Gustavo Castro do Amaral

Linear-Optic Two-Photon Interference with Coherent States

TESE DE DOUTORADO

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

Advisor : Prof. Guilherme Penello Temporão
Co–Advisor: Prof. Jean Pierre von der Weid

Rio de Janeiro
April 2016

Gustavo Castro do Amaral

Linear-Optic Two-Photon Interference with Coherent States

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

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

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

Prof. George Svetlichny
Departamento de Matemática – PUC-Rio

Prof. Stephen Patrick Walborn
Instituto de Física – UFRJ

Prof. Paulo Henrique Souto Ribeiro
Departamento de Física – UFSC

Prof. Daniel Felinto Pires Barbosa
Departamento de Física – UFPE

Prof. Márcio da Silveira Carvalho
Coordinator of the Centro Técnico Científico — PUC–Rio

Rio de Janeiro, April 18th, 2016

Gustavo Castro do Amaral

Gustavo C. Amaral was born in Rio de Janeiro, Brazil, in 1989. He graduated from the Pontifical Catholic University in Rio de Janeiro in Electrical Engineering in 2011 and, later, received his M.Sc. degree in Electrical Engineering in 2014 from the same institution with the dissertation entitled "FPGA Applications on Single-Photon Detection Systems". His present areas of interest are quantum optics, two-photon interference, coherent optical effects, SCM/WDM-PON transmission and monitoring, and electronic digital circuits design. He is a member and an active participant of the Optoelectronics Laboratory and all its projects.

Bibliographic data

Amaral, Gustavo Castro

Linear-Optic Two-Photon Interference with Coherent States / Gustavo Castro do Amaral; advisor: Guilherme Penello Temporão; co–advisor: Jean Pierre von der Weid. — 2016.

134 f: il. color. ; 30 cm

Tese (doutorado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Engenharia Elétrica, 2016.

Inclui bibliografia.

1. Engenharia Elétrica – Tese. 2. Óptica Quântica. 3. Inteferência de Dois Fótons. 4. Fontes de Fótons Únicos. 5. Espectroscopia de Poucos Fótons. 6. Efeitos Ópticos Coerentes. I. Temporão, Guilherme Penello. II. von der Weid, Jean Pierre. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. IV. Título.

CDD: 621.3

Acknowledgments

To Monique Lamhut, the only thing that I love more than my work.

To Professors G. P. Temporão and J. P. von der Weid, teachers, colleagues, and friends.

To my colleagues, Doctors T. Ferreira da Silva and L. E. Y. Herrera, and J. D. Garcia, F. Calliari, and M. Albarracin.

To Mom and Dad.

I would also like to thank brazilian agencies CNPq and FAPERJ, and The Innovation Centre, Ericsson Telecomunicações S.A., Brazil for financial support.

Abstract

Amaral, Gustavo Castro; Temporão, Guilherme Penello; von der Weid, Jean Pierre. **Linear-Optic Two-Photon Interference with Coherent States**. Rio de Janeiro, 2016. 134p. PhD Thesis — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Photon bunching is one of the most celebrated effects of two-photon interference, related to the tendency of indistinguishable photons to take the same path when there is a wave-packet overlapping in a symmetric beam splitter. We explore the two-photon interference phenomena and show that: the spectral characteristics of a light source can be determined with a high resolution Few-Photon Fourier Transform Spectroscopy which proves to be a useful asset for spectral characterization of faint optical sources below the range covered by classical heterodyne beating techniques; a sub-Poisson photon source, the Linear-Optic Heralded Photon Source, can be constructed based only on linear optics and weak coherent states by time-tuning a Hong-Ou-Mandel interferometer fed with frequency-displaced coherent states and yields a second-order correlation function at zero time below one; a modified version of the Hong-Ou-Mandel interferometer produces a peak of coincidences instead of a dip when the wave-packets are perfectly overlapped and the announcement of photons time-tuned to this coincidence peak yields a photon stream with sub-Poisson photon statistics. The mathematical description of each experiment is detailed and an extensive review of the most important theoretical and practical tools for understanding the results is presented.

Keywords

Quantum Optics; Two-Photon Interference; Single-Photon Sources; Few-Photon Spectroscopy; Optical Coherent Effects.

Resumo

Amaral, Gustavo Castro; Temporão, Guilherme Penello; von der Weid, Jean Pierre. **Interferência de Dois Fótons em Óptica Linear com Estados Coerentes**. Rio de Janeiro, 2016. 134p. Tese de Doutorado — Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

O *bunching* de fótons é um dos mais celebrados efeitos de interferência de dois fóotons, associado à tendéncia de fótons indistinguíveis de tomarem o mesmo caminho quando há uma superposição dos pacotes de onda em um combinador de feixes óptico simétrico. Nós exploramos o fenômeno de interferência de dois fótons e mostramos que: a característica espectral de uma fonte de luz pode ser determinar através da técnica de Espectroscopia de Transformada de Fourier de Poucos Fótons de alta resolução que se mostra como uma técnica útil para a caracterização espectral de fontes ópticas débeis abaixo do limite coberto por técnicas clássicas de batimento heteródino; uma fonte de fótons com estatística sub-Poisson, a Fonte de Fótons Anunciadas com Óptica Linear, pode ser construída baseada apenas em óptica linear e estados coerentes atenuados uma vez que os anúncios sejam sintonizados nos picos de coincidência de um interferograma de Hong-Ou-Mandel quando o interferômetro é alimentado com estados em frequências diferentes; uma modificação do interferômetro de Hong-Ou-Mandel produz um aumento no número de coincidências, ao invés de sua diminuição, quando os pacotes de onda estão perfeitamente superpostos no interferômetro e o anúncio de fótons sintonizados nesse pico gera um feixe com distribuição sub-Poisson. A descrição matemática de cada experimento é detalhada e uma revisão extensa das ferramentas teóricas e práticas necessárias para o entendimento dos resultados é apresentada.

Palavras-chave

Óptica Quântica; Inteferência de Dois Fótons; Fontes de Fótons Únicos; Espectroscopia de Poucos Fótons; Efeitos Ópticos Coerentes.

Contents

List of Figures

A photon is what a photodetector detects.

Roy Glauber.

Summary of notations

G-APD Geiger-mode Avalanche Photodiode.
SPAD Single-Photon Avalanche Diode.
QKD Quantum Key Distribution.
HPS Heralded Photon Source.
SPDC Spontaneous Parametric Down Conversion.
FWM Four-Wave Mixing.
WCS Weak-Coherent State
FPGA Field Programmable Gate Array.
ESA Electrical Spectrum Analyzer.
FLS Faint Laser Source.
GLLP Gottesman, Lo, Lütkenhaus, and Preskill security proof.
HSPS Heralded Single-Photon Source.
H Hilbert Space.
$\hat{O}$ Hilbert Space Operator.
$\hat{O}^{\dagger}$ Hilbert Space Adjoint Operator.
$\hat{H}$ Hamilton Operator.
$\hat{q}$ Linear Momentum Operator.
$\hat{p}$ Position Operator.
$\hat{a}$ Photonic mode Annihilation Operator.
$\hat{a}^{\dagger}$ Photonic mode Creation Operator.
$\hbar$ Planck's Constant. Unity: $m^2 \cdot kg/s$.
ω Angular Frequency. Unity: rad/s.
$|n\rangle$ n-photon Fock State.
$\hat{n}$ Photon Number Operator.
t Time. Unity: s.
$\hat{E}(t)$ Time-Dependent Electric Field Operator.
$|\alpha\rangle$ Coherent State.
$\hat{D}(\alpha)$ Displacement Operator.
I Optical Intensity. Unity W/m^2.
$g(t)$ FirstOrder Temporal Correlation Function.
$\mathscr{F}\{\}$ Fourier Transform Operator.
$s(\nu)$ Power Spectral Density. Unity: W/Hz
$g^{(2)}(t)$ Second-Order Temporal Correlation Function.

k Wave Number. Unity: rad/m.

μ_0 Vacuum Permeability. Unity: $V \cdot s/\left(A \cdot m\right)$.

ϵ_0 Vacuum Permittivity. Unity: F/m.

ε_0 Electric Field Amplitude. Unity: V/m.

$\xi\left(z,t\right)$ Spatio-Temporal Wave-Packet. Unity: V/m.

1
Introduction

This work is a compilation of three main results associated to two-photon interference with coherent states: a mathematical model and experimental confirmation of high-resolution heterodyne spectroscopy in the few-photon regime; the possibility of generating a sub-Poisson stream of light taking advantage of an interference peak in the Hong-Ou-Mandel interferometer fed with frequency-displaced photonic wave-packets, the linear-optic heralded photon source; and a further investigation of the sub-Poisson light stream generation using two symmetric beam-splitters in a stable, more simple configuration. Two-photon interference in a linear-optic context is associated to the Hong-Ou-Mandel interferometer, the experimental apparatus whose characteristics were thoroughly exploited throughout the development of the results.

The document is divided in such a way (or at least meant to be so) that the reader's trail of thought is not compromised by the technicality of the subject, especially in terms of its mathematical description. We begin with a historical, sociological, and rather philosophical take on the subject of the photon. Since, as the epigraph states, we need to detect the photon in order to attest its existence, we follow the historical introduction with a state-of-the-art description of single-photon detectors and specific photon sources. Understanding of the theoretical and experimental results presented in Chapters 3, 4, and 5 is a product of centuries of scientific developments so, in Chapter 2, the basic theoretical ideas are laid out in an – hopefully – intuitive manner. Still aiming at a pleasant reading, the mathematical developments and proofs are delegated to Chapter 7, i.e., the Appendices. Each of the results is delegated to its own chapter, which contain a brief introduction, the description of theoretical and experimental details, and conclusions.

1.1
A Brief History of Light – The Wave-Particle Duality Retrospective

The photon is a twentieth-century concept[1] intimately tied to the birth of quantum mechanics and quantum electrodynamics. In order to avoid later

[1]This Retrospective section is a compilation of bibliographic revision taken from [1–7] and references therein.

philosophical query, we start by introducing the photon in the words of Roy Glauber:

"A photon is what a photodetector detects."

With no rest mass, the photon cannot be "stopped" except by an absorption process that destroys it. Also associated with the absence of rest mass is the lack of photon localizability: there is no probability density for the position of the photon.

Even though the history behind the development of quantum optics and of the "'photon" concept is very rich and concerns a plethora of different propositions, experiments and even sociological intrigue, it is surprising how the question that still remains over the corpuscular-wave nature of the photon had its roots long before the advent of quantum physics. The first notion of light as a propagating wave was introduced by Descartes. He considered light to be a longitudinal wave propagating in a perfectly elastic medium, the luminiferous aether. The aether, as we will see, remained as a conceptual milestone for the theory of light propagation until the early nineteen hundreds regardless of its controversy. This perfectly elastic medium was thought to fill all space and, as Descartes proposed, was responsible for the diversity of colours due to different velocities of particles in this medium.

It was Hooke who first proposed that light consisted of rapid vibrations propagated instantaneously, or with a very great speed, and that these vibrations would generate a steadily growing propagation sphere (in case of a homogeneous medium of propagation). Huygens extended the idea that light propagates as a wave and that each point of the wavefront forms a subsequent wavefront. By that time, it was thought that the wavefronts were created due to the interaction between the luminous disturbance and the aether. It was also Huygens who came across the phenomena of polarization when studying light diffraction. Newton interpreted that the polarization arose from the fact that light rays have "sides" which imply a transversal condition for the propagating light wave. Scientists at the time were only familiar with longitudinal waves such as the sound vibrations so this, among other aspects of the wave theory, especially the difficulty in reconciling the rectilinear propagation of light, led Newton to completely negate the wave theory of light. He devoted himself to the development of an emission (or corpuscular) theory according to which light was emitted and propagated in the form of discrete particles.

The rejection from an eminent physicist such as Newton swept the wave theory under the rug for almost a century. It was only in 1801 that Young enunciated the principle of interference of light and once again enforced the

view of light as a wave. Later, Fresnel synthesized Huygen's Wavefront Principle with Young's Principle of Interference and showed that this was sufficient to account for the rectilinear propagation of light as well as for the phenomena of diffraction. Only when Fresnel, together with Arago, investigated the interference of polarized light and discovered that two rays with perpendicular polarization could not interfere was that the transverse vibration of light was considered. It was Young who reconciled the phenomena discovered by Fresnel with the wave theory of light by the deconstruction of the longitudinal propagation of light which was already taken for granted. This progress, however, did not convince the Laplacian school which firmly advocated in favor of the emission theory proposed by Newton.

In the mean time, Fresnel, due to Young's proposition, drew numerous conclusions concerned with the nature of the aether. Since longitudinal waves are only possible in a fluid, he stated that the aether should behave like a solid body. At the time, however, a theory of elastic waves in solids had not yet been formulated so Fresnel proceeded by inference over the experimental observation. He managed to elucidate the laws of light propagation in crystals and later reduced them to a few simple assumptions. Curiously, it was due to the study of dynamical models for the aether vibration that Fresnel deduced the laws that govern the intensity and polarization of light rays produced by reflection and diffraction. An important experiment proposed by Arago and later conducted by Foucault and others in 1850 was the one regarding the measurement of light's velocity in water and air. This was definite for the acceptance of Fresnel's and Huygen's wave theory. According to the proposition of the emission theory, refraction was caused by the attraction of light corpuscles by the denser optical medium which would imply a greater velocity in the denser medium. The wave theory, on the other hand, provides that the inverse should happen, which was experimentally demonstrated.

Until the complete deconstruction of the luminiferous aether theory with the Michelson-Morley experiment and, later, Special Relativity, many efforts were directed to the development of the elastic aether theory to account for the wave theory of light as soon as the propositions of Fresnel and Huygen were well established. Although mechanical boundary conditions in the passage between two contiguous elastic media always conflicted with the results of diffraction, the corpuscular theory still found a way to resist to the experimental evidence of the wave theory. Even though a number of optics related issues found their solution during the last half of the nineteenth century, the foundations of optics remained in an unsatisfactory state. In parallel, the development of electricity and magnetism culminated in the discoveries of Faraday which led Maxwell

to sum up all the experimental evidence in a system of equations which not only established the possibility of electromagnetic waves but that their velocity could be calculated from the results of purely electrical measurements. Finally, when the experiments were carried out, the velocity turned out to be that of light. The electromagnetic theory of light was then proposed by Maxwell which, until its experimental verification by Hertz in 1888, suffered much criticism and many attacks. After its acceptance, though, it became clear that the theory did not suffice to explain certain phenomena such as emission and absorption of light by matter.

The late eighteen hundreds had brought about the spectrum analysis, which was first motivated by an effect on the continuum spectrum of the sun. The observed effect was that the spectrum is filtered exactly in the absorption lines of certain gases that compose the sun's atmosphere. Even though spectroscopy often tells more about the structure of the emitting particles rather than about the nature of the emitted light itself, it was, and still is, essential for the elucidation of the interaction between matter and the optical field. The problem of the spectrum of emission of black body radiation, for instance, motivated Planck to develop the idea that an oscillating electric system does not impart its energy to the electromagnetic field in a continuous manner, but in finite amounts. Later, Einstein was responsible for reviving the corpuscular theory of light by assuming that energy quanta existed as real light-particles, the photons, which were not merely a representation of the absorption and emission process as proposed by Planck. This re-introduced the particulate nature of light, not as localization in space as Newton's corpuscles, but in discreteness of energy. Some phenomena inexplicable by wave theory were successfully explained due to the transformation of light into corpuscular energy, namely the photo-electric effect and photochemistry. The interpretation of Einstein of the photo-electric effect, though, is not to be mistaken with quantization of the radiation field.

At this point the validity of both wave and corpuscular theories of light had to be recognized. It was only during the third decade of the twentieth century, however, that the development of quantum mechanics led to a partial elucidation of the wave-particle duality. Later, Quantum Optics had its foundations laid when Dirac quantized the electromagnetic radiation field reconciling the wave and particle theories. In the words of Fermi, in his 1932 Review of Modern Physics article [4]

> "Until a few years ago it had been impossible to construct a theory of radiation which could account satisfactorily both for interference phenomena and the phenomena of emission and absorption of light

> by matter. The first set of phenomena was interpreted by the wave theory, and the second set by the theory of light quanta. It was not until in 1927 that Dirac succeeded in constructing a quantum theory of radiation which could explain in an unified way both types of phenomena."

Energy quantization is the essence of the old quantum theory of the atom proposed by Bohr. Planck's hypothesis and Einstein's interpretation of the photoelectric effect follow from considerations of how energy is exchanged between radiation and matter. This leads to forbidden energies of absorption and emission. In the case of Bohr's atom, this is reflected in the discrete orbitals available for the electron and in the fact that the transition between them is excited by a vibration of the right frequency which could be a *photon* - a quantum of radiation - or a *phonon* - a quantum of vibration. De Broglie's analogy to standing waves in a cavity quantizes the wavelength of the electron due to the restriction that a finite number of wavelengths should fit the circular orbit's radius. Following this development, Schrödinger introduced the wave equation for matter waves. By this time, then, both light and matter were neither wave nor particle, but an intermediate entity that obeys the superposition principle. The equal validity of both perspectives in Young's two slit experiment, depending on the configuration, advocated for such complementarity.

Even though the progress of Schrödinger, De Broglie, and others had laid the foundations of quantum mechanics, the theory was still not completely quantized. The semiclassical approach, as it is called, treats light classically – although with discrete energies – while only matter is quantized: quantizing the energy differs greatly from quantizing the electromagnetic field. The semiclassical approach, even though remarkably accurate for a large class of problems, is an attempt to equalize the treatments of light and matter in a self-consistent wave theory: Maxwell equations deal with the wave theory of light; and the Schrödinger Equation deals with the wave theory of matter. The self-consistency of semiclassicality relies on the interpretation of the light-matter interaction as a resonance phenomena. In case of light absorption, the ground state is coupled to the excited state by means of the beat frequency between these two permitted energy levels inside the atom. The beat frequency, or energy, is conveyed by the photon. In the case of absorption and later emission of a photon by an atom, for example, the interaction is interpreted such that the electron cloud is polarized by the incident light field producing a dipole moment which corresponds to excitation. This dipole eventually re-radiates a classical – quantized – Maxwell field proportional to the beat frequency (or the

dipole's stored energy). The agreement between incident and radiated fields indicates a self-consistent coupling of the Maxwell-Schrödinger equations.

To take a glimpse on the very profound difference between the quantization of the energy, in a semiclassical approach, and the field quantization, in the quantum optics approach, regard the photoelectric effect. It is observed, in this experiment, that, at negligible times after light had been directed to the metal plate, electrons are already being detected. Even though the detection flux and the kinetic energy are consistent with energy quantization, it does not account for how energy can be imparted from light to matter at seemingly infinitesimal times. In terms of electromagnetic radiation, the energy conveyed by the field is proportional to the field's amplitude, the atom's cross-section, and time; for short enough times, the energy is just negligible compared to the energy gap. Semiclassicaly, there is just no way of accounting for the "quantum jump" for the field energy. The change in perspective gained from this subtle effect is that not only the amount of energy that can be imparted from light to matter is discrete, but the time that it takes for the radiation field to actually transfer energy to matter is discrete. In other words, the discrete levels of energy also come in discrete packets in time and space! The quantized view of the electromagnetic field which fully accounts for the probabilistic nature of light and its inherent fluctuations was introduced by Dirac in 1927. For the first time the photon concept was placed on a logical foundation and the quantum theory of radiation was born. To quote Dirac [3] in the conclusion of his article

> "(...) the theory enables one to understand how it comes about that there is no violation of the law of the conservation of energy when, say, a photo-electron is emitted from an atom under the action of extremely weak incident radiation. (...) In particular, one cannot say that the interaction energy tends to zero as the intensity of the incident radiation tends to zero. There is thus always an unspecifiable amount of interaction energy which can supply the energy for the photo-electron."

The photon, although being an intrinsic conundrum of nature and to the physical community, is one of the most interesting fundamental particles: the theoretical field quantization performed by Dirac sets it as the most important quantum electrodynamical entity as well as poses quantum optics as a resourceful area of physics research since exclusively quantum effects such as single-photon and two-photon interference are of paramount importance for the investigation of the underlying nature of quantum physics. In this context, to get a glimpse of the nature of the photon, one must, once again, turn back

to Glauber's words and, therefore, *detect the photon*. This is utterly important not just for itself, but because being able to detect the photon is an absolutely necessary step towards being able to generate it or, at least, being able to *attest* it has been generated. In the next section, therefore, we review the basics of single-photon detection culminating in the Single-Photon Avalanche Diode, and generation with the very recent high-rate sub-Poissonian Heralded Single-Photon Sources. We also brush on the basics of quantum communication, maybe the most celebrated application of the single-photon in present days.

1.2 Single-Photon Detection and Single-Photon Generation

1.2.1 Single-Photon Detectors

The first experimental demonstration of the Photoelectric Effect was developed by Heinrich Hertz in 1887 [8]. The theory behind the Photoelectric Effect, elaborated by Einstein [9], permitted the construction of an apparatus capable of detecting light with very low intensity, the Photoelectric Tube, which dates from 1913 and whose inventors were Elster and Geiter [10]. Subsequent developments gave birth to the Photomultiplier Tube (PMT), a device which, despite the development of solid state photodetectors, is still used in several fields of research such space research, archeology, medicine, geology, biology, art, astronomy, metallurgy, chemistry, agriculture, high energy physics, and astroparticle physics [11]. Photodiodes are devices created with doped semiconductor junctions and condensate, in a solid-state structure, the mechanism of light detection of the Photoelectric Tube: when a photon with sufficient energy to excite an electron to the conduction band of the semiconductor is directed to the photodiode, it creates an electron-hole pair; each carrier then migrates in opposite directions under the influence of the electric field across the Depletion Region [12]; the moving carriers, therefore, conduct current proportional to the number of photons arriving at the junction along the semiconductor.

Avalanche Photodiodes are solid-state Photomultipliers that undergo an avalanche process whenever a photon reaches the absorption region and excites an electron-hole pair that collects sufficient kinetic energy from the applied electric field to start an impact ionization cascaded effect [13–15]. The basis of this effect is an operation at the Breakdown Voltage so the avalanche may be sustained. When it comes to the necessary number of photons for a detection, however, APDs are within some more than 20, so single-photon detection is

not possible [10]. Geiger-mode APDs (G-APDs) go further into the Breakdown Region of a photodiode as to be able to detect single-photons [10]. When biased above the Breakdown Voltage, electrons and holes are ionized faster than they can be extracted from the semiconductor lattice so, eventually, the junction becomes saturated [16, 17]. The effect of a photoexcited electron-hole with enough energy to produce cascaded ionization is an exponential growth in the population of holes and electrons in the Multiplication Region and of the associated photocurrent. This goes on for as long as the electric field in the device is not altered by the photocurrent growth, i.e., until the space charge effect limits the photocurrent to a constant value leading the circuit into a steady-state condition [16, 17]. In order to bring the device back from the steady-state, it is necessary to discharge the device's saturated junction in a process called *quenching*, which can be active or passive [14, 15]. A passive quenching circuit is simply a high impedance load connected in series to the G-APD [15, 18, 19]. Even though the impedance of the semiconductor junction is usually very high (above the range of MΩ) when the device is not operative, once it undergoes an avalanche process, the impedance drops to a few kΩ, so the inverse bias voltage appears over the high-impedance resistor and the diode can recover from the avalanche. The recovery time, however, may be very long in passive quenching [15, 18]. Active quenching resorts on a fast comparator device which detects the avalanche pulse and triggers a quenching pulse to be superposed to the reverse bias voltage alleviating the semiconductor junction [18,20]. Pulse shaping, filtering, and fast electronics are all necessary for successful active quenching, but maybe the most important factor is a tailored circuit which compensates the effects of its particular APD characteristics since they vary abruptly from device to device [18, 20, 21].

The binary behaviour of G-APDs introduces two new parameters of operation: Dead Time and Afterpulsing. Dead Time is the period between an avalanche and the end of the quenching process during which the photodetector is inoperative [10]. Since G-APDs become unresponsive during the Dead Time, active quenching is more suited for fast detection applications [16, 17, 20, 21]. Although already present in other photodetector devices, the Afterpulsing effect is more critical in G-APDs. The Afterpulse effect may be characterized by a higher probability of a Dark Count, i.e., a false avalanche, right after a detection due to carrier trapping and delayed release inside the semiconductor junction, which might last several microseconds [10, 17]. In order to diminish the probability of thermally generated avalanches, the temperature of the photodetector is often decreased leading to longer delayed releases and, thus, to longer periods of high Afterpulsing probability [10].

The physical parameters and the design of the photodetector structure has direct implication on the operation of the device. The doping concentration of each layer and its thickness, for instance, affect the range of sensitive wavelengths and the operating voltage, respectively. Dark Counts and Afterpulsing, on the other hand, can be reduced by controlling the impurities and crystal defects [10]. The application of G-APDs is vast: High Energy Physics, Astroparticle Physics, and Medical Applications, in which a number of such devices are used in an array [22]; and Quantum Optics, especially Quantum Communication, where the G-APD is used to assemble a structure called the Single Photon Avalanche Diode (SPAD). Gated operation is applicable to Quantum Communications since the arrival times of the photons is usually synchronized by an external clock signal common to the communicating parties. The result is high detection efficiency during the operational gate width and low dark count rate when the device is inoperative.

