum memories storing multi-photon states. The source was designed in particular for the implementation of two-photon gates [23, 27], to be performed in collaboration with external research groups working with Rb atoms.

The chapter is structured as follows. After a review of the state of the art of narrow-band photon generation, the realized experimental set-up and the results of the source

characterization are presented. In the end of the chapter, strategies for efficient spectral filtering of the source, which currently operates at multiple longitudinal modes, are described.

5.1 Narrow-bandwidth photons: state of the art

In this section, the main techniques for the generation of single photons with sub-GHz bandwidth are discussed.

A first category of methods relies on direct photon emission from material systems having energy transitions with sub-GHz linewidth. For instance, atoms or ions trapped in optical cavities [197, 198, 199, 200, 201] or electromagnetically induced transparency (EIT) in cold or warm atomic ensembles [202, 203] can be used for deterministic generation of photons with bandwidth on the order of 1 MHz. These sources, however, require complicated experimental setups and are typically affected by intermittent atom or ion loads and slow dynamics, resulting into low photon-emission rates. Furthermore the range of possible emission wavelengths is limited.

Recently the advances in nanofabrication techniques and materials science have allowed for the development of several deterministic solid-state single-photon emitters [204], among which quantum dots (QD) are suitable for the generation of sub-GHz-bandwidth photons. Currently, these systems attract much interest in the quantum photonic community, as the insights gained in the last two decades have allowed for the realization of single-photon sources that, for the first time, surpass SPDC-based sources in many aspects [205].

It has been shown, in fact, that QDs can generate photons that are coupled to single-mode fibers at a rate on the order of 10^7 per s, with $g^{(2)}(0)$ below 0.05 and high indistinguishability between consecutive emissions [206, 207, 208]. Furthermore, they can be used for deterministic generation of entangled states of two or more photons [209, 36]. Photons emitted by QDs typically have a bandwidth ranging from a few hundreds of MHz to a few GHz, depending on the specific type of dot and whether enhancement

cavities are used, which makes interaction with matter possible [210].

The main drawbacks of QDs are that they require cryogenic cooling and the range of emission wavelengths is quite limited. In fact, the most mature technology is that of InGaAs/GaAs QD, which emit in the $900 - 970$ nm range. Nevertheless, emission at 780 nm, 1300 nm and 1550 nm has also been shown for other systems [210, 211, 212]. A further problem is that it is not easy to fabricate two QDs with exactly the same properties, even though great progress has been made in this direction, allowing for high level of indistinguishability between photons from two different emitters [213]. Moreover, solid state emitters do not allow for the direct generation of photons with bandwidth on the order of 10 MHz or less. To date, the main methods for this task rely on second- or third-order non-linear effects in optical materials.

A promising route is provided by SFWM in CMOS-compatible micro-ring resonators, scalable systems that offer the great advantage of easy integration with electronics. Sources based on high-index-glass and silicon-nitride microresonators have in fact achieved single-photon emission at telecom wavelengths with bandwidths as narrow as 110 and 30 MHz [214, 215]. The silicon-nitride devices, in particular, show a spectral brightness as high as 5×10^5 pairs/(s mW MHz), with the possibility of pumping at relatively high power without adverse effects, thus allowing for detected counting rates on the order of 10^7 counts/s. Furthermore, this platform allows for generation of frequency-time entanglement, with visibility of about 90% [215].

The most used technique for the generation of narrow-bandwidth photons, however, is currently CE-SPDC. Even though this technology is not easily integrable on chip, its versatility and the high quality of the emitted photons makes it suitable for quantum optics and quantum information experiments. After the first experimental demonstration [216], in fact, many single-photon sources based on CE-SPDC have been realized at different wavelengths [217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232].

The narrowest bandwidth ever obtained was 0.43 MHz [228, 229], for a source at 795 nm with a spectral brightness (after correcting for detection losses) of 4×10^3 pairs/(s

mW MHz) and a maximum detected coincidence rate of about 500 counts/s. The main realizations of CE-SPDC-based sources are summarized in Table 5.1. As shown in the table, the spectral brightness can vary significantly, according to the employed system, the phase-matching configuration and wavelength. However, the spectral brightness alone is not enough to compare the actual count rates provided by two different sources. In order to have a clearer idea, in fact, the bandwidth and the maximum possible pump power must also be considered.

Typically CE-SPDC-based sources are able to provide photons with low higher-order contamination, as witnessed by the values of the heralded auto-correlation function $g_h^{(2)}(0)$, which, when reported, are usually below 0.1.

Previous to the implementation described in this chapter, two other sources of degenerate photon pairs at 780 nm have been reported [219, 222]. The source realized during this Ph.D. project, however, shows better performance, in particular regarding brightness, as shown in Table 5.3.

Although in some cases compact monolithic resonators have been realized, with mirrors directly coated on the facets of the employed non-linear crystals [223, 231], CE-SPDC-based sources are still bulky and hard to miniaturize. Schemes employing waveguides [174, 220] made of second-order non-linear material have shown easier coupling to fiber and integrated optics but, to date, scalable devices have not yet been realized.

Reference	Wavelength (nm)	Bandwidth (MHz)	Generated/Detected Brightness (pairs/(s mW MHz))	Pump Power (mW)	$g_h^{(2)}(0)$
[219]	780	9.6	6 / -	< 27	-
[221]	893	2.7	330 / -	< 10	< 0.01
[222]	780	21	-/2.7	1.08	-
[223]	1064	8.3	1.34×10^4 / 63	< 10	-
[224]	$1000 - 1120$	$7.2 - 13$	1.3×10^7 / 4×10^3	< 0.002	< 0.2
[225]	$606 + 1436$	$2.9 + 1.7$	8×10^3 / 1	< 1	-
[226]	1560	8	134/ 7×10^{-4}	< 200	-
[174]	$890 + 1320$	60	3×10^4 / -	< 10	0.02
[228]	795	0.43	4×10^3 / -	0.5	0.032
[230]	795	4.5	3.67×10^5 / 2.12×10^4	0.03	-
[231]	$780 + 852$	6.6	1.06×10^5 / 853	< 5	-
[232]	$795 + 825$	226	930 / 17	1.2	< 0.01

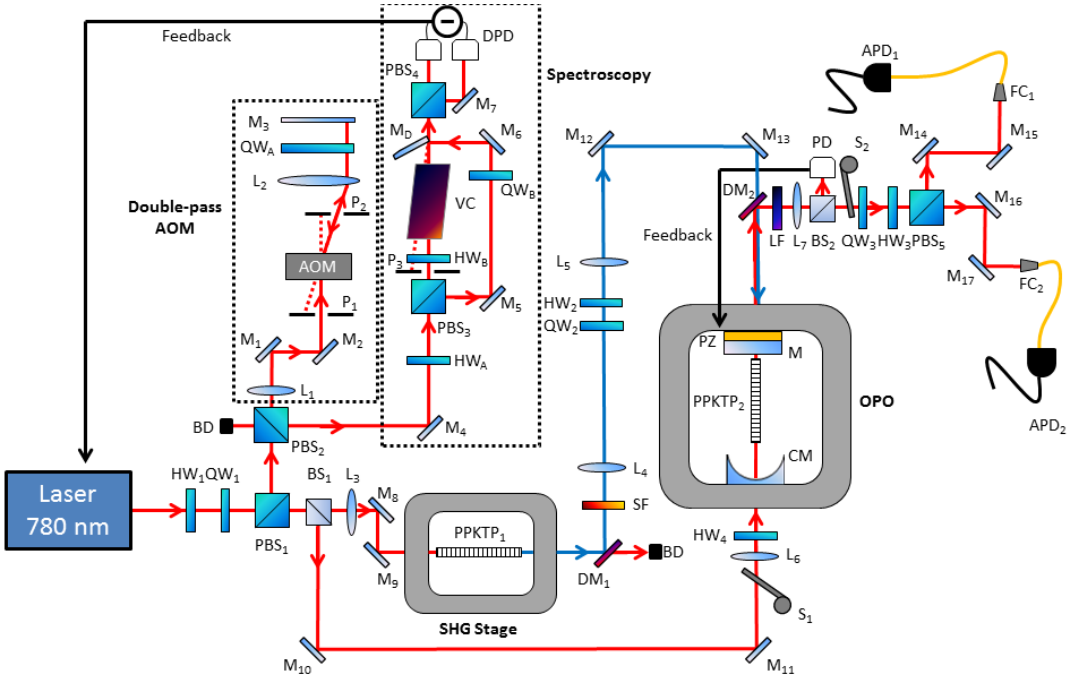
Table 5.1: **Specifications of some selected CE-SPDC-based narrow-band sources realized up to date.** The table covers devices realized at different wavelengths and with different schemes. Some works do not report all the considered parameters. The operating pump power generally is bound by practical limitations of the experimental set-up, although values that are far below 1 mW reflect a fundamental limitation of the source. This limitation is set by the threshold of the OPO used for CE-SPDC. In these cases, the spectral brightness referred to the pump power in mW is no longer a significant indicator for the source performance. The value of the heralded auto-correlation function at zero delay, $g_h(0)$ is considered for a heralding rate of 5×10^3 counts/s.

5.2 Experimental setup

In this section the experimental setup for the realization of the source is presented. A sketch of the setup is outlined in Figure 5.1.

The actual source is the OPO, which is operated far below threshold, at a pump power of at most a few mW. The OPO cavity is kept resonant to laser light (probe beam) coming from a tapered-amplified laser (Toptica TAPro780, up to about 1.5 W of power in single-mode fiber), which is tuned to Rb D2 line through polarization spectroscopy [233]. The same laser is used to pump a resonant monolithic frequency-doubler (SHG Stage), which provides the pump light for the OPO, at about 390 nm. The frequency at which the laser is locked, and, consequently, at which the photons are emitted, may be detuned from the Rb transitions by up to 180 MHz by means of an acousto-optic modulator (AOM, Gooch& Housego 3080-125) in a double-pass configuration [234].

The emitted photons have orthogonal polarizations and therefore can be separated at



AOM:	Acousto-Optic Modulator	HW:	Half-wave Plate
APD:	Avalanche Photo-Diode	M:	(Flat) Mirror
BD:	Beam Dump	M_D:	D-shaped Mirror
BS:	90:10 Beam Splitter	P:	Pinhole
CM:	Curved Mirror	PBS:	Polarizing Beam Splitter
DM:	Dichroic Mirror	PD:	Photo-Diode
DPD:	Differential Photo-Diode	PZ:	Piezo
FC:	Fiber Coupler	QW:	Quarter-wave Plate
L:	Lens	S:	Shutter
LF:	Long-pass Filter	SF:	Short-pass Filter
		VC:	Rubidium Vapour Cell

Figure 5.1: **Experimental setup.** Laser light at about 780 nm from a tapered-amplified laser (red lines in the figure) impinges onto the waveplates HWP_1 and QWP_1 and the polarizing beam splitter PBS_1. The reflected beam from PBS_1 is sent to a double-pass AOM and, afterwards, to a polarization-spectroscopy setup. This allows one to tune the laser to Rb D2 line with a variable frequency detuning, which is set by the AOM. The transmitted beam from PBS_1 is further split into two by means of a 90:10 beam splitter (BS_1), which transmits about 90% of the input power and reflects the remaining 10%. The reflected output beam (probe beam) is used for locking an OPO far below threshold, which constitutes the single-photon source, while the transmitted beam is used for resonant frequency doubling, so as to provide the pump at about 390 nm for the source (blue lines). The OPO is composed of three elements: a PPKTP crystal ($PPKTP_2$), a highly-reflective curved mirror and a partially reflective flat mirror with a piezo ring actuator. The flat mirror is used both as pump input and photon output coupler. The photon pairs produced in the OPO are separated from the pump by means of a dichroic mirror (DM2) and a long-pass filter (LF). The two photons of each pair are split at PBS_5, after compensation of polarization misalignment (by means of QWP_3 and HWP_3), and finally steered to two fiber-coupled APDs (APD_1 and APD_2) for photon counting. On the photon path, another 90:10 BS (BS_2) samples part of the probe beam, which perfectly overlaps with the single photons, in order to produce the feedback signal for the cavity piezo. Two shutters (S_1 and S_2) are used to switch between a cavity-locking phase and a photon-counting phase. More details about the setup are given in the text.

a polarizing beam splitter (PBS_5). After being separated, the photons are coupled to two single-mode fibers that are connected to avalanche photo-diodes (APD_1 and APD_2) for single-photon detection, respectively. Both single counts and coincidences are observed for the source characterization.

As the laser light used for cavity locking would make impossible single-photon detection and damage the APDs, cavity locking and photon counting are not performed simultaneously. The source operation cycle includes a cavity-locking phase, which lasts 0.2 s, followed by a photon-counting phase of 0.8 s. Two shutters (S_1 and S_2) are used to block the probe beam during the photon-counting phase and the path to the APDs during the cavity-locking phase, respectively. The different parts of the setup are described in more detail below.

Double-pass AOM

The AOM is used to shift in frequency the laser beam going to the spectroscopy part of the setup. This means that, if ν_t is the frequency of the selected Rb hyperfine transition and $\Delta\nu_{\mathrm{AOM}}$ the frequency shift induced by the AOM, the laser must be locked at $\nu_0 = \nu_t - \Delta\nu_{\mathrm{AOM}}$. The AOM can apply a variable frequency shift ranging from 60 to 90 MHz. As the AOM is built in a double-pass configuration, $\Delta\nu_{\mathrm{AOM}}$ may be tuned between 120 and 180 MHz. All the data presented in this dissertation are taken with $\Delta\nu_{\mathrm{AOM}}$ set to 180 MHz.

After reflection from PBS_1, the beam is transmitted by PBS_2, focused by the lens L_1 and steered to the AOM by means of mirrors M_1 and M_2, which are used to optimize the first-order diffraction efficiency to about 80%. The first-order-diffracted beam, which is shifted in frequency by $\Delta\nu_{\mathrm{AOM}}/2$, is separated from other diffraction orders by means of the pinhole P_2, then collimated by the lens L_2 and reflected back with orthogonal polarization by the combination of QWP_A and M_2. As a change in the AOM frequency shift also implies a slight change of the diffraction angle, the collimation lens L_2 is used to ensure that the beam is always reflected back along the same path while tuning $\Delta\nu_{\mathrm{AOM}}$. After the second passage into the AOM, the beam is diffracted back to the initial path

and reaches again PBS_2, where this time is reflected to the polarization spectroscopy setup. Pinhole P_1 cuts all other undesired diffraction orders. The overall efficiency of the double-pass AOM, defined as the power available for spectroscopy divided by the input power of the AOM, is about 64%.

Polarization Spectroscopy and Laser Lock

The purpose of the polarization spectroscopy setup is to provide an error signal for locking the laser to the frequency ν_0, which was defined in the previous paragraph.

The beam coming from PBS_2 is split into two beams with different power by means of HWP_A and PBS_3. The reflected beam is the more powerful and is called "pump", the transmitted beam instead is indicated as "probe" and is about 10 times less powerful than the pump. The pump polarization is set to circular by QW_B, while the probe (linear) polarization is rotated by 45° by means of HW_B. Pump and probe beams are both sent to a Rb vapour cell (VC) in counter-propagating directions, as in any doppler-free-spectroscopy scheme [235]. A distinctive feature of polarization spectroscopy is that absorption of the circularly polarized pump induces circular birefringence in the vapour cell, which is detected by the probe. This detection is performed by means of PBS_4 and a differential photo-diode (DPD). The photo-diode provides a voltage signal that is proportional to the difference between the optical power at the two outputs of PBS_4. In absence of the pump beam, the diagonally polarized probe beam impinging onto PBS_4 would be split into two beams with the same power and therefore determine a zero signal. With the pump beam travelling through VC, instead, the probe polarization is rotated by a frequency-dependent angle, which follows the spectral profile of the Rb hyperfine transitions, as explained in detail in [236]. By scanning the laser frequency, therefore, a signal that is proportional to the derivative of the Rb hyperfine spectral lines is obtained from the DPD, as shown in Figure 5.2. The frequency scanning is performed by means of a piezo that is integrated in the laser cavity.

The plot in Figure 5.2 is linear around the central frequencies of the transitions. This feature is particularly suitable for laser locking, as, when the laser frequency drifts away

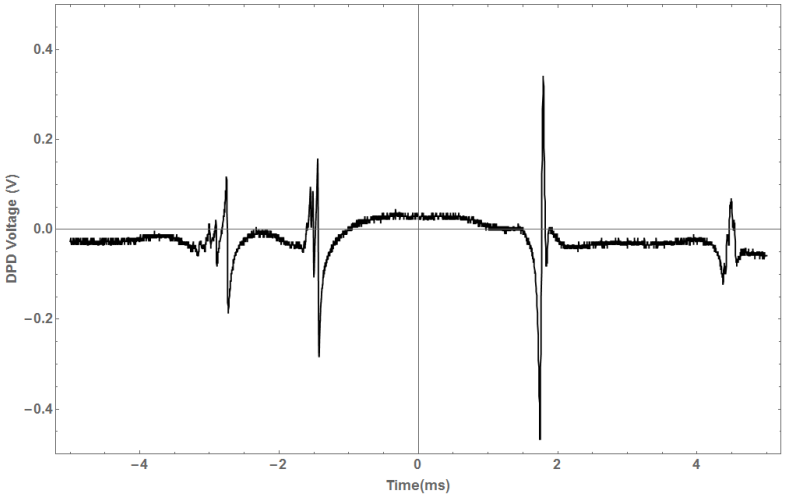


Figure 5.2: **Rb spectrum from polarization spectroscopy.** The figure shows the signal from the DPD while the laser frequency is scanned. The signal is recorded on an oscilloscope, which is set to show only one period of the laser scan. The four groups of hyperfine transitions constitute the D2 lines of Rb^{85} and Rb^{87}, respectively, with two groups associated to each isotope. The laser is locked at the frequency corresponding to the most prominent transition of the first group on the left, the $5^2S_{1/2}, F = 2 \rightarrow 5^2P_{3/2}, F' = 3$ transition of ^{87}Rb (from a comparison with [237]).

from a given transition frequency, the DPD produces an error signal that is proportional to the frequency drift. The laser controller (Toptica DLPro) includes an analog Proportional-Integral-Differential (PID) Control Loop [238] that takes this error signal as an input and provides feedback to the laser piezo in order to compensate the drift. The slope of the line influences the quality of the lock; ideally one wishes a steep line so that a tiny drift in the laser frequency determines a large error signal. From this point of view, the implemented polarization spectroscopy setup, with a PBS for detection of polarization rotation, provides a better signal than other spectroscopic methods [236].

The selected transition for laser lock, $5^2S_{1/2}, F = 2 \rightarrow 5^2P_{3/2}, F' = 3$ of ^{87}Rb, occurs at 384.228115 THz [239], leading to $\nu_0 = 384.227935$ THz. The laser frequency is measured to be 384.2276 THz with a wavemeter (HighFinesse WS-600) having 600 MHz accuracy, which is compatible with the expected value of ν_0. The reading of the wavemeter over an interval of several hours shows no frequency drift within the precision of the instrument (≈ 5 MHz). The bandwidth of the laser could not be measured precisely due to the insufficient sensitivity of the available instruments. Measurements performed

with a Fabry-Perot spectrum analyser (Thorlabs SA200-8B) suggest that the laser has sub-MHz bandwidth when locked, as also confirmed by the manufacturer.

The resonant frequency doubler

The pump light at 390 nm for the source is obtained by frequency doubling the frequency-stabilized laser at 780 nm. The frequency doubling occurs in a 20 mm long, type-I PPKTP crystal (from Raicol Crystals) whose input and output facets are mirror-coated (the coatings were applied by LaserZentrumHannover). The facets' dimensions are 1×2 mm; one of them (the input one, closer to mirror M_9) has a radius of curvature of 34 mm, while the other one is flat. The nominal reflectivity of the input facet is $94.0 \pm 0.5\%$ at 780 nm and $99.9 \pm 0.5\%$ at 390 nm. The output facet has a reflectivity of $97.0 \pm 0.5\%$ at 780 nm and is AR-coated for 390 nm (reflectivity lower than 0.2%). This means that the frequency-doubling resonator is only resonant at 780 nm, the fundamental wavelength. The second-harmonic radiation exits the resonator from the output facet only and is separated from the fundamental light by means of dichroic mirror DM_1. The PPKTP crystal is placed in a copper oven, which is is temperature stabilized by a Peltier element and is controlled by an analog PI temperature controller (WavelengthElectronics PTC5K-CH) interfaced with LabView through a Digital-to-Analog Converter (DAC, MeasurementComputing DT9847-2-2). The temperature is measured by means of a thermistor (Epcos B57045, negative thermistor), which is located in a hole in the copper holder. The oven is placed inside a stainless steel box with optical windows, for thermal and vibration isolation.

The PPKTP crystal was characterized prior to the mirror coating of the facets. The phase-matching temperature for second-harmonic generation at the laser frequency was found to be 46.3 C° with a temperature bandwidth of 0.7 C°. The group index of the crystal for the phase-matched polarization at the fundamental wavelength is 1.917 at 46.3°C [240]. Considering this value and the geometric parameters of the resonator, the waist of the resonator TEM_{00} mode is calculated to be 62.4 μm. Lens L_3 is used for mode-matching, whereas mirrors M_8 and M_9 are used to align the beam to the resonator

axis. The fraction of the total power transmitted at the fundamental wavelength and in the TEM_{00} mode is 95%.

In the single-pass configuration, a maximum SHG power of 0.5 mW was measured, at 160 mW of power at 780 nm. After mirror coating, the maximum SHG power with the same fundamental power was 7.2 mW, resulting in a conversion efficiency of 4.5%. The resonator, therefore, induces an improvement of more than one order of magnitude to the generated UV power.

This value, however, is far below the expected SHG power of about 44 mW, which is calculated following the treatment of [241]. The potential factors contributing to this mismatch are multiple. One of them is significant absorption of blue power in the crystal, which was not considered in the calculation of the expected conversion efficiency. In fact, a previous work on resonant frequency doubling in a ring resonator with a 10-mm-long PPKTP crystal has found an overall absorption of 27% at 390 nm [242]. For the SHG stage of the narrow-band source, an even higher absorption is expected, given the higher length of the crystal and the standing-wave configuration of the OPO cavity.

Another cause of non-optimal emission is given by opto-thermal effects. Among them, the most relevant are thermal lensing, which degrades the mode-matching to the resonator TEM_{00} mode, and thermally-induced inhomogeneity of the crystal refractive index, due to inhomogeneous power distribution in the cavity, which prevents the phase-matching condition from being fully satisfied over the whole crystal. Furthermore, the dependence of the circulating power in the monolithic resonator on the temperature is complicated by absorption of both fundamental and frequency-doubled radiation, and the consequent heating of the crystal. Due to this effect, it is difficult to stably keep the cavity at full resonance.

The thermal effects represent the ultimate limiting factor to the conversion efficiency when the power is increased. The obtained SHG power, in fact, tends to saturate for higher fundamental power at about 7.3 mW. For a given fundamental power, the SHG power slowly drifts with time by about 10% after a few hours.

Finally, the high power inside the resonator may induce *gray tracking* in the PPKTP,

i.e. the laser-induced creation of color centers or other microscopic structural deformations in the crystal, which significantly increases absorption [243].

After the SHG stage, the radiation at 390 nm is reflected by DM_1, further cleaned from residual radiation at 780 nm with two short-pass filters, forming a single filtering stage (SF) with a transmission of 10^{-9} at 780 nm, and collimated by the lens L_4. The UV beam passes through the polarization-controlling elements QWP_2 and HWP_2, and then is steered to the OPO via the mirrors M_{12} and M_{13}, after transmission through DM_2. Mode-matching with the OPO is ensured by lens L_5.

The OPO

The OPO is composed of a curved mirror (CM), a flat mirror (M) and a 20 mm-long type-II PPKTP crystal, phase-matched for collinear degenerate SPDC from 390 nm to 780 nm. The curved mirror has a radius of curvature of 100 mm and a nominal reflectivity of $(99.9 \pm 0.1)\%$ at 780 nm while being AR-coated for 390 nm. The flat mirror has a nominal reflectivity of $(97 \pm 1)\%$ at 780 nm and a measured reflectivity of $(30 \pm 2)\%$ at 390 nm. The crystal facets are AR-coated for both 780 and 390 nm with a nominal residual reflectivity at 780 nm of $0.50 \pm 0.05\%$. A ring piezo-actuator (PZ) is glued to the flat mirror for scanning and locking the OPO cavity. The maximum elongation of the piezo is 2 μm corresponding to about 5 times the cavity FSR.

The crystal is placed in an oven (see Figure 5.3). The oven is mounted vertically on a 5-axis stage (Thorlabs PY005), which allows one to translate the crystal in all directions in space and adjust its pitch and yaw. The temperature-controlling elements (thermistor, Peltier, controller and related digital interface) are the same as for the SHG stage. The accessible temperature range for both ovens is between 10°C and 50°C, in which the temperature stability is about 0.001°C. The whole OPO is inserted into a stainless steel box for thermal and vibration isolation.

The reflected 10% output of BS_1 (probe beam) is steered and mode-matched to the OPO cavity by means of mirrors M_{10}, M_{11} and lens L_6, respectively. The half-wave plate HW_4 is used to rotate the polarization of the beam and thus to observe the resonant

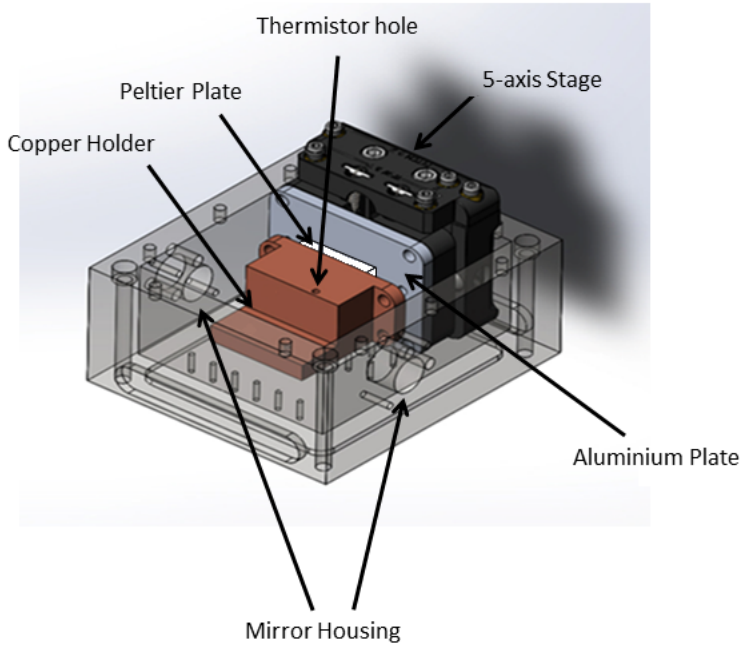


Figure 5.3: **Opto-mechanical parts of the OPO.** The crystal holder, made of copper, is fixed to the 5-axis stage through an aluminium adapter plate. A Peltier plate providing heating or cooling power is inserted between the holder and the 5-axis stage. Temperature is measured by means of a thermistor, which is inserted into the thermistor hole. Peltier Plate and thermistor are connected to a PI temperature controller, which is interfaced to LabView via a DAC. The temperature-controlling elements are the same as used for the oven of the SHG stage. The oven is inserted into a stainless steel box, with two holes functioning as mirror housing. The whole system, with the addition of mirrors and crystal, thus constitutes the OPO. The other holes shown in the box are designed for screws fixing the box to the optical table or connecting the lower part of the box to an upper lid.

modes for both polarizations, which do not coincide due to the birefringence of the OPO. A coupling efficiency of about 90% to the TEM_{00} mode of the cavity is observed. The TEM_{00} mode has a calculated waist of 108 μm at mirror M for both polarizations. The output beam from the OPO is measured at a photodiode (PD), after sampling 10% of it at BS_2. In this way, the resonance modes of the cavity can be analyzed while either the red laser frequency or the cavity length is scanned.

The transmission peaks at PD obtained from the cavity-length scan are used to provide the error signal for a PID controller (Toptica DigiLock), which sends feedback to the piezo to keep the cavity resonant to the probe beam. The cavity is locked side-of-the-fringe, with the lock intensity set at about 90% of the maximum. The locking cycle of

the OPO is the following:

1. Shutter S_2 opens while S_1 is closed so that the produced photons can be safely detected. This is the counting phase, which lasts 0.8 s. During this phase, the PID controller is not active, meaning that the cavity length is free to drift. The transmitted power stays within 10% of the value at lock after 1 s of free drift, which justifies the chosen duration of the counting phase.

2. Shutter S_2 closes and both shutter stay closed for 0.1 s. This waiting time is used to prevent damage to the detector due to delays in shutter operation.

3. Shutter S_1 opens, the cavity length is scanned and the side-of-the-fringe lock is performed. This is the locking phase, whose duration is 0.2 s. This value is determined by the time needed for scanning and locking the cavity.

4. Shutter S_1 closes and both shutter stay close for 0.1 s. This phase has the same purpose of phase 2.

5. The cycle starts again from phase 1.

The overall cycle lasts 1.2 s and can run for hours without significant changes. The shutters are controlled by a LabView code, while the cavity lock and scan are set within the DigiLock control software, provided by the PID manufacturer.

Photon splitting and detection

The photons exit the OPO from mirror M, which serves as output coupler for the radiation at 780 nm. As they are produced in the OPO cavity, their spatial properties are exactly the same as the transmitted red beam, which is therefore used for alignment and calibration purposes. Residual pump is cut by a long-pass filter (LF), after which the photon beam is collimated (lens L_7). Part of the photons are lost at BS_2 due to the sampling of the red beam for the lock. After the shutter S_2, the photons are separated by means of a polarizing beam splitter (PBS_5), preceded by two compensation waveplates,

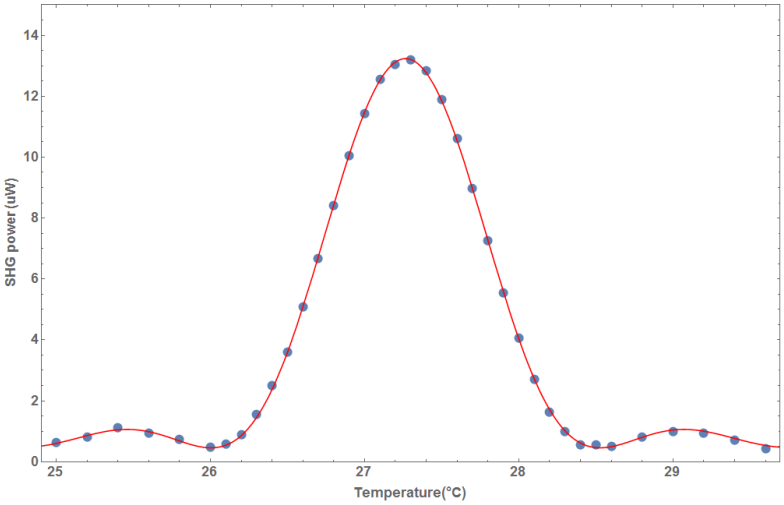


Figure 5.4: **Phase-matching curve for the PPKTP crystal.** The plot shows the generated second-harmonic power (at about 390 nm) with respect to the crystal temperature when pumping at 107 mW of NIR power (780 nm). The power is measured after a dichroic mirror and a short-pass filter, whose losses are neglected. The experimental points (in blue) are fitted with a function of the kind $P = B + M\mathrm{Sinc}[A(T - T_0)]^2$ (red line), where P is the SHG power, T is the temperature and B, M, A and T_0 are the fit parameters. The phase-matching temperature, T_0, is found to be $(27.266 \pm 0.001)°\mathrm{C}$. The parameter A is $(2.489 \pm 0.006)°\mathrm{C}^{-1}$, from which the phase-matching bandwidth, ΔT_{FWHM} can be extracted, according to the formula $\Delta T_{\mathrm{FWHM}} = (2\pi\ 0.4425)/A$. The maximum generated second-harmonic power, after background ($B = (0.46 \pm 0.02)\mu\mathrm{W}$) subtraction, is $M = (12.78 \pm 0.03)\mu\mathrm{W}$.

which correct for polarization misalignments or alterations. Each of the photon beams after the beam splitter is coupled into a single-mode fiber using two mirrors and a fiber coupler. The fibers are connected to two avalanche photo-diodes (Excelitas SPCM AQRH-13) with about 60% detection efficiency. The fiber-coupling efficiency is measured to be 85% for both fibers. The photons experience an additional loss of 10% between the cavity and the detectors due to the long-pass filter and absorption or scattering at the optical elements on their path.