Indium-Phosphide-based single-photon avalanche diodes, especially Indium-Gallium-Arsenide / Indium-Phosphide (InGaAs/InP), are the elected devices for quantum communications since they operate inside the infrared 1550 nm wavelength region of telecommunication at almost room temperature [18, 23–27]. Therefore, we focus a little bit more on the operation characteristics of such devices. Nevertheless, Silicon-based single-photon avalanche diodes, which operate in the visible region of the electromagnetic spectrum from 400 to 1000 nm wavelength, attract a great deal of attention in free-space optics especially due to their high efficiency on the order of 70% [15, 20, 21]. In InGaAs/InP devices, the infrared photons are absorbed in the InGaAs region forming an electron-hole pair which dissociates due to the intrinsic field of the junction so that the photon-generated hole drifts to a high-filed InP region where it can accelerate and initiate the avalanche process [18]. The efficiency of the absorption process for InGaAs devices revolves around 10% [28] although it can be made higher if one is willing to compromise the system noise by raising the reverse bias voltage over the semiconductor heterostructure. Even though sub-nanosecond jitter can be achieved in low temperatures, the longer trap lifetimes is a serious issue in such devices since the avalanche may fill trap states between the gaps of the InGaAs and InP structures [18]. To avoid this phenomena, the only solution that does not diminish the device's efficiency, is to improve the active quenching method; gigahertz clock rates at near room temperature have been reported using approaches such as the *very rapid gating* [29, 30]. Free-running operation at 210K with the same approach has also been reported [31, 32]. Even with its afterpulsing limitations, InGaAs/InP are outstanding candidates for practical

single-photon detection in the infrared region and a number of studies have already shown that the traps responsible for afterpulsing are related to the InP layers of the device, so future improvements and research in the area are supposed to yield reduced dark count rates [18, 33, 34].

1.2.2 Applications in Quantum Cryptography

Widely used in quantum cryptography, the single-photon avalanche diode is the focus of the majority of the so-called *quantum hacking* schemes, in which a third party is able to temper with the communication channel gaining information without being noticed by the actual communicating parties. In general lines, quantum cryptography and, more specifically, Quantum Key Distribution (QKD) [35], benefits from the laws of quantum physics to provide absolutely secure communication (at least from a theoretical point of view) between two (or more) parties. The No-Cloning Theorem [36, 37] states that non-orthogonal quantum systems cannot be duplicated due to the intrinsic loss of information during measurement, in which such loss refers to the Heisenberg's view on measurements over quantum systems and Heisenberg's Uncertainty Principle [38]. Based on this theorem, various protocols [39–42] were developed in which the presence of an *eavesdropper* can be detected based on the results of exchanging single-photon states between the communicating parties so the effective losses due to unexpected tempering during quantum communication are accounted for. QKD also relies on a classical communication step so that the errors due to the losses along the quantum communication channel (those expected such as fiber attenuation and those unexpected such as an eavesdropper) can be computed and measured against a threshold from which one can determine whether the system has been tempered with or if the communication is secure [35]. Even though the performance of the devices employed in practical quantum cryptography, namely the single-photon detector and the single-photon source, is still far from the idealized ones, several solutions have been devised in order to overcome their limitations [35]. One of the most severe imperfections is that of multi-photon pulse emission by the transmitter which enables the photon-number splitting attack [35]. Even though a deterministic single-photon source would be highly desirable in this context, it is not yet available. Nevertheless, the single-photon source limitation of practical QKD is secured by strict mathematical proofs and counter measures such as the decoy states method [43–46].

When it comes to the detector, several so-called loopholes – or imperfections – of the device can be exploited by the *quantum hacker*, usually referred

to as Eve. Since measuring the quantum state in mid-flight will occasionally result in its identification, the quantum hacker is forced to either cloak its act of measurement or to alter the properties of the state without measuring it and then use the result of the real measurement to gain information. Acting on the system timing, Eve can implement the class of time-shift attacks based on the non-uniformity of the detection efficiency inside the gating window so it becomes possible to infer the results of the measurements [47–50]; forcing the detectors to operate in linear regime instead of in the avalanche mode by sending pulses of bright – classical – light is a means of controlling the results of detection and, thus, cloak Eve's own measurement [51–55]. Most of these attacks have been demonstrated against real-life QKD systems [56–58] for which specific counter-measures have been devised [47, 59]. Nevertheless, perfectly secure practical quantum key distribution is still a matter of research. Recently, however, a protocol independent of the measuring apparatus has been proposed [60] – the Measurement-Device Independent Quantum Key Distribution protocol – for which experimental implementation with different quantum state encoding schemes have been reported [61–64] against which a successful quantum hacking attack has not yet been devised. The advent of such protocol not only promises a solution for practical QKD but somehow shifts the focus from the imperfections of the detectors to the single-photon sources, which are now expected to operate in higher and higher rates so that the secure key generation rate raises to meet the demands of real-life applications such as internet banking and mailing services.

1.2.3 Single-Photon Sources

Single-photon sources are a fundamental resource not only in Quantum Cryptography and Quantum Computing, perhaps the most celebrated features of Quantum Information, but in a broad range of applications as well [35, 65–67]. Practically, the photon number statistics of any pseudo-single-photon source is always a concern, and the compromise between vacuum-, single- and multi-photon emission probabilities directly impacts the source's, as well as the experiment's, performance [68]. A practical and low-cost way to probabilistically producing single photon pulses is to use a faint laser source (FLS), whose output pulses approach coherent states [5, 69]. Although the light pulses emitted by the stabilized laser seem regular in amplitude, this is a direct consequence of the extremely high number of photons that it contain which render the quantum fluctuations negligible on a macroscopic scale [70]. Actually, each pulse is described as a superposition of number states – states

of a well-defined number of photons n – following the Poisson distribution. If one bounds the emitted power to extremely low levels by means of an optical attenuator, for instance, the proportion of multi-photon to single-photon pulses diminishes, but this leads to an increase in the probability of emitting vacuum-pulses, i.e., pulses containing no photons at all [5, 18]. This is a source of concern in Quantum Cryptography since vacuum pulses cannot contribute to secret key generation and often reduces the security of a system [68]. A typical value for the average number of photons generated in a light pulse by an attenuated light source for QKD applications is on the order of 0.1 [59, 61, 71–76] which results in an approximated chance of 5% to generate a multi-photon pulse[2]. The eavesdropper Eve can, therefore, gain information over the transmitted quantum states in approximately 5% of the transmitted pulses without employing any kind of quantum hacking scheme, let alone her resourceful plethora of attacks.

Consider, now, a single-atom system which can occupy two different energy levels, the ground and excited states, separated by an energy gap. This system would be ideal for single-photon generation in the wavelength corresponding to the energy separation between the ground and excited states. One is compelled to ask, therefore, why is it so hard to harness a system such as a semiconductor junction – described by pretty much the same structure of energies but, instead of ground and excited, one has the valence and conduction bands [12] – for single-photon generation. For one thing, the interaction (either absorption or emission) between the electromagnetic radiation and matter scarcely occurs for a single frequency – or energy – but, rather, for a range of frequencies – a band – around the *natural oscillatory* frequency of the system. This is intimately related to the interaction cross-section of the atomic structure, which is usually considered to be a lorentzian-shaped function centred around the resonant frequency [69] and which defines the bandwidth of emission. Ideally, the lorentzian-shaped function would collapse to a delta distribution so only a single frequency is permitted to oscillate with the radiation-matter system. This, however, is in disagreement with Heisenberg's Uncertainty Principle and is somewhat a dead-end in terms of single-photon generation. Suppose, however, this last assumption could, indeed, be achieved: one would still have the task to guarantee that only a single atom performs the transition between energy states to either generate or absorb a single-photon. In a crystal lattice with an unimaginable number of atoms, that task turns out to be an extremely difficult one. The idea behind quantum-dot-based

[2]This result is straightforward when one substitutes the parameter of the Poisson distribution with the value of the average number of photons per pulse.

single-photon sources is exactly this last one: isolate a single-atom system in a semiconductor lattice so that the emission may occur inside the bandwidth defined by the interaction cross-section but so that only this single-atom system participates in the process.

Strictly speaking, a quantum dot is a structure which confines electrons in three dimensions, leading to a quantization of the available energy transitions for carriers similar to that of a single atom, which is capable of single-photon emission [77–79]. A disadvantage of quantum dots is that the artificial states that populate the energy gap to form the dots depend on very low temperatures not to deteriorate, so the devices usually operate below 20 K for which the rate of single-photon generation excited electrically has been reported to achieve the gigahertz range [80]. Experiments have been reported in which the distribution of the number of photons per pulse generated by the quantum dots are shown to be much closer to the single-photon than the states generated by attenuating a conventional laser source [77–79]. In general, one attempts to measure the rate between single-photon and multi-photon emission so that one's proposed source can be contrasted with the Poisson distribution of an attenuated laser; this figure of merit is the second-order autocorrelation function at zero time, obtained through the Hanburry-Brown and Twiss experiment. Both the figure of merit and the experiment itself will be discussed in details in future sections. For the present discussion, imagine that the output of the source (a series of optical pulses containing any number of photons) is directed to a device which splits the optical beam in two and detections from two single-photon detectors are acquired after such device: qualitatively, if the number of coincident detections is high, the rate of multi-photon is high; on the other hand, if the coincident counts are low, the multi-photon emission is low since a single-photon can only be detected by a single detector.

Alternatively to faint lasers and quantum dots, non-linear optical processes can be explored to assemble a single-photon source with sub-Poisson photon-number distribution, i.e., a source with a rate between single and multi-photon pulses much higher than that of an attenuated laser. Let us first consider a very profound limitation of the sources discussed so far but which was not mentioned: the certainty of a single-photon emission. Even in the case of quantum dots, which perform much more like an ideal single-photon source than the attenuated laser, one is never sure about the single-photon emission up to the point where the light pulse is detected. In quantum communications, for instance, this presents a harsh limitation since the two communicating parties should know when the photon is transmitted to synchronize their protocol and, as we have seen, synchronization is a vital feature of quantum communication

due to the single-photon detector limitations and so that the efficiency and dark count can be raised and lowered, respectively. A unique feature of the aforementioned non-linear optical processes is the generation of not only one single-photon but, rather, a pair of single-photons which obey the law of conservation of energy and fit the purpose of single-photon generation *on demand*: whenever one photon is generated, the other one must also be generated so the detection of one photon can be used to announce, or herald, the presence of the other photon in the so-called *heralded single-photon source* [81–89]. Even though some of the heralded single-photon sources (HSPSs) are based on Four-Wave Mixing (FWM) [88, 89], the majority exploits the phenomenon of Spontaneous Parametric Down Conversion (SPDC) [7, 90, 91].

Parametric Down-Conversion is the phenomenon in which an energetic photon (short wavelength, high frequency) interacts with a non-linear medium (usually a crystal which exhibits optical nonlinearity) and generates two less energetic (longer wavelength, lower frequency) photons [69]. The non-linear factor that rules the SPDC process is a second order susceptibility whereas the one that rules the FWM process is a third order susceptibility for which two photons must interact with the non-linear medium in order to generate the pair of output photons [5]. By adjusting the phase-matching of the interaction, one is able to generate photons with different wavelengths or both photons within a specific wavelength range [87,92]: an intelligent design is to convert an energetic photon into a photon in the infrared region proper for quantum communication and another photon – the heralder photon – in the visible region of the spectrum as to exploit the higher efficiency of the single-photon detectors in this region to enhance the heralding probability [93,94]. Even though heralded single-photon sources exhibit a reduction of the rate between multi- and single-photon pulses by a factor of up to 500 when compared to Poissonian light, there are a few drawbacks associated to employing such sources: the process creates low-coherence photons [84] which renders the synchronization of QKD systems critical – specially if it involves the joint measure of two single-photon pulses from distinct remote sources (as in the case of the Measurement-Device Independent Quantum Key Distribution [61, 95, 96]); the heralding rate is proportional to the susceptibility factor of the non-linear crystal which is usually very low so, in order to raise the rate, one must raise the optical input power. Recently, an ultra-fast heralded single photon source with heralding rates as high as 15 MHz has been reported using InGaAs/InP single-photon avalanche diodes, telecommunication optical fibres, and a 1550 nm laser pump with a repetition rate of 10 GHz [87]. In order to generate the pump photons in a lower wavelength, the infrared photons from the high-repetition laser were

up-converted in a non-linear crystal and then directed to the SPDC non-linear crystal. This experiment is a breakthrough in terms of the compromise between heralding rates and the ratio between multi- and single-photon pulse emission representing the evolution of single-photon generation technology.

1.2.4 Highlights in Single-Photon Detection

It is easy to see that, parallel to the development of single-photon sources, ideas for new technologies of single-photon detection also came forward: the two processes are somewhat the inverse of each other so by inverting the mechanism of single-photon generation, one could, in turn, be able to detect a single-photon. For SPDC, the converse can be interpreted as the process of up-conversion in which a photon is directed to a quadratic non-linear medium along with a pump beam: due to energy conservation conditions, the energy of the output must be the sum of the energies of the input photons so a higher energy photon is generated [97, 98]. Up-conversion is often used in order to shift the absorption region to a shorter wavelength so that higher efficiency detectors can be employed with direct applications to the detection of infrared telecom photons by silicon avalanche photo diodes which exhibit much higher detection efficiency [99–101]. A successful application of up-conversion in quantum cryptography has been reported where the 1550 nm photons proper for long-distance fiber optical communications were directed into the non-linear medium with a pump beam at 1320 nm to generate photons at 713 nm; the system made use of very fast silicon SPADs operating at 1 GHz clock frequency and permitted secure key exchange in a distance of 100 km [101]. For quantum dots, the converse is quite straightforward: if a trapped electron can decay producing a single-photon, it can also be excited by a single-photon. Even though the study on the application of quantum dots to single-photon detection attracts a great deal of attention, such devices are yet bound to very low temperature operating range and low detection efficiencies [102–104]. A highlight can be made about the work reported in [105], where a detection efficiency of $\sim 68\%$ has been achieved but, again, the wavelength of the photons were far from the infrared telecom band and the detector had to operate at 4 K.

In order to complete our brief revision on single-photon detection and generation, we mention the superconducting single-photon detector, a device capable of offering very high detection efficiency (on the order of 88%), infrared telecom compatibility, and very low dark count rates (on the order of 10 Hz) [106]. Superconductivity is often associated simply to the complete vanishing of

all electric resistance below a certain temperature (the transition temperature) as so it seemed from the time of its discovery, in 1911, until the discovery of the Meissner effect, in 1933 [107]: a superconductor exhibits perfect diamagnetism, the magnetic flux inside the material is excluded from all but a thin penetration region near the surface [108]. Even though not much experimental progress could be achieved in the first half of the twentieth century due to the poor techniques for material growing, the area of superconductivity saw an uprise in research attention in the late eighties when high transition temperature (in excess of 77 K, above the boiling point of liquid nitrogen) superconductor materials were discovered [109, 110]. In the scope of single-photon detection, superconductor materials are employed as ultra-sensitive bolometers, devices capable of detecting incident electromagnetic radiation by measuring the voltage drop across a temperature-dependent electrical resistance. The idea behind the superconducting single-photon detector (SSPD) is to use a superconductor with a sharp transition edge between the *superconducting* and *conducting* temperatures so that the absorption of a single-photon is capable to take the device out of its superconductor state and the voltage drop across the device can be measured [18]. The change in current from the *on/off* superconducting states of the device due to the absorption of a photon can be measured with a superconducting quantum-interference device (SQUID) [111–113]. Single-photon detector devices combining transition edge sensors and SQUIDs exhibit poor timing characteristics besides the necessity of extremely low temperature of around 100 mK, but offer high detection efficiency, low dark count rates and photon number resolving capability [72]. This last feature is made possible due to the change in temperature (and thus current) being proportional to the absorbed photon's energy and, since the SQUID is capable of differentiating between these extremely low current levels, the number of photons in a pulse of monochromatic light can be determined [106].

2
Theoretical Background

2.1
Quantum Mechanics Basics, Annihilation and Creation Operators and Fock States

According to the first postulate of quantum mechanics, associated to any isolated physical system is a complex Hilbert space and the system is completely described by its state vector, which is a unit vector in the system's Hilbert space [114]. A Hilbert space, in turn, is a complete vector space with inner product [115]. A convenient notation for representing vectors in a Hilbert space is Dirac's notation, composed of *bra*s and *ket*s, $\langle\cdot|$ and $|\cdot\rangle$, respectively: *ket*s represent column vector whereas *bra*s represent the conjugate transposed of a *ket*. While $|x\rangle$ is a point in the Hilbert space H, $\langle x|$ is a point in $H^\dagger$, the dual space of H, with $|x\rangle^\dagger = \langle x|$ [115, 116]. One of the many usefulness of this notation comes when one writes inner products between two vectors, say $|\phi\rangle$ and $|\psi\rangle$, which assumes the form $\langle\psi|\phi\rangle$.

Maybe the most important property of Hilbert spaces is that any vector of the space can be represented by a set of linearly independent vectors, which are called a *basis*. Every basis for a given Hilbert space has the same size n, which is said to be the dimension of the Hilbert space. As an example, let $\{|0\rangle, |1\rangle\}$ be a basis for a 2-dimensional Hilbert space H; an arbitrary vector $|x\rangle$ of H is written as $|x\rangle = \alpha|0\rangle + \beta|1\rangle$. According to Born's postulate [114, 116], when dealing with quantum states, the normalization condition is imposed so that $|\alpha|^2 + |\beta|^2 = 1$ and $|\alpha^2|$, $|\beta^2|$ represent the probabilities of $|x\rangle$ being measured as either $|0\rangle$ or $|1\rangle$. Examples of 2-dimensional Hilbert spaces that represent quantum systems are the spin states of an electron, or the polarization state of a photon, whereas infinite-dimensional Hilbert spaces can be used to represent, for instance, the number of photons inside a cavity. We can use one of the properties of inner products to summarize the normalization condition as $\langle\psi|\psi\rangle = 1$ for every $|\psi\rangle$ that represents a pure quantum state.

Evolution and transformations of quantum states, or normalized vectors in the Hilbert space that describes the quantum system, are given by *operators* [117]. In fact, one of the postulates of quantum mechanics states that the

time evolution of any closed quantum system is given by an unitary operator [5, 114, 116, 117]. By an *operator*, we simply mean a bounded linear – or continuous – transformation of a Hilbert space into itself [115] [1]. Operators that operate on $H^\dagger$, the dual space of a Hilbert space H are denoted $\hat{O}^\dagger$, where $\hat{O}^\dagger$ is said to be the adjoint operator of $\hat{O}$. [114, 115, 117]. A distinct feature of Dirac's notation is that an operator $\hat{O}$ can be represented in a simple form as $\hat{O} = \sum_{i,j} \alpha_{i,j} |i\rangle \langle j|$, where $\alpha_{i,j}$ represents the entry in the ith row and the jth column of the matrix form of $\hat{O}$. Finally, a projective measurement operator on a state $|\psi\rangle$ is represented by an outer product of the form $|\psi\rangle \langle\psi|$ and can be used to condensate Born's postulate in a simple but powerful statement: $\sum_i \langle\phi| |\psi_i\rangle \langle \psi_i| |\phi\rangle = 1$ [2]. In finite-dimensional Hilbert spaces, operators take on the very familiar form of matrices [116, 117]. An example is the operator associated to a polarization rotator, which alters the state of polarization of a photon. Since the Hilbert space that describes the system is 2-dimensional [116], this particular operator will be described by a 2×2 matrix. 2-dimensional systems are very usual, especially in Quantum Cryptography [35]. Indeed, the concept of *qubit* comes from the fact that, in a 2-dimensional Hilbert space, every quantum state can be described by the linear combination of the two eigenstates of the basis and, therefore, are said to be in a superposition of 2 states with its corresponding normalized probability amplitudes.

A very useful mathematical result of Hilbert space theory is the Fourier Series Theorem. It states among other things, the following: let $B = \{e_\gamma\}_{\gamma\in\Gamma}$ be an orthonormal set in a Hilbert space H with, possibly, infinite uncountable dimension Γ; then, if B is a basis, every $x \in H$ has a unique expansion on B, namely

$$|x\rangle = \sum_{\gamma\in\Gamma} \langle x|e_\gamma\rangle |e_\gamma\rangle \tag{2.1}$$

which is referred to as the Fourier series expansion of $|x\rangle$ where the elements of the family of scalars $\{\langle x|e_\gamma\rangle\}_{\gamma\in\Gamma}$ are the Fourier coefficients of x with respect to B [115]. One should note that some vector spaces have elements (vectors) that are not finite strings of numbers such as in $\mathbb{R}^N$ but, instead, their elements are the most varied of objects. For instance, L^2, the space of quadratically integrable functions, is not only a vector space but also a Hilbert space [115]. A more tangible result of the Fourier Series Theorem is that any function on

[1] A more general definition is that an operator is a bounded linear transformation of a *normed* space into itself but the simplified version will suffice since Hilbert spaces are, themselves, *normed* spaces.

[2] Projective measurement operators are Hermitian (they are equal to their conjugate transposed) and idempotent (its square is equal to itself) [114, 116].

a finite interval can be written as a Fourier series [118]. For example, any real-valued function $f(x), x \in (0, d)$ can be expanded in a series of exponentials,

$$f(x) = \sum_{m=-\infty}^{\infty} c_m e^{im\frac{2\pi x}{d}} \tag{2.2}$$

where the c_m are the complex Fourier coefficients of $f(x)$ [118]. This is usually taken as the starting point when quantising the electromagnetic field inside a perfect optical resonator or inside a dielectric slab or a so-called open cavity [5, 119–130]. Usually, a finite quantisation volume is considered and the electromagnetic field observables are written as Fourier series of discrete sets of eigenfunctions. These eigenfunctions are the basic solutions of Maxwell's equations for the vector potential of the electromagnetic field in Coulomb gauge [131]. We shall follow this same procedure but considering the *single-mode* case instead of the *multimode* for simplicity. Extending the result, however, is quite straightforward and we will do so, come the necessity.

Let us go back to the case of photons inside cavities and let $|n\rangle$ represent a state of well-defined number of photons inside such cavity. Being able to operate with number states is important since we will be interested in determining the number of photons – or, at least, the expectation value of the number of photons – present in different experimental situations. The Hilbert space that describes this state is infinite-dimensional and, therefore, the operators can be thought of as infinite-dimensional matrices. Operating over such state with the Hamiltonian operator yields the state's energy such that $\hat{H}|n\rangle = E_n|n\rangle$ [5]. One can show that the Hamiltonian operator for a single-mode electromagnetic field inside a cavity has the form of a harmonic oscillator:

$$\hat{H} = \frac{1}{2}\left(\hat{p}^2 + \omega^2\hat{q}^2\right), \tag{2.3}$$

where $\hat{p}$ and $\hat{q}$ correspond to the linear momentum and position operators, respectively, and ω is the frequency mode of the field [5]. Defining operators $\hat{a}$ and $\hat{a}^\dagger$ as

$$\begin{aligned} \hat{a} &= (2\hbar\omega)^{-1/2}(\omega\hat{q} + i\hat{p}), \\ \hat{a}^\dagger &= (2\hbar\omega)^{-1/2}(\omega\hat{q} - i\hat{p}), \end{aligned} \tag{2.4}$$

it is possible to re-write the Hamiltonian operator in a simplified expression

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right), \tag{2.5}$$

where $\hbar$ is Planck's constant and the product $\hbar\omega$ corresponds to the photon's energy. The operators $\hat{a}$ and $\hat{a}^\dagger$ obey the commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$ [3]. It is worth emphasizing that $\hat{a}^\dagger$ is the adjoint of $\hat{a}$.

Returning to the photon number state inside the cavity, it is interesting to observe the action of the operators $\hat{a}$ and $\hat{a}^\dagger$ in terms of the energy of the state:

$$\begin{aligned} \hat{H}\left(\hat{a}\left|n\right\rangle\right) &= \left(E_n - \hbar\omega\right)\hat{a}\left|n\right\rangle; \\ \hat{H}\left(\hat{a}^\dagger\left|n\right\rangle\right) &= \left(E_n + \hbar\omega\right)\hat{a}^\dagger\left|n\right\rangle. \end{aligned} \tag{2.6}$$

The operator $\hat{a}$, or annihilation operator, lowers the energy of the system in a unit of $\hbar\omega$, i.e., it subtracts, or annihilates, a photon from the system, hence its name. The creation operator $\hat{a}^\dagger$, on the other hand, raises the energy of the system in a unit of $\hbar\omega$ therefore adding, or creating, a photon in the system. Straightforward calculations lead to the following results: $\hat{a}\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle$; and $\hat{a}^\dagger\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle$ [4]. The annihilation and creation operators can be associated to the backward unilateral shift and the unilateral shift operators of functional analysis, respectively [115].

Operating indefinitely over a state of well-defined number of photons with the annihilation operator eventually extinguishes the energy of the system. By definition, $\hat{a}\left|0\right\rangle = 0$. Conversely, operating n times over the $\left|0\right\rangle$ state with the creation operator, except for a constant factor, yields the state $\left|n\right\rangle$. It is interesting to note that the vacuum state $\left|0\right\rangle$ (a state with zero photons) has a non-zero energy which can be calculated applying the Hamiltonian operator:

$$\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)\left|0\right\rangle = \frac{\hbar\omega}{2}\left|0\right\rangle. \tag{2.7}$$

States of well-defined number of photons are also called Fock states which are extremely useful when one devises a simplified description of an experiment. Furthermore, Fock states present two important properties: they form an *orthogonal* and *complete* set[5]. Fock states can also be characterized as the eigenstates of the photon number operator, $\hat{n} = \hat{a}^\dagger\hat{a}$, so $\hat{n}\left|n\right\rangle = n\left|n\right\rangle$.

According to one of the postulates of quantum mechanics, the expectation value of an operator $\hat{O}$ when applied over a state $\left|\psi\right\rangle$ is given by $\left\langle\psi\right|\hat{O}\left|\psi\right\rangle$. We express the time-dependent electric field operator in terms of the annihilation and creation operators as $\hat{E}\left(t\right) = \varepsilon_0\left[\hat{a}\left(0\right) + \hat{a}\left(0\right)^\dagger\right]$, where the time dependence of the annihilation and creation operators can be shown to be

[3] Refer to Appendix 7.1 for the complete mathematical development.

[4] Refer to Appendix 7.2 for the complete mathematical development.