5.3 Source characterization

In this section the results of the source-characterization measurements are presented. As the properties of the emitted photons strongly depend on the OPO parameters, a preliminary characterization of the OPO is performed with laser light. The single-photon

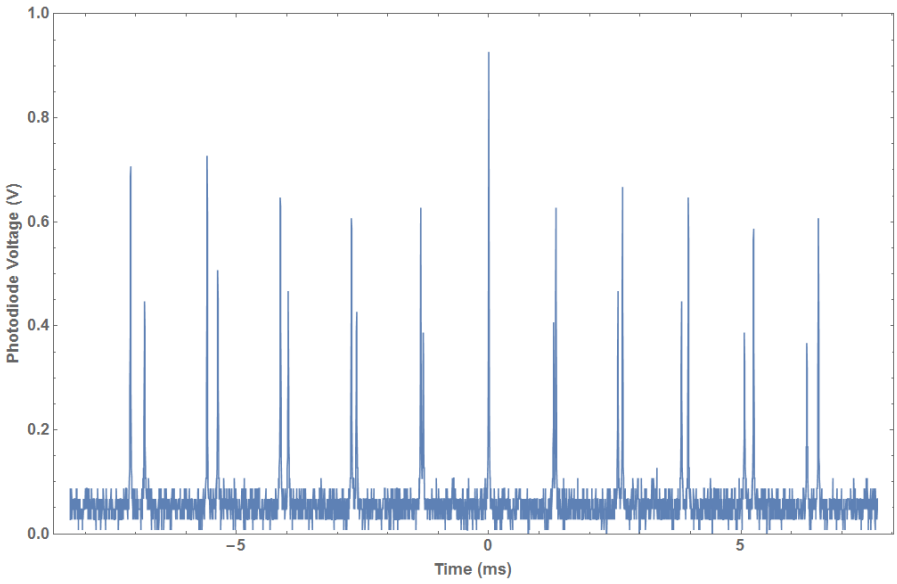


Figure 5.5: **Transmission peaks from the OPO.** The peaks are obtained by scanning the laser around the frequency ν_0 and by measuring the transmitted power after the OPO cavity with a photo-diode, which is connected to an oscilloscope. The figure shows a single scan of the laser frequency in one direction. The input polarization to the cavity is set such that the horizontal component (signal) is smaller than the vertical component (idler), so as to easily distinguish the two sets of peaks of the birefringent cavity. Two peaks from the two different sets fully overlap at frequency ν_0, corresponding to 0 ms in the plot. The separation between the corresponding peaks of the two sets increases with the distance from the overlapping pair. The different peaks of each set appear to have different heights due to the limited sampling rate of the oscilloscope over the visualized time range.

measurements are then used to confirm the results of the preliminary characterization and to provide more information on the source performance.

5.3.1 Classical characterization of the OPO

Characterization of the PPKTP crystal

In order to efficiently operate the source, it is necessary to know exactly at what temperature the desired SPDC process is phase-matched in the PPKTP crystal and what is the allowed temperature mismatch. Therefore, before inserting the OPO mirrors, the crystal was placed in the oven and type-II second-harmonic generation with the fundamental wave at frequency ν_0 was studied. This process in fact has the same phase-matching properties as type-II degenerate SPDC that produces single photons at ν_0 from

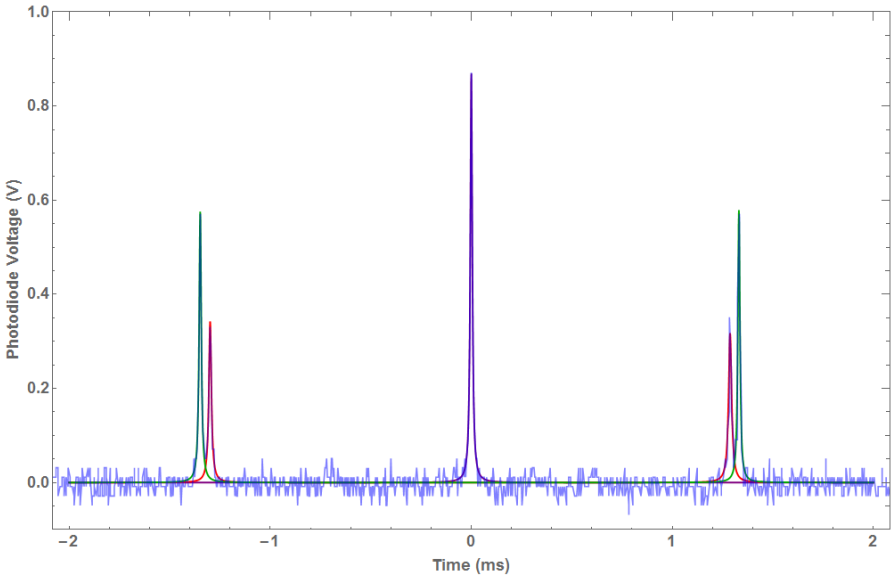


Figure 5.6: **Lorentzian fit of the OPO peaks.** The fit curves of the signal peaks are indicated in red, while those for the idler peaks in green. The fit of the central peak, for which signal and idler modes overlap, is drawn in purple. In order to simplify the fits, the background noise voltage has been subtracted. The function used for the fits is therefore $V(t) = V_{max}(1 + \frac{1}{4}\gamma^2(t - to)^2)^{-1}$, where t represents time, V voltage and the fit parameters are the maximum voltage, V_{max}, the peak position, t_0, and the width parameter γ.

an UV pump at $2\nu_0$. The fundamental power of the near-infrared (NIR) beam was set to 107 mW and the generated UV power was measured after the crystal, the dichroic mirror DM_2 and a short-pass filter, while varying the oven temperature. The results are shown in Figure 5.4. The phase-matching curve has a maximum at (27.266 ± 0.001)°C and a FWHM of (1.117 ± 0.003)°C. A second-harmonic conversion efficiency of about 0.1%/W can be inferred from the curve maximum.

Characterization of the cavity modes

The OPO cavity is characterized by using the laser at 780 nm. The laser frequency is scanned by about 20 GHz and the corresponding cavity transmission is measured at the photodiode that is placed after BS_2. Prior to the measurement, the laser was locked to the frequency ν_0 and double resonance was obtained by tuning the temperature of the crystal within the phase-matching bandwidth and by adjusting its pitch and yaw by a few degrees at most. This adjustment set the temperature of operation to 27.52°C.

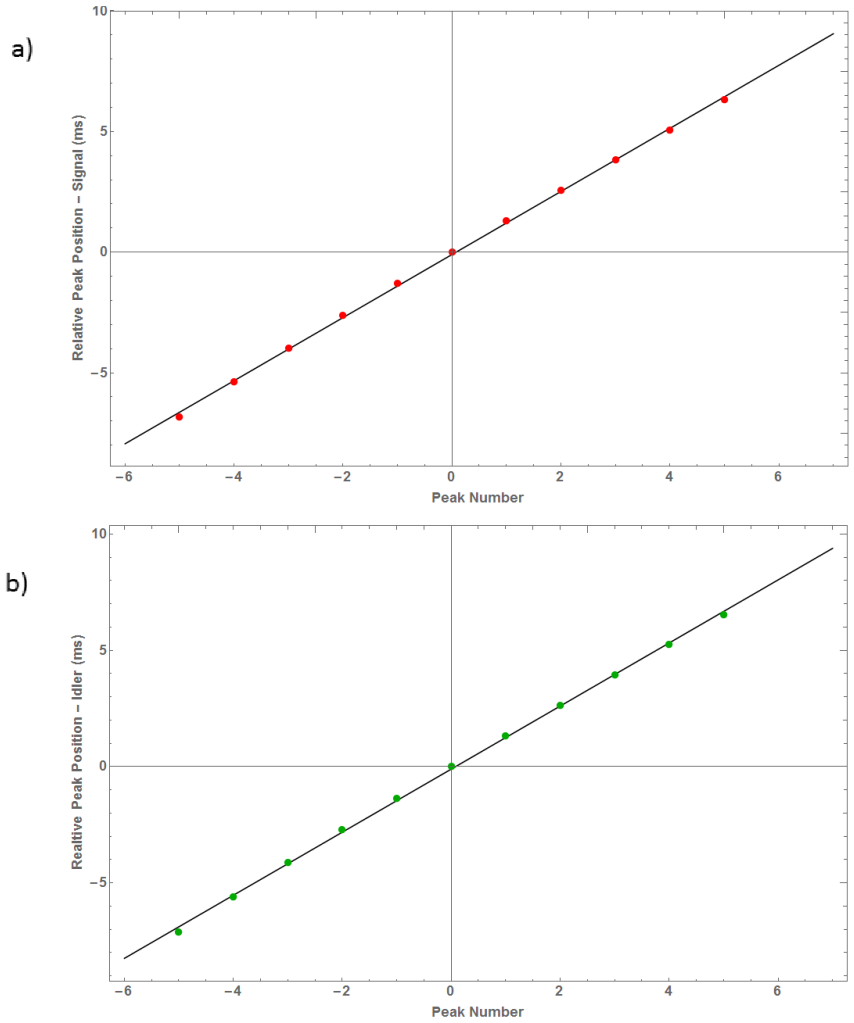


Figure 5.7: **Peak position vs peak number for signal and idler.** The experimental points are indicated in red for the signal (a) and in green for the idler (b), respectively, while the fitted lines are in black. The equation for the lines is, for both plots, $t_n = t_{\mathrm{FSR}} \times n$, where t_n is the position of the $n-$th peak, n is the peak number relative to the central peak and t_{FSR} is the time interval in which the laser frequency changes by a FSR. From the fits, it is obtained: $t_{\mathrm{FSR}_s} = (1.36 \pm 0.01)$ ms and $t_{\mathrm{FSR}_i} = (1.31 \pm 0.01)$ ms. The FSR in frequency can be obtained from the relation $\mathrm{FSR} = v \times t_{\mathrm{FSR}}$, with v scan speed.

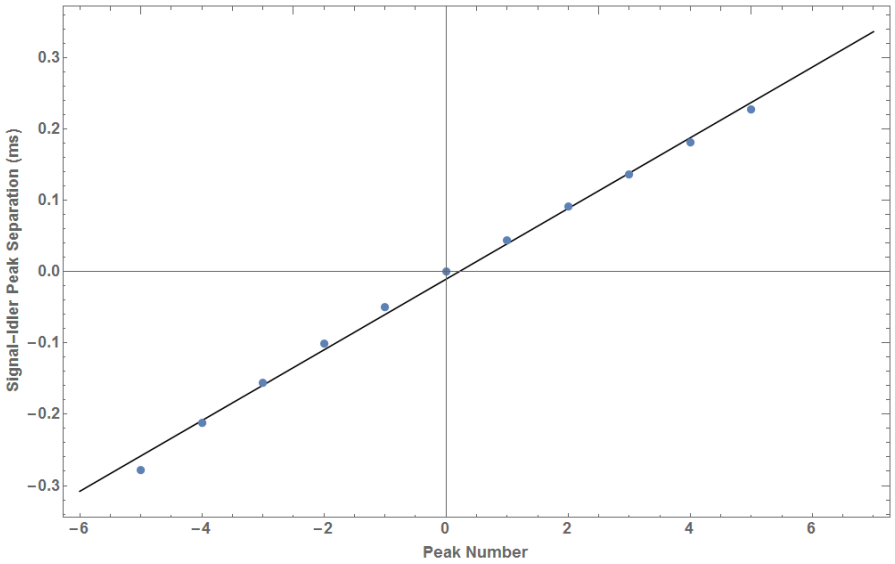


Figure 5.8: **Signal-idler peak separation vs peak number.** The experimental points are in blue, while the fitted line is in black. The equation for the line is $\Delta t_n = \Delta t_{\mathrm{FSR}} \times n$, with Δt_{FSR} difference between the values of t_{FSR} for signal and idler. From the fit it is obtained $\Delta t_{\mathrm{FSR}} = (50 \pm 1) \times 10^{-3}$ ms.

After that, the laser was scanned around ν_0 and the measurement was started. As the cavity is not locked during the measurement, the scanning period is set to 30 ms so as to avoid any drift from the double-resonance condition within a single scan.

The signal from the photo-diode is visualized on an oscilloscope and reported in Figure 5.5. All the peaks are fitted with Lorentzian functions such that the precise position in time and the linewidth of each peak is obtained. An example of the fits is shown in Figure 5.6.

In Figure 5.7 the peak positions obtained from the fits are plotted with respect to the peak number, relative to the central peak, both for signal and idler. As expected, the dependence is linear, as the peaks of each set are separated by a fixed distance, corresponding to the time interval in which the frequency of the laser changes by a cavity FSR. In order to convert this time into frequency, it is necessary to know the scan speed. This is measured by using a wavemeter and is found to be $v = (1.855 \pm 0.002)$ GHz/ms. Consequently, the values of FSR for signal and idler are calculated to be: $\mathrm{FSR}_s = (2.52 \pm 0.02)$ GHz and $\mathrm{FSR}_i = (2.42 \pm 0.02)$ GHz. In order to calculate the cluster

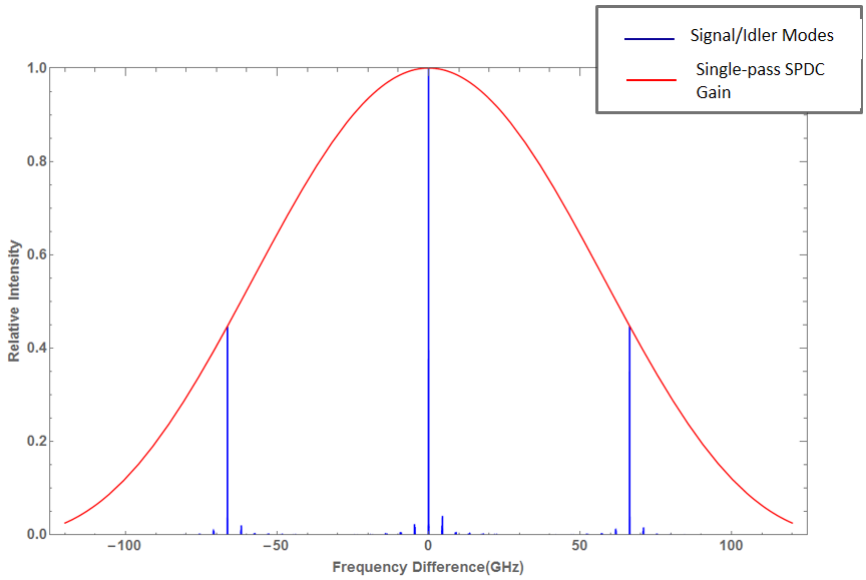


Figure 5.9: **Expected spectrum for the SPDC signal/idler fields.** The photon spectrum (blue peaks) is obtained from the analysis of the OPO cavity transmission peaks. The frequency difference on the horizontal axis is referred to the central mode at frequency ν_0. The spectrum is made of three clusters, separated by $\Delta\nu_C$, which contain each a main mode, corresponding to full overlap of the signal and idler peaks, and a few side modes, corresponding to the partial overlap of cavity modes with different polarizations. The central cluster represents degenerate emission, while the side ones emission of photons at different frequencies. The red solid line is the single-pass SPDC gain, which is obtained from Equation 2.22. The FWHM of the red curve is 125 GHz, calculated according to Equation 2.31.

separation, the difference $\mathrm{FSR}_s - \mathrm{FSR}_i$ is needed. However, calculating this difference from the single values of the FSR would lead to a very large relative error. Alternatively, the signal-idler peak separation may be plotted with respect to the peak number. This dependence is expected to be of the form: $\Delta t_n = (t_{\mathrm{FSR}_s} - t_{\mathrm{FSR}_i}) \times n = \frac{\mathrm{FSR}_s - \mathrm{FSR}_i}{v} \times n$. The required difference can then be obtained with higher precision from a linear fit of the plot. The fit is shown in Figure 5.8, from which it results $\mathrm{FSR}_s - \mathrm{FSR}_i = (92 \pm 2)$ MHz. This leads to a cluster separation (see Equation 2.41) of $\mathrm{FSR}_c = (66 \pm 1)$ GHz. Based on this value, it is possible to estimate the spectrum of the SPDC fields, which is shown in figure5.9, together with the SPDC single-pass gain, obtained from Equation 2.22.

From the fit of the transmission peaks, the linewidth of the cavity modes, and consequently the finesse of the cavity, may be extracted. The average time width (FWHM) of the peaks is $(13 \pm 1) \times 10^{-3}$ ms for the signal modes and $(16 \pm 2) \times 10^{-3}$ ms

Parameter	Value	Error	Unit
Phase-matching temperature	27.266	0.001	°C
Phase-matching bandwidth	1.117	0.003	°C
Signal FSR	2.52	0.02	GHz
Idler FSR	2.42	0.02	GHz
Cluster Separation	66	13	GHz
Signal Finesse	107	5	-
Idler Finesse	83	11	-
Threshold power	≈ 2	-	W

Table 5.2: **OPO parameters.** The parameters are obtained from the classical characterization of the OPO. The phase-matching properties of the crystal are extracted from the phase-matching curve of type-II collinear degenerate SHG from 780 nm to 390 nm. The resonator properties are measured by means of laser light and a wavemeter.

for the idler modes. After multiplying these widths by the scan speed v, the frequency linewidth of the cavity modes are found to be (24 ± 2) MHz and (30 ± 4) MHz for signal and idler, respectively. This means that the finesse is $\mathcal{F}_s = 107 \pm 5$ for horizontally polarized light and $\mathcal{F}_i = 83 \pm 11$ for vertically polarized light. This difference shows that the losses in the OPO are polarization-dependent. Such a dependence might be caused by a polarization-dependent behaviour of the coatings of mirrors and crystal facets and/or scattering or deflection of the extraordinary polarization in the crystal due to crystal tilting. The measured values of the finesse are compatible with the nominal finesse of 120 ± 30, which has a large error due to the uncertainty of the nominal values of mirror and AR-coating reflectivities. Inserting the values of the finesse in expression 2.35, the threshold power of the OPO is estimated to be $P_{th} \approx 2W$. For the calculation of the threshold power, the refractive indices of the KTP are $n_s = 1.80$, $n_i = 1.92$, $n_p = 2.41$ [240], the non-linear coefficient is assumed to be $\chi^{(2)} = 2d_{15} = 3.8$ pm/V [244] and the illuminated area A is approximated as $\pi w_{0_p}^2$, with $w_{0_p} = 76$ μm waist of the pump beam in the cavity. The results of the classical characterization of the OPO are summarized in Table 5.2.

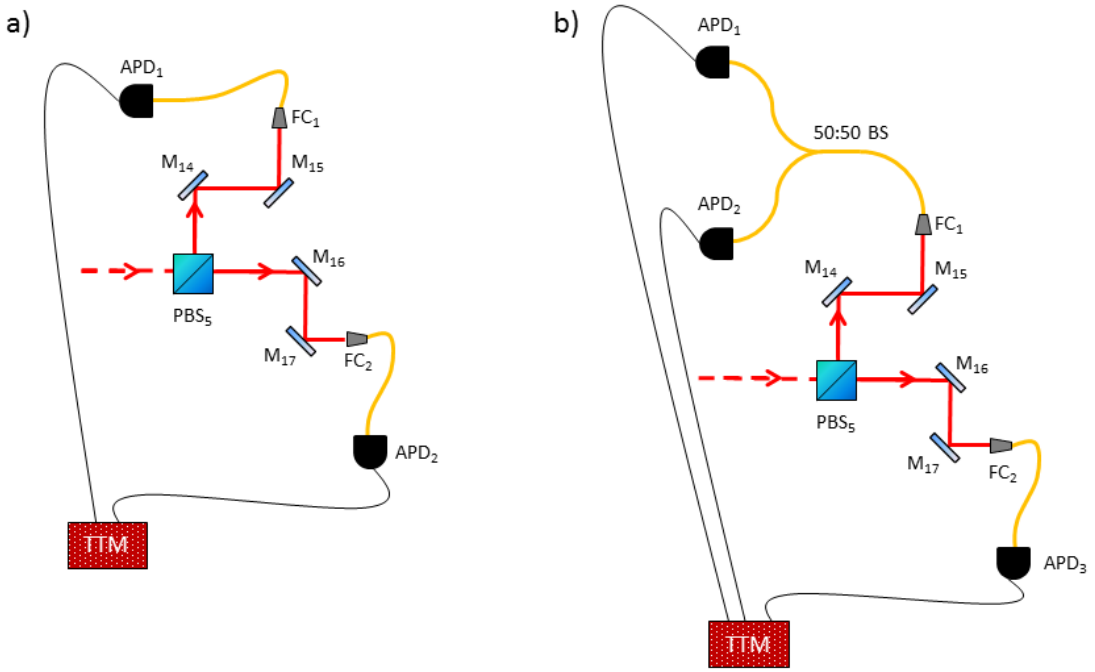


Figure 5.10: **Detection configurations for single-photon counting.** The notation follows that in Figure 5.1. In both configurations the output electronic signal of the APDs is connected to a time-tagging module (TTM). In configuration a), two detectors are used and the TTM records the single-detection and coincidence rates, together with the related arrival-time information. This information is used to extract the signal-idler cross-correlation function. In configuration b), the idler arm is split into two by means of a 50:50 fiber beam splitter, whose outputs are connected to detectors APD_1 and APD_2. In this case, it is possible to record the two-fold coincidence rate between any two detectors as well as the three-fold coincidence rate, with the related time information. This configuration is used to measure the auto-correlation functions and the multi-photon generation rate.

5.3.2 Single-photon measurements

The measurement with single photons are taken with the two detection configurations shown in Figure 5.10. The signal from the APDs is connected to a time-tagging module (TTM, RoithnerLaserTechnik TTM8000), which records the time at which each detection occurs, relative to an internal clock, and therefore can provide single-detection rates and coincidence rates of two or more detectors. The TTM is also used to reconstruct the temporal profile of the coincidences.

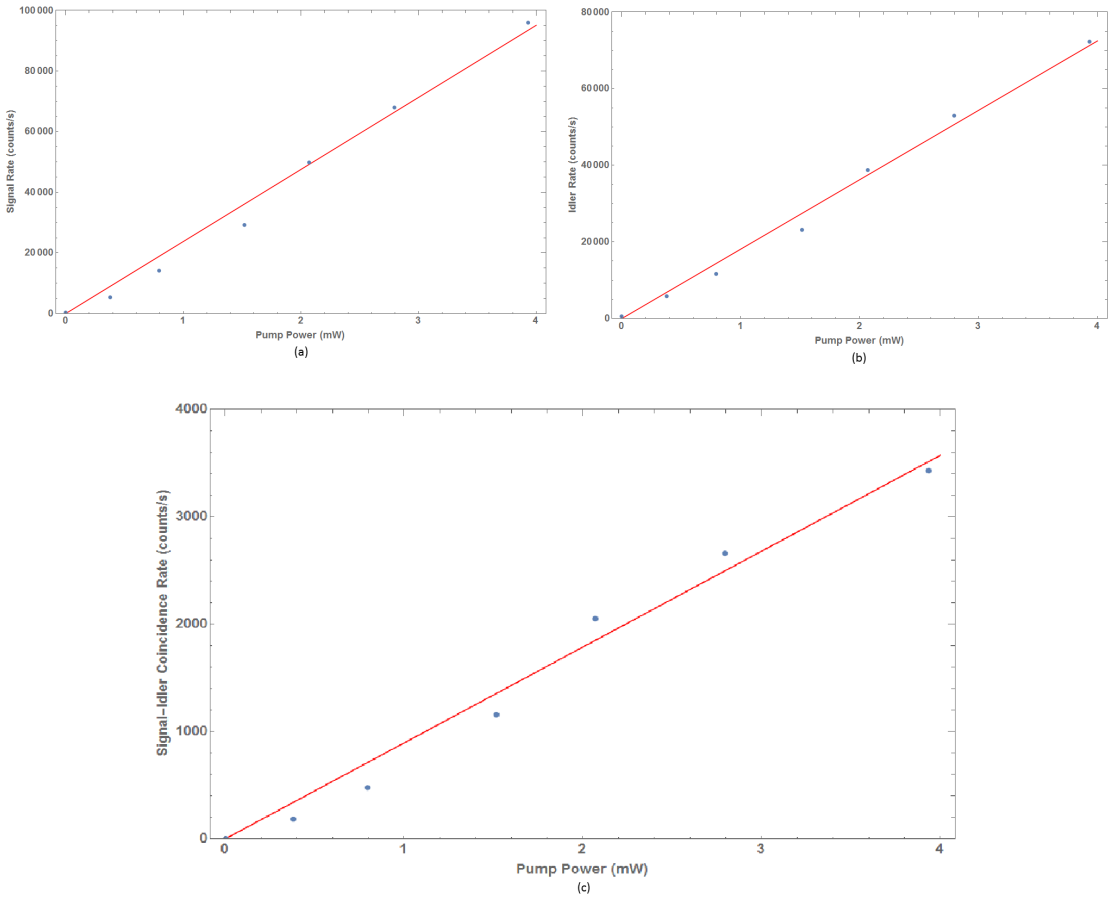


Figure 5.11: **Single-detection (a,b) and coincidence rates (c) vs pump power.** The rates are measured in the configuration shown in Figure 5.10-a. The error bars, obtained assuming Poissonian errors on the counts, are within the size of the experimental points. The coincidence rate is corrected for accidentals, which are calculated as the product of the two single-detection rates and the coincidence window (20 ns). The red lines are linear fits of the rate-power dependence. The angular coefficients of the lines are $(23 \pm 2) \times 10^3$ counts/(s mW) for the signal counts, $(18 \pm 1) \times 10^3$ counts/(s mW) for the idler counts and $(0.89 \pm 0.06) \times 10^3$ counts/(s mW) for the coincidence counts.

Photon rates

Figure 5.11 shows the measured single-detection and signal-idler coincidence rates with respect to the pump power. The maximum concidence rate, obtained at 3.9 mW of pump power entering the OPO cavity results to be 3429 ± 8 counts/s. The corresponding pair generation rate, R_0, can be calculated as the ratio between the product of the two single-detection rates and the coincidence rate. The result of this calculation is $R_0 = (2.022 \pm 0.008) * 10^6$ pairs/s. This corresponds to an overall transmission of about 5% for the signal and 4% for the idler, which correspond to the heralding efficiencies for idler and signal, respectively. Taking into account the escape probability from the cavity (59%), the transmission of the optical elements that are placed after the OPO (80%), the fiber-coupling and detection efficiency (85% and 60%, respectively), the overall transmission for both fields is expected to be about 24%. This means that significant additional losses occur in the crystal or at the interface between the crystal and air. The bi-photon detection and generation rates normalized to the pump power are $(0.89 \pm 0.06) \times 10^3$ counts/(s mW) and $(4.6 \pm 0.6) \times 10^5$ counts/(s mW), respectively.

In order to characterize higher-order emission from the source, the idler-idler coincidence rate is recorded (with the detector configuration depicted in Figure 5.10-b). This is shown in Figure 5.12. The highest idler-idler coincidence rate, for a pump power of 3.9 mW is (16.0 ± 0.3) counts/s. The coincidences scale quadratically with the power with a scaling factor $A = 1.13 \pm 0.17$ counts/(s mW^2). By considering the losses, this means that the source produces double pairs with a rate of $(5.7 \pm 0.8) \times 10^2$ counts/(s mW^2). Clearly, this rate is negligible with respect to the single-pair generation rate.

Signal-Idler Cross-correlation function

In order to obtain spectral information on the produced photons, the signal-idler cross-correlation function is measured (see Section 2.4.1), using the setup shown in Figure 5.10-a. This function is inferred from measuring the number of coincidences between the signal and idler arms with respect to the delay between the two single detections. The result of the measurement is shown in Figure 5.13.

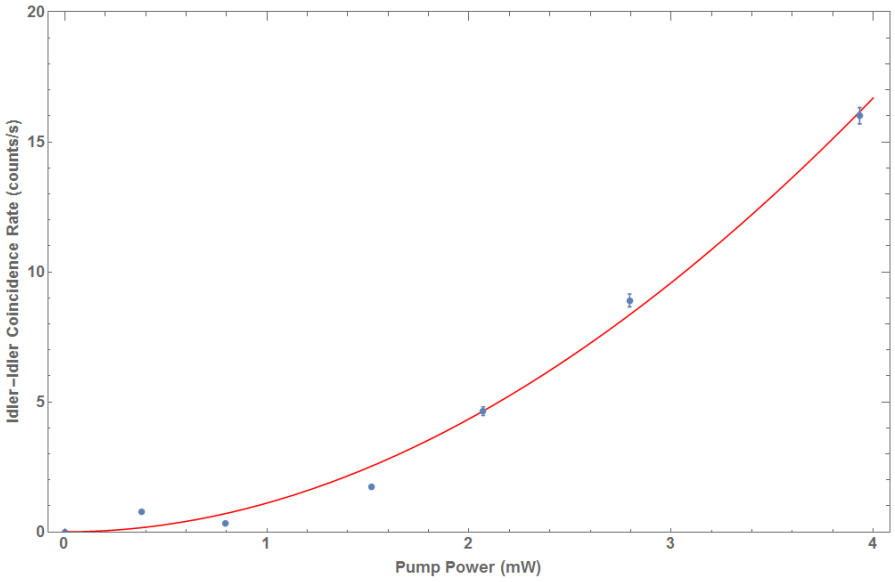


Figure 5.12: **Idler-Idler coincidence rate vs pump power.** Here the coincidences between detectors APD_1 and APD_2 in Figure 5.10-b are reported, after correction for accidentals and with the coincidence window set to 20 ns. These coincidences can be only produced by double-pair-emission (or higher) terms in the idler arm. The Poissonian error bars are visible given the lower values of the counts. The red solid line represents a polynomial fit function, of equation $r = A * P^2 + B * P^3$, with r coincidence rate and P pump power. The fit provides $A = 1.13 \pm 0.17$ counts/(s mW)^2 and $B = -0.02 \pm 0.05$ counts/(s mW)^3. The value of B is far lower than that of A, and statistically compatible with 0, meaning that the curve is dominated by double-pair emission.

The cross-correlation data are fitted with a double-exponential function:

$$c = B + M(\theta(t - t_0)e^{-2\gamma_s(t-t_0)} + \theta(t_0 - t)e^{2\gamma_i(t-t_0)}), \tag{5.1}$$

where c is the recorded number of coincidences, θ the Heaviside step function, t represents the time delay, t_0 is the time delay for which the coincidences are maximum, B is the number of background coincidences, M is the maximum number of coincidences and γ_s, γ_i are the decay rates for positive (signal) and negative delays (idler), respectively.