[5] An orthogonal set stands for a set in which every element is orthogonal to any other element except to itself whereas a complete set refers to a set which spans the whole space.

$\hat{a}(t) = \hat{a}(0)\, e^{-i\omega t}$ and $\hat{a}^{\dagger}(t) = \hat{a}^{\dagger}(0)\, e^{i\omega t}$ [6,7]. Due to the orthogonality of Fock states, we find that $\langle n|\, \hat{E}(t)\, |n\rangle = 0$[8], a result stating that, even though Fock states are states of well-defined number of photons, they are not states of well-defined electric field since the mean field is zero. The reasoning is simple: with n different from zero, the system is composed by a non-zero number of photons for which the electric field cannot be zero; nevertheless, the mean field is zero and so it must oscillate around this value.

Calculating the expected value of the square of the electric field operator yields $\langle n|\, \hat{E}^2(t)\, |n\rangle = \varepsilon_0^2 (2n+1)$[9], an important result due to two distinct reasons. Firstly, we find field oscillations even when the number of photons is zero, i.e., vacuum oscillations which are responsible for a number of effects not relevant in the present moment, such as spontaneous emission. Secondly, we note that the field fluctuations increase in intensity as the number of photons increases, a result that is completely in contrast with what is observed classically: as the number of photons in the field increases, it approaches a classical field for which the uncertainty is negligible. If the classical field, however, was described by Fock states, we would perceive a completely different physical picture. This strange result, however, has its origin in good agreement with Heisenberg's Uncertainty Principle [5, 38]: the photon number operator and the electric field operator do not commute. Was the field surely known, the number of photons would be completely uncertain. Interestingly, though, the number state which yields the lower uncertainty for the electric field operator is the vacuum state.

An interesting observation about annihilation and creation operators is that they are not Hermitian. Observables, in quantum mechanics, i.e., operators associated to a quantifiable and measurable quantity, are represented by Hermitian operators: these have orthogonal eigenstates and real eigenvalues [10]. This implies that one cannot determine the expected value of the annihilation or creation operators by a direct measurement [5].

2.2 Coherent States

We have seen that Fock states are states of uncertain electric field and are, therefore, a poor model for describing classical fields. Even though subtle, the

[6] We disregard the spatial dependence of the electric field operator for simplicity.
[7] Refer to Appendix 7.3 for the complete mathematical development.
[8] Refer to Appendix 7.4 for the complete mathematical development.
[9] Refer to Appendix 7.4 for the complete mathematical development.
[10] This result comes directly from the fact that Hermitian operators are *Normal* operators which obey $N^{\dagger}N = NN^{\dagger}$ and that have a spectral decomposition according to the spectral theorem [115, 116].

implications of this result are quite unsettling: say a laser source is turned on with its full power which can be modeled by classical electrodynamics; suppose an optical attenuator is placed after the laser source and that it is possible to raise the attenuation value until very few photons arise from its output. If Fock states were a good model for such few-photon states, somewhere in the transition between the classical and quantum regime – as one raises the attenuation level –, the electromagnetic field characteristics would have to change completely since its description also changes and is not compatible with both regimes simultaneously. As it turns out, Fock states are infeasible in practice for reasons which are still in connection with Heisenberg's Uncertainty Principle [5], so attenuating a laser source does not yield states of well-defined number of photons. The question, however, remains: what is the description of the quantized electromagnetic field that agrees with the classical description?

The so-called Coherent States are constructed as a superposition of Fock states and arise mathematically when one seeks eigenstates of the annihilation operator. Given the eigenvalue equation

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.8}$$

one is interested in determining which state $|\alpha\rangle$, when operated by the annihilation operator, yields the same state multiplied by a scalar, the eigenvalue. An important property of Fock states which have already been mentioned, is that they form a complete set which is the same as saying that they form a basis for the Hilbert space describing the system so any other state can be written as a linear combination (or superposition) of Fock states. The fact that Fock states also form an orthogonal set and that they obey the normalization condition due to Born's postulate means that they are an *orthonormal* base for the Hilbert space. Writing $|\alpha\rangle$ as a superposition of Fock states and substituting in the eigenvalue equation yields

$$\sum_{n=0}^{\infty} c_n \hat{a}\,|n\rangle = \alpha\,|\alpha\rangle\,. \tag{2.9}$$

Even though extensive, the calculation that leads to the final mathematical expression of Coherent states is quite straightforward[11], and the result is as follows:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.10}$$

[11]Refer to Appendix 7.5 for complete mathematical development.

The factor $\mu = |\alpha|^2$ represents the mean number of photons of the quantized electric field represented by the Coherent state. As the power of the electric field rises, μ rises, but the uncertainty does not rise: as the vacuum state, Coherent states minimize the uncertainty of the electric field operator [5] [12]. This result is in accordance with the phenomenon observed classically, i.e., the uncertainty on the electric field becomes irrelevant when the power is raised and gains importance when the mean number of photons approaches the quantum, or few-photon, regime.

Other testimony to the accordance between the classical and the quantized description of Coherent states comes when one determines the probability distribution of finding a specific Fock state within a wave-packet. One of the postulates of quantum mechanics states that quantum measurements are described by a collection of *measurement operators* which satisfy the completeness equation, a fact that expresses the normalization condition, i.e., that the probabilities must sum to one as required by Born's postulate. To determine, therefore, the desired probability, one projects the state $|\alpha\rangle$ over the projective measurement operator $|k\rangle\langle k|$, where $|k\rangle$ is an arbitrary state of well-defined number of photons. The result is[13]

$$P_{|\alpha\rangle}(k) = e^{-\mu}\frac{\mu^k}{k!}, \tag{2.11}$$

which corresponds to a Poissonian distribution, the same distribution expected from the number of photons arising from the output of a laser source [5]. The fact that the statistics of photons of coherent states is Poissonian indicates that a source generating such states does so in a completely random process, an important property of laser sources.

Note that the vacuum state is a state that minimizes the uncertainty of the electric field operator such as coherent states. Also, regard that, through the consecutive action of the creation operator, one can create Fock states from the vacuum state. Coherent states can also be created from the vacuum state but through a different operator, the *displacement* operator. Since both coherent states and the vacuum state minimize the uncertainty of the electric field operator, one can think of coherent states as the *displaced* vacuum, where the displacement corresponds to μ, the average number of photons of the coherent state. This view is closely related to the mechanism for generating coherent states from classical currents such as in a laser source [5]. The displacement operator is defined as [132] $\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}$ and the coherent

[12] Refer to Appendix 7.6 for complete mathematical development.
[13] Refer to Appendix 7.7 for complete mathematical development.

states are given by $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$[14].

2.3 Coherence and Beam Splitters

It is particularly interesting to investigate the effect of beam splitters on both Fock and coherent states: beam splitters offer an evidence to the existence of photons. Suppose one directs a beam of light to a beam splitter and measures the coincidences between detection events of two detectors placed at the beam splitter's output arms and then proceeds to mitigate the light intensity to the point where at most only one photon goes through the device at a time. The expectation is that no coincidence events will result since the photon can only be detected by one detector. This, however, is not the case when one uses a thermal source, such as a gas flame used by Taylor in 1909 [133], since it does not produce photons one-at-a-time but, rather, produces photons in groups, or bunches.

The now familiar phenomenon of *photon bunching* was discovered by Hanburry Brown and Twiss in 1956 [134] and is associated to the tendency of single-photons to group together, an effect owing to the bosonic nature of photons [135]. In contrast, Grangier *et al.* [136], which the developed one of the first *antibunched* photon sources[15], observed what was expected: no coincidence events between detectors since photons were produced close to the *one-at-a-time* limit. The same experiment was conducted by Rarity et al. [138] with highly attenuated light produced by a laser source (coherent states). The coincidence events, in this case, are more frequent than in the case of an antibunched source, but less frequent than in the case on a bunched source, a difference outlined by the diminished visibility[16] of the interference curve which falls from 100% in the case of antibunched sources, to 50% in the case of a randomly distributed source [7, 138]. The very distinction between classical and non-classical states is outlined by this difference in visibility. The necessary condition for having over 50% visibility in two-photon interference is that the two interfering fields must be non-classical fields that violate the Schwartz inequality relating their intensities as $\langle I_1^2\rangle \langle I_2^2\rangle \geq \langle I_1 I_2\rangle^2$. Antibunched states of the field are, in general, non-classical [137, 139].

The tendency of photons being generated in bunches, one-at-a-time, or in a random process, can be explained by the quantum theory of coherence [5, 7, 69, 134, 140, 141]. The quantum theory of coherence is imperative when

[14]Refer to Appendix 7.8 for complete mathematical development.

[15]The first ones to actually observe an *antibunched* photon stream were Kimble et al [137]

[16]The visibility of an interferogram is commonly defined as $(V_{max} - V_{min}) / (V_{max} + V_{min})$ [69].

describing quantum interference phenomena and permits one to assess to what degree a light source is monochromatic (through its temporal autocorrelation function and spectral shape) as well as to determine the statistical properties of light (through its second order temporal autocorrelation function). Classically, the Interference Equation of two partially coherent waves is given by $I = I_1 + I_2 + 2\sqrt{I_1 I_2}|g_{12}(t)|\cos\varphi$ [69], where I_1 and I_2 are the respective intensities of each source, $g_{1,2}(t)$ is their temporal mutual coherence function, and φ is their relative phase difference. The temporal mutual coherence function assumes values in the range $0 \leq |g_{1,2}(t)| \leq 1$ and dictates whether or not interference will occur, the condition for the positive case being $|g_{1,2}(t)| > 0$. The limiting cases discern three types of coherence: complete coherence when $|g_{1,2}(t)| = 1$; complete incoherence when $|g_{1,2}(t)| = 0$. Partial coherence is associated to all the other cases which are not the limiting ones. The temporal coherence function is associated to the spectral shape of the light source, $s(\nu)$, through the Fourier Transform, $\mathscr{F}\{|g_{1,2}(t)|\} = s(\nu)$ which, as previously commented, indicates the frequency modes that compose the light beam and, thus, is a measure of how close, spectrally, it is to a monochromatic source. Quantum mechanically, the quantum temporal coherence function is quite similar to its classical counterpart in the sense that it measures the degree of coherence of a light source, although defined using electrical field operators and density matrices [5, 141]. Density matrices provide a convenient means for describing quantum systems whose state is not completely known, i.e., in a *mixture* or *ensemble* of pure states [114, 116]. For the present discussion, however, it is not necessary to define such formalism.

The second order temporal correlation function involves the correlation of intensities rather than of fields as in the case of the (first order) temporal correlation function. In a way, it permits the generalization of field interference to intensity interference, i.e., to quantum effects involving numbers of photons instead of amplitudes of electric fields [6, 70, 140]. In the experiment of Hanburry-Brown and Twiss [134], two detectors are placed at the output ports of a beam splitter and the temporal delay between the detections is swept, i.e., the setup measures a delayed coincidence rate where one of the detectors registers a count at time t and the other at $t + \tau$, or the joint probability of counting a photon at t and another at $t+\tau$. This probability is proportional to the correlation function $G^{(2)}(\tau) = \langle \hat{n}(t)\,\hat{n}(t+\tau)\rangle$, where $\hat{n}(t)$ is the photon number operator at time t [139, 141]. When τ is within the mutual coherence time of the photons (the condition for partial coherence and, therefore, for interference), measured as the full-width at half maximum (FWHM) of the temporal correlation function [114], the statistical properties of the wave-

packets impinging on the beam splitter can be determined [5]. The second-order degree of coherence, or second-order temporal correlation function, is defined as [139]

$$g^{(2)}(\tau) = \frac{G^{(2)}(\tau)}{|\langle \hat{n} \rangle|^2}. \tag{2.12}$$

The second-order temporal autocorrelation function indicates whether the photons in the optical beam are *bunched* ($g^{(2)}(0) > g^{(2)}(\tau)$), *antibunched* ($g^{(2)}(0) < g^{(2)}(\tau)$), or randomly distributed ($g^{(2)}(0) = g^{(2)}(\tau)$) [139]. Also, by inspecting the value of $g^{(2)}(0)$, one is able to determine the ratio between multi- and single-photon pulses in the beam: when the value drops below 1, the ratio surpasses that of a coherent field and the beam is said to be *sub-Poissonian* [135, 139]. This result alone may also impart information regarding the antibunched nature of the photons: $g^{(2)}(0) < 1$ implies $g^{(2)}(0) < g^{(2)}(\tau)$ and, therefore, antibunching [139]. The relation between sub-Poissonian statistics and antibunching, however, is subtle, since one can have a field with Poissonian, or even super-Poissonian, statistics which exhibits antibunching even though the converse does not apply [139].

To asses the temporal correlation functions of a light beam, as done by Hanburry-Brown and Twiss and others [134, 136], it is necessary to employ the optical beam splitter. The quantum description of this device, however, is delicate since at the level of single-photons, the classical approach produces erroneous results. Nevertheless, for coherent and thermal beams the quantum and classical treatments of beam splitters agree, which is only natural since these are classical fields. Let us consider a classical light field with amplitude ε_{in} incident upon a lossless beam splitter. ε_r and ε_t are the amplitudes of the reflected and transmitted beams with $\varepsilon_r = r\varepsilon_{in}$ and $\varepsilon_t = t\varepsilon_{in}$ where r and t are the reflectance and transmittance of the device, respectively. For a symmetrical beam splitter, $|r| = |t| = 1/\sqrt{2}$ and, since it is lossless, $|\varepsilon_{in}|^2 = |\varepsilon_r|^2 + |\varepsilon_t|^2$, a relation that imposes, upon r and t, the relation $|r|^2 + |t|^2 = 1$. Quantum mechanically, we replace the field amplitude by a set of annihilation and creation operators for each of the beam splitter spatial modes: $\hat{a}_{in}$, $\hat{a}_r$, and $\hat{a}_t$. In analogy with the classical case, $\hat{a}_r = r\hat{a}_{in}$ and $\hat{a}_t = t\hat{a}_{in}$.

Before we go any further, we must analyze the commutation relations of this set of operators in light of the newly developed beam splitter relations. We know that $\left[\hat{a}_{in}, \hat{a}_{in}^{\dagger}\right] = 1$, which must also hold for $\hat{a}_r$ and $\hat{a}_t$. Also, the commutator of operators associated to different spatial modes of the beam

splitter should equal zero [5], i.e.,

$$\left[\hat{a}_{in}, \hat{a}_r^\dagger\right] = \left[\hat{a}_{in}, \hat{a}_t^\dagger\right] = \left[\hat{a}_r, \hat{a}_t^\dagger\right] = 0. \tag{2.13}$$

The results assuming the beam splitter spatial modes relations are

$$\begin{aligned}
\left[\hat{a}_r, \hat{a}_r^\dagger\right] &= |r|^2 \left[\hat{a}_{in}, \hat{a}_{in}^\dagger\right] = |r|^2 \neq 1 \\
\left[\hat{a}_t, \hat{a}_t^\dagger\right] &= |t|^2 \left[\hat{a}_{in}, \hat{a}_{in}^\dagger\right] = |t|^2 \neq 1 \\
\left[\hat{a}_r, \hat{a}_t^\dagger\right] &= rt^* \left(\hat{a}_{in}\hat{a}_{in}^\dagger - \hat{a}_{in}^\dagger\hat{a}_{in}\right) \\
&= rt^* \left(\hat{a}_{in}\hat{a}_{in}^\dagger - \hat{a}_{in}\hat{a}_{in}^\dagger + 1\right) = rt^* \neq 1,
\end{aligned} \tag{2.14}$$

which indicate, therefore, that it does not provide the correct quantum description of the device. A solution for this issue is indebted to the vacuum state. The vacuum state, even though vacant of photons, is a state of the quantized field which has been shown to present energy fluctuations, so it must be taken into account in the description of the beam splitter. Since the device is actually composed of four ports, one of which is usually left unused, we must associate operators to this otherwise unused mode taking it into consideration. Introducing $\hat{a}_0$, the operator associated to the unused port of the beam splitter, with the redefined transmittance and reflectance relations $\hat{a}_r = r\hat{a}_{in} + t'\hat{a}_0$, and $\hat{a}_t = t\hat{a}_{in} + r'\hat{a}_0$, it is possible to satisfy the commutation relations given $|r'| = |r|$, $|t'| = |t|$, $|r|^2 + |t|^2 = 1$, and $r^*t' + r't^* = r^*t + r't'^* = 0$. In order to correctly model the input state of a two-input modes beam splitter, we make use of the tensor product formalism. In synthesis, the tensor product is a singular means of representing two Hilbert spaces which describe independent systems as a more general Hilbert space that describes both systems together. As a matter of fact, this constitutes one of the postulates of quantum mechanics, which states that *if H_1 is the Hilbert space associated with the physical system s_1, and H_2 is the Hilbert space associated to another physical system s_2, then the composite system $s_1 + s_2$ will be associated with the tensor product of the two Hilbert spaces $H_1 \otimes H_2$* [114,116]. The product state of, say, two well-defined photon number states $|n_a\rangle$ and $|m_b\rangle$ incident on independent input spatial modes (a and b) of a beam splitter is written $|n_a\rangle \otimes |m_b\rangle$, where it is usual to drop the $\otimes$ notation and simply write $|n_a, m_b\rangle$.

An important observation is related to the manufacturing of beam splitters: if the beam splitter is constructed as a single dielectric layer, which is the most common manufacturing process [69], the reflected and transmitted beam will differ in phase by a factor of $e^{\pm i\pi/2} = \pm i$ [5]. Therefore, a symmetric

beam splitter assumed to induce a $\pi/2$ phase shift between beams has its output and inputs modes related (since there is no preferred input or output spatial mode, we change the notation to a simpler one) as:

$$\begin{aligned}\hat{a}_c &= \frac{1}{\sqrt{2}}\left(\hat{a}_a + i\hat{a}_b\right) \\ \hat{a}_d &= \frac{1}{\sqrt{2}}\left(i\hat{a}_a + \hat{a}_b\right),\end{aligned} \tag{2.15}$$

which also holds for creation operators. We recall that any state of well-defined number of photons can be written as the consecutive operation of the creation operator over the vacuum state. To construct the output states in case a Fock state enters the beam splitter we can, therefore, use the previously defined relations between spatial mode creation operators since input vacuum states transform to output vacuum state ($|0_a, 0_b\rangle \xrightarrow{BS} |0_c, 0_d\rangle$) [5].

As an example, let us consider the single-photon input state written as the product state $|0_a, 1_b\rangle$ which can also be expressed as $\hat{a}_b^\dagger |0_a, 0_b\rangle$. The beam splitter transformation defined by

$$\begin{aligned}\hat{a}_a^\dagger &\xrightarrow{BS} \frac{1}{\sqrt{2}}\left(\hat{a}_c^\dagger + i\hat{a}_d^\dagger\right) \\ \hat{a}_b^\dagger &\xrightarrow{BS} \frac{1}{\sqrt{2}}\left(i\hat{a}_c^\dagger + \hat{a}_d^\dagger\right)\end{aligned} \tag{2.16}$$

acts on the creation operator and the result reads:

$$\begin{aligned}\hat{a}_b^\dagger |0_a, 0_b\rangle \xrightarrow{BS} &\frac{1}{\sqrt{2}}\left(i\hat{a}_c^\dagger + \hat{a}_d^\dagger\right)|0_c, 0_d\rangle \\ = &\frac{1}{\sqrt{2}}\left(i\,|1_c, 0_d\rangle + |0_c, 1_d\rangle\right).\end{aligned} \tag{2.17}$$

This is a rather pictorial result: when a single-photon state enters a symmetric beam splitter, the output state is in an equal superposition (the probability amplitudes are equal) of the photon being in output arm a and the photon being in output arm b. Therefore, the probability of detecting a photon on each of the arms is one half which is the result found by Grangier in his 1986 experiment using a heralded photon source, a symmetric beam splitter and a single-photon detector [136].

2.4 The Hong-Ou-Mandel Interferometer and Photon Bunching

Photon bunching is one of the most celebrated effects of two-photon interference, related to the tendency of indistinguishable photons to group together

rather than staying apart from each other [5]. The bunching nature of photons was first observed by Hanbury-Brown and Twiss in 1956 during stellar intensity interference measurements [134]. Its explanation from a quantum mechanical perspective was due to Fano [142], but its experimental familiarization only came when Hong, Ou and Mandel demonstrated that photons generated from Spontaneous Parametric Down Conversion (SPDC) tend to bunch together when directed into a symmetric optical beam splitter given that there is a wave-packet overlapping [143]. The Hong-Ou-Mandel (HOM) “dip", which characterizes the two-photon bunching effect, is the drop in coincidence counts between two detectors placed one at each output of the beam splitter when the indistinguishability condition is satisfied. The destructive interference involving two indistinguishable photons responsible for bunching is intimately linked to the Bose nature of photons and its atomic analog has been observed with bosonic atoms whereas the antibunching effect, intrinsically related to Fermions, was also reported with fermionic atoms [135].

Photon antibunching is the counterpart of the photon bunching effect and, in turn, reflects the tendency of photons to stay apart from each other. In a two-photon interference context, it is related to photons taking different output spatial modes of a symmetric beam splitter [7]. Even though quantum optics is unable to present an experiment involving fermions due to the bosonic nature of photons, Kimble *et al.* had already predicted that for quantum states of the electromagnetic field that have no classical description, the probability functional describing the interference may assume negative values yielding the opposite of the bunching effect, with an increase in the coincidence counts as the wave packets superpose in the beam splitter [137]. Indeed, photon antibunching has been observed when the photon wave packets are made antisymmetric by means of polarization rotation and projection into a specific measurement basis in an Hong-Ou-Mandel interferometer [144, 145]. The frequency displacement of wave packets has been shown to yield anti-bunching peaks, a result confirmed by the analysis of the second-order cross-correlation function at zero time in a Hanbury-Brown and Twiss (HBT) experiment [68].

Let us consider the two input optical spatial modes a and b of a 50:50 beam splitter that carry annihilation and creation operators $\hat{a}_a$, $\hat{a}_a^\dagger$ and $\hat{a}_b$, $\hat{a}_b^\dagger$ fed with two identical photons described by the Fock States $\hat{a}_a^\dagger \hat{a}_b^\dagger \left|0_a, 0_b\right\rangle = \left|1_a, 1_b\right\rangle$. The beam splitter output modes are labeled c and d. The output state

after the interaction between the input state and the beam splitter is

$$\begin{aligned}\hat{a}_a^\dagger \hat{a}_b^\dagger \left|0_a, 0_b\right\rangle \xrightarrow{BS} &\frac{1}{2}\left(i\hat{a}_c^\dagger + \hat{a}_d^\dagger\right)\left(\hat{a}_c^\dagger + i\hat{a}_d^\dagger\right)\left|0_c, 0_d\right\rangle \\ =&\frac{1}{2}\left(i\hat{a}_c^\dagger\hat{a}_c^\dagger - \hat{a}_c^\dagger\hat{a}_d^\dagger + \hat{a}_d^\dagger\hat{a}_c^\dagger + i\hat{a}_d^\dagger\hat{a}_d^\dagger\right)\left|0_c, 0_d\right\rangle .\end{aligned} \tag{2.18}$$

The fact that the input photons are assumed to be indistinguishable is crucial for this analysis since the two terms with opposite signs cancel each other. This happens because, since they are indistinguishable, one can not differentiate between the cases in which both photons are transmitted and in which both are reflected. The absence of the so-called “which-way information" and, thus, of differentiability between the wave-packets describing the two-photon ensemble interacting with the beam splitter, creates an interference phenomena in such a way that photons always exit the device together [5, 82, 135]. The resulting state after re-normalization

$$\frac{i}{\sqrt{2}}\left(\left|2_c, 0_d\right\rangle + \left|0_c, 2_d\right\rangle\right) \tag{2.19}$$

indicates a superposition between two photons in output mode c and two photons in output mode d. States such as these, which are in superposition between an N-photon state and vacuum, are usually called NOON states and have recently attracted great interest, specially in the field of quantum metrology [146].

The Hong-Ou-Mandel Dip is traced when two detectors are placed at each output mode of the beam splitter and the coincidence detection events are stored while the relative temporal delay between detections is swept. Since the wave packets of the photons should overlap in order for them to interfere, an important aspect of such interferometric experiment is the mutual temporal correlation function of the wave-packets, $g_{1,2}(\tau)$, which characterizes the photons mutual coherence time τ_c [69]. When the relative delay between detectors matches the mutual coherence time of the photons, the post-selected events correspond to indistinguishable photons impinging on the beam splitter. The coincidental events will drop since the photons either go to one of the detectors or to the other. When the relative delay is unmatched, however, the post-selected events correspond to fully distinguishable photons which do not interfere so any optical path taken by the photons is equally probable and the coincidental events will resume to an average value which corresponds directly to the number of photons per time interval entering the beam splitter. This result is in accordance with the effect of a coherent state entering a symmetrical

beam splitter[17].

2.5 Frequency-Displaced Two-Photon Interference

Two-Photon interference has been a much more familiar concept since the late eighties, when Hong, Ou and Mandel demonstrated that photons generated from Spontaneous Parametric Down Conversion (SPDC) tend to bunch together when directed into a symmetric optical beam splitter [143]. This experimental breakthrough deconstructed a strong view, advocated by Dirac, by which photons would only interfere with themselves [147]. In this context, the temporal correlation among photons is a major concern for multi-photon interference since, in fact, the photons do not interfere with each other but, rather, the wave packet that describes both photons interferes with itself [7]. When the relative phase delay between the two wave packets is matched within the photon's mutual coherence in the HOM Interferometer [143], a destructive quantum interference effect is seen in the form of a "dip" in the coincidence counting rate, the so-called *HOM dip*. Even though it may seem, due to the nature of the HOM experiment, that the interference is generated owing to a somewhat local interaction between two single photons, this is not exactly the case. Two-photon interference between photons arriving at the beam splitter at much different times has been experimentally demonstrated, for which the picture of interference between two individual photons is not applicable [145].