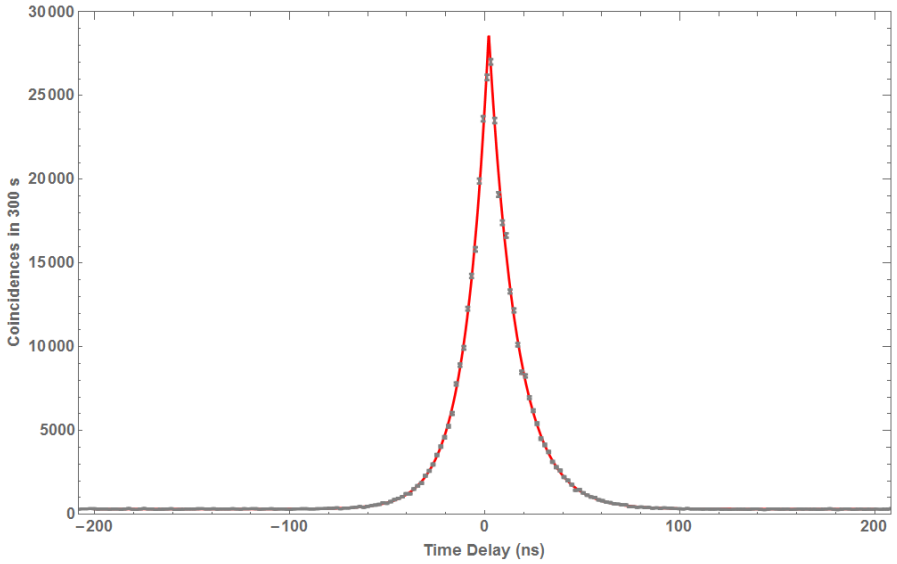


Figure 5.13: **Signal-idler cross-correlation profile.** The experimental points are indicated in gray and the error bars are obtained by assuming Poissonian statistics for the counts. Each point expresses the number of coincidences in 300 s occurring in a time bin of 0.98 ns around the corresponding delay, which is equal to about 2 times the coincidence time jitter of the APDs (0.495 ns). The red line indicates the double-exponential fit, whose expression is in the main text. The fit parameters are found to be: $t_0 = (2.03 \pm 0.03)$ ns, $B = 316 \pm 7$, $M = 28460 \pm 70$, $\gamma_s = (35.0 \pm 0.2)$ MHz and $\gamma_i = (41.4 \pm 0.2)$ MHz.

From the decay rates, it is possible to extract the time constants for signal and idler, $\tau_{s(i)} = \frac{1}{2\gamma_{s(i)}}$, thus obtaining:

$$\tau_s = (14.30 \pm 0.07)\text{ns}, \tag{5.2}$$

$$\tau_i = (12.08 \pm 0.06)\text{ns}. \tag{5.3}$$

The photon bandwidth (FWHM) is $\Delta\nu_{s(i)} = 0.64\frac{e}{4\pi\tau_{s(i)}}$, leading to:

$$\Delta\nu_s = (9.68 \pm 0.05)\text{MHz}, \tag{5.4}$$

$$\Delta\nu_i = (11.45 \pm 0.04)\text{MHz}. \tag{5.5}$$

The correlation time $\tau_c = \frac{2(\tau_s+\tau_i)}{e}$, defined as the FWHM of the cross-correlation profile, is $\tau_c = 19.41 \pm 0.07$ ns and, consequently the biphoton spectral bandwidth is $\Delta\nu = 0.64\frac{1}{\pi\tau_c} = 10.50 \pm 0.04$ MHz. The correction factor 0.64 comes from the fact that the

photons are produced in a doubly resonant OPO [245].

The obtained photon bandwidths before correction are about half the values that result from the classical characterization of the OPO cavity. This could occur for different reasons. On the one hand, the bandwidth of the cavity modes can be overestimated due to finite spectral bandwidth of the laser and the limited sampling rate of the oscilloscope; on the other hand, due to an incomplete overlap of signal and idler modes at frequency ν_0, the actual photons may be spectrally narrower with respect to what results from the classical characterization of the OPO.

Another possibility is that the cross-correlation profile is broadened by the finite jitter time of the detectors. The actually measured profile in fact is a convolution of the double exponential decay in Equation 5.1 and a gaussian function having the detectors' combined jitter as time bandwidth. This hypothesis is however excluded by calculating the convolution of double exponential functions with different time constants and the gaussian function expressing the time uncertainty due to detector jitter. The time constants that better reproduce the experimental results are compatible with the measured ones within the experimental errors.

Idler-Idler Auto-correlation function

The spectral properties of the emitted photons can be further verified by measuring the idler-idler (or alternatively, signal-signal) second-order correlation function, as explained in Section 2.4. This is measured in the detection configuration depicted in Figure 5.10-b by recording the coincidences between detectors APD_1 and APD_2 with respect to the time delay between the single detections. The corresponding correlation function is shown in Figure 5.14.

The auto-correlation function, $g^{(2)}(\tau)$ is fitted with a Lorentzian function, of equation:

$$g^{(2)}(\tau) = 1 + \frac{V}{1 + (\frac{1}{2}\gamma(\tau - \tau_0))^2}, \tag{5.6}$$

with V, γ and τ_0 fit parameters. The effective number of modes, N, in the signal

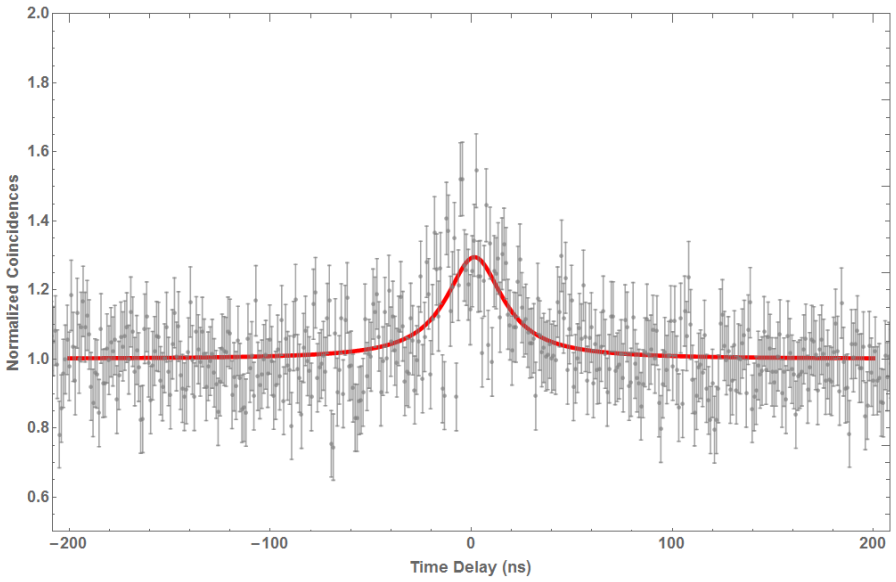


Figure 5.14: **Idler-Idler auto-correlation function.** The coincidences are counted for about 3 hours and normalized to the value at large delays. The temporal resolution for this plot is the same as for the cross-correlation measurement. The error bars are relatively large due to the low counts. A Lorentzian fit curve is shown in red, whose equation can be found in the text. The fit parameters are $V = 0.30 \pm 0.03$, $\gamma = (116 \pm 15)$ MHz and $x_0 = (1.6 \pm 1.5)$ ns.

spectrum can be obtained from the parameter V using the equation: $N = \frac{1}{V}$. In this case, $N = 3.4 \pm 0.4$, which is compatible with the spectrum in Figure 5.9. The large errors on the fit parameters come from the low number of counts recorded during the measurement, which was performed at about 4 mW of pump power entering the cavity. At this power, in fact, the number of double-pair emission is quite low (see Figure 5.12). Since the only coincidences between detectors APD_1 and APD_2 are due to multi-photon emission from the source, a low double-pair emission rate implies low counts for the second-order auto-correlation function, as demonstrated here.

The information on the number of modes may be used to calculate an effective spectral brightness per mode, by dividing the normalized count rates by N and by the biphoton bandwidth $\Delta\nu$. A spectral brightness per mode of 25 ± 2 counts/(s mW MHz) is detected and a value of $(1.29 \pm 0.09) \times 10^3$ biphotons/(s mW MHz) before losses is calculated.

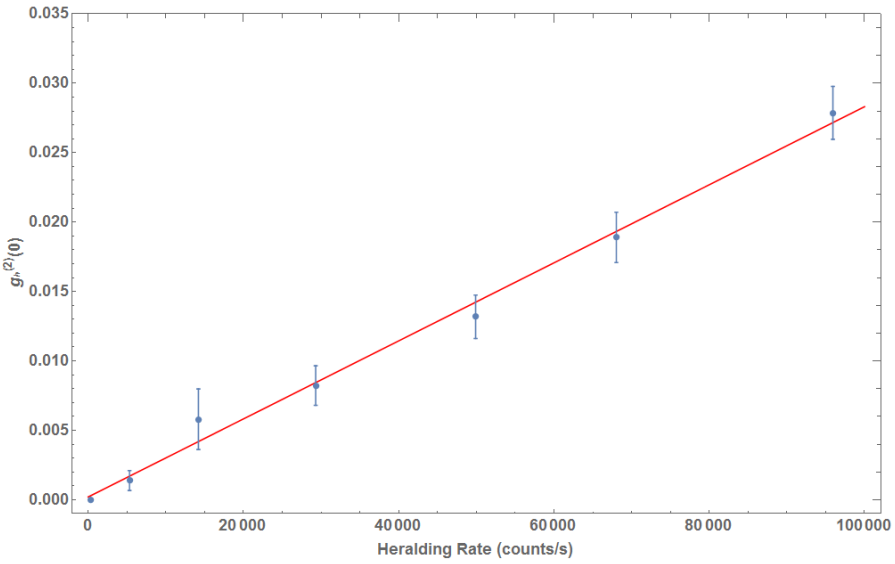


Figure 5.15: $g^{(2)}(0)$ **vs heralding rate,** R_3**.** The error bars on the experimental point come from Poisson-distributed errors on all the rates of expression 5.7. The points are fitted with a linear function (red solid line), which passes through all the error bars. This indicates that the plotted dependence has the expected linear behaviour for low-power regimes. The coincidence window for this measurement is set to 6 ns.

Heralded auto-correlation function at zero delay

The single-photon character of the source is certified by measuring the heralded second-order auto-correlation function at zero delay, $g_h^{(2)}(0)$. This is obtained from the following expression [246]:

$$g_h^{(2)}(0) = 2\frac{R_3 R_{123}}{(R_{13}+R_{23})^2}, \tag{5.7}$$

where R_3 is the detection rate at detector APD_3, R_{13} and R_{23} are the two-fold coincidence rates between detectors APD_1 and APD_3, and APD_2 and APD_3, respectively, whereas R_{123} is the three-fold coincidence rate among APD_1, APD_2 and APD_3. The factor 2 takes into account the splitting probability at the beam splitter. Figure 5.15 shows the dependence of $g_h^{(2)}(0)$ on the heralding rate R_3, which is linearly proportional to the pump power. The value of $g_h^{(2)}(0)$ at the maximum measured heralding rate, corresponding to about 4 mW of pump power, is $g_h^{(2)}(0) = 0.028 \pm 0.002$. This value is in line with those reported in Table 5.1, thus confirming the good single-photon quality of the source at this pump power.

Parameter	Value	Error	Unit
Signal Bandwidth	9.68	0.05	MHz
Idler Bandwidth (MHz)	11.45	0.04	MHz
Number of longitudinal modes	3.4	0.4	-
Measured brightness per mode	25	2	counts/(s mW MHz)
Generated brigthness per mode	1.29×10^3	0.09×10^3	pairs/(s mW MHz)
Signal/Idler heralding efficiency	3.9/4.9	0.5	%
Highest used pump power	3.9	0.1	mW
Highest value of $g_h^{(2)}(0)$	0.028	0.002	-

Table 5.3: **Specifications of the realized source.** The reported value of $g_h^{(2)}(0)$ refers to a heralding rate of about 100×10^3 counts/s. At 5×10^3 counts/s, $g_h^{(2)}(0) < 0.005$. The specifications of the source are in line with those of Table 5.1.

The source specifications obtained from single-photon measurements are summarized in Table 5.3.

5.4 Mode-selection Strategies

In this section, a few possible strategies for mode-filtering of the realized source are discussed. The aim of these techniques is filtering out only the central cluster in Figure 5.9. The side clusters, in fact, correspond to non-degenerate emission at frequencies that are not tuned to Rb transitions. Consequently, they represent just a source of noise when the single photons from the source are interfaced with Rb atoms. For this reason, they need to be suppressed.

The most natural solution is to use additional filters after the OPO. Given the cluster separation of $\mathrm{FSR}_c = (66 \pm 1)$ GHz, volume bragg gratings [247], working either on transmission or reflection, can be a simple and viable solution for this task, as several companies offer devices with a bandwidth below 0.15 nm at 780 nm, which corresponds to about 75 GHz. Such devices work at room temperature, do not require length stabilization (even though they might require thermal stabilization) and are often sold off-the-shelf (not as customized products), which significantly reduces costs and waiting times. The peak transmission/reflection can reach values as high as 90%, which allows for keeping high count rates.

Alternatively, additional optical cavities can be used for filtering. The advantage of this kind of filter is that they can be tuned to select even the single central mode of each cluster, so as to completely suppress the noise from undesired longitudinal modes. However, they present several disadvantages: they need thermal and length stabilization, they typically introduce additional losses due to imperfect mirrors and non-optimal mode-matching to the fundamental TEM_{00} mode and their realization is not a trivial task, while buying them from companies is particularly expensive, due to the fact they need to be customized.

Another promising option is tuning the source such that it directly emits photons in a single cluster, or even in a single longitudinal mode. In this case, the OPO must be configured such that only one cluster falls within the phase-matching curve. Assuming that a cluster occurs at the center of the curve, where the SPDC gain is maximum, the single-cluster condition is:

$$\mathrm{FSR}_c > \Delta\nu_{\mathrm{SPDC}}, \tag{5.8}$$

where $\Delta\nu_{\mathrm{SPDC}}$ is the phase-matching linewidth. A possible way of satisfying condition 5.8 is narrowing the SPDC gain profile below the cluster separation. This can be achieved by making one of the cavity mirrors high reflective for the pump so that the effective length of the parametric interaction is doubled and $\Delta\nu_{\mathrm{SPDC}}$ consequently halved. This technique was used to achieve single-mode emission in monolithic CE-SPDC [223, 231].

A more versatile mode-selection method was developed in the research group in which this Ph.D. project was conducted. This method consists in tuning FSR_c independent of $\Delta\nu_{\mathrm{SPDC}}$ by inserting a second birefringent element into the cavity, which provides dedicated degrees of freedom for tuning the cluster separation. In this scheme, therefore, the OPO cavity includes two birefringent elements, the parametric crystal, with length L and group indices for signal and idler, n_s and n_i, respectively, and a *tuning crystal*, with length L' and indices n'_s, n'_i, as depicted in Figure 5.16. The cavity also comprises some air gaps between the two crystals and between each crystal and the closer mirror. The overall length of the air gaps is L_{gap}. Therefore:

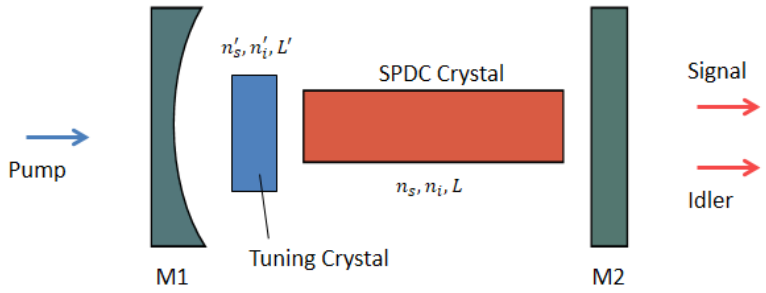


Figure 5.16: **Scheme of a direct-single-mode OPO.** The OPO in the figure includes two birefringent crystals. The SPDC crystal has group refractive indices n_s and n_i for signal and idler, respectively, and length L. The tuning crystal has parameters n'_s, n'_i and L'. The tuning crystal is chosen so as to tune the birefringence of the cavity such that only a single cluster falls below the SPDC bandwidth. The relation between the parameters of the two crystals necessary to achieve this task is reported in the main text.

$$\mathrm{FSR}_x = \frac{c}{2|N_x L + N'_x L' + L_{gap}|}, \tag{5.9}$$

where $x = s$ or i, c is the speed of light in vacuum, and the group index of air is approximated to 1. By using equations 2.41 and 5.9, the cluster separation becomes:

$$\mathrm{FSR}_c = \frac{c}{2|(n_s - n_i)L + (n'_s - n'_i)L'|}. \tag{5.10}$$

The FWHM of the phase-matching profile can be obtained from Equation 2.31. By approximating the factor $5.56/2\pi$ to 1, the SPDC bandwidth reads:

$$\Delta\nu_{\mathrm{SPDC}} \approx \frac{c}{|n_s - n_i|L}. \tag{5.11}$$

Then, condition 5.8 becomes:

$$\frac{1}{2}\left|\frac{n_s - n_i}{n'_s - n'_i}\right| < \frac{L'}{L} < \left|\frac{n_s - n_i}{n'_s - n'_i}\right|, \tag{5.12}$$

with $\frac{n_s - n_i}{n'_s - n'_i} < 0$, reflecting the fact that the tuning crystal must partially compensate the birefringence of the parametric crystal. By suitably choosing the parameters of the tuning crystal, therefore, single-cluster emission can be achieved. This concept was recently used to achieve single-mode emission from a narrow-band source at 852 nm [248].

In addition to the central brighter mode, each cluster comprises a few weaker neighbouring modes, deriving from the partial overlap of signal and idler resonances, as shown in Figure 2.5. It is clear that, if the longitudinal modes of the cavity are narrow enough, this partial overlap is cancelled and the neighbouring modes are suppressed. A criterion for a sufficiently low overlap can be considered:

$$\frac{\Delta\nu_s}{2} + \frac{\Delta\nu_i}{2} < |\mathrm{FSR}_s - \mathrm{FSR}_i|, \tag{5.13}$$

where $\Delta\nu_s$ and $\Delta\nu_i$ are the linewidth of the signal and idler cavity modes, respectively. By using the relation $\Delta\nu_x \approx \frac{\mathrm{FSR}_x}{\mathcal{F}_x}$, with $\mathcal{F}_x$ finesse of the cavity for the field x, with x being s or i, the previous condition becomes:

$$\frac{1}{2}\left(\frac{\mathrm{FSR}_s}{\mathcal{F}_s} + \frac{\mathrm{FSR}_i}{\mathcal{F}_i}\right) < |\mathrm{FSR}_s - \mathrm{FSR}_i|. \tag{5.14}$$

If, as it is often the case, $\mathcal{F}_s \approx \mathcal{F}_i = \mathcal{F}$, a condition on the finesse $\mathcal{F}$ can be extracted:

$$\mathcal{F} > \frac{1}{2}\frac{\mathrm{FSR}_s + \mathrm{FSR}_i}{|\mathrm{FSR}_s - \mathrm{FSR}_i|}. \tag{5.15}$$

Assuming that the optical path for the idler is larger than that for the signal, Equation 5.15 becomes:

$$\mathcal{F} > \frac{1}{2}\frac{(n_i + n_s)L + (n_i' + n_s')L'}{(n_i - n_s)L + (n_i' - n_s')L'}. \tag{5.16}$$

This, together with fulfilment of condition 5.12, ensures generation of photons in a single longitudinal mode without further filtering.

Frequency tuning of the OPO can be realized by controlling temperature and tilt of the parametric crystal and/or the tuning crystal, as long as condition 5.11 is satisfied. Additionally, a pockels cell, an electro-optic device whose refractive indices depend on the applied voltage, can be used as a tuning crystal in order to tune the resonance condition in a fully independent way of the phase-matching condition.

5.5 Summary of the results

The obtained achievements can be summarized as it follows.

- A narrow-band single-photon source based on CE-SPDC in a PPKTP crystal was set up. The crystal is phase-matched for type-II degenerate emission at 780 nm. The cavity is kept resonant to laser light that in turn is frequency-stabilized to a hyperfine transition of Rb D2 line. This ensures emission at the correct frequency for interaction with Rb atoms.

- The spectral properties of the source are found both by classical characterization of the cavity and by measuring first- and second-order correlation functions. The spectrum of both signal and idler photons is composed of three clusters separated by (66 ± 1) GHz. The main mode of each cluster has a bandwidth of (9.68 ± 0.05) MHz for the signal and (11.45 ± 0.04) MHz for the idler, thus ensuring efficient coupling to the Rb transitions (a few MHz bandwidth). The detected/generated spectral brightness per cluster is $(25 \pm 2)/(1.29 \pm 0.09) \times 10^3$ pairs/(s mW MHz). The source outperforms the two other sources of degenerate photon pairs at 780 nm reported in literature [219, 222].

- The dependence of the heralded second-order correlation function at zero delay on the pump power was obtained. A maximum value of $g_h^{(2)}(0) = 0.028 \pm 0.002$ was found at the highest pump power of $P_{max} = 3.9$ mW. This ensures low multi-photon contamination.

- Strategies for filtering out the central cluster have been individuated and will be applied in the near future. The first technique to be attempted will be the employment of volume bragg gratings.

Conclusions

In this thesis, three experimental works have been presented, all involving generation and manipulation of single photons for quantum information applications.

The first two works, reported in Chapters 3 and 4, respectively, consist in the development and implementation of novel quantum communication protocols, both based on single photons in superposition between two distant locations. An important aspect of the theoretical and experimental investigation in both cases is the reduction of resources for quantum communication.

In Chapter 3, in fact, it is experimentally shown that a single quantum particle, a photon, allows for the simultaneous two-way transmission of two classical bits between two distant parties. This concept is used to design and implement a communication protocol that allows one of the two parties to anonymously send classical bits to the other, employing, in the ideal case, one photon per classical bit. The demonstrated protocol determines an advantage in terms of resources to be used, either number of particles or time, with respect to the case where only classical particles are allowed. Such advantage is preserved when applying suitably designed error correction techniques.

In terms of users' hardware, instead, a resource advantage is obtained with the semi-classical QKD protocol of Chapter 4, as, contrary to previous schemes, the users neither need to generate quantum states nor to store quantum information in quantum memories. Notably, the server only has to provide a feasible resource such as single photons in superposition. The secure key rate is obtained in the finite-key scenario and considering the main experimental imperfections of the adopted setup.

In both cases, the realized implementations are proof-of-principle demonstrations and as such have mostly a foundational value, showing what features are gained in communication when quantum resources are used compared to classical ones. However, the experiments can be improved to approach real-world applications by using state-of-the-art phase-stabilization techniques and optical switches, as well as deterministic single-photon sources, which can be done in future work. Further theoretical investigation of the concept of two-way-communication-with-one-particle, moreover, can lead to relax the assumption for the protocol security and thus increase practicality. This scheme, in fact, represents a primitive that can be used for different communication modes, such as QSDC and QKD. Additional applications can be found in the future.

Chapter 5 describes the realization and characterization of a narrow-band single-photon source, which emits degenerate photon pairs capable of interaction with Rb D2 line. The source outperforms the previous realizations of narrow-band photon-pair emitters at 780 nm and constitutes a useful piece of equipment for the research group in which it was developed. In fact, several future directions are currently under investigation. The first obvious one is interfacing the produced photons to Rb atoms for the demonstration of two-photon gates and quantum memories. This will be done in collaboration with research groups working on atomic setups. Furthermore, the possibility of increasing the pump power and accessing a regime in which double-pair emission from the source is non-negligible is under consideration. This would allow for the production of multi-photon narrow-band states for the realization of more complex photon-atom hybrid systems and for a richer characterization of atomic setups. The possibility of producing narrow-band multi-photon entanglement will also be investigated.

List Of Publications

Here the list of all publications produced during the Ph.D. project is presented. The publications related to this thesis are marked in bold.

- Hilweg, C., Massa, F. Martynov, D., Mavalvala, N., Chruściel P.T., Walther, P., Gravitationally induced phase shift on a single photon, *New Journal of Physics*, 19, 3 (2017).

- Rubino, G., Rozema, L. A., Massa, F., Araújo, M., Zych, M., Brukner, Č., Walther, P, Experimental entanglement of temporal orders, *arXiv:1712.06884* (2018)

- Moqanaki, A., Massa, F. and Walther, P., "Apparatus for generating narrow-band single-photon and multi-photon states with long coherence length." U.S. Patent No. 10,331,012. 25 Jun. 2019.

- **Massa, F., Moqanaki, A., Baumeler, Ä., Del Santo, F., Kettlewell, J. A., Dakić, B., Walther, P., Experimental two-way communication with one photon., *Advanced Quantum Technologies* (2019).**

- Moqanaki, A., Massa, F., Walther, P., Novel single-mode narrow-band photon source of high brightness tuned to cesium D2 line, *APL Photonics*, 4, 9 (2019).

- **Massa, F., Yadav, P., Moqanaki, A., Krawec, W.O., Mateus, P., Paunković, N., Souto, A., Walther, P., Experimental quantum cryptography with classical users, *arXiv:1908.01780*.**

Bibliography

[1] P. Benioff. "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of Statistical Physics* 22.5 (1980), pp. 563–591.

[2] R. P. Feynman. "Simulating physics with computers". *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488.

[3] P. W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". *SIAM Review* 41.2 (1999), pp. 303–332.

[4] I. Kassal et al. "Simulating chemistry using quantum computers". *Annual Review of Physical Chemistry* 62 (2011), pp. 185–207.

[5] C. H Bennett. "Quantum crytography". *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India.* 1984, pp. 175–179.

[6] Q. A. Turchette et al. "Measurement of conditional phase shifts for quantum logic". *Physical Review Letters* 75.25 (1995), p. 4710.

[7] E. Knill, R. Laflamme, and G. J. Milburn. "A scheme for efficient quantum computation with linear optics". *Nature* 409.6816 (2001), p. 46.

[8] H. J. Briegel et al. "Measurement-based quantum computation". *Nature Physics* 5.1 (2009), p. 19.

[9] H. J. Briegel et al. "Quantum repeaters: the role of imperfect local operations in quantum communication". *Physical Review Letters* 81.26 (1998), p. 5932.

[10] L. M. Duan et al. “Long-distance quantum communication with atomic ensembles and linear optics”. *Nature* 414.6862 (2001), p. 413.

[11] K. Azuma, K. Tamaki, and H.-K. Lo. “All-photonic quantum repeaters”. *Nature communications* 6 (2015), p. 6787.

[12] R. Loudon. *The quantum theory of light*. 3rd ed. Oxford University Press, 2000.

[13] J. J. Sakurai. *Modern quantum mechanics*. 2nd ed. Pearson, 1993.

[14] J. S. Bell. “On the Einstein Podolsky Rosen paradox”. *Physics Physique Fizika* 1.3 (1964), pp. 195–200.

[15] J.-W. Lee et al. “Quantum cryptography using single-particle entanglement”. *Physical Review A* 68.1 (2003), p. 012324.

[16] A. Barenco et al. “Elementary gates for quantum computation”. *Physical Review A* 52.5 (1995), pp. 3457–3467.

[17] W. K. Wooters and W. H. Zurek. “A single quantum cannot be cloned”. *Nature* 299 (1982), pp. 802–802.

[18] P. Krantz et al. “A quantum engineer’s guide to superconducting qubits”. *Applied Physics Reviews* 6.2 (2019), p. 021318.

[19] M. Saffman. “Quantum computing with atomic qubits and Rydberg interactions: progress and challenges”. *Journal of Physics B: Atomic, Molecular and Optical Physics* 49.20 (2016), p. 202001.

[20] C. D. Bruzewicz et al. “Trapped-ion quantum computing: Progress and challenges”. *Applied Physics Reviews* 6.2 (2019), p. 021314.

[21] S. Slussarenko and G. J. Pryde. “Photonic quantum information processing: A concise review”. *Applied Physics Reviews* 6.4 (2019), p. 041303.

[22] D. E. Chang, V. Vuletić, and M. D. Lukin. “Quantum nonlinear optics photon by photon”. *Nature Photonics* 8.9 (2014), p. 685.

[23] J. Volz et al. “Nonlinear π phase shift for single fibre-guided photons interacting with a single resonator-enhanced atom”. *Nature Photonics* 8.12 (2014), p. 965.

[24] K. M. Beck et al. “Large conditional single-photon cross-phase modulation”. *Proceedings of the National Academy of Sciences* 113.35 (2016), pp. 9740–9744.

[25] D. Tiarks et al. “Optical π phase shift created with a single-photon pulse”. *Science Advances* 2.4 (2016), e1600036.

[26] B. Hacker et al. “A photon-photon quantum gate based on a single atom in an optical resonator”. *Nature* 536.7615 (2016), p. 193.

[27] O. Bechler et al. “A passive photon-atom qubit swap operation”. *Nature Physics* 14.10 (2018), p. 996.

[28] P. Androvitsaneas et al. “Deterministic giant photon phase shift from a single charged quantum dot”. *Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC, 2017 Conference on)*. 2017, pp. 1–1.

[29] L. K. Grover. “A fast quantum mechanical algorithm for database search”. *Proceedings of the28th Annual ACM symposium on Theory of Computing*. 1996, pp. 212–219.

[30] C. Xiong et al. “Active temporal multiplexing of indistinguishable heralded single photons”. *Nature Communications* 7 (2016), p. 10853.

[31] T. Rudolph. “Why I am optimistic about the silicon-photonic route to quantum computing”. *APL Photonics* 2.3 (2017), p. 030901.

[32] I. Aharonovich, D. Englund, and M. Toth. “Solid-state single-photon emitters”. *Nature Photonics* 10.10 (2016), p. 631.

[33] H. Wang et al. “Near-transform-limited single photons from an efficient solid-state quantum emitter”. *Physical Review Letters* 116.21 (2016), p. 213601.

[34] P. Senellart, G. Solomon, and A. White. “High-performance semiconductor quantum-dot single-photon sources”. *Nature Nanotechnology* 12.11 (2017), p. 1026.

[35] N. H. Lindner and T. Rudolph. “Proposal for pulsed on-demand sources of photonic cluster state strings”. *Physical Review Letters* 103.11 (2009), p. 113602.

[36] I. Schwartz et al. “Deterministic generation of a cluster state of entangled photons”. *Science* 354.6311 (2016), pp. 434–437.

[37] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg. “Surface code quantum computing with error rates over 1%”. *Physical Review A* 83.2 (2011), p. 020302.

[38] A. G. Fowler, A. C. Whiteside, and L. C. L. Hollenberg. “Towards practical classical processing for the surface code”. *Physical Review Letters* 108.18 (2012), p. 180501.

[39] R. Prevedel et al. “High-speed linear optics quantum computing using active feed-forward”. *Nature* 445.7123 (2007), p. 65.

[40] S. Aaronson and A. Arkhipov. “The computational complexity of linear optics”. *Proceedings of the 43rd Annual ACM symposium on Theory of Computing*. ACM. 2011, pp. 333–342.

[41] M. Reiher et al. “Elucidating reaction mechanisms on quantum computers”. *Proceedings of the National Academy of Sciences* (2017), p. 201619152.

[42] I. M. Georgescu, S. Ashhab, and F. Nori. “Quantum simulation”. *Reviews of Modern Physics* 86.1 (2014), p. 153.

[43] A. Aspuru-Guzik and P. Walther. “Photonic quantum simulators”. *Nature Physics* 8.4 (2012), p. 285.

[44] R. Cleve and H. Buhrman. “Substituting quantum entanglement for communication”. *Physical Review A* 56.2 (1997), p. 1201.

[45] L. Hardy and W. van Dam. “Quantum communication using a nonlocal Zeno effect”. *Physical Review A* 59.4 (1999), p. 2635.

[46] H. Buhrman et al. “Multiparty quantum communication complexity”. *Physical Review A* 60.4 (1999), p. 2737.

[47] Č. Brukner, M. Żukowski, and A. Zeilinger. “Quantum communication complexity protocol with two entangled qutrits”. *Physical Review Letters* 89.19 (2002), p. 197901.

[48] H. Buhrman et al. “Nonlocality and communication complexity”. *Reviews of Modern Physics* 82.1 (2010), p. 665.