After the first demonstration of the *photon bunching* effect [143], the phenomenon was also observed for weak coherent states, the highly attenuated light emerging from a conventional laser source [138, 148]. The higher probability of multi-photon emission in this case, however, limits the visibility to 50% while, for SPDC states, the visibility may reach almost 100% [7]. In recent developments, it has been shown that frequency-displaced indistinguishable photons generate a beat pattern that modulates the interference curve [149]. The resulting interferogram translates the spectral characteristics of the beating photons and, as it was shown in [148], spectroscopy on the few-photon regime can be achieved. Even though mention is made to the possibility of arbitrary laser characterization, it has not been experimentally demonstrated. The reported proof-of-principle is constructed based on a self-heterodyne setup in which two weak coherent states are mutually characterized.

In order to describe the phenomena of two-photon interference when there is a frequency-displacement between the wave-packets, it is necessary to

[17] Refer to Appendix 7.9 for complete mathematical development

consider the spatial, frequency, and time characteristics of the wave-packets. Unlike the case of the bunching effect, where the creation operators sufficed, the creation operators of photonic modes are neither specified in space, frequency, nor time, so quantitative results for photon wave-packets cannot be obtained from this approach [149]. We must therefore consider the electric field operator description of the photons taking into account the spatial, frequency and space dependence of the wave-packet. As mentioned earlier, the extension from the single-mode to the multi-mode case (necessary since we ought to consider non-monochromatic wave-packets) is straightforward. The quantized electric field inside the cavity is now considered to be expressed as a superposition of plane waves indexed by their respective wave vector κ. The Hamiltonian describing the quantized field takes on the form

$$\hat{H} = \frac{1}{2}\sum_{\kappa}\left(\hat{p}_{\kappa}^{2} + \omega_{\kappa}^{2}\hat{q}_{\kappa}^{2}\right). \tag{2.20}$$

The creation and annihilation operators are defined in the same manner, but indexed by the wave-vector. Since all the previous commutation relations are satisfied in the multi-mode case [5], the energy of the field becomes the Hamiltonian operator

$$\hat{H} = \sum_{\kappa}\hbar\omega_{\kappa}\left(\hat{a}_{\kappa}^{\dagger}\hat{a}_{\kappa} + \frac{1}{2}\right). \tag{2.21}$$

Since the modes are each independent of the other (a result that comes directly from the Fourier Series Theorem), each have an associated set of eigenvectors $|n_{\kappa}\rangle$.

From the single-mode expression of the electric field operator[18], we can extend to the multi-mode expression. We take the liberty of skipping a few steps and writing the electric field operator as a function of the creation and annihilation operators remembering that the temporal dependency of these operators has already been derived[19]. The multi-mode electric field operator reads

$$\hat{E}(\mathbf{r},t) = i\sum_{\kappa}\left(\frac{\hbar\omega_{j}}{2\varepsilon_{0}V}\right)^{\frac{1}{2}}\mathbf{e}_{\kappa}\left(\hat{a}_{\kappa}(t)\,e^{i\kappa\mathbf{r}} - \hat{a}_{\kappa}^{\dagger}(t)\,e^{-i\kappa\mathbf{r}}\right). \tag{2.22}$$

It is usual to write this operator as the sum of two parcels corresponding to a collective annihilation and collective creation operator associated to the positive and negative frequency parts of the electric field operator, respectively,

[18]Refer to Appendix 7.2.
[19]Refer to Appendix 7.3.

$\hat{E}(\mathbf{r},t) = \hat{E}^{(+)}(\mathbf{r},t) + \hat{E}^{(-)}(\mathbf{r},t)$ [5, 150, 151] where

$$\begin{aligned}\hat{E}^{(+)}(\mathbf{r},t) &= i\sum_{\kappa}\left(\frac{\hbar\omega_j}{2\varepsilon_0 V}\right)^{\frac{1}{2}}\mathbf{e}_\kappa \hat{a}_\kappa(t)\, e^{i\kappa\mathbf{r}} \\ \hat{E}^{(-)}(\mathbf{r},t) &= \left(\hat{E}^{(+)}(\mathbf{r},t)\right)^{\dagger}.\end{aligned} \tag{2.23}$$

We now wish to define the electric field operator as a function of the wave-packet, i.e., a one-dimensional spatio-temporal mode function which creates or annihilates photons in arbitrary modes. Let the wave-packet be described by [149]

$$\xi(z,t) = \epsilon_\kappa(t - z/c)\, e^{-i\phi_\kappa(t-z/c)}, \tag{2.24}$$

where ϕ_κ is an arbitrary phase evolution, $\epsilon_\kappa(t)$ is the amplitude envelope, and c is the light speed in vacuum. Born's postulate demands that the normalization condition is applied to the wave-packet and, thus, $\int dt|\epsilon_\kappa(t)|^2 = 1$. By placing the beam splitter to which the beams are directed in $z = 0$, we can omit the spatial coordinate and simplify the notation to write the collective creation and annihilation operators as

$$\begin{aligned}\hat{E}^{(+)}(t) &= \sum_{\kappa}\xi_\kappa(t)\,\hat{a}_\kappa, \\ \hat{E}^{(-)}(t) &= \sum_{\kappa}\xi^*_\kappa(t)\,\hat{a}^\dagger_\kappa.\end{aligned} \tag{2.25}$$

This description permits one to calculate the probability of a photon to be detected at a time t in a detector placed in output spatial mode i of the beam splitter,

$$P_i(t) = \langle 1_i|\,\hat{E}^{(-)}_i(t)\,\hat{E}^{(+)}_i(t)\,|1_i\rangle = |\epsilon_\kappa(t)|^2. \tag{2.26}$$

This result is rather intuitive since it states that the probability of a photon being detected in a given detector is proportional to the wave-packet amplitude at the detector's spatio-temporal mode.

For the two input ports of the beam splitter, we only consider the occupied modes which are described by the mode functions $\xi_a(t)$ and $\xi_b(t)$, respectively. This restricts the Hilbert subspaces of the input ports to single modes. Therefore the field collective creation operators that belong to the two input ports can be written as $\hat{E}^{(-)}_a(t) = \xi^*_a(t)\,\hat{a}^\dagger_a$ and $\hat{E}^{(-)}_b(t) = \xi^*_a(t)\,\hat{a}^\dagger_b$, respectively. By combining the description of the field in terms of the wave-packets to the beam splitter transformation, we can attribute the collective creation operators to each of the output spatio-temporal modes of the beam

splitter,

$$\begin{aligned}\hat{E}_a^{(-)}(t) &\xrightarrow{BS} \tfrac{1}{\sqrt{2}}\left(\xi_c^*(t)\,\hat{a}_c^\dagger + i\xi_d^*(t)\,\hat{a}_d^\dagger\right),\\ \hat{E}_b^{(-)}(t) &\xrightarrow{BS} \tfrac{1}{\sqrt{2}}\left(i\xi_c^*(t)\,\hat{a}_c^\dagger + \xi_d^*(t)\,\hat{a}_d^\dagger\right).\end{aligned} \tag{2.27}$$

It is interesting to note that, when all the wave-packets are identical, the above expression is equivalent to the simple case where no spatio-temporal dependency is enforced upon the creation operators. Also, from this expression, it is straightforward to write the electric field operator on spatial modes c and d as a function of the input wave-packets of modes a and b:

$$\begin{aligned}\hat{E}_c^{(-)}(t) &\xrightarrow{BS} \tfrac{1}{\sqrt{2}}\left(\xi_a^*(t)\,\hat{a}_a^\dagger + i\xi_b^*(t)\,\hat{a}_b^\dagger\right),\\ \hat{E}_d^{(-)}(t) &\xrightarrow{BS} \tfrac{1}{\sqrt{2}}\left(i\xi_a^*(t)\,\hat{a}_a^\dagger + \xi_b^*(t)\,\hat{a}_b^\dagger\right).\end{aligned} \tag{2.28}$$

Let us now examine the effect of two photons described by spatio-temporal wave-packets entering a symmetrical beam splitter in the context of a Hong-Ou-Mandel interferometer: we are interested in the coincidence detection probability between two detectors placed at the output ports of the device. Furthermore, since we are interested in the results from a Hong-Ou-Mandel interferometer, we are interested in measuring the cross-correlation function of the wave-packets at the output ports, so we must apply electric field operators $\hat{E}_c^{(\pm)}(t)$ and $\hat{E}_d^{(\pm)}(t+\tau)$ as to compute the coincidence probability of detecting a photon at time t at output arm c and a photon at time $t+\tau$ at output arm d. The *joint photon-detection probability* reads [149]

$$\begin{aligned}&P_{joint}(t,\tau) = g_{c,d}(t,t+\tau) =\\ &\langle 0|\,\hat{a}_a\hat{a}_b\hat{E}_c^{(-)}(t)\hat{E}_d^{(-)}(t+\tau)\hat{E}_c^{(+)}(t+\tau)\hat{E}_d^{(+)}(t)\hat{a}_b^\dagger\hat{a}_a^\dagger\,|0\rangle\,.\end{aligned} \tag{2.29}$$

When we substitute the expression for the electric field operators on modes c and d as a function of the input wave-packets, the result yields[20]

$$\begin{aligned}P_{joint}(t,\tau) &= g_{c,d}(t,t+\tau) =\\ &= \tfrac{1}{4}|\varepsilon_a(t+\tau)\,\varepsilon_b(t) - \varepsilon_b(t+\tau)\,\varepsilon_a(t)\,|^2.\end{aligned} \tag{2.30}$$

One of the most interesting features of this result is that, no matter the shape of the wave-packet (its mathematical expression), the *joint photon-detection probability* vanishes at $\tau = 0$, i.e., the characteristic Hong-Ou-Mandel dip is recovered albeit the spectral shape of the photons [149].

In Chapter 3, we show that the derived expression for the *joint photon-detection probability* of two wave-packets entering a Hong-Ou-Mandel inter-

[20]Refer to Appendix 7.10 for complete mathematical development.

ferometer carries the information regarding the spectral density function of the photons. In other words, we develop the mathematical model which permits one to associate the Fourier Transform of the interferogram of the two-photon interference in a Hong-Ou-Mandel interferometer to the spectral shape of the interfering wave-packets and experimentally demonstrate the feasibility of spectral characterization of an arbitrary laser source in the few-photon regime. Furthermore, the limitations of the the few-photon spectral characterization and the region of operation in terms of the average number of photons of the sources being characterized are discussed. Before that, however, we take a step back to consider an utterly important aspect of the experimental verification of all results discussed in the following sections: the Time-Delay-Offset Coincidence Station.

2.6 Postselection and the Time-Delay-Offset Coincidence Station

In probability theory, to postselect is to condition a probability space upon the occurrence of a given event. Postselection is indispensable in experimentally assessing the effect of quantum interference phenomena: in the Hong-Ou-Mandel intereferometer, we are not interested in all detection events from the two detectors placed after the beam splitter but, rather, on the coincidence events so we condition the probability space upon the occurrence of coincidence counts. Not only that, but, as we sweep the time delay between detectors, we are interested in postselecting the coincidence events given that the wave-packet describing the two-photons after the interaction with the beam splitter are shifted by an arbitrary amount of time. As we have seen, when the time delay between postselected detections matches the indistinguishable condition, we see a drop in the coincident events characterizing the Hong-Ou-Mandel dip. Conversely, when the coincidental events are postselected when the wave-packet is such that the photons can be distinghished, no interference phenomena is observed. Since the devices usually employed experimentally for the detection of light pulses in the few-photon regime are gated avalanche photodiodes, the most common means of postselecting the coincidental events in a Hong-Ou-Mandel experiment, as we have already mentioned, is to trigger one of the detectors, say detector b, only when the other detector, say a, has already been triggered: this simple design offers the number of coincidences directly as the number of counts in b (apart from dark count events which are often considered negligible) since they are intrinsically conditioned to a detection in a.

In principle, enabling the detections on b in case of a detection in a in

the Hong-Ou-Mandel experiment, or any other postselection experiment, is harmless. The probability of two light pulses, present at the output spatial modes of the beam splitter, being detected by both a and b when b is enabled by a is $\eta^a \times \eta^b$, with η^a and η^b as the detection efficiency of detectors a and b respectively. Suppose, now, that there is some sort of electronic device capable of imposing a time delay to a detection pulse from a and checking if the delayed version is coincidental to a detection pulse from b. This is equivalent to the first process with the difference that the detectors can be triggered independently while the electronic structure is held responsible for sweeping the time delay between detections and postselecting those coincidental events. In this second experimental picture, the probability of two light pulses, present at the output spatial modes of the beam splitter, being detected by both a and b is $\eta^a \times \eta^b$, the same as in the first case where a triggers b. Of course this is the case due to our assumption that the efficiencies on a and b are not in anyway dependent on the origin of the *trigger* pulse, whether it is generated by another detector, by an external common pulse generator, or by the detectors own internal *trigger* pulse generator. Consider, however, that the light intensity arriving at the detectors is very low, as usual to experiments involving light pulses in the few-photon regime: the detection rate would be low in comparison to the trigger rate since, even considering perfect detection efficiencies, most of the time, no photons impinge on the detectors.

In this context, there is a defining difference between the two methods of postselection: in the second picture, the trigger rate of b is kept at its maximum rate independently from a, which is also kept at its maximum rate; in the first picture, the trigger rate on b is lowered to the rate of detections on a. The issue related to the drop of triggering rate on a single-photon avalanche photodiode is delicate and was first stumbled upon during the preparation of the experimental setup for the Measurement-Device-Independent Quantum Key Distribution proof-of-principle demonstation [61][21]. In this setup, four SPADs are employed to construct a Bell-State Projection unit, a linear-optic based structure which attempts to project two uncorrelated quantum states onto the maximally entangled Bell states [61]. Initially, the setup consisted of a *master* SPAD which, upon a detection, resumed to trigger the remaining three *slave* SPADs, much like our first picture of experimental postselection. The effects of this postselection method for this specific experiment is twofold with its own implications detailed as follows. The coincidence events between detectors in a Bell-State Projection are intimately linked to its application and

[21] A brief revision on the No-Cloning Theorem, the BB84 Protocol, the possible attacks on the protocol, and on the MDI-QKD can be found in Appendices 7.12, 7.13, 7.14, and 7.15

all the possible coincidental events should be achievable for proper operation (except for those which depend on photon-number resolving, a resource still under development for single-photon detectors of the lineage of InGaAs-InP G-APDs [152]). Triggering three *slave* SPADs conditioned to a *master* SPAD eliminates the possibility of a coincidental detection between any of the slave SPADs unless the *master* has been triggered, i.e., many successful Bell state projections can be lost during the link operation due to this postselection topology [61]. Observe that this limitation, which is ultimately crucial for achieving a minimum secret-key generation rate, has no dependency on the optical part of the experiment whatsoever but, rather, is associated to the postselection (in this case, we should call it a *willingly discard*) of results otherwise useful. Firstly addressed in [153], the second effect is the increase of the dark count detection probability of the SPADs as the trigger rate is diminished. The roots of this effect, even though still undetermined, were empirically attributed to a defective over-voltage electronics control system at the time of its discovery [153]. This permitted that a bypass to the problem could be devised since it was preventing the experimental MDI-QKD link to beat the minimum secret-key generation rate necessary for its secure operation [154]. In Fig.2.1, we present the results of measuring the dark count probability for the employed SPADs when the gate frequency is varied.

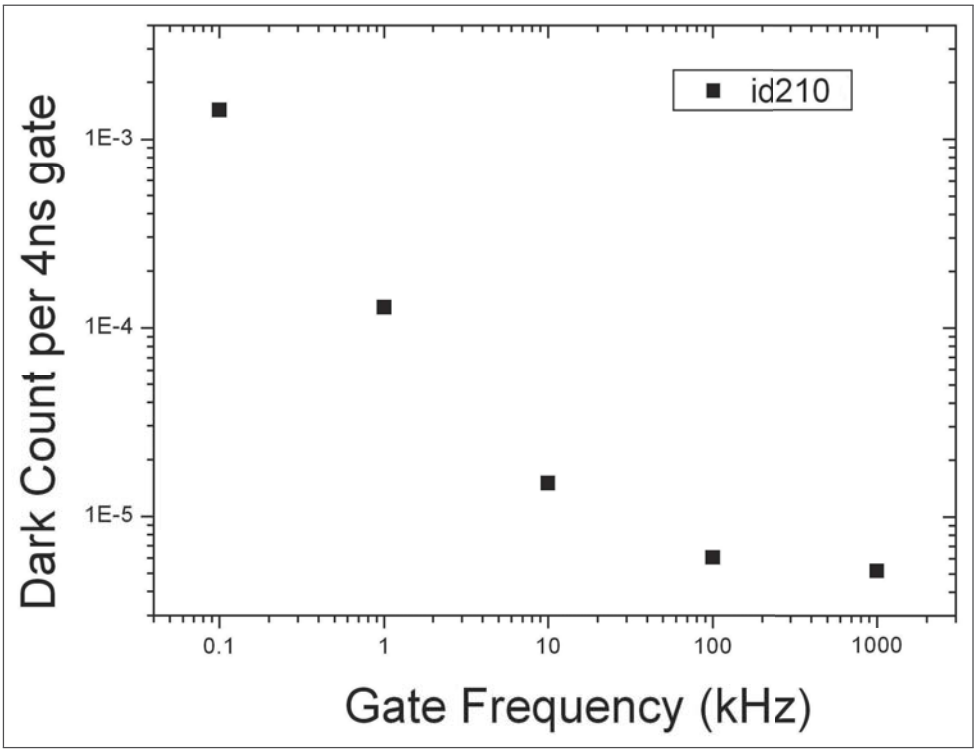

Figure 2.1: Dark count probability of the Id201 SPAD model for different values of the gate frequency. We see that, below 100 kHz, the dark count probability rises abruptly.

The answer to both of the issues raised in the MDI-QKD experiment by the naive method of postselection, or our first picture of experimental postselection, is the Time-Delay-Offset Coincidence Station (TDO-CS), which is in alignment with our second picture of experimental postselection. The TDO-CS attempts to transfer all the responsibility of identifying coincidental events to an electronic unit independent of the detectors while maximizing the triggering rate even when the relative temporal delay between detectors is required. The system is composed of a Digital Delay Generator (DDG) with time resolution up to 50 picoseconds [155] and an FPGA-based postselection hardware [153]. The goal is to create delayed versions of a common clock signal by inputting it into the DDG [22] and then compensate the different time of arrivals of the detection pulses in the FPGA-based structure. When one wishes to impose a relative temporal delay between two or more detectors, the DDG delays the clock versions of such detectors and the FPGA compensates the time of arrival by delaying the detection pulse of the detector which had not been delayed. This way, the pulses are examined at the same time basis and the coincidental events can be identified.

Working with the TDO-CS is quite straightforward once the system is time-equalized; we will now discuss the steps of equalization and operation to clarify the usage of the devised system. The first step, hereby referred to as *equalization step*, aims on setting all the detection pulses on the same time basis in the FPGA-based coincidence unit by compensating eventual differences in the response time of the detectors and the time of flight in the electric cables that connect the latter to the former. For that, one resets the delays imposed by the FPGA structure and attempts to maximize the number of coincidence detections by adjusting the high-resolution delays in the DDG[23]. When the coincidences between all the detectors are maximized, the system is said to be *equalized*, meaning that all intrinsic time delays external to the relative temporal delay sweep between detectors have been compensated. Let us now suppose that the detection pulses p_{D1}, p_{D2}, and p_{D3} from three different detectors D_1, D_2, and D_3, when fed by the same initially not equalized clock signal p_{clk}, have intrinsic temporal delays given, respectively, by τ_1, τ_2, and τ_3 represented in the time diagram of Fig.2.2[24]. The hypothetical resulting time

[22]The device's structure available in our laboratory permits one to access up to 4 different delayed versions of the same input signal.

[23]From an experimental point of view, it is straightforward to guarantee that the detectors are operative and indeed detecting light pulses whilst the equalization process is running by turning on the light sources.

[24]As we will see in further sections, this particular setup with three detectors is important when assessing the second order temporal autocorrelation function at zero time for linearly heralded photons.

diagram, after the equalization step is completed, is also presented in Fig.2.2.

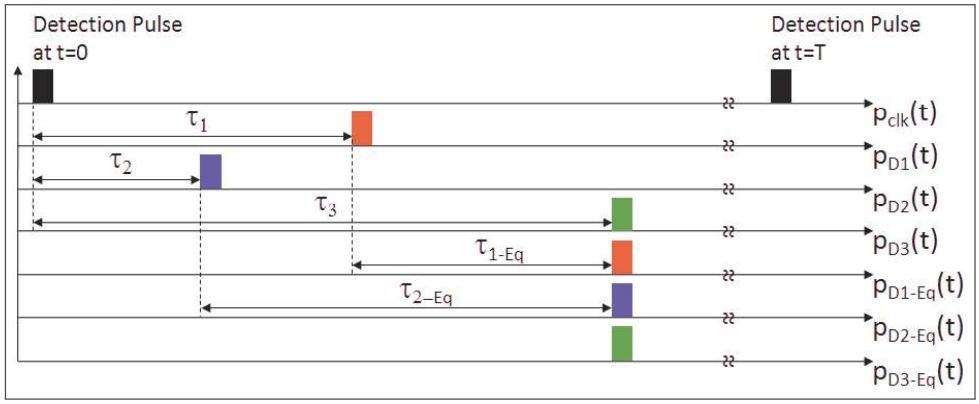

Figure 2.2: Hypothetical experimental setup where one is interested in the coincidence events between three different detectors. The intrinsic delay that results from the time-of-flight of the electrical pulses inside the cables and the response time of the detectors cause each pulse to arrive at the Time-Delay-Offset Coincidence Station at different times. This is represented by axes $p_{D1}(t)$, $p_{D2}(t)$, and $p_{D3}(t)$. The equalization step attempts to offset each individual temporal delay so that all detection pulses arrive simultaneously at the coincidence station. This is represented by axes $p_{D1-Eq}(t)$, $p_{D2-Eq}(t)$, and $p_{D3-Eq}(t)$.

With the TDO-CS equalized, the relative temporal delays can be swept and the interferogram, acquired. For that, two simultaneously coordinated processes assure the consistency of the interferogram time-basis acquisition: the DDG imposes a delay on the pulse signal directed to the detector which one wishes to sweep; the FPGA-based structure imposes an internal and identical temporal delay to the detection pulse from the detector which is *not* being swept so that both pulses can be analysed in the same time-basis. We present, in Fig.2.3, the time diagram of a hypothetical interferogram acquisition run for an equalized TDO-CS in which one is interested on the swept detections between two detectors.

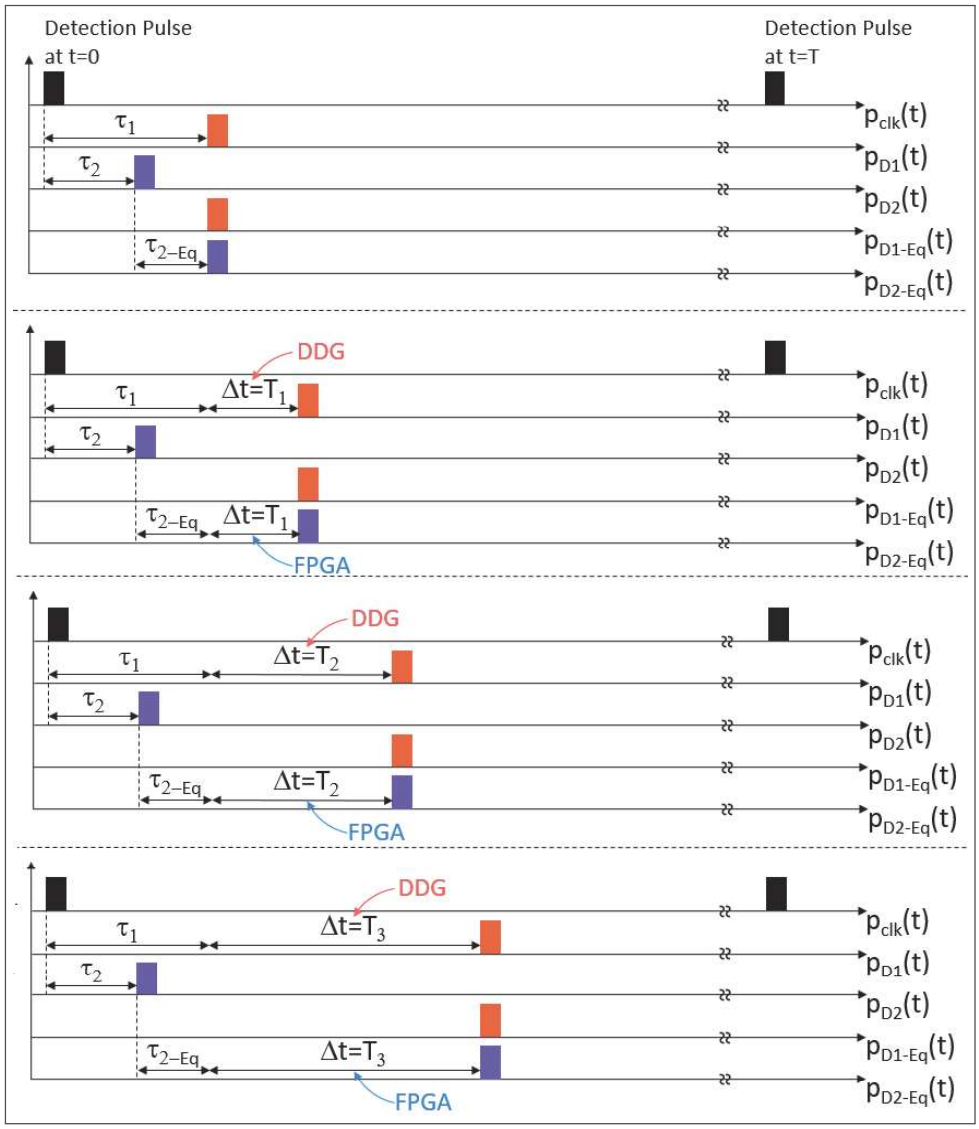

Figure 2.3: Hypothetical experimental setup where one is interested in sweeping the relative temporal delay between two detectors and recording the coincidence events. The DDG is responsible for delaying ($\Delta t = T_1$) the trigger pulse that goes to the detector which is swept and the FPGA compensates the delay internally enforcing the very same delay on the detection pulse.