[49] A. Tavakoli et al. “Quantum communication complexity using the quantum Zeno effect”. *Physical Review A* 92.1 (2015), p. 012303.

[50] S. Massar. “Quantum fingerprinting with a single particle”. *Physical Review A* 71.1 (2005), p. 012310.

[51] J. M. Arrazola and N. Lütkenhaus. “Quantum fingerprinting with coherent states and a constant mean number of photons”. *Physical Review A* 89.6 (2014), p. 062305.

[52] P. Trojek et al. “Experimental quantum communication complexity”. *Physical Review A* 72.5 (2005), p. 050305.

[53] P. Trojek et al. “Experimental multipartner quantum communication complexity employing just one qubit”. *Natural Computing* 12.1 (2013), pp. 19–26.

[54] M. Smania et al. “Experimental quantum multiparty communication protocols”. *npj Quantum Information* 2 (2016), p. 16010.

[55] F. Xu et al. “Experimental quantum fingerprinting with weak coherent pulses”. *Nature Communications* 6 (2015), p. 8735.

[56] J.-Y. Guan et al. “Observation of quantum fingerprinting beating the classical limit”. *Physical Review Letters* 116.24 (2016), p. 240502.

[57] C. H. Bennett and S. J. Wiesner. “Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states”. *Physical Review Letters* 69.20 (1992), p. 2881.

[58] K. Mattle et al. “Dense coding in experimental quantum communication”. *Physical Review Letters* 76.25 (1996), p. 4656.

[59] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat. “Beating the channel capacity limit for linear photonic superdense coding”. *Nature physics* 4.4 (2008), p. 282.

[60] C. H. Bennett et al. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. *Physical Review Letters* 70.13 (1993), p. 1895.

[61] D. Bouwmeester et al. “Experimental quantum teleportation”. *Nature* 390.6660 (1997), p. 575.

[62] R. Ursin et al. “Communications: Quantum teleportation across the Danube”. *Nature* 430.7002 (2004), p. 849.

[63] J.-G. Ren et al. “Ground-to-satellite quantum teleportation”. *Nature* 549.7670 (2017), p. 70.

[64] G. S. Vernam. “Cipher printing telegraph systems: For secret wire and radio telegraphic communications”. *Journal of the AIEE* 45.2 (1926), pp. 109–115.

[65] C. E. Shannon. “Communication theory of secrecy systems”. *Bell System Technical Journal* 28.4 (1949), pp. 656–715.

[66] W. Stallings. *Cryptography and network security: principles and practice*. Pearson Upper Saddle River, 2017.

[67] C. H. Bennett et al. “Generalized privacy amplification”. *IEEE Transactions on Information Theory* 41.6 (1995), pp. 1915–1923.

[68] C. H. Bennett. “Quantum cryptography using any two nonorthogonal states”. *Physical Review Letters* 68.21 (1992), p. 3121.

[69] D. Bruß. “Optimal eavesdropping in quantum cryptography with six states”. *Physical Review Letters* 81.14 (1998), p. 3018.

[70] H. Bechmann-Pasquinucci and N. Gisin. “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography”. *Physical Review A* 59.6 (1999), p. 4238.

[71] A. K. Ekert. “Quantum cryptography based on Bell’s theorem”. *Physical Review Letters* 67.6 (1991), p. 661.

[72] J. F. Clauser et al. “Proposed experiment to test local hidden-variable theories”. *Physical Review Letters* 23.15 (1969), p. 880.

[73] C. H. Bennett, G. Brassard, and N. D. Mermin. “Quantum cryptography without Bell’s theorem”. *Physical Review Letters* 68.5 (1992), p. 557.

[74] N. Gisin et al. “Quantum cryptography”. *Reviews of Modern Physics* 74.1 (2002), p. 145.

[75] H.-K. Lo, M. Curty, and K. Tamaki. “Secure quantum key distribution”. *Nature Photonics* 8.8 (2014), p. 595.

[76] F. Xu et al. “Quantum cryptography with realistic devices”. *arXiv:1903.09051* (2019).

[77] C. H. Bennett et al. “Experimental quantum cryptography”. *Journal of Cryptology* 5.1 (1992), pp. 3–28.

[78] S.-K. Liao et al. “Satellite-to-ground quantum key distribution”. *Nature* 549.7670 (2017), p. 43.

[79] S.-K. Liao et al. “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication”. *Nature Photonics* 11.8 (2017), p. 509.

[80] S.-K. Liao et al. “Satellite-relayed intercontinental quantum network”. *Physical Review Letters* 120.3 (2018), p. 030501.

[81] T. Jennewein et al. “Quantum cryptography with entangled photons”. *Physical Review Letters* 84.20 (2000), p. 4729.

[82] D. S. Naik et al. “Entangled state quantum cryptography: eavesdropping on the Ekert protocol”. *Physical Review Letters* 84.20 (2000), p. 4733.

[83] W. Tittel et al. “Quantum cryptography using entangled photons in energy-time Bell states”. *Physical Review Letters* 84.20 (2000), p. 4737.

[84] T. Honjo et al. “Long-distance entanglement-based quantum key distribution over optical fiber”. *Optics Express* 16.23 (2008), pp. 19118–19126.

[85] N. Namekata et al. “High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes”. *Optics Express* 19.11 (2011), pp. 10632–10639.

[86] M. Bourennane, A. Karlsson, and G. Björk. “Quantum key distribution using multilevel encoding”. *Physical Review A* 64.1 (2001), p. 012306.

[87] S. Gröblacher et al. “Experimental quantum cryptography with qutrits”. *New Journal of Physics* 8.5 (2006), p. 75.

[88] I. Ali-Khan, C. J. Broadbent, and J. C. Howell. “Large-alphabet quantum key distribution using energy-time entangled bipartite states”. *Physical Review Letters* 98.6 (2007), p. 060503.

[89] M. Mafu et al. “Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases”. *Physical Review A* 88.3 (2013), p. 032305.

[90] T. Zhong et al. “Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding”. *New Journal of Physics* 17.2 (2015), p. 022002.

[91] A. Sit et al. “High-dimensional intracity quantum cryptography with structured photons”. *Optica* 4.9 (2017), pp. 1006–1010.

[92] N. T. Islam et al. “Provably secure and high-rate quantum key distribution with time-bin qudits”. *Science Advances* 3.11 (2017), e1701491.

[93] D. Mayers. “Quantum key distribution and string oblivious transfer in noisy channels”. *Annual International Cryptology Conference*. 1996, pp. 343–357.

[94] H.-K. Lo and H. F. Chau. “Unconditional security of quantum key distribution over arbitrarily long distances”. *Science* 283.5410 (1999), pp. 2050–2056.

[95] P. W. Shor and J. Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. *Physical Review Letters* 85.2 (2000), p. 441.

[96] V. Scarani et al. “The security of practical quantum key distribution”. *Reviews of Modern Physics* 81.3 (2009), p. 1301.

[97] G. Brassard et al. “Limitations on practical quantum cryptography”. *Physical Review Letters* 85.6 (2000), p. 1330.

[98] N. Lütkenhaus. “Security against individual attacks for realistic quantum key distribution”. *Physical Review A* 61.5 (2000), p. 052304.

[99] V. B. Braginsky and K. S. Vorontsov Y. I .and Thorne. “Quantum nondemolition measurements”. *Science* 209.4456 (1980), pp. 547–557.

[100] P. Grangier, J. A. Levenson, and J.-P. Poizat. “Quantum non-demolition measurements in optics”. *Nature* 396.6711 (1998), p. 537.

[101] N. Lütkenhaus and M. Jahma. “Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack”. *New Journal of Physics* 4.1 (2002), p. 44.

[102] V. Makarov. “Controlling passively quenched single photon detectors by bright light”. *New Journal of Physics* 11.6 (2009), p. 065003.

[103] L. Lydersen et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. *Nature Photonics* 4.10 (2010), p. 686.

[104] R. H. Hadfield. “Single-photon detectors for optical quantum information applications”. *Nature photonics* 3.12 (2009), p. 696.

[105] W.-Y. Hwang. “Quantum key distribution with high loss: toward global secure communication”. *Physical Review Letters* 91.5 (2003), p. 057901.

[106] X.-B. Wang. “Beating the photon-number-splitting attack in practical quantum cryptography”. *Physical Review Letters* 94.23 (2005), p. 230503.

[107] H.-K. Lo, X. Ma, and K. Chen. “Decoy state quantum key distribution”. *Physical Review Letters* 94.23 (2005), p. 230504.

[108] X. Ma et al. “Practical decoy state for quantum key distribution”. *Physical Review A* 72.1 (2005), p. 012326.

[109] Y. Zhao et al. “Experimental quantum key distribution with decoy states”. *Physical Review Letters* 96.7 (2006), p. 070502.

[110] C.-Z. Peng et al. “Experimental long-distance decoy-state quantum key distribution based on polarization encoding”. *Physical Review Letters* 98.1 (2007), p. 010505.

[111] T. Schmitt-Manderbach et al. “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km”. *Physical Review Letters* 98.1 (2007), p. 010504.

[112] A. R. Dixon et al. “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate”. *Optics Express* 16.23 (2008), pp. 18790–18797.

[113] A. Boaron et al. “Secure quantum key distribution over 421 km of optical fiber”. *Physical Review Letters* 121.19 (2018), p. 190502.

[114] M. Sasaki et al. “Field test of quantum key distribution in the Tokyo QKD Network”. *Optics Express* 19.11 (2011), pp. 10387–10409.

[115] H.-K. Lo, M. Curty, and B. Qi. “Measurement-device-independent quantum key distribution”. *Physical Review Letters* 108.13 (2012), p. 130503.

[116] Y. Liu et al. “Experimental measurement-device-independent quantum key distribution”. *Physical Review Letters* 111.13 (2013), p. 130502.

[117] A. Rubenok et al. “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks”. *Physical Review Letters* 111.13 (2013), p. 130501.

[118] T. Ferreira Da Silva et al. “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits”. *Physical Review A* 88.5 (2013), p. 052303.

[119] Z. Tang et al. “Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution”. *Physical Review Letters* 112.19 (2014), p. 190503.

[120] H.-L. Yin et al. “Measurement-device-independent quantum key distribution over a 404 km optical fiber”. *Physical Review Letters* 117.19 (2016), p. 190501.

[121] L. C. Comandar et al. “Quantum key distribution without detector vulnerabilities using optically seeded lasers”. *Nature Photonics* 10.5 (2016), p. 312.

[122] Y.-L. Tang et al. “Measurement-device-independent quantum key distribution over untrustful metropolitan network”. *Physical Review X* 6.1 (2016), p. 011024.

[123] S. Pirandola et al. “Fundamental limits of repeaterless quantum communications”. *Nature Communications* 8 (2017), p. 15043.

[124] H. J. Kimble. “The quantum internet”. *Nature* 453.7198 (2008), p. 1023.

[125] N. Sangouard et al. “Quantum repeaters based on atomic ensembles and linear optics”. *Reviews of Modern Physics* 83.1 (2011), p. 33.

[126] R. J. Hughes et al. “Network-centric quantum communications with application to critical infrastructure protection”. *arXiv:1305.0305* (2013).

[127] C. Ma et al. “Silicon photonic transmitter for polarization-encoded quantum key distribution”. *Optica* 3.11 (2016), pp. 1274–1278.

[128] P. Sibson et al. “Integrated silicon photonics for high-speed quantum key distribution”. *Optica* 4.2 (2017), pp. 172–177.

[129] M. Lucamarini et al. “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters”. *Nature* 557.7705 (2018), p. 400.

[130] X. Ma, P. Zeng, and H. Zhou. “Phase-matching quantum key distribution”. *Physical Review X* 8.3 (2018), p. 031043.

[131] C. Cui et al. “Twin-Field Quantum Key Distribution without Phase Postselection”. *Physical Review Applied* 11.3 (2019), p. 034053.

[132] M. Curty, K. Azuma, and H.-K. Lo. “Simple security proof of twin-field type quantum key distribution protocol”. *npj Quantum Information* 5.1 (2019), p. 64.

[133] J. Lin and N. Lütkenhaus. "Simple security analysis of phase-matching measurement-device-independent quantum key distribution". *Physical Review A* 98.4 (2018), p. 042332.

[134] M. Minder et al. "Experimental quantum key distribution beyond the repeaterless secret key capacity". *Nature Photonics* 13.5 (2019), p. 334.

[135] S. Wang et al. "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system". *Physical Review X* 9.2 (2019), p. 021046.

[136] Y. Liu et al. "Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending". *Physical Review Letters* 123.10 (2019), p. 100505.

[137] X. Zhong et al. "Proof-of-principle experimental demonstration of twin-field type quantum key distribution". *arXiv preprint arXiv:1902.10209* (2019).

[138] J.-P. Chen et al. "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km". *arXiv:1910.07823* (2019).

[139] M. Boyer, D. Kenigsberg, and T. Mor. "Quantum key distribution with classical Bob". *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*. IEEE. 2007, pp. 10–10.

[140] M. Boyer et al. "Semiquantum key distribution". *Physical Review A* 79.3 (2009), p. 032341.

[141] X. Zou et al. "Semiquantum-key distribution using less than four quantum states". *Physical Review A* 79.5 (2009), p. 052312.

[142] W. Zhang, D. Qiu, and P. Mateus. "Security of a single-state semi-quantum key distribution protocol". *Quantum Information Processing* 17.6 (2018), p. 135.

[143] M. Boyer et al. "Experimentally feasible protocol for semiquantum key distribution". *Physical Review A* 96.6 (2017), p. 062335.

[144] W. O. Krawec. "Practical security of semi-quantum key distribution". *Quantum Information Science, Sensing, and Computation X*. Vol. 10660. International Society for Optics and Photonics. 2018, p. 1066009.

[145] W. O. Krawec. “Mediated semiquantum key distribution”. *Physical Review A* 91.3 (2015), p. 032323.

[146] Z.-R. Liu and T. Hwang. “Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement”. *Annalen der Physik* 530.4 (2018), p. 1700206.

[147] K.-N. Zhu et al. “Semi-quantum key distribution protocols with GHZ states”. *International Journal of Theoretical Physics* 57.12 (2018), pp. 3621–3631.

[148] K. Boström and T. Felbinger. “Deterministic secure direct communication using entanglement”. *Physical Review Letters* 89.18 (2002), p. 187902.

[149] A. Wójcik. “Eavesdropping on the “ping-pong” quantum communication protocol”. *Physical Review Letters* 90.15 (2003), p. 157901.

[150] Q.-Y. Cai. “The “Ping-Pong” Protocol Can Be Attacked without Eavesdropping”. *Physical Review Letters* 91 (10 Sept. 2003), p. 109801.

[151] F.-G. Deng et al. “Eavesdropping on theping-pong’quantum communication protocol freely in a noise channel”. *Chinese Physics* 16.2 (2007), p. 277.

[152] Q.-Y. Cai and B.-W. Li. “Improving the capacity of the Boström-Felbinger protocol”. *Physical Review A* 69.5 (2004), p. 054301.

[153] M. Lucamarini and S. Mancini. “Secure deterministic communication without entanglement”. *Physical Review Letters* 94.14 (2005), p. 140501.

[154] F.-G. Deng, G. L. Long, and X.-S. Liu. “Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block”. *Physical Review A* 68.4 (2003), p. 042317.

[155] F.-G. Deng and G. L. Long. “Secure direct communication with a quantum one-time pad”. *Physical Review A* 69.5 (2004), p. 052319.

[156] C. Wang, F. G. Deng, and G. L. Long. “Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state”. *Optics Communications* 253.1-3 (2005), pp. 15–20.

[157] Z.-R. Jian, G.-S. Jin, and T.-J. Wang. "Efficient Quantum Secure Direct Communication Using the Orbital Angular Momentum of Single Photons". *International Journal of Theoretical Physics* 55.3 (2016), pp. 1811–1819.

[158] J.-Y. Hu et al. "Experimental quantum secure direct communication with single photons". *Light: Science & Applications* 5.9 (2016), e16144.

[159] W. Zhang et al. "Quantum secure direct communication with quantum memory". *Physical Review Letters* 118.22 (2017), p. 220501.