The TDO-CS is completely automatic and offers an user-friendly dedicated interface which can be connected to the FPGA and to the DDG. Fig.2.4 presents the interface of the TDO-CS: the detection pulses of all detectors are connected to the FPGA unit which communicates via *USB* to the interface routine developed in *Python*; the DDG is also connected to the interface, but via *GPIB*; the interface displays the number of detections on each detector and coincidences between detectors with an adjustable refresh time and plots the results for each value of the relative temporal delay between detectors; all

adjustable time configurations are accessible through the interface.

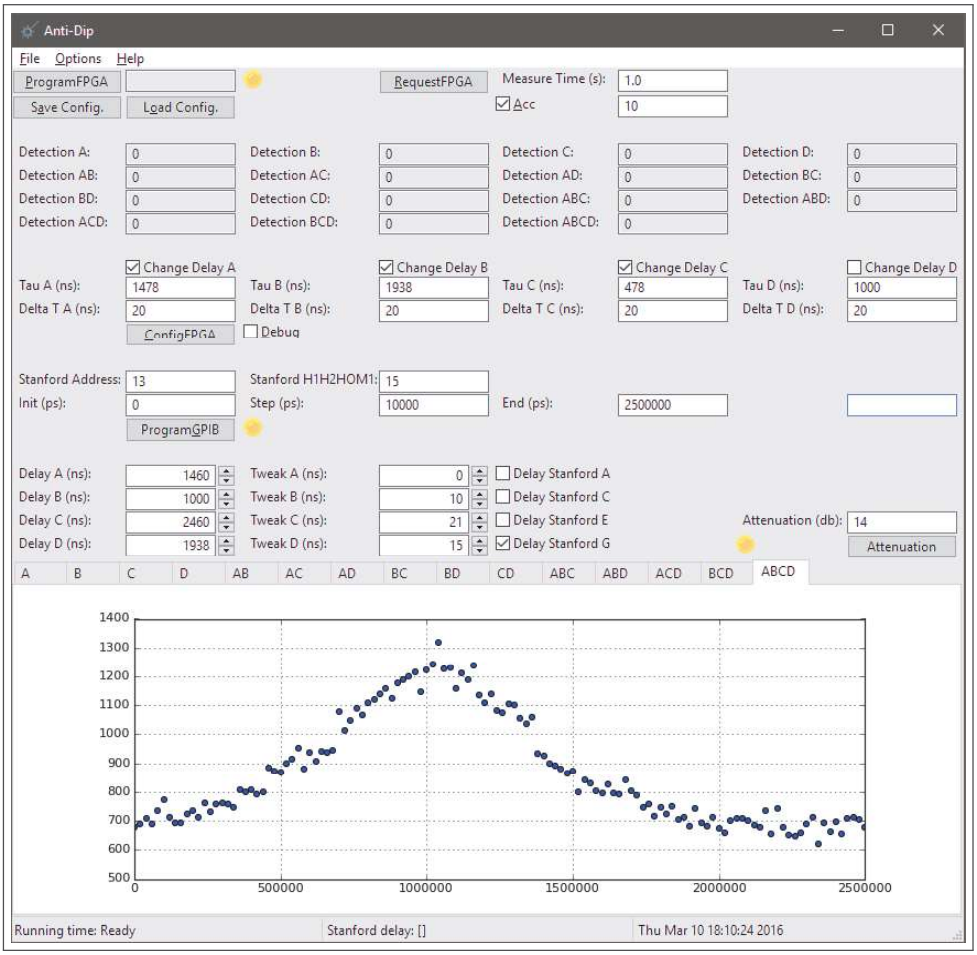

Figure 2.4: The Time-Delay-Offset Coincidence Station *Python* interface.

In Fig.2.5, we present a photograph the real-life setup used for the acquisition of experimental data presented throughout this document. The photograph depicts: six single-photon detectors; the DDG responsible for enforcing the time delays on the trigger pulses; the fiber-optic-based setup; the interface of the TDO-CS.

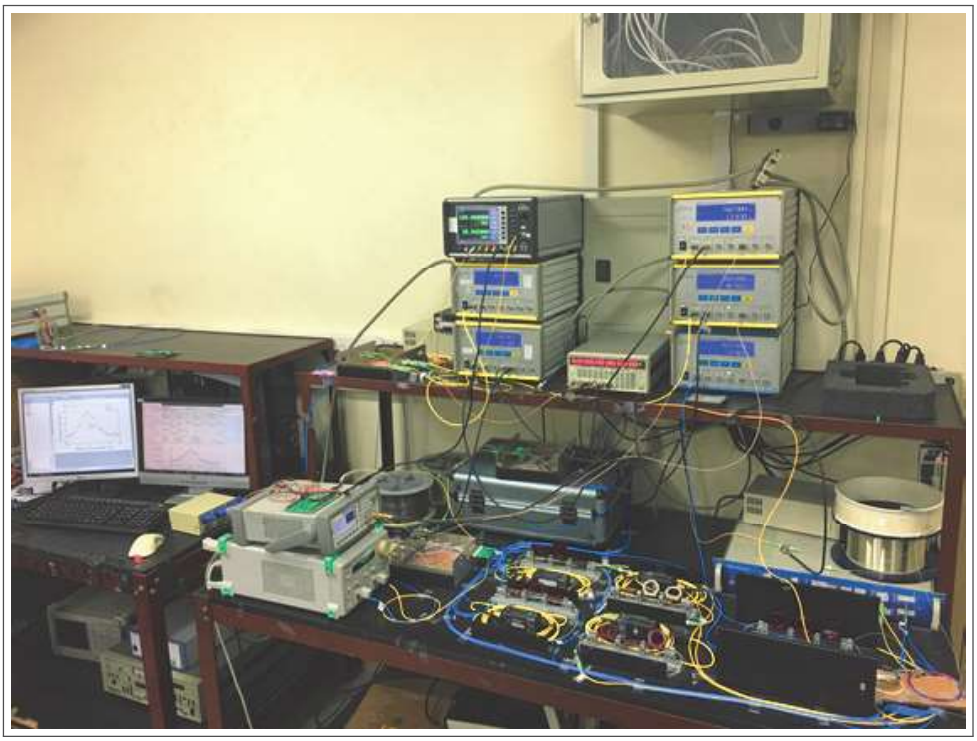

Figure 2.5: Photograph of the real-life experimental setup.

3
Few-Photon Fourier Transform Spectroscopy

The basic experimental apparatus for the spectral characterization in the few-photon – or weak – regime is shown in Fig. 3.1-a, where two independent lasers, *reference* and *test*, and single-mode fibers are employed. The *reference* laser is an external cavity laser diode frequency-stabilized at 1547.32 nm by a high Q-factor gas cell. The attenuated signal from the *reference* laser is directed to a HOM Interferometer along with the optical signal of the *test* laser. The *test* source is composed of a tunable wavelength laser, a 90/10 splitter, a second gas-cell, and a PID system connected to the wavelength tuning input of the laser. By controlling the region of the gas-cell's absorption line to which the PID system is locked, one can enforce the desired frequency-displacement between *reference* and *test* sources. This way, we could assess the validity of the Few-Photon FTS with a wide range of values for f_{beat}, the relative frequency displacement between coherent states. The input coherent states are power-balanced by variable optical attenuators as to reach the few-photon regime with the same average number of photons per pulse. Also, the counts in InGaAs-based Single-Photon Avalanche Photodiodes (SPADs) connected to a polarizing beam splitter are minimized so that the photons reaching the interferometer are polarization-aligned. Fig. 3.1-b shows the drop in the interferogram visibility as a function of the distinguishability of the states, which is governed by their relative states of polarization and relative intensities inside the time delay for which the temporal modes are overlapped in the interferometer since we consider the single-mode case. The bunching effect depends on the indistinguishability between wave-packets that describe the interaction between two photons and the beam splitter so, if the photons can be distinguished, the interference pattern is lost [143, 148]. The HOM Interferometer is completed by connecting the output spatial modes of the 50/50 beam splitter in two SPADs – D_A and D_B – operating in gated Geiger mode. D_A triggers D_B whenever a photon-counting event occurs therefore each count at D_B corresponds to a coincidence event which, as a function of the relative delay between detectors, compose the HOM interferometer's visibility curve. This process of postselection guarantees that only the mode-matched photons contribute to the interferogram. An optical fiber loop is connected

before D_B to optically compensate the electrical delay between the detectors. Both detectors are set to 15% efficiency and 4 ns gate width which corresponds to the best compromise between dark counts (on the order of 10^{-5} per detection gate) and efficiency.

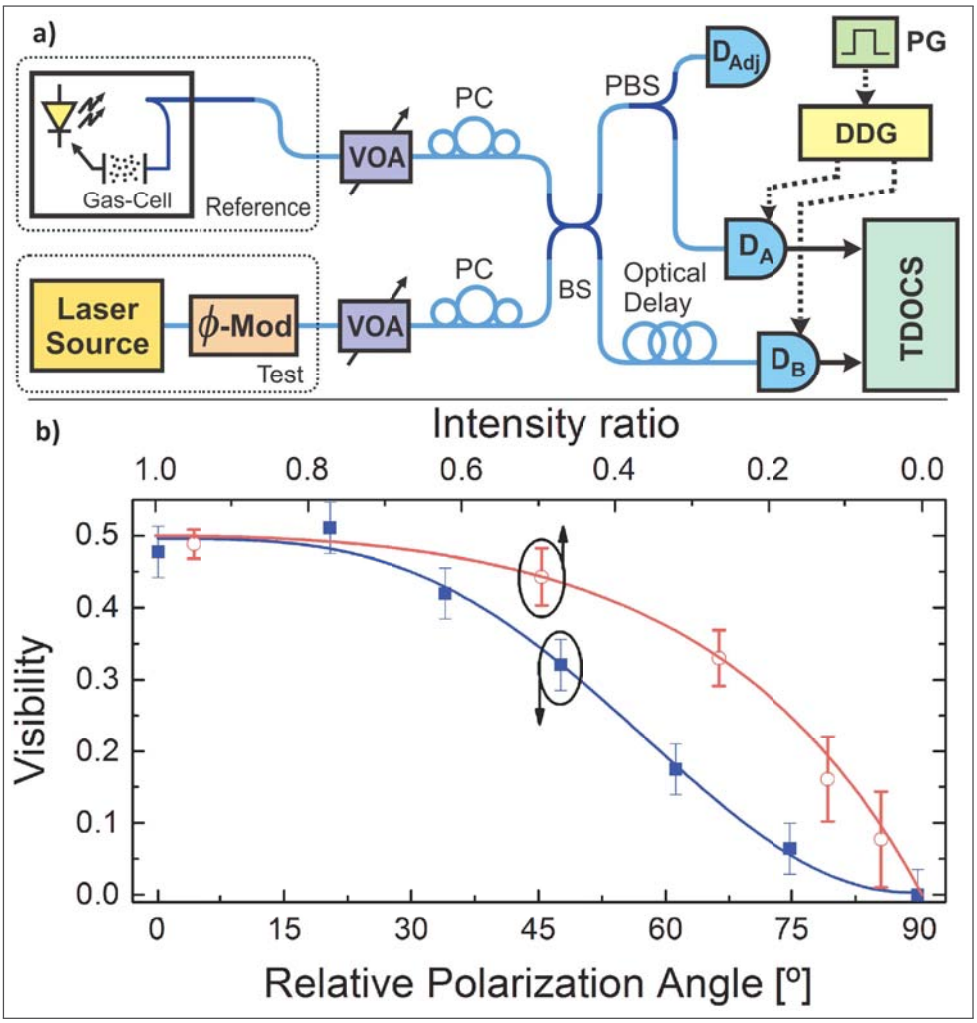

Figure 3.1: a) Experimental setup for the spectral characterization of optical sources in the few-photon regime. VOA: variable optical attenuator; PC: polarization controller; φ-Mod: phase modulator; PBS: polarization beam splitter; D_n: single-photon detector. b) Dependence of the interference visibility on the relative polarization and intensity ratio of the states: *red line* visibility versus relative intensity ratio; *blue line* visibility versus relative polarization angle.

Comparative classical heterodyne spectroscopic measurement can be performed by slightly modifying the setup of Fig. 3.1-a to overlap bright (non-attenuated) versions of *test* and *reference* lasers in a *pin* photodiode. The frequency beat is visualized in an Electrical Spectrum Analyzer (ESA). The results of Fig. 3.1-b show that the visibility drop due to misalignment in the interferometer, even though a concern, is not extremely severe. Deviations of

20% in both polarization alignment and intensity ratio can still be tolerated and fall well inside the SPAD's sensitivity. The fitting model for the relative intensity ratio is the visibility equation: $V = 2R/(1+R)^2$ [138], where R is the average number of photons per gate ratio between the two sources and V is the visibility. In the case of the relative state of polarization (SOP) alignment, the fitting model is obtained using Malus's Law [69] applied to the the visibility equation. We consider the projection on the measurement basis to write $R = cos^2(\theta_r)/[1+\sin^2(\theta_r)]$, where θ_r is the relative polarization angle between the interfering beams. The maximum value of the visibility in the case presented in Fig. 3.1-b is $V_{max} = 0.5$ due to the limitation associated to coherent states. The method is therefore robust regarding polarization, intensity and spatial-temporal mode-matching conditions.

Classically, the Interference Equation of two partially coherent waves has the form $I = I_1 + I_2 + 2\sqrt{I_1 I_2}|g_{12}|\cos\varphi$ [69], where I_1 and I_2 are the respective intensities of each source, g_{12} is their mutual coherence, and φ is their relative phase difference. Writing the Interference Equation in terms of the wave's power spectral density, $S(\nu)$, yields $I(\tau) = 2\int_0^\infty S(\nu)[1+\cos(2\pi\nu\tau)]d\nu$ if one assumes $I_1 = I_2$ and where τ is the relative temporal delay between the two optical wave-packets. From this result, it is possible to determine the spectrogram of the beat of two light sources by taking the inverse-Fourier transform of the respective interferogram in a process known as *Fourier-transform Spectroscopy* [69]. The proposed Few-Photon Spectroscopy is an application of the Fourier-transform spectroscopy to light with low average photon flux taking advantage of two-photon interference in a Hong-Ou-Mandel Interferometer.

In the quantum mechanical context, the mutual coherence of the wave-packets ($g_{A,B}$) defines the joint detection probability between detectors D_A and D_B and has the following mathematical expression dependent on the temporal wave-packets describing *reference* and *test* states, $f_1(t)$ and $f_2(t)$ respectively [149, 156]:

$$g_{A,B}(t_0,\tau) = \tfrac{1}{4}\left|f_1(t_0+\tau)f_2(t_0) - f_1(t_0)f_2(t_0+\tau)\right|^2 \tag{3.1}$$

One can manipulate Eq. 3.1 to find that

$$\begin{aligned} g_{A,B}(t_0,\tau) = \tfrac{1}{4}\Big[&\left|f_1(t_0)\right|^2\left|f_2(t_0+\tau)\right|^2 + \left|f_1(t_0+\tau)\right|^2\left|f_2(t_0)\right|^2 \\ &- \left[f_1(t_0)f_2(t_0+\tau)f_1^*(t_0+\tau)f_2^*(t_0)\right. \\ &\left. + f_1(t_0+\tau)f_2(t_0)f_1^*(t_0)f_2^*(t_0+\tau)\right] \end{aligned} \tag{3.2}$$

where * denotes the complex conjugate. Now we define $r(t) = \left|f_1(t)\right|^2$, $s(t) = \left|f_2(t)\right|^2$, and $f_1(t)f_2^*(t) = z(t)$. To obtain the probability of detecting two photons in detectors D_A and D_B with a time difference of τ ($P_c(\tau)$), one integrates over all

possible values of t_0, the arrival time of the photons, obtaining the curve that corresponds to the interferogram as a function of τ. Upon integration over t_0, we find that P_c has the following expression

$$\begin{aligned} P_c(\tau) = \frac{1}{4}\Big[&\int_{-\infty}^{\infty} r(t_0)s(t_0+\tau)dt_0 + \int_{-\infty}^{\infty} r(t_0+\tau)s(t_0)dt_0 \\ &- \left(\int_{-\infty}^{\infty} z(t_0)z^*(t_0+\tau)dt_0 + \int_{-\infty}^{\infty} z^*(t_0)z(t_0+\tau)dt_0\right)\Big] \end{aligned} \tag{3.3}$$

Taking the Fourier Transform of Eq. 3.3 yields

$$\begin{aligned} \mathscr{F}\{P_c(\tau)\} = \tfrac{1}{4}\big(&R(\omega)S(\omega) + R(\omega)S(\omega) \\ &- [Z(\omega)Z^*(\omega) + Z^*(\omega)Z(\omega)]\big) \end{aligned} \tag{3.4}$$

Using properties of the Fourier Transform, and setting $\mathscr{F}\{f_i(t)\} = \phi_i(\omega)$, a somewhat extensive but straightforward calculation allows one to rewrite Eq. 3.4 as[1]:

$$\begin{aligned} \mathscr{F}\{P_c(\tau)\} = \tfrac{1}{2}\big[&\phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega) \\ &- \phi_1(\omega) * \phi_2^*(\omega) \cdot \phi_1^*(\omega) * \phi_2(\omega)\big] \end{aligned}, \tag{3.5}$$

where the operator $*$ stands for the convolution. Upon close examination of Eq. 3.5, one distinguishes that the first term corresponds to the DC component of both $f_1(t)$ and $f_2(t)$, and also to a component centered at twice the central frequency of the optical carriers. This high-frequency component is filtered out since the detectors are not sufficiently broad-band to account for its detection whereas the DC component can be neglected since it doesn't contain any spectral information – it is associated to the average number of coincidence events. The second term, however, corresponds to the spectral component centered at the beat frequency between the optical carrier frequencies shaped as the modulus squared of the convolution of the spectral shapes of the temporal wave-packets. This component is the frequency beat that can be visualized in the Electrical Spectrum Analyzer from which classical spectral characterization can be performed.

We find, therefore, that the spectral characterization of optical sources in the few-photon regime is performed by taking the Fourier Transform of the two-photon interferogram which yields the convoluted spectral shapes of the individual states centered at the beat frequency between the optical carriers, a result condensed by Eq. 3.6 which defines the *Few-Photon Fourier Transform Spectroscopy* (Few-Photon FTS).

[1]Refer to Appendix XIII-11 for the complete mathematical development.

$$\left|\phi_1(\omega) * \phi_2(\omega)\right|^2 \simeq \mathscr{F}\left\{\int_{-\infty}^{\infty} g_{A,B}(t_0,\tau)\, dt_0\right\} \tag{3.6}$$

Even though the final result is in a convolution form, the process of deconvolution in order to determine the spectrum of *test* source is straightforward since the spectral characteristics of the *reference* source are known *a priori* [157]. It is worth noting that the *test* source's intensity is related to the average number of photons impinging on the detector during a temporal gate window and, therefore, can be easily determined.

A typical interferogram curve is presented in Fig. 3.2 for a frequency of 40 MHz. The time delay span was chosen taking into account mutual temporal coherence of the wave-packets as to cover the whole region of overlapping temporal modes. The polarization states are aligned up to the detector's sensitivity level and the average number of photons per detection gate is set to $\mu = 0.2$. The interferogram presented in Fig. 3.2 was acquired by sweeping the relative delay between the detectors in the HOM interferometer in steps of 500 ps respecting the two-photon interference conditions described in Fig. 3.1-b and the discussion thereupon.

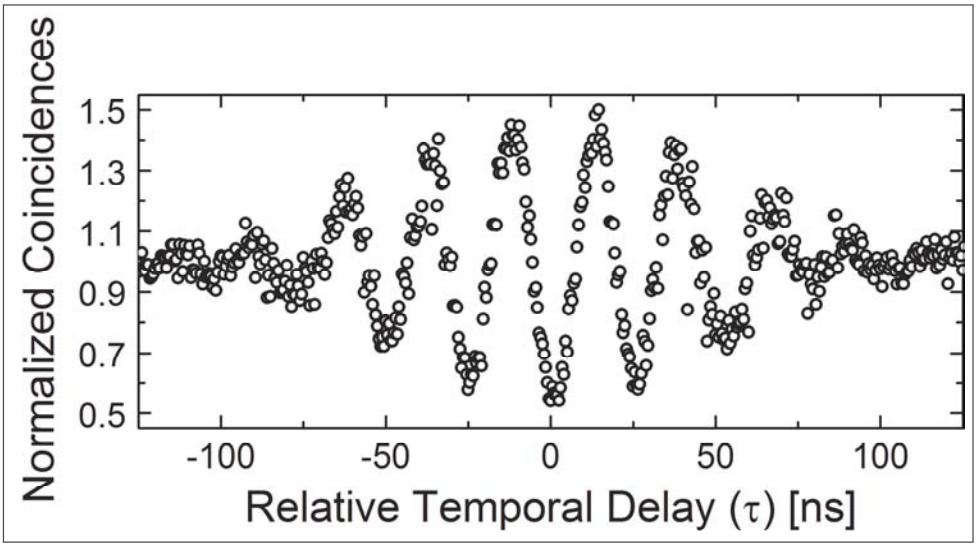

Figure 3.2: Interferogram of the two-photon HOM interference between *test* and *reference* weak-coherent states frequency-displaced by 40 MHz with $\mu = 0.2$.

Figure 3.3 superposes the resulting spectral shapes of the Few-Photon FTS and those measured in the ESA for different values of f_{beat}, ranging from 10 MHz to 200 MHz, with good agreement. Slight relative shifts are due to the instability of the gas-cell that locks the frequency of the *test* source. We also enforced non-gaussian spectra on the *test* laser by means of a phase modulator at its output driven by an Arbitrary Waveform Generator (AWG) (refer to Fig. 3.1). By selecting the modulation parameters, the spectrum can be widened,

which reflects on the temporal narrowing of the HOM interferogram due to the inverse relation between the mutual temporal coherence (τ_c) and the spectral linewidth ($\Delta\nu$) [69]. Such spectral widening is restored from the interferogram when we employ the Fourier Transform and is presented in Fig. **??** where, once again, we compare the results of the Few-Photon FTS and of the classical heterodyne beat.

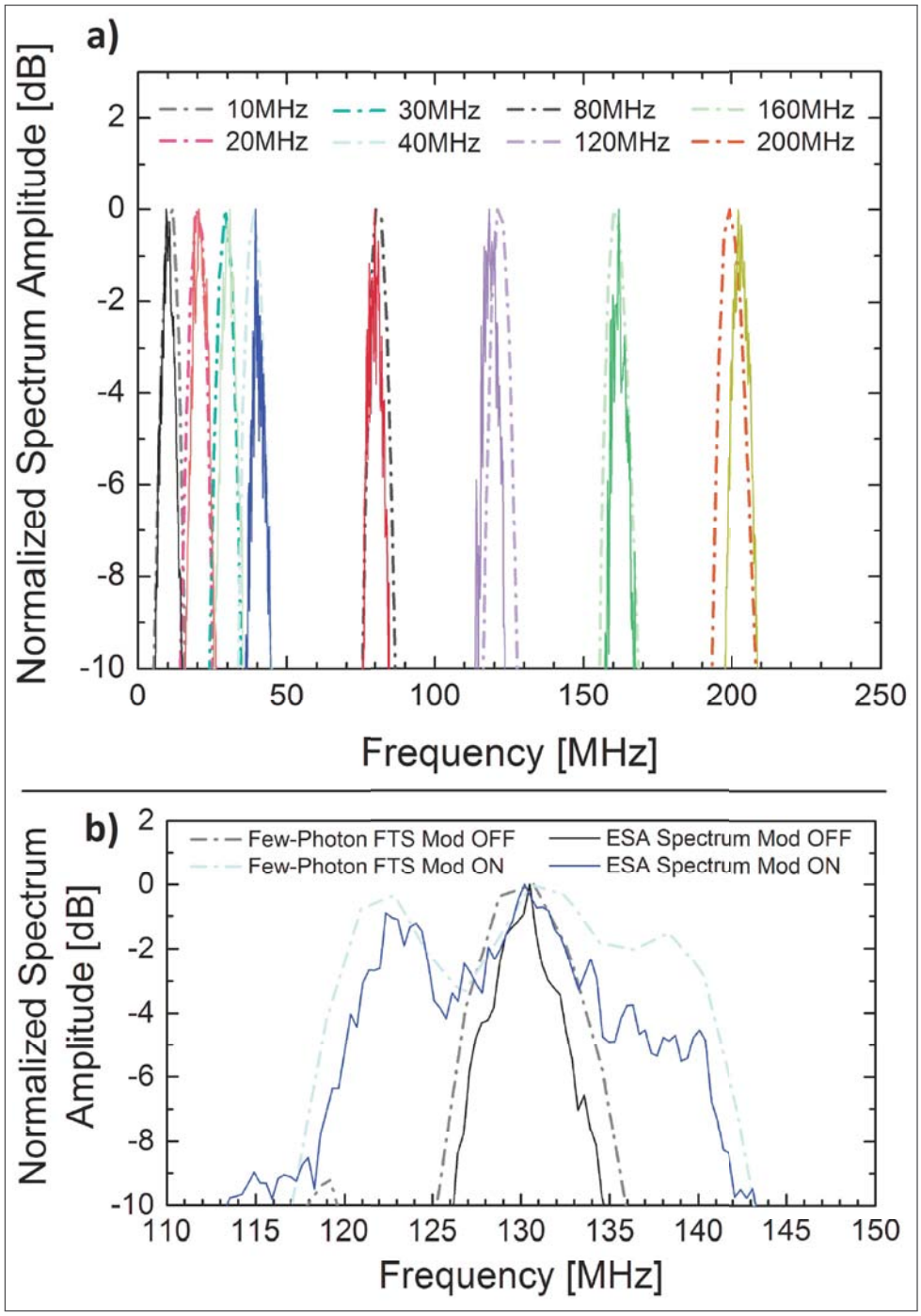

Figure 3.3: a) Comparison between the two spectral characterization techniques: Few-Photon FTS (dashed lines) and classical heterodyne beat (solid lines). The results show good agreement for a wide range of frequencies. b) The electro-optic phase modulator is switched on and off for a constant beat frequency of the lasers. The enlargement of the spectrum with respect to f_{beat} is accurately described by the Few-Photon FTS.

Note that, due to the relative nature of the method and the folding nature of the FFT spectrum, there is an ambiguity in determining the *test* source's

center frequency which can lie on $f_{ref} \pm f_{beat}$. Running the method twice while displacing the reference frequency by an amount smaller than f_{beat} eliminates this ambiguity. Considering the deconvolution process, it is also worth noting that a proper choice of the reference frequency must result in an unfolded frequency spectrum, so that f_{beat} should be larger than the width of the *test* source spectrum [157].

Since both techniques are shown to be equivalent both by the mathematical model and by the experimental results, a distinction has to be made between them. This is translated in the region of effectiveness of each method, the Few-Photon FTS figuring as a better candidate as soon as the average number of photons per pulse falls below a certain value. Fig. 3.4 displays the region of effectiveness of the classical heterodyne beat and the Few-Photon FTS as a function of the average number of photons per gate of the *test* source. The employed criterion of effectiveness for the Few-Photon FTS is the Visibility of the interferogram curve since no spectral analysis can be performed once this value goes to zero. In the case of the classical heterodyne beat, the data acquired in the ESA was approximated to a simple model when one assumes gaussian wave-packets for the interfering beams, i.e., a gaussian-shaped spectral curve centered at the beat frequency. The R^2 (R-squared) parameter of the approximation, which translates the likelihood between the model and the acquired data, was used as a criterion for the technique's effectiveness.

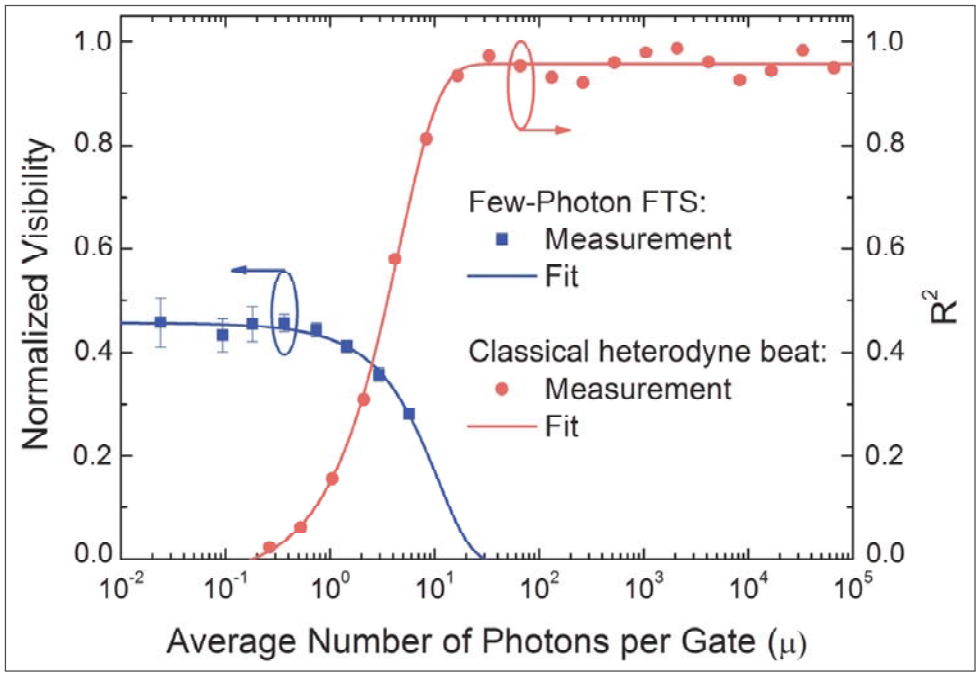

Figure 3.4: Range of application of the Few-Photon FTS and classical spectroscopy methods in terms of the average number of photons per pulse, μ, of the *test* source. The R^2 parameter of the approximated model and the visibility of the HOM interferometer are set as parameters of the accuracy and, therefore, the validity of each technique. The data sets were fit to evidence the dependency of the effectiveness on μ. Maximum P_{ref} is +13dBm.

Throughout all measurements, the relative intensity level and polarization angle was kept at the optimal value to guarantee maximum visibility in the interference pattern, i.e., $\mu_{ref} = \mu_{test}$. Even so, the visibility does not match the expected 50% value as can be observed from Fig. 3.4, an effect we attribute to experimental misalignment up to the detector's sensitivity and polarization fluctuations inside the fiber link which, once again, are in accordance with the results of Fig. 3.1-b. We experimentally extended the average number of photons per time interval to the limit of the SPAD ($\mu \approx 10$ for $w_g = 4$ ns, the detector's gate width) and observed that, even though the visibility starts to decay abruptly, the interference pattern is still reproduced in the interferometer. The results of Fig. 3.4 therefore show that the upper limitation of the Few-Photon FTS can be extended beyond the model of [148] at the cost of loss in visibility.

At the same time, a high power local oscillator allows the classical technique to read optical signals down to tens of photons per nanosecond on the nano-watt level. The heterodyne beat between optical signals results in an oscillatory term with electrical power directly proportional to the product of

the optical signals, $P_{beat}^{elec} \propto P_{ref}^{opt} P_{test}^{opt}$. This means that low-power test signals can, in principle, be read with a sufficiently high-power reference laser. The power range of the classical technique is therefore upper- and lower-limited by the saturation of the detector and the noise floor of the detection system, respectively. The Relative Intensity Noise is also a concern and can limit the SNR of the classical technique [158].

The Few-Photon FTS technique allows for the characterization of states with average number of photons per time interval down to the limit imposed by the dark count probability of the SPADs. The average number of photons per time interval in this case corresponds to -118 dBm in the Telecom C-band – computed as $P = \mu hc/(\lambda w_g)$, where P is the optical power, h is Planck's constant, c is the speed of light in vacuum, and λ is the wavelength in vacuum. The Few-Photon FTS is therefore capable of stretching the achievable region of spectral characterization of optical sources, from the nano-watt level of the classical technique, down to the femto-watt level.

Recall from Fig. 3.2 that, to some values of τ, the visibility curve of the frequency-displaced two-photon interference raises above the baseline that corresponds to distinguishable photons. Since we deal, throughout the experiment, with weak-coherent states, the baseline indicates the probability of randomly distributed number of photons to impinge simultaneously on both detectors since, as we have already claimed, when an incoherent mixture of coherent states interact with the beam splitter, the output is an incoherent mixture of coherent states. The Hong-Ou-Mandel dip, characterized by the drop of the coincidence counts (the minimum of the visibility curve at $\tau = 0$), reflects the bunching effect. We are therefore compelled to argue that the increase in the coincidence counts, or the maximum of the visibility curve, indicates that the local detection of a photon in one of the interferometer's output modes could be used to announce a single-photon pulse at the other output mode with a higher probability than a regular faint laser source. In the next section, we present the Linear-Optic Heralded Photon Source, a sub-Poissonian photon source that harness the characteristics of the coincidence peaks when frequency-displaced photons are directed to a beam splitter [68].

4
Linear-Optic Heralded Photon Source

In order to create the optical beat note and explore its coincidence peaks, two frequency-displaced independent WCSs were generated through an all-fibered self-heterodyne setup [148] as depicted in Fig.4.1. The self-heterodyne approach avoids stability issues regarding both optical power and relative frequency drift and makes use of only one laser source. Two frequency-locked lasers, however, could also be employed in generating the optical beat note as demonstrated in the Few-Photon Fourier Transform Spectroscopy section.

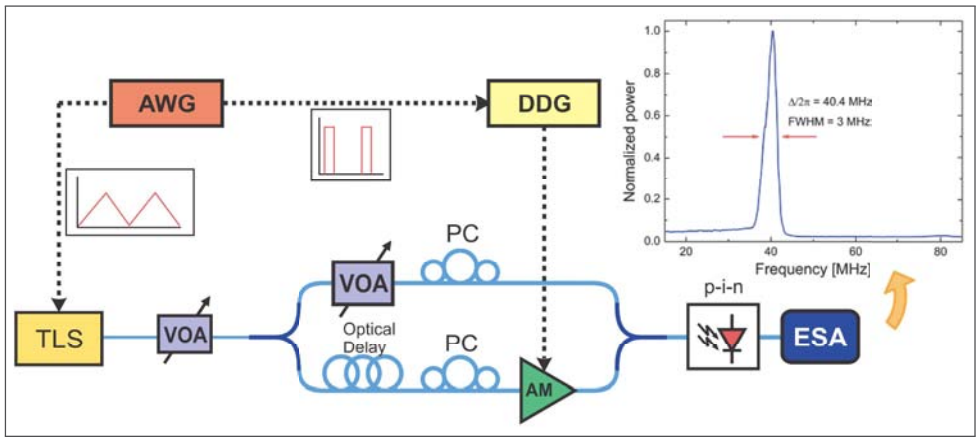

Figure 4.1: Preparation of frequency displaced WCSs with a self-heterodyne setup. Inset: Classical beat spectrum measured with bright versions of the WCSs. AWG: arbitrary waveform generator; FM: frequency modulation; TLS: tunable laser source; VOA: variable optical attenuator; DG: delay generator; PC: polarization controller; AM: amplitude modulator.

The attenuated CW signal of an external cavity laser diode is frequency modulated with modulation depth A and period T and sent into a balanced Mach-Zehnder Interferometer (MZI). An optical switch at one of the MZI's arms selects the photons with constant frequency offset ($\Delta/(2\pi) = 2A\tau/T =$ 40 MHz) relative to the other arm. This is verified by measuring the bright-light version of the optical beat note with a p-i-n photodiode and an electrical spectrum analyzer at the output of the MZI (Fig.4.1b). The output of the MZI is converted into an HOM interferometer to build up the Linear-Optic HPS. The HOM interferometer can be time-tuned so the local detection at the

heralder mode enables the source's optical output which is announced by the heralding signal. In order to determine the operational point of the Linear-Optic HPS, the interference pattern is measured with a Photon Statistics Analyzer (PSA) connected to the Linear-Optic HPS, as depicted in Fig.4.2a. The PSA is composed of a remote detector triggered by a delayed version of the heralding signal. All detectors are InGaAs APD-based single-photon detectors (SPD) operating in gated-Geiger mode with 2.5 ns temporal gate width, 15% detection efficiency and 10 μs deadtime.

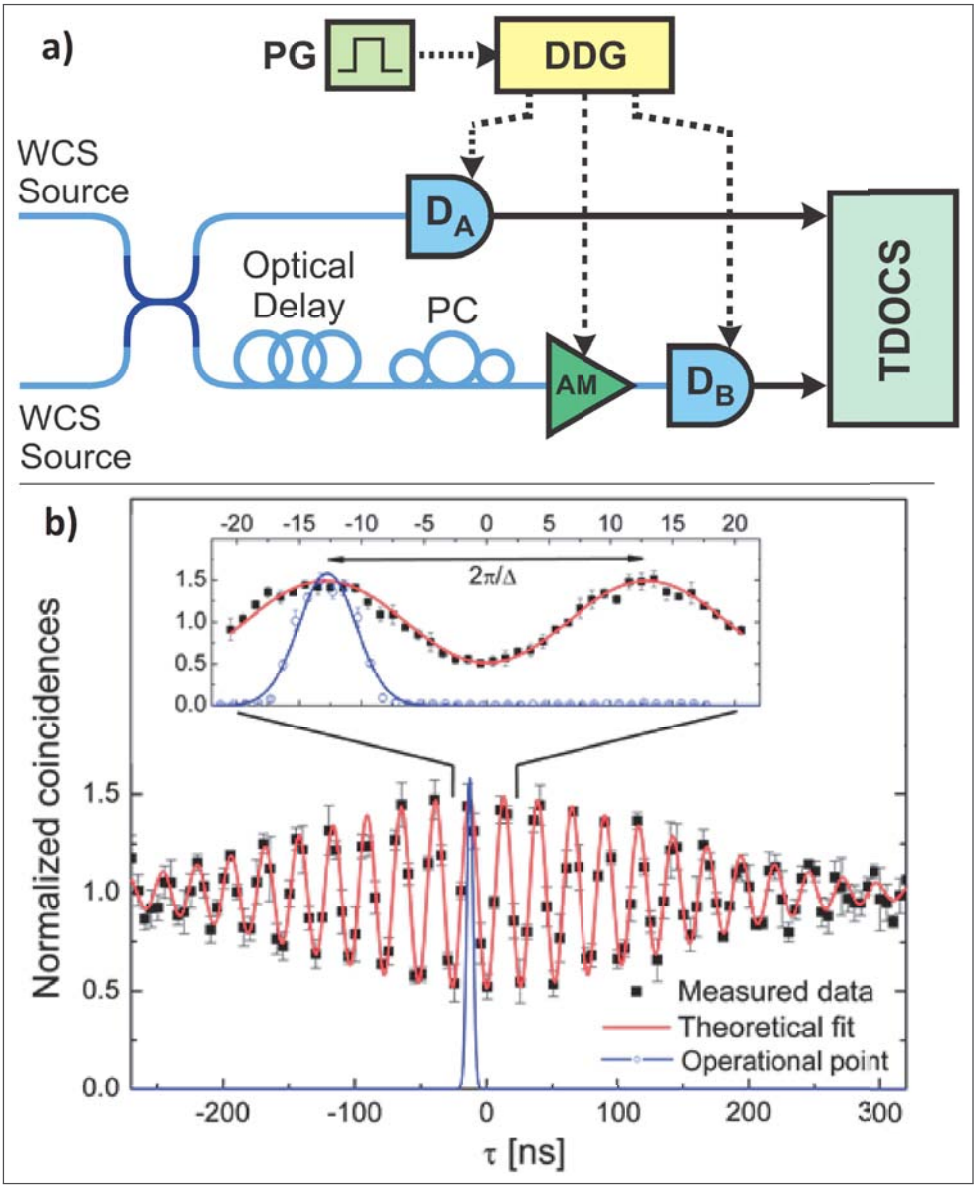

Figure 4.2: (a) HOM interferometer with overlapping WCSs and PSA. (b) Interference pattern measured with the PSA for the 40MHz-displaced WCSs with optical switch fixed at the operational point (blue circles) and synchronously swept with the detector (black squares). The theoretical model is fit to data (red line).

The beat pattern, obtained by scanning the relative delay of the HOM interferometer (depicted in the inset of Fig.4.2), is characterized by the mutual coherence time of the sources and by Δ [148, 149]. The theoretical prediction for the normalized coincidence counts [148]

$$C_c = \frac{1}{2}\left(2 - e^{-\frac{\tau^2}{2\sigma^2}}\cos\left(\tau\Delta\right)\right) \tag{4.1}$$

is fit to data. The operational point is obtained when the spatio-temporal modes are matched with $\tau = \pm\pi/\Delta$, the coincidence peak.

The operational point of the Linear-Optic HPS is defined as the selected time interval in which photons are most likely to exit the interferometer from different spatial modes, the coincidence peak. Operation in this mode is assured by the electro-optical modulator at the source's output which is triggered by a delayed version of the heralding signal. In this configuration, the system is expected to exhibit sub-poissonian photon statistics if one of the photons is used to announce the presence of the other. The setup, however, offers time tunability so the source can behave as an FLS – if the selected time interval corresponds to the interference of distinguishable photons – or even at the HOM dip, where it is expected to exhibit super-poissonian photon statistics since the photons are most likely to exit the interferometer from the same spatial mode. Fig.4.3 illustrates the selection of the operational point through time tunability.

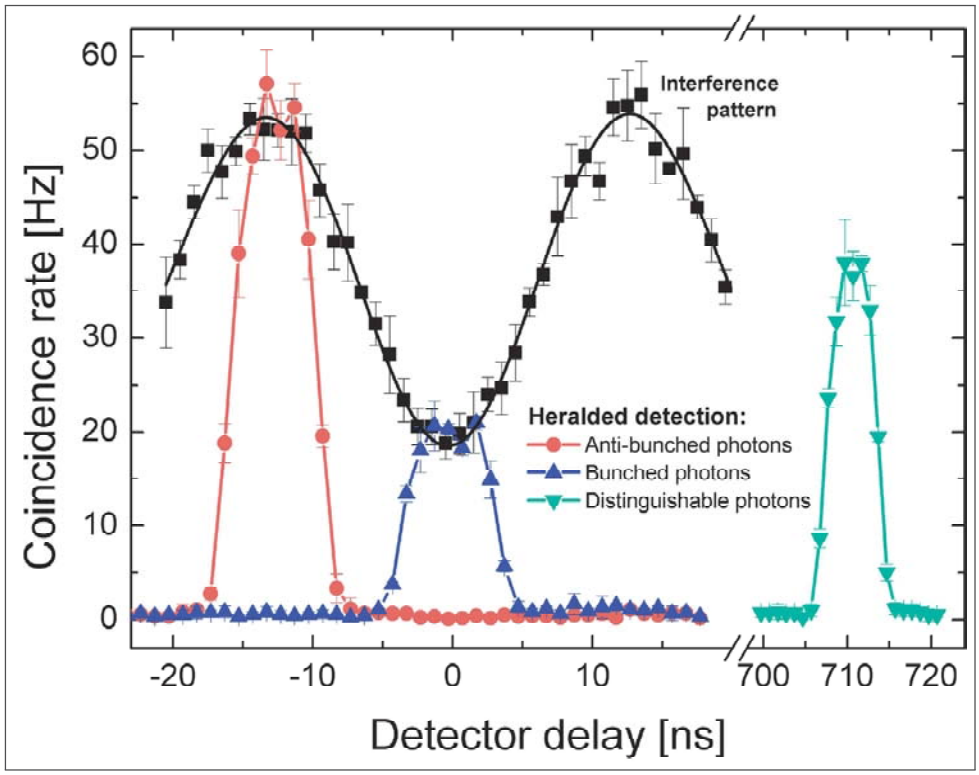

Figure 4.3: Three distinct possible operational points for the source. The Linear-Optic HPS is characterized by the operational point at the coincidence peak.

The frequency-displaced WCSs are implemented through a self-heterodyne setup in order to avoid experimental drawbacks such as identical values of μ and parallel states of polarization (SOP). On the other hand, however, this setup shows a crucial dependency on the synchronism of the devices. In Fig.4.4, a simplified overview of the self-heterodyne setup is depicted detailing the Mach-Zender Interferometer responsible for generating the frequency-displaced photons and the synchronism signals necessary for setting the source at its operational point.

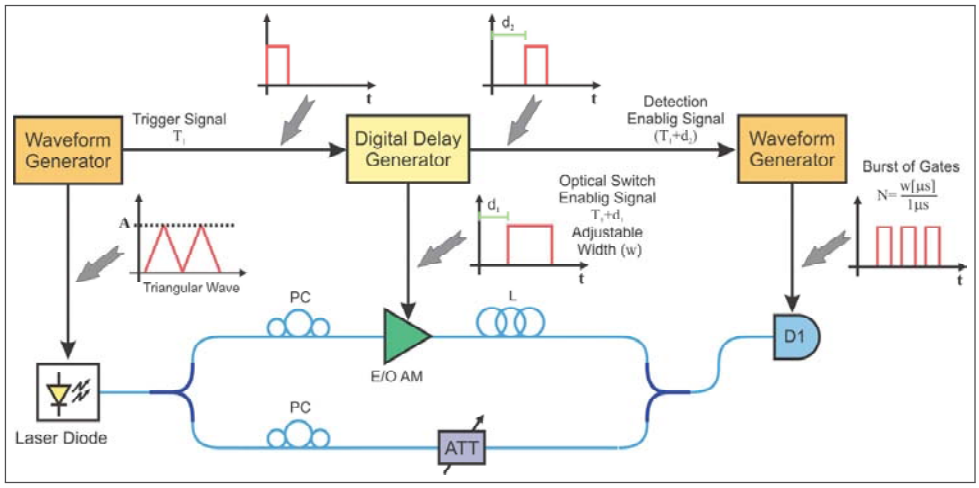

Figure 4.4: Detailed synchronization signals of the Linear-Optic HPS.

In order to guarantee that the optical switch is activated at the correct moment, the trigger signal of the triangular wave that sweeps the Laser's optical frequency is delayed by d_1 and sent to the electro-optical amplitude modulator of the MZI's upper arm – see Fig.4.4. This is to enforce the frequency displacement between photons in different arms. The values of the triangular wave's amplitude ($A = 2.04$V), its period ($T = 322.6$ms) and the delay necessary to compensate the fiber delay ($L = 8.5$km) and to enable the optical switch at the right moment ($d_1 = 44\mu$s), as well as the maximum duration of the enabling pulse ($w = 30\mu$s), were experimentally determined by adjusting a 40-MHz beat spectrum between bright versions of the frequency displaced WCSs with the p-i-n + ESA setup (not shown in Fig.4.4). The effect of the variation of the modulation parameters and the importance of synchronization to yield the right frequency displacement between the states is clarified in Fig.4.5.

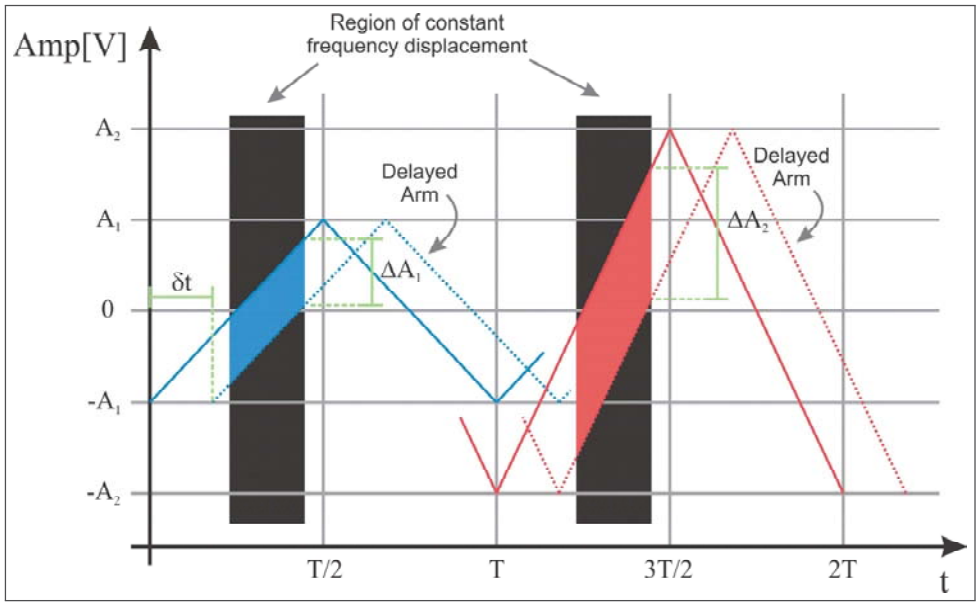

Figure 4.5: Arrival of frequency modulated light pulses at the HOM Interferometer. Depending on the amplitude of the modulating triangular wave, its period, and the fiber delay, the frequency displacement at the HOM Interferometer will vary.

Since the operation period of the optical switch (30 μs)is higher than that of the detector's *dead time*, a train of gates can be used to trigger the detector every time the optical switch is operational for maximal detection rate. In order to generate the train of gates, a function generator is triggered by a delayed version of the enabling pulse. The result of the synchronization of the gate burst and the photon wave packet arriving at the SPD is displayed in Fig.4.6 where two operation modes of the photodetector, with respect to dead time, were scanned: $DT = 0$ and $DT = 10\mu$s. The operation mode during the experiment is set to $DT = 10\mu$s to avoid the afterpulse effect and to diminish dark count events. However, as it becomes clear in Fig.4.6, a finer synchronization is performed with $DT = 0$.

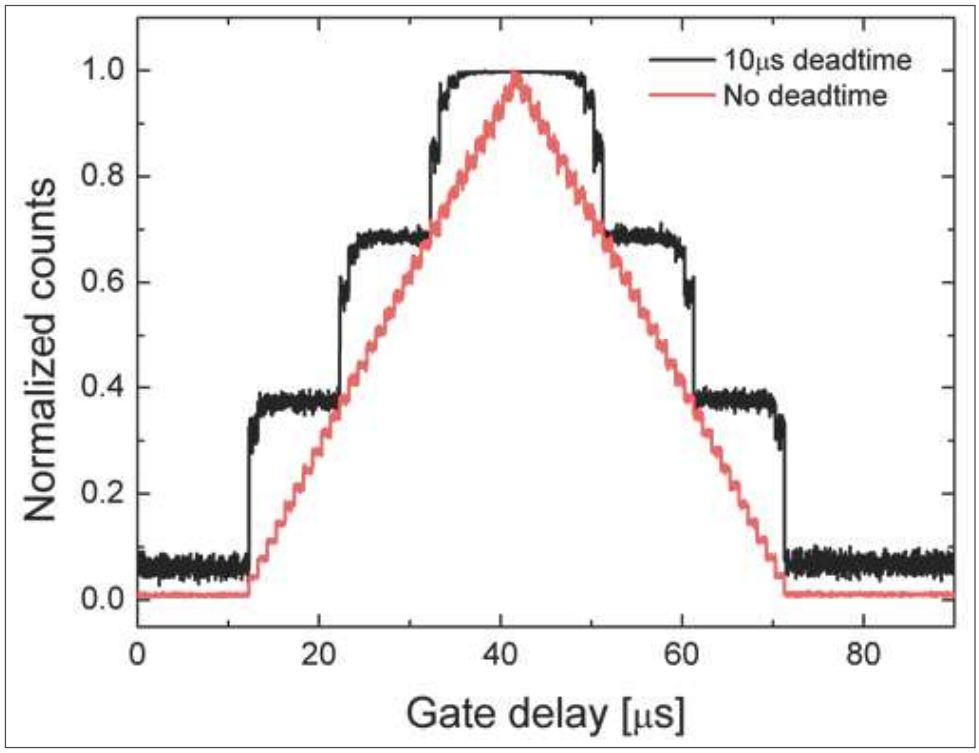

Figure 4.6: Gate delay synchronization. (black) Experimental curve of the number of detections in SPD_1 using a $10\mu s$ dead time. (red) Equivalent curve with the dead time set to 0.