[160] R. Qi et al. "Implementation and security analysis of practical quantum secure direct communication". *Light: Science & Applications* 8.1 (2019), p. 22.

[161] R. W. Boyd. *Nonlinear optics*. 3rd ed. Academic Press, Inc., 2008.

[162] R. G. Newton. *Scattering theory of waves and particles*. 2nd ed. Springer Verlag, 1982.

[163] B. E. A. Saleh and M. C. Teich. *Fundamentals of photonics*. 2nd. Wiley, 2007.

[164] M. Born and E. Wolf. *Principles of optics : electromagnetic theory of propagation, interference and diffraction of light*. 7th expanded ed. Cambridge University Press, 1999.

[165] M. Yamada et al. "First-order quasi-phase matched LiNbO3 waveguide periodically poled by applying an external field for efficient blue second-harmonic generation". *Applied Physics Letters* 62.5 (1993), pp. 435–436.

[166] Z.-Y. J. Ou. *Multi-photon quantum interference*. 1st ed. Springer, 2007.

[167] P. J. Mosley et al. "Heralded Generation of Ultrafast Single Photons in Pure Quantum States". *Physical Review Letters* 100 (13 2008), p. 133601.

[168] M. D. Eisaman et al. "Invited Review Article: Single-photon sources and detectors". *Review of Scientific Instruments* 82.7 (2011), p. 071101.

[169] N. Hodgson and H. Weber. *Optical resonators: fundamentals, advanced concepts and applications*. 1st ed. Springer, 1997.

[170] U. L. Andersen et al. “30 years of squeezed light generation”. *Physica Scripta* 91.5 (2016), p. 053001.

[171] Z.-Y. Ou and Y.-J. Lu. “Cavity Enhanced Spontaneous Parametric Down-Conversion for the Prolongation of Correlation Time between Conjugate Photons”. *Physical Review Letters* 83 (13 1999), pp. 2556–2559.

[172] Y.-J. Lu and Z.-Y. Ou. “Optical parametric oscillator far below threshold: Experiment versus theory”. *Physical Review A* 62 (3 2000), p. 033804.

[173] I. Breunig, D. Haertle, and K. Buse. “Continuous-wave optical parametric oscillators: recent developments and prospects”. *Applied Physics B* 105.1 (2011), p. 99.

[174] K.-H. Luo et al. “Direct generation of genuine single-longitudinal-mode narrowband photon pairs”. *New Journal of Physics* 17.7 (2015), p. 073039.

[175] I. E. Zadeh et al. “A single-photon detector with high efficiency and sub-10ps time resolution”. *arXiv:1801.06574* (2018).

[176] B. A. Korzh et al. “Demonstrating sub-3 ps temporal resolution in a superconducting nanowire single-photon detector”. *arXiv:1804.06839* (2018).

[177] H. Wang, T. Horikiri, and T. Kobayashi. “Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion”. *Physical Review A* 70 (4 2004), p. 043804.

[178] R. J. Glauber. “The Quantum Theory of Optical Coherence”. *Physical Review* 130 (6 1963), pp. 2529–2539.

[179] E. Bocquillon et al. “Coherence measures for heralded single-photon sources”. *Physical Review A* 79 (3 2009), p. 035801.

[180] M. Bashkansky et al. “Significance of heralding in spontaneous parametric down-conversion”. *Physical Review A* 90.5 (2014), p. 053825.

[181] F. Del Santo and B. Dakić. “Two-way communication with a single quantum particle”. *Physical Review Letters* 120.6 (2018), p. 060503.

[182] M. L. Almeida et al. "Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage". *Physical Review Letters* 104.23 (2010), p. 230404.

[183] C. Branciard et al. "The simplest causal inequalities and their violation". *New Journal of Physics* 18.1 (2015), p. 013008.

[184] A. Nayak and J. Salzman. "On communication over an entanglement-assisted quantum channel". *Proceedings of the 34th Annual ACM symposium on Theory of Computing*. ACM. 2002, pp. 698–704.

[185] T. Kim, M. Fiorentino, and F. N. C. Wong. "Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer". *Physical Review A* 73.1 (2006), p. 012316.

[186] I. H. Malitson. "Interspecimen comparison of the refractive index of fused silica". *Journal of Optical Society of America B* 55.10 (1965), pp. 1205–1209.

[187] A. Checko et al. "Cloud RAN for mobile networks—A technology overview". *IEEE Communications Surveys & Tutorials* 17.1 (2014), pp. 405–426.

[188] S.-B. Cho and T.-G. Noh. "Stabilization of a long-armed fiber-optic single-photon interferometer". *Optics Express* 17.21 (2009), pp. 19027–19032.

[189] F. Lenzini et al. "Active demultiplexing of single photons from a solid-state source". *Laser & Photonics Reviews* 11.3 (2017), p. 1600297.

[190] E. A Dauler et al. "Review of superconducting nanowire single-photon detector system design options and demonstrated performance". *Optical Engineering* 53.8 (2014), p. 081907.

[191] P. Senellart, G. Solomon, and A. White. "High-performance semiconductor quantum-dot single-photon sources". *Nature Nanotechnology* 12.11 (2017), p. 1026.

[192] R. H. Dicke. "Interaction-free quantum measurements: A paradox?" *American Journal of Physics* 49.10 (1981), pp. 925–930.

[193] A. C. Elitzur and L. Vaidman. "Quantum mechanical interaction-free measurements". *Foundations of Physics*. 23.7 (July 1993), pp. 987–997. ISSN: 1572-9516.

[194] P. Kwiat et al. “Interaction-Free Measurement”. *Physical Review Letters* 74 (24 June 1995), pp. 4763–4766.

[195] V. Scarani and R. Renner. “Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing”. *Physical Review Letters* 100.20 (2008), p. 200501.

[196] W. O. Krawec. “Quantum key distribution with mismatched measurements over arbitrary channels”. *Quantum Information and Computation* 17.3 and 4 (2017), pp. 209–241.

[197] A. Kuhn, M. Hennrich, and G. Rempe. “Deterministic single-photon source for distributed quantum networking”. *Physical Review Letters* 89.6 (2002), p. 067901.

[198] M. Keller et al. “Continuous generation of single photons with controlled waveform in an ion-trap cavity system”. *Nature* 431.7012 (2004), p. 1075.

[199] J. Beugnon et al. “Quantum interference between two single photons emitted by independently trapped atoms”. *Nature* 440.7085 (2006), p. 779.

[200] S. Chen et al. “Deterministic and storable single-photon source based on a quantum memory”. *Physical Review Letters* 97.17 (2006), p. 173004.

[201] J. K. Thompson et al. “A high-brightness source of narrowband, identical-photon pairs”. *Science* 313.5783 (2006), pp. 74–77.

[202] S. Du et al. “Subnatural linewidth biphotons with controllable temporal length”. *Physical Review Letters* 100.18 (2008), p. 183603.

[203] C. Shu et al. “Subnatural-linewidth biphotons from a Doppler-broadened hot atomic vapour cell”. *Nature Communications* 7 (2016), p. 12783.

[204] I. Aharonovich, D. Englund, and M. Toth. “Solid-state single-photon emitters”. *Nature Photonics* 10.10 (2016), p. 631.

[205] P. Senellart, G. Solomon, and A. White. “High-performance semiconductor quantum-dot single-photon sources”. *Nature Nanotechnology* 12.11 (2017), p. 1026.

[206] J. Loredo et al. “Scalable performance in solid-state single-photon sources”. *Optica* 3.4 (2016).

[207] H. Wang et al. “Near-transform-limited single photons from an efficient solid-state quantum emitter”. *Physical Review Letters* 116.21 (2016).

[208] H. Wang et al. “High-efficiency multiphoton boson sampling”. *Nature Photonics* 11.6 (2017), p. 361.

[209] D. Huber et al. “Semiconductor quantum dots as an ideal source of polarization-entangled photon pairs on-demand: a review”. *Journal of Optics* 20.7 (2018), p. 073002.

[210] N. Akopian et al. “Hybrid semiconductor-atomic interface: slowing down single photons from a quantum dot”. *Nature Photonics* 5.4 (2011), p. 230.

[211] J.-H. Kim et al. “Two-photon interference from a bright single-photon source at telecom wavelengths”. *Optica* 3.6 (2016), pp. 577–584.

[212] K. Takemoto et al. “Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors”. *Scientific Reports* 5 (2015), p. 14383.

[213] W. B. Gao et al. “Quantum teleportation from a propagating photon to a solid-state spin qubit”. *Nature Communications* 4 (2013), p. 2744.

[214] C. Reimer et al. “Integrated frequency comb source of heralded single photons”. *Optics Express* 22.6 (2014), pp. 6535–6546.

[215] S. Ramelow et al. “Silicon-nitride platform for narrowband entangled photon generation”. *arXiv:1508.04358* (2015).

[216] Z. Y. Ou and Y. J. Lu. “Cavity enhanced spontaneous parametric down-conversion for the prolongation of correlation time between conjugate photons”. *Physical Review Letters* 83.13 (1999), p. 2556.

[217] H. Wang, T. Horikiri, and T. Kobayashi. "Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion". *Physical Review A* 70.4 (2004), p. 043804.

[218] F. Wolfgramm et al. "Bright filter-free source of indistinguishable photon pairs". *Optics Express* 16.22 (2008), pp. 18145–18151.

[219] X.-H. Bao et al. "Generation of narrow-band polarization-entangled photon pairs for atomic quantum memories". *Physical Review Letters* 101.19 (2008), p. 190501.

[220] E. Pomarico et al. "Waveguide-based OPO source of entangled photon pairs". *New Journal of Physics* 11.11 (2009), p. 113042.

[221] M. Scholz, L. Koch, and O. Benson. "Statistics of narrow-band single photons for quantum memories generated by ultrabright cavity-enhanced parametric down-conversion". *Physical Review Letters* 102.6 (2009), p. 063603.

[222] F.-Y. Wang, B.-S. Shi, and G.-C. Guo. "Generation of narrow-band photon pairs for quantum memory". *Optics Communications* 283.14 (2010), pp. 2974–2977.

[223] C.-S. Chuu, G. Y. Yin, and S. E. Harris. "A miniature ultrabright source of temporally long, narrowband biphotons". *Applied Physics Letters* 101.5 (2012), p. 051108.

[224] M. Förtsch et al. "A versatile source of single photons for quantum information processing". *Nature Communications* 4 (2013), p. 1818.

[225] J. Fekete et al. "Ultranarrow-band photon-pair source compatible with solid state quantum memories and telecommunication networks". *Physical Review Letters* 110.22 (2013), p. 220502.

[226] Z.-Y. Zhou et al. "Cavity-enhanced bright photon pairs at telecom wavelengths with a triple-resonance configuration". *Journal of Optical Society of America B* 31.1 (2014), pp. 128–134.

[227] A. Ahlrichs and O. Benson. "Bright source of indistinguishable photons based on cavity-enhanced parametric down-conversion utilizing the cluster effect". *Applied Physics Letters* 108.2 (2016), p. 021111.

[228] M. Rambach et al. "Sub-megahertz linewidth single photon source". *APL Photonics* 1.9 (2016), p. 096101.

[229] M. Rambach et al. "Erratum:"Sub-megahertz linewidth single photon source"[APL Photonics 1, 096101 (2016)]". *Apl Photonics* 2.11 (2017), p. 119901.

[230] C.-H. Wu et al. "Bright single photons for light-matter interaction". *Physical Review A* 96.2 (2017), p. 023811.

[231] P.-J. Tsai and Y.-C. Chen. "Ultrabright, narrow-band photon-pair source for atomic quantum memories". *Quantum Science and Technology* 3.3 (2018), p. 034005.

[232] J. Wolters et al. "An efficient, tunable and robust source of narrow-band photon pairs at the Rubidium D1 line". *arXiv:1908.00590* (2019).

[233] C. Wieman and T. W. Hänsch. "Doppler-free laser polarization spectroscopy". *Physical Review Letters* 36.20 (1976), p. 1170.

[234] E. A. Donley et al. "Double-pass acousto-optic modulator system". *Review of Scientific Instruments* 76.6 (2005), p. 063112.

[235] W. Demtröder. *Laser spectroscopy: basic concepts and instrumentation*. Springer Science & Business Media, 2013.

[236] C. P. Pearman et al. "Polarization spectroscopy of a closed atomic transition: applications to laser frequency locking". *Journal of Physics B: Atomic, Molecular and Optical Physics* 35.24 (2002), p. 5141.

[237] H. D. Do, G. Moon, and H.-R. Noh. "Polarization spectroscopy of rubidium atoms: theory and experiment". *Physical Review A* 77.3 (2008), p. 032513.

[238] M. Araki. "PID control". *Control Systems, Robotics and Automation: System Analysis and Control: Classical Approaches II* (2009), pp. 58–79.

[239] D. A. Steck. *Rubidium 87 D line data*. 2001.

[240] K. Kato and E. Takaoka. “Sellmeier and thermo-optic dispersion formulas for KTP”. *Applied Optics* 41.24 (2002), pp. 5040–5044.

[241] R. Le Targat, J. J. Zondy, and P. Lemonde. “75%-efficiency blue generation from an intracavity PPKTP frequency doubler”. *Optics Communications* 247.4-6 (2005), pp. 471–481.

[242] F.-Y. Wang et al. “Efficient cw violet-light generation in a ring cavity with a periodically poled KTP”. *Optics Communications* 281.15-16 (2008), pp. 4114–4117.

[243] B. Boulanger et al. “Study of KTiOPO4 gray-tracking at 1064, 532, and 355 nm”. *Applied Physics Letters* 65.19 (1994), pp. 2401–2403.

[244] D. N. Nikogosyan. *Nonlinear optical crystals: a complete survey*. Springer Science & Business Media, 2006.

[245] U. Herzog, M. Scholz, and O. Benson. “Theory of biphoton generation in a single-resonant optical parametric oscillator far below threshold”. *Physical Review A* 77 (2 Feb. 2008), p. 023826.

[246] R.-B. Jin et al. “Efficient detection of an ultra-bright single-photon source using superconducting nanowire single-photon detectors”. *Optics Communications* 336 (2015), pp. 47–54.

[247] A. L. Glebov et al. “Volume Bragg gratings as ultra-narrow and multiband optical filters”. *Micro-Optics 2012*. Vol. 8428. International Society for Optics and Photonics. 2012, p. 84280C.

[248] A. Moqanaki, F. Massa, and P. Walther. “Novel single-mode narrow-band photon source of high brightness tuned to cesium D2 line”. *APL Photonics* 4.9 (2019), p. 090804.

Acknowledgements

Doing a Ph.D. can be very challenging without support from other people, which luckily was not my case. For this reason I would like to write here a few words of thanks for those who have accompanied me during this journey.

First of all, I would like to thank my supervisor, Prof. Philip Walther, for giving me the opportunity of doing a Ph.D. in his group and for being there whenever I needed something, if only for moral support. I owe a thank you also to Dr. Borivoje Dakić for always trying to put to use the experimental results I got in the lab and for continuously providing ideas for new experiments.

Two colleagues have been particularly important for the completion of this dissertation. One of them is Amir Moqanaki, with whom I was happy to share most of the good and bad moments of my Ph.D. because of his intuition and positive attitude. The other one is Chiara Greganti, whose alternative vision of the world always helped me to overcome crises.

A special thank you goes to all the friends and colleagues who proofread my thesis and gave me useful comments for its improvement: Rui Vasconcelos, Jonas Zeuner, Teodor Strömberg, Stella, Bob Peterson, Cameron Salter and Armin Shayeghi.

I would also like to thank all the past and present members of the Walther group for their role in my life as a Ph.D. student. All of them contributed somehow to my evolution both as a person and as a researcher.

More broadly, I am grateful to all the members of the Vienna Center for Quantum Science and Technology for the many pleasant coffee breaks, evenings, holidays and

institutional social events spent together.

Finally, I thank my family, in particular my parents, and my girlfriend, Jisoo. Although they might not have any clue of the content of this thesis and the obstacles encountered to put it together, they have always given me trust, love and support, and that's the best I could hope for.