An interesting feature of this setup is that most of the synchronization was performed empirically. However, was the laser's FM response known *a priori*, this wouldn't have to be the case. Knowing the length of the fiber used to decorrelate the MZI arms, the amplitude of the triangular function that modulates the laser, its period, and the laser's (unknown) FM transfer function [Hz/V], both the delay d_1 – to the optical switch – and the beat note frequency between the arms could have been determined. Once the system is empirically set, the reversed experiment can be performed to determine the FM transfer function. Plotting the beat note frequency versus the modulation amplitude yields a line with slope proportional to the transfer function, the length of the fiber delay and the light speed inside the fiber depicted in Fig.4.7. The slope found for the Δf vs A_p curve was $\alpha = 20.155$ [MHz/V] which represents the laser's FM transfer function.

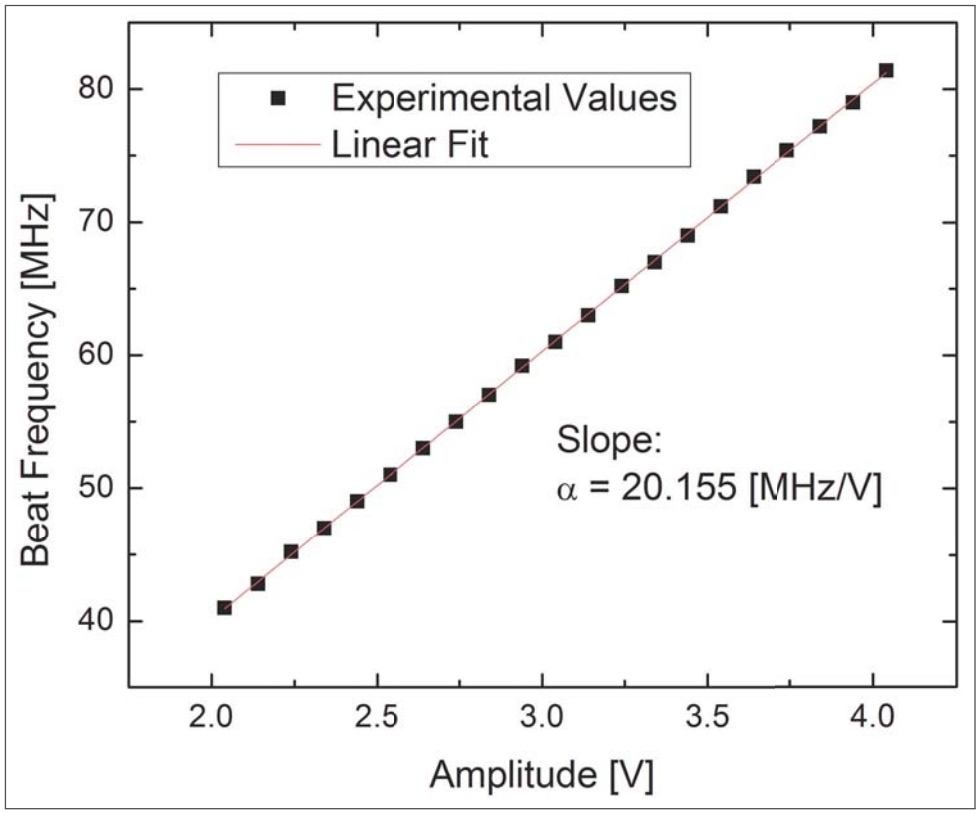

Figure 4.7: Δf vs A_p curve of the self-heterodyne experiment. The red curve is the linear fit of the experimental points.

Even though the beat frequency shows a linear correspondence to the amplitude of the modulating FM triangular wave, the linewidth of the beat tone broadens as the amplitude is raised. This reflects the non-linearity of the FM response which imposes a limitation to the region of constant frequency displacement selected by the electro-optical switch. The relative delay δt between the photon wave packets was empirically determined to be of 41.6μs. Since the period of the triangular wave is 322.6μs, the expected interval of constant frequency displacement is 281μs. In order to achieve a narrow (3MHz) beat tone, however, the region was considerably reduced to 30μs.

Let us now model the output photon statistics of our proposed source. Consider a symmetric beam splitter with input spatial modes a and b and output spatial modes c and d. As we have discussed thoroughly in Section 2.5, a quantum beat pattern is expected when the photons impinging on the device have different frequencies and the effect can be observed in temporal modes if their coherence time is high enough [149, 159]. The optical beat note corresponds to the frequency displacement between the photons even if independent WCSs are used [148]. We wish to model the output states from a heralded source time-tuned to the coincidence peaks of the interferometer so, considering that the input states are generated by two independent continuous-

wave (CW) optical sources emitting spatial-mode matched parallel-polarized photons with identical average number of photons per time interval, we decompose the input frequency-mismatched WCSs into pairs of Fock states with m and n photons, $|m_a, n_b\rangle$. The error associated to the simplification of bounding $M + N \leq 3$ is estimated from the Poisson cumulative distribution function, $\sum_{m=0}^{3}\sum_{n=0}^{3}\mu^{m+n}e^{-2\mu}/\left(m!n!\right)$ [5], as being lower than 1% for $\mu < 0.67$, a value which is in accordance with the experimental conditions necessary for visibility close to 50%.

The case of interest is the one where two frequency-displaced single photons enter the Hong-Ou-Mandel interferometer, one in each of the input modes. This main result is then used to compose the other non-trivial cases of one- and two-photon states entering each input mode $|1_a, 2_b\rangle$ and $|2_a, 1_b\rangle$. The case in which any number of photons enter the interferometer through one of the input modes, with vacuum at the other, $|m_a, 0_b\rangle$ or $|0_a, n_b\rangle$, has a straightforward solution: a random distribution of photons between the two output spatial modes. After all input states up to $M + N \leq 3$ are considered, the possible outcomes of the interferometer are then combined and weighted by the probability of occurrence of the correspondent input states. This information consists on the source's output statistics once the probability of a heralding event is considered. As we have already mentioned, the input state can be written in terms of creation operators applied to the vacuum state, $|1_a, 1_b\rangle = \hat{a}_a^\dagger \hat{a}_b^\dagger |0\rangle$. From now on, we shall adopt the notation $P_{r,s}^{m,n}$ for the conditional probability of finding r and s photons at output modes c and d, respectively, given that we had m and n photons at the input modes a and b, respectively. The *joint photon-detection probability* has already been derived for wave-packets described by one-dimensional spatio-temporal functions in a Hong-Ou-Mandel interferometer, and we shall re-write it adopting our new notation for clarity

$$P_{1,1}^{1,1}(t,\tau) = \frac{1}{4}|\varepsilon_a(t+\tau)\,\varepsilon_b(t) - \varepsilon_b(t+\tau)\,\varepsilon_a(t)|^2. \tag{4.2}$$

The coincidence probability of finding a photon at output port d at time $t + \tau$ given a photon is detected in output port c at time t can be found when one integrates over all possible values of t, a procedure much like the one performed in the Few-Photon Fourier Spectroscopy [160]. Right now, however, we are not interested in how this expression relates to the spectral density function of the wave-packets but, rather, with an analytic expression for this probability calculated for different τs so the photon statistics of the source can be determined. For an arbitrary wave-packet, it is not an easy task to

determine the coincidence probability from Eq. 4.2. Fortunately, it can be solved analytically when one considers gaussian-shaped wave-packets [149], an assumption not very far from the usual (which is to assume Lorentzian-shaped wave-packets [69]). We also assume gaussians with identical half-width at 1/e, σ, and well-defined angular frequency modes ω_a and ω_b ($\omega = \omega_a/2 + \omega_b/2$). The frequency difference $\Delta = \omega_b - \omega_a$ is fixed and the wave-packets can be expressed as

$$\begin{aligned} \xi_A(t) &= \frac{1}{\sqrt[4]{\pi\sigma^2}} e^{-(t-\delta\tau/2)^2/(2\sigma^2)} e^{-j(\omega-\Delta/2)t} \\ \xi_B(t) &= \frac{1}{\sqrt[4]{\pi\sigma^2}} e^{-(t+\delta\tau/2)^2/(2\sigma^2)} e^{-j(\omega+\Delta/2)t}, \end{aligned} \tag{4.3}$$

where $\delta\tau$ is the relative delay between the wave-packets. Integration from $-\infty$ to ∞ over t (as we are only interested in the effective time delay τ between the wave packets) and over $\delta\tau$ (to take into account the CW nature of the optical sources) yields [148]

$$P_{1,1}^{1,1} = \frac{1}{2}\left(1 - e^{-\frac{\tau^2}{2\sigma^2}} \cos(\tau\Delta)\right). \tag{4.4}$$

To simplify the terms that follow, we set $\beta = e^{-\frac{\tau^2}{2\sigma^2}} \cos(\tau\Delta)$.

It is now clear, from inspection of Eq. 4.4, that two distinct values of the relative temporal delay, τ, are of importance in modeling the source: τ greater than the mutual coherence time of the wave-packets (τ_{coh}) and $\tau = \pi/(2\Delta)$, when the temporal modes are matched and the wave-packets, superposed in the interferometer. In the first case, the oscillatory pattern of the interference vanishes since the states are fully distinguishable, so each photon sent into the HOM interferometer takes a random output. Any attempt to herald such states will fall into the same statistics of an equally-bright non-heralded attenuated laser source. This condition is further used as reference for evaluating the second order correlation function of the Linear-Optic Heralded Photon Source. In the second case, however, coincident counts increase up to 50% in relation to the distinguishable case [148].

Due to normalization and symmetry arguments, the probability of finding two photons in one output spatial mode and vacuum in the other is found to be

$$P_{2,0}^{1,1} = P_{0,2}^{1,1} = \frac{1}{4}(1+\beta). \tag{4.5}$$

The solutions for all cases up to 3 photons entering the Hong-Ou-Mandel interferometer is derived based on this result. The solution considering a single photon entering one of the input ports of the beam splitter with vacuum entering the other, $|1_a, 0_b\rangle$ and $|0_a, 1_b\rangle$, is straightforward,

$$P_{1,0}^{1,0} = P_{0,1}^{1,0} = P_{1,0}^{0,1} = P_{0,1}^{0,1} = 1/2. \tag{4.6}$$

The same analysis applies to the case in which either two (Eq.4.7) or three photons (Eq.4.8) enter the same input port and vacuum enters the other

$$\begin{aligned} P_{2,0}^{2,0} = P_{0,2}^{2,0} = P_{2,0}^{0,2} = P_{0,2}^{0,2} = 1/4, \\ P_{1,1}^{2,0} = P_{1,1}^{0,2} = 1/2; \end{aligned} \tag{4.7}$$

$$\begin{aligned} P_{3,0}^{3,0} = P_{0,3}^{3,0} = P_{3,0}^{0,3} = P_{0,3}^{0,3} = 1/8, \\ P_{2,1}^{3,0} = P_{1,2}^{3,0} = P_{2,1}^{0,3} = P_{1,2}^{0,3} = 3/8. \end{aligned} \tag{4.8}$$

The cases $|2_a, 1_b\rangle$ and $|1_a, 2_b\rangle$ are modeled as a superposition of a pair of single photons, one at each input port, and an independent photon in either one of the input ports,

$$\begin{aligned} P_{3,0}^{2,1} = P_{0,3}^{2,1} = P_{3,0}^{1,2} = P_{0,3}^{1,2} = \frac{1}{8}\left(1+\beta\right), \\ P_{2,1}^{2,1} = P_{1,2}^{2,1} = P_{2,1}^{1,2} = P_{1,2}^{1,2} = \frac{1}{8}\left(3-\beta\right). \end{aligned} \tag{4.9}$$

The probabilities of finding one of the above output states in modes c and d are obtained by grouping the conditional probabilities of this one output state weighted by the probabilities of occurrence of each input state. The former are given by the Poisson distribution $P\left(m,n|\mu\right)_{a,b} = \frac{\mu^{m+n}}{m!n!}e^{-2\mu}$ since the states impinging on the beam splitter are coherent states [5]. The general form of the probability of occurrence of the output state $|r_c, s_d\rangle$ when the beam splitter is fed by frequency-displaced weak-coherence states when we fix $\max\left(m+n\right) = 3$ is

$$P_{r,s} = \sum_{m=0}^{3}\sum_{n=0}^{3} P_{r,s}^{m,n} P_{m,n}, \begin{cases} r,s,m,n \in \mathbb{N} \\ r+s \leq 3 \\ m+n \leq 3 \end{cases} \tag{4.10}$$

The output states of the Linear-Optic HPS are characterized by a heralding event to which, disregarding dark counts, are associated to the presence of a photon – or more than one – at spatial mode c, hereby addressed to as the *heralder* arm (or spatial mode). As we are only interested in those such cases for computing the statistics of the source's output, the total probability, used for normalization, is

$$P_T = \sum_{r=1}^{3}\sum_{s=0}^{2} \left[\eta_p\right] P_{r,s}, \begin{cases} r,s \in \mathbb{N} \\ r+s \leq 3 \end{cases} \tag{4.11}$$

Therefore, the probabilities of the three distinct events of heralding vacuum P_v, single- P_s or multi-photon P_m pulses at spatial mode d (disregarding the dark count probability) are given by

$$P_v = \left(\eta_1 P_{1,0} + \eta_2 P_{2,0} + \eta_3 P_{3,0}\right)/P_T, \tag{4.12}$$

$$P_m = \eta_1 P_{1,2}/P_T, \tag{4.13}$$

$$P_s = \left(\eta_1 P_{1,1} + \eta_2 P_{2,1}\right)/P_T, \tag{4.14}$$

respectively. Here, the p-photon detection efficiency at the *heralder* arm, $\eta_P = 1-(1-\eta_h)^p P$, was considered. This parameter depends on the detector efficiency η_h. With $\alpha = \exp(-2\mu)$, the normalized heralding probabilities of vaccum, multi-photon, and single-photon pulses for the Linear-Optic Heralded Photon Source ($\tau = \pm\pi/\Delta$), as a function of μ and the heralder SPD efficiency (η_h), are:

$$P_v = \frac{8+\mu\left(4-2\eta_h\right)+\mu^2\left(1-\eta_h+\eta_h^2/3\right)}{8+\mu\left(16-2\eta_h\right)+\mu^2\left(16-6\eta_h+\eta_h^2/3\right)}; \tag{4.15}$$

$$P_m = \frac{5\mu^2}{8+\mu\left(16-2\eta_h\right)+\mu^2\left(16-6\eta_h+\eta_h^2/3\right)}; \tag{4.16}$$

$$P_s = \frac{12\mu+\mu^2\left(10-5\eta_h\right)}{8+\mu\left(16-2\eta_h\right)+\mu^2\left(16-6\eta_h+\eta_h^2/3\right)}. \tag{4.17}$$

In Table 4.1, we present the normalized heralding probabilities of vaccum, multi-photon and single-photon pulses for the Linear-Optic Heralded Photon Source at the operational point and considering $\mu << 1$ and $\eta_h = 1$, compared to the probability of finding similar pulses at the outputs of a conventional Poisson statistics source such as an attenuated laser. Even though the multi-photon emission probability is slightly higher for the Linear-Optic HPS, the emission of vacuum is relatively suppressed, and the single-photon pulses occur with higher probability. This characterizes the narrowing of the photon-number distribution of the squeezed WCS at the output of the source.

Table 4.1: Normalized Probabilities ($\mu << 1$,$\eta_h = 1$)

Pulse	Linear-Optic HPS	FLS	Ratio
Vacuum	$1-\frac{3}{2}\mu+\frac{15}{8}\mu^2$	$1-\mu+\frac{1}{2}\mu^2$	$1-\frac{1}{2}\mu$
Multi-Photon	$\frac{5}{8}\mu^2$	$\frac{1}{2}\mu^2$	$\frac{5}{4}-\frac{677}{500}\mu$
Single-Photon	$\frac{3}{2}\mu-2\mu^2$	$\mu-\mu^2$	$\frac{3}{2}-\frac{1}{2}\mu$

The second-order temporal correlation function at zero time is experi-

mentally determined via the Hanburry-Brown and Twiss experiment as[1]

$$D_{F,G} = \frac{P_s \eta_{F,G}}{2} + \left(\eta_{F,G} - \frac{\eta_{F,G}^2}{4}\right) P_m. \tag{4.18}$$

Given our previous suppositions drawn throughout the theoretical modeling, coincident detections are triggered by half the multi-photon probability events, resulting in

$$D_{FG} = \frac{\eta_F \eta_G}{P_m/2}. \tag{4.19}$$

The $g^2(0)$ parameter is then re-written as a function of the photon statistics of the Linear-Optic HPS and the detection efficiency values as

$$g^2(0) = \frac{P_m}{a_1 P_s^2 + a_2 P_m^2 + a_3 P_s P_m}, \tag{4.20}$$

where $a_1 = 1/2$, $a_2 = (2 - \eta_F/4 - \eta_G/4 + \eta_F\eta_G/8)$, and $a_3 = (2 - \eta_F/4 - \eta_G/4)$. From the modeled single and multi-photon probabilities, we find that $g^2(0)$ is 0.56 at the coincidence peak and 1 for the distinguishable case. Figure 4.8 presents the predicted values for $g^2(0)$ and the experimental values. The inset exhibits the predicted values for $g^2(\tau)$ considering $\mu = 0.1$ and the detectors efficiency $\eta_{H,F,G} = 0.15$. The agreement between experimental and theoretical results validates the model.

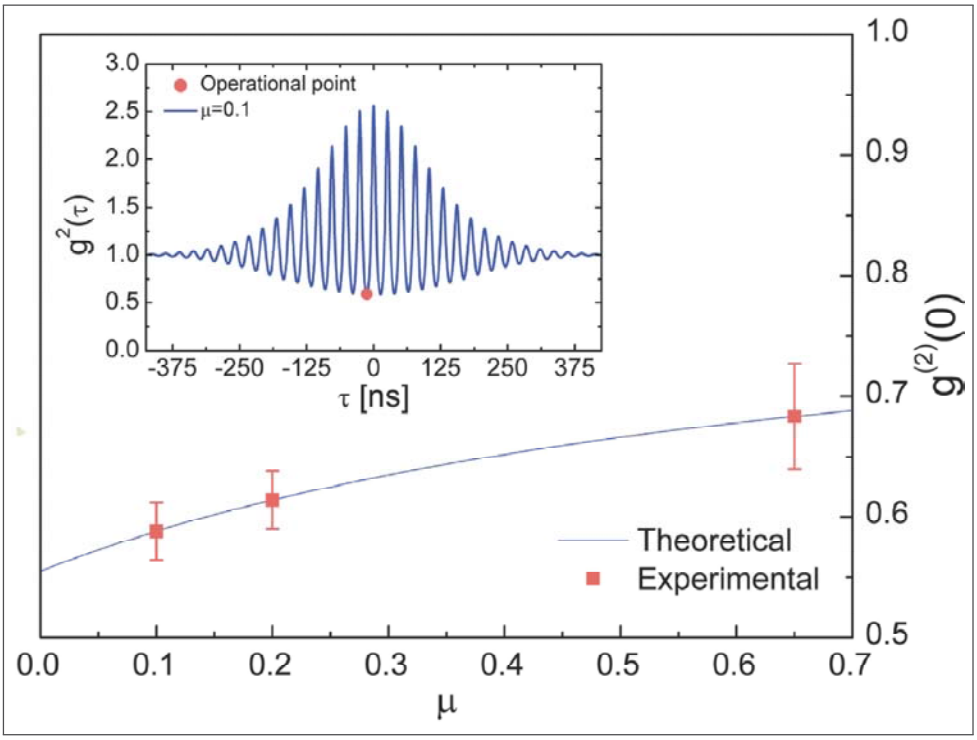

Figure 4.8: Theoretical values and experimental results for $g^2(0)$ for the Linear-Optic HPS at the operational point (shown in the inset over the $g^2(\tau)$ function).

[1]Refer to Appendix 7.16. Note that we replaced modes a and b by modes f and g for notation consistency.

The states produced at the Linear-Optic HPS output are squeezed WCSs for which the photon-number distribution is narrower than the coherent state but with wider bandwidth, obeying Heisenberg's Uncertainty Principle [5,139]. The frequency-broadening with respect to the original linewidth is due to the frequency modulation of the optical signal. The frequency-modulation input at the TLS is excited by a triangular wave with frequency 3.1 kHz corresponding to a period of 322.6 microseconds. The optical switch at one of the MZI's arm selects photons with a fixed frequency displacement during a 30 microsecond period – 9.3 % of the triangular wave period – which yields a 40 MHz tone as observed in the Electrical Spectrum Analyzer and shown in Fig. 4.1. Therefore, the total frequency sweep that characterizes the Linear-Optic HPS output linewidth is given by $\Delta\nu = 40 \times (0.093)^{-1} = 430$ MHz. By connecting a high-resolution Optical Spectrum Analyzer (OSA) to the source's output, one can measure the output linewidth of the states, which is displayed in Fig. 4.9.

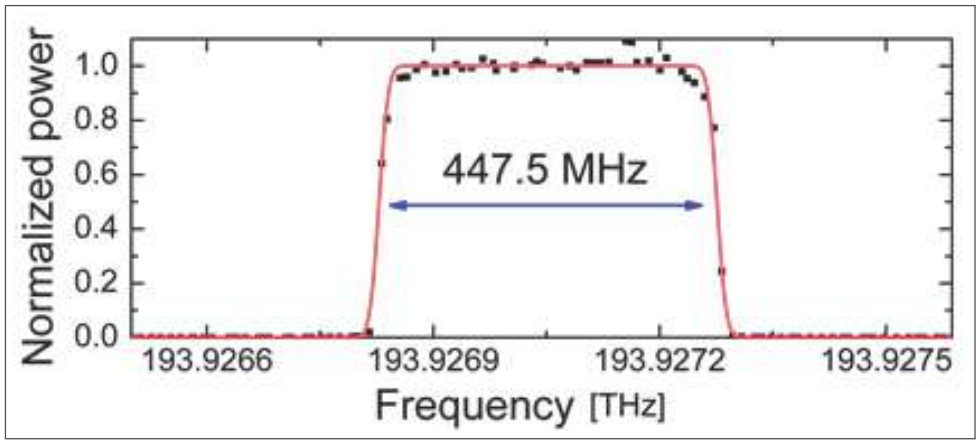

Figure 4.9: Overall output linewidth of the Linear-Optic HPS. The curve was acquired during a 2 hour period using a high-resolution OSA.

The expected linewidth of the squeezed WCS heralded by the Linear-Optic HPS agrees well with the 447 MHz linewidth. The correspondent coherence time of 2.2 ns is more than 7 times greater than for highly filtered asynchronous SPDC-HSPS [84]. Even though the overall output of the Linear-Optic HPS shows a broad linewidth, it is important to note that, in a single-photon interference context, the linewidth is actually that of the original optical source, around 600 kHz. The resulting coherence time would be as high as 530 ns, several orders of magnitude higher than SPDC-based HSPS. This is important, for instance, in the time-bin-based prepare and measure schemes [35], where the emitted photons interfere with themselves. The Linear-Optic HPS can, then, be made as coherent as a faint-laser source with improved photon emission statistics.

4.1 Quantum Key Distribution Link Employing the Linear-Optic HPS

The performance of a QKD system is directly dependent on the photon statistics of the optical source. We therefore analyze the secret key generation probability and the maximum achievable link distance for the Linear-Optic HPS, for a FLS, and for an SPDC-HSPS, following the GLLP [161] and the decoy states analysis [46]. The parameters P_0, P_1 and P_2 are the probability of Alice sending vacuum, single- or multi-photon pulses for each kind of source considered. The yield is the conditional probability of detection for Bob, given that Alice has sent an i-photon pulse. This is given by $Y_i \approx P_d + \eta_i$, where P_d is the detector dark count probability and $\eta_i = 1 - (1-\eta)^i$. The overall transmittance η includes the detection efficiency (η_{SPD}), the transmittance of Bob's devices (η_{Bob}) and is proportional to the link loss ($\eta \approx 10^{-\alpha L/10}$) – where α is the attenuation coefficient (dB/km) of the fiber with length L (km) at the operation wavelength. The gain of the i-photon state is given by $Q_i = P_i Y_i$, and the overall gain is obtained by summing over the contribution of all states $Q_\mu = \sum_{i=0}^{\infty} Q_i$.

The error probability of the i-photon state is given by $e_i = (e_0 Y_0 + e_{opt}\eta_i)/Y_i$, where $e_0 = 1/2$ is the probability of a dark count occurrence at the wrong detector and e_{opt} corresponds to the optical misalignment of Bob's apparatus. The overall error is given by $E_\mu = \frac{1}{Q_\mu}\sum_{i=0}^{\infty} e_i Q_i$. The secret key generation probability is computed as

$$R \geq q\left\{Q_1\left[1 - H_2\left(e_1\right)\right] - Q_\mu H_2\left(E_\mu\right) f\left(E_\mu\right)\right\}, \tag{4.21}$$

where $H_2(x)$ is the Shannon binary entropy, $f(x)$ is the inefficiency of the error correction (1.16 here), and $q = 1/2$ appears due to the bases matching probability. Considering the GLLP security analysis [161], the gain of single-photon pulses is lower bounded by

$$Q_1 = Q_\mu - \sum_{i=2}^{\infty} P_i \approx Q_\mu - P_m\left(\mu\right). \tag{4.22}$$

This assumption is the pessimistic one where all multi-photon pulses sent by Alice are eavesdropped. In this analysis, the single-photon error is given by

$$e_1 = (E_\mu Q_\mu)/Q_1. \tag{4.23}$$

When using the decoy states method, the values of Q_1 and e_1 can be estimated without the pessimistic assumption. This is possible due to the random choice of intensities sent by Alice. The i-photon yield does not depend on Alice's choice, so Eve cannot predict nor fake the output of Alice's source. Furthermore, due to these tighter bounds, Alice can usually

use higher intensity values without jeopardizing the system security. The simulation parameters were extracted from [74]: α=0.21 dB/km; η_{Bob}=0.045; P_d=0.85×10^{-6}; e_{opt}=0.033. The value of μ was optimized at each link distance for the faint laser source and Linear-Optic HPS. The efficiency of the heralder detector of the Linear-Optic HPS is 15%. The probabilities for the SPDC-based HPS were obtained from [86]: P_1=0.42 and $g^2(0)$=0.018, with $P_2 = g^2(0)\,P_1^2/2$ [83]. The results for the secret key generation probability obtained as a function of the link length for different sources are shown in Fig. 4.10.

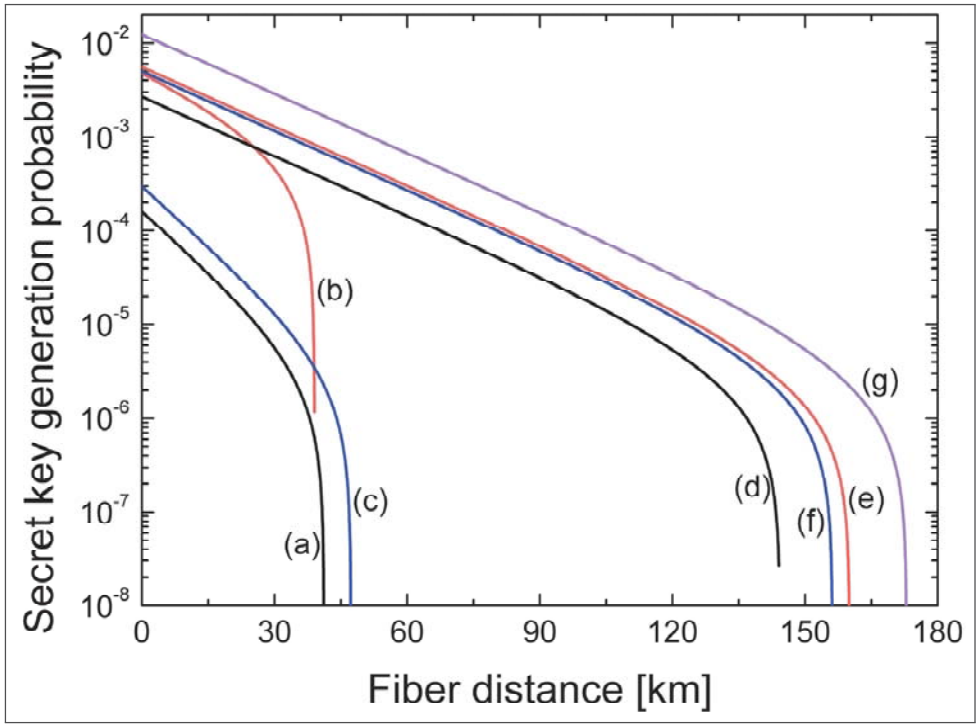

Figure 4.10: Simulation of the secret key generation probability for a BB84-based QKD system considering: GLLP analysis with (a) faint laser source, (b) SPDC-based HPS, and (c) Linear-Optic HPS; decoy states method with (d) faint laser source, (e) SPDC-based HPS, and (f) Linear-Optic HPS; and (g) a true single-photon source.

The reported Linear-Optic HPS [68], when conditioned to the temporal selection of pulses at the operational point, exhibits improved statistics when compared to that of coherent states. The output states may be regarded as squeezed photon-number distribution weak coherent states since the second-order correlation function at zero time is less than one [5, 139]. The present QKD link simulation reveals that, under GLLP analysis, the proposed source increases the maximum achievable distance of a QKD link with a factor of 1.15 when compared to both the faint laser source and SPDC-based HPS. Considering short links, the secret key generation probability of the source

is (at least 1.86 times) greater than for the faint laser source, while largely overcome by the SPDC-based HPS (with a factor 16). Considering the decoy states approach, we found that the proposed source outperforms the faint laser source in secret key generation probability and in distance. Its performance is also highly competitive with state-of-the-art SPDC-based HPS concerning both parameters. The maximum achievable distance is slightly shorter (4 km, corresponding to a length reduction of 2.5%) and the secret key generation probability presents a small penalty on the simulation. Parameters taken from [87] were also tested with qualitatively similar results not shown in the figure.

5
Sub-Poisson Statistic Photon Stream Heralded at a Hong-Ou-Mandel Interference Peak

As we show throughout this chapter, the HOM dip counterpart, the HOM *peak*, can be observed in a modified version of the Hong-Ou-Mandel interferometer fed with weak coherent states. The peak is characterized by an increase in the coincidence events between detectors placed at the output of the interferometer when the wave-packets overlap. Even though this phenomenon is purely classical as it involves the interference of classical weak coherent states in a beam splitter, the higher coincidence rate indicates that, by time tuning the interferometer, it is possible to post-select states which are more likely to take on different output paths after the interaction. Following the findings of Ferreira da Silva *et al.* [68], we attempted to herald the presence of a photon in one of the output arms of the interferometer given a detection on the opposite output arm.

Let us consider the modified Hong-Ou-Mandel interferometer fed with weak coherent states, as depicted in Fig. 5.1, in which a second beam splitter is connected to spatial mode c and Single-Photon Avalanche Diodes (SPADs) operating in gated-mode are connected to spatial modes f and g. An electronic unit is responsible for sweeping the relative temporal delay between detections and also accumulating the coincidence events. A polarizing beam splitter (PBS) and an additional SPAD are used to guarantee that the polarization of the photons is matched: the counts in the auxiliary SPAD connected to the PBS are minimized down to the detector's noise floor. This condition is a sufficient one for the visualization of the two-photon interference effect [160].

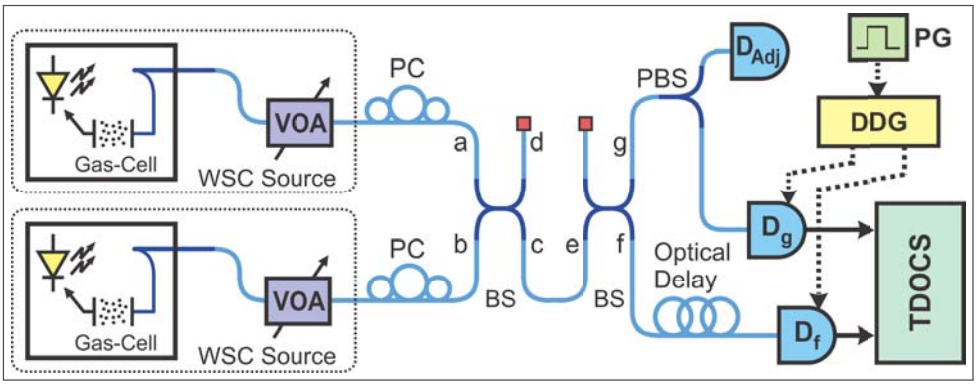

Figure 5.1: Modified HOM interferometer. An additional beam splitter is connected to output spatial mode c of the first beam splitter and the SPADs are connected to its outputs. An electronic unit is responsible for sweeping the relative temporal delay between detections and storing the coincidence events. VOA: Variable Optical Attenuator, PBS: Polarization Beam Splitter, D_{adj}: polarization alignment SPAD, D_n: SPAD at spatial mode n, PC: Mechanical Polarization Controller.

The case of interest is $|\psi_{in}\rangle = |1_a, 1_b\rangle = \hat{a}_a^\dagger \hat{a}_b^\dagger |0\rangle$ representing two photons entering the interferometer from input spatial modes a and b respectively. In the Heisenberg picture [162], the beam splitter transformation acts on the creation operators as

$$\hat{a}_a^\dagger \rightarrow \frac{1}{\sqrt{2}}\left(\hat{a}_c^\dagger + i\hat{a}_d^\dagger\right) \quad ; \quad \hat{a}_b^\dagger \rightarrow \frac{1}{\sqrt{2}}\left(i\hat{a}_c^\dagger + \hat{a}_d^\dagger\right). \tag{5.1}$$

Two-photon interference in the Hong-Ou-Mandel interferometer depends on the indistinguishability between the wave packets that describe the interaction. By enforcing a long-enough relative delay between the detections on spatial modes g and f, one can establish the condition of distinguishability. Therefore, we analyze the two cases, that of distinguishable and that of indistinguishable photons, separately. For the first case, the state that describes the system after the interaction on the first beam splitter, $|\psi_{partial}\rangle$, reads

$$|\psi_{partial}\rangle = \frac{1}{2}\left(i\hat{a}_c^\dagger\hat{a}_c^\dagger + \hat{a}_c^\dagger\hat{a}_d^\dagger - \hat{a}_d^\dagger\hat{a}_c^\dagger + i\hat{a}_d^\dagger\hat{a}_d^\dagger\right)|0\rangle. \tag{5.2}$$

We note that the middle terms are not canceled out since the states are distinguishable and $\hat{a}_c^\dagger\hat{a}_d^\dagger \neq \hat{a}_d^\dagger\hat{a}_c^\dagger$. The second beam splitter transforms the creation operators in the same fashion as the first with notation changing accordingly due to the different spatial modes label. The final output state

reads

$$|\psi_{out}\rangle = \Big[\frac{i}{4}\big(\hat{a}_f^\dagger\hat{a}_f^\dagger + i\hat{a}_f^\dagger\hat{a}_g^\dagger + i\hat{a}_g^\dagger\hat{a}_f^\dagger - \hat{a}_g^\dagger\hat{a}_g^\dagger\big) + \\ + \frac{1}{2\sqrt{2}}\big(i\hat{a}_g^\dagger\hat{a}_d^\dagger + \hat{a}_f^\dagger\hat{a}_d^\dagger - \hat{a}_d^\dagger\hat{a}_f^\dagger - i\hat{a}_d^\dagger\hat{a}_g^\dagger\big) + \frac{1}{2}i\hat{a}_d^\dagger\hat{a}_d^\dagger\Big]|0\rangle\,. \tag{5.3}$$

From this result, we can calculate the probability of a photon impinging on the detector placed at output spatial mode g. We associate a detection to the presence of at least one photon in this spatial mode. Since the maximum number of photons per spatial mode, in our case, is 2, the upper bound of the summation can be restricted and we find the probability of a detection recorded on D_g to be

$$P_g^{det} = \sum_{i=1}^{2} \langle\psi_{out}|i_g\rangle\,\langle i_g|\psi_{out}\rangle = \frac{7}{16}. \tag{5.4}$$

We associate the probability of a coincidence count event between detectors g and f to the probability of one or more photons to be present in mode f conditioned to one or more photons being present in mode g. The result is $P_{coinc} = P_g^{det}\cdot P_{f|g}^{det} = 7/16\cdot 2/7 = 2/16$. In the second case, namely the one in which the photons are indistinguishable, we note that the middle term in Eq. 5.3 cancels out since one cannot distinguish between $\hat{a}_f^\dagger\hat{a}_d^\dagger$ and $\hat{a}_d^\dagger\hat{a}_f^\dagger$ or $\hat{a}_g^\dagger\hat{a}_d^\dagger$ and $\hat{a}_d^\dagger\hat{a}_g^\dagger$. After re-normalization, the output state in the indistinguishable case reads

$$|\psi_{out}\rangle = \left[\frac{i}{2\sqrt{2}}\big(\hat{a}_f^\dagger\hat{a}_f^\dagger - \hat{a}_g^\dagger\hat{a}_g^\dagger\big) + \frac{i}{2}\hat{a}_f^\dagger\hat{a}_g^\dagger + \frac{i}{\sqrt{2}}\hat{a}_d^\dagger\hat{a}_d^\dagger\right]|0\rangle\,. \tag{5.5}$$

We can calculate the same probabilities as before and find that a detection on output spatial mode g occurs, now, with probability 6/16. Coincidence count events, on the other hand, occur with probability $P_{coinc} = P_g^{det}\cdot P_{f|g}^{det} = 6/16\cdot 4/6 = 4/16$.

The effect on the coincidence count events between detectors g and f, as one sweeps the time delay between the detections in the analyzed conditions, is an increase by a factor of two due to the photons becoming indistinguishable, i.e., the photons are more likely to take on different output paths within the condition of overlapping wave packets, in contrast with the effect observed in the traditional Hong-Ou-Mandel interferometer. The expected interferogram is a coincidence peak in contrast with the coincidence dip of usual HOM experiments.

5.1 Simulation Results with the Spatio-Temporal Wave-Packet Description

The spatio-temporal wave-packet formalism developed in Section 2.5 permits one to associate the probability of a coincidence photon detection to the wave-packet of the input states. Furthermore, from the expression of the joint photon-detection probability, we have mathematically extracted the spectral information of the states directed to the Hong-Ou-Mandel interferometer. A distinct feature that have been highlighted in the end of the theoretical development of Section 2.5 is that, independently from the wave-packet format, the joint photon-detection probability expression recovers the vanishing character of the Hong-Ou-Mandel dip in $\tau = 0$. When we employ the same formalism to the case of the modified Hong-Ou-Mandel interferometer, the results should hold their consistency.

Let us first present, in Fig.5.2, the numerical simulation results when gaussian wave-packets are considered for the input frequency-displaced states entering a Hong-Ou-Mandel interferometer. The frequency displacement is set to 20MHz. As expected, the probability of a coincidence event is zero at $\tau = 0$ and raises to a maximum at $\tau = pi/\Delta = 0.16\mu$s.

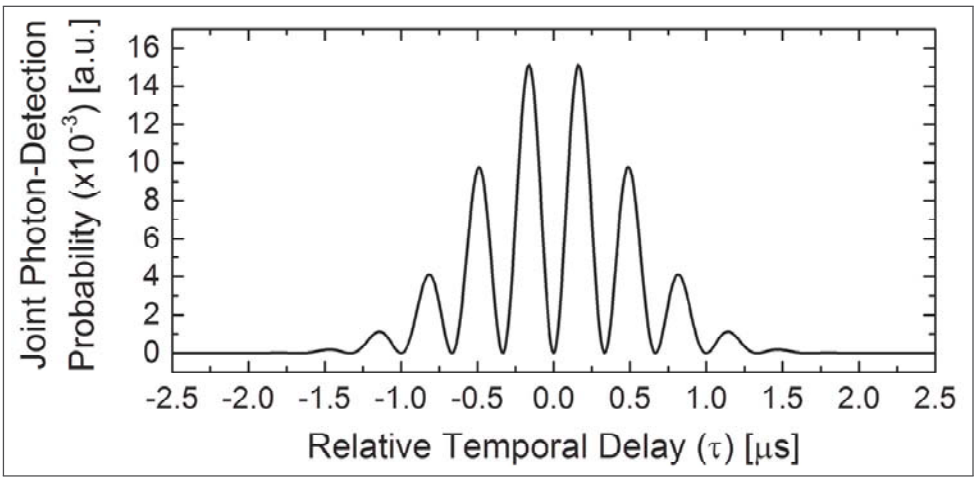

Figure 5.2: Numerical Simulation results when a gaussian wave-packet is assumed for the input states of a conventional Hong-Ou-Mandel interferometer. The probability is normalized to 1.

In the case of the modified Hong-Ou-Mandel interferometer, we are interested in the coincidence event probability of detectors D_f and D_g placed at the output of the second symmetric beam splitter. We must, therefore, attempt to write the electric field operators for modes f and g as a function of the input spatio-temporal wave-packets of modes a and b. We recall that the

electric field operators of modes c and d may be written as:

$$\begin{aligned}\hat{E}_c^{(-)}(t) &= \tfrac{1}{\sqrt{2}}\left(\hat{E}_a^{(-)}(t) + i\hat{E}_b^{(-)}(t)\right);\\ \hat{E}_d^{(-)}(t) &= \tfrac{1}{\sqrt{2}}\left(i\hat{E}_a^{(-)}(t) + \hat{E}_b^{(-)}(t)\right).\end{aligned} \tag{5.6}$$

The electric field operators of modes g and f, in turn, can be written as a function of the electric field operators of modes c and e, where we named mode e the disconnected input mode of the second beam splitter of the modified Hong-Ou-Mandel interferometer:

$$\begin{aligned}\hat{E}_f^{(-)}(t) &= \tfrac{1}{\sqrt{2}}\left(i\hat{E}_c^{(-)}(t) + \hat{E}_e^{(-)}(t)\right);\\ \hat{E}_g^{(-)}(t) &= \tfrac{1}{\sqrt{2}}\left(\hat{E}_c^{(-)}(t) + i\hat{E}_e^{(-)}(t)\right).\end{aligned} \tag{5.7}$$

Combining these equations, we find that

$$\begin{aligned}\hat{E}_f^{(-)}(t) &= \tfrac{i}{2}\left(\hat{E}_a^{(-)}(t) + i\hat{E}_b^{(-)}(t)\right) + \tfrac{1}{\sqrt{2}}\hat{E}_e^{(-)}(t);\\ \hat{E}_g^{(-)}(t) &= \tfrac{1}{2}\left(\hat{E}_a^{(-)}(t) + i\hat{E}_b^{(-)}(t)\right) + \tfrac{i}{\sqrt{2}}\hat{E}_e^{(-)}(t).\end{aligned} \tag{5.8}$$

Once again, we are interested in the joint photon-detection probability at modes f and g given that two single-photons are directed each to a different input port of the modified Hong-Ou-Mandel interferometer. The expression is quite similar to the one for the usual Hong-Ou-Mandel interferometer, but with a slight change of notation due to the fact that the modes are different:

$$\begin{aligned}&P_{joint}(t,\tau) = g_{f,g}(t, t+\tau) =\\ &\langle 0|\,\hat{a}_a\hat{a}_b\hat{E}_f^{(-)}(t)\hat{E}_g^{(-)}(t+\tau)\hat{E}_f^{(+)}(t+\tau)\hat{E}_g^{(+)}(t)\hat{a}_b^{\dagger}\hat{a}_a^{\dagger}\,|0\rangle.\end{aligned} \tag{5.9}$$

When we substitute the expression for the electric field operators on modes f and g as a function of the input wave-packets, the result yields[1]

$$\begin{aligned}P_{joint}(t,\tau) &= g_{f,g}(t, t+\tau) =\\ &= \tfrac{1}{16}|\varepsilon_a(t+\tau)\,\varepsilon_b(t) + \varepsilon_b(t+\tau)\,\varepsilon_a(t)\,|^2.\end{aligned} \tag{5.10}$$

One of the most interesting features of this result is that, no matter the shape of the wave-packet (its mathematical expression), the *joint photon-detection probability* is at its maximum value at $\tau = 0$, characterizing the Hong-Ou-Mandel dip and showing that the results of the wave-packet formalism are consistent with the Fock states analysis. The numerical simulation of the new expression for the joint photon-detection probabilty have been performed with the same parameters of Fig.5.2 and are depicted in Fig.5.3. The probability

[1]Refer to Appendix 7.17 for complete mathematical development.

approaches its peak value as τ goes to zero and goes to zero when $\tau = \pi/\Delta$.

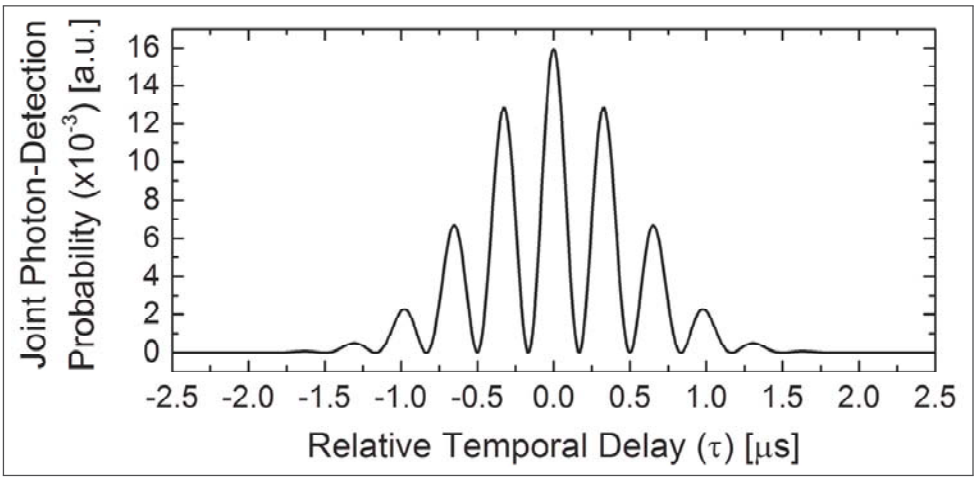

Figure 5.3: Numerical Simulation results when a gaussian wave-packet is assumed for the input states of a modified Hong-Ou-Mandel interferometer. The probability is normalized to 1.

5.2 Experimental Results

To perform the experimental verification of the above theoretical predictions, the optical output of a frequency-locked CW semiconductor laser centered at 1551.7 nm was directed to one of the input ports of the first symmetric beam splitter through a polarization controller and a variable optical attenuator. The remaining input port of the beam splitter was connected to another frequency-locked CW semiconductor laser centered at the same wavelength as the first. Frequency stabilization is possible by locking the laser wavelength to the absorption line of a high-Q factor gas-cell through a PID control loop. Polarization and intensity control was also enforced onto the second laser to guarantee the indistinguishable and few-photon conditions necessary for observation of the two-photon interference phenomenon with weak-coherent states [160]. The result of the experiment is presented in Fig. 5.4, where the red curve corresponds to the normalized HOM dip acquired by placing detectors at spatial modes c and d, and the black curve corresponds to the HOM peak when the detectors are placed at spatial modes f and g (refer to Fig. 5.1). Both detectors are set to 15% efficiency and 4-ns wide gates which corresponds to the best compromise between dark counts (on the order of 10^{-5} per detection gate) and efficiency.

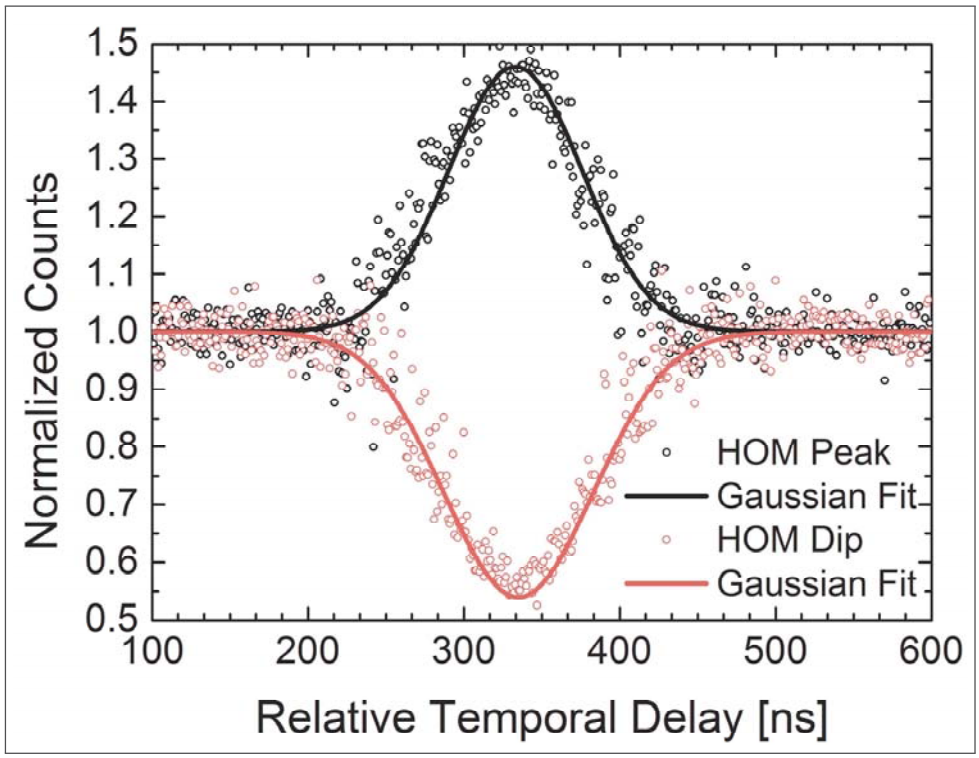

Figure 5.4: HOM dip (red) and HOM peak (black) interferogram. The HOM dip is acquired by placing detectors at spatial modes c and d, whereas the HOM peak is acquired by placing the detectors at spatial modes f and g.

In order to guarantee that the relative temporal delay for both experiments was identical as observed in Fig. 5.4, the same optical fibre loop was employed to impose an optical delay between the output of the second beam splitter and the input of the SPAD, which corresponds to ~ 343 ns. We see that the intrinsic multi-photon limitation associated to employing weak-coherent states in two-photon interference experiments [7] also affects the HOM peak, the visibility does not reach 100% and is limited by 50% [138]. In Fig. 5.5, the interferogram for both the HOM dip and the HOM peak are presented when the frequency displacement condition is enforced. We used the model developed in [148] for data-fitting the interferogram with good correspondence. We also assumed gaussian wave packets and assured that the average number of photons per gate μ was kept smaller than the 0.2 limitation of the theoretical model [148].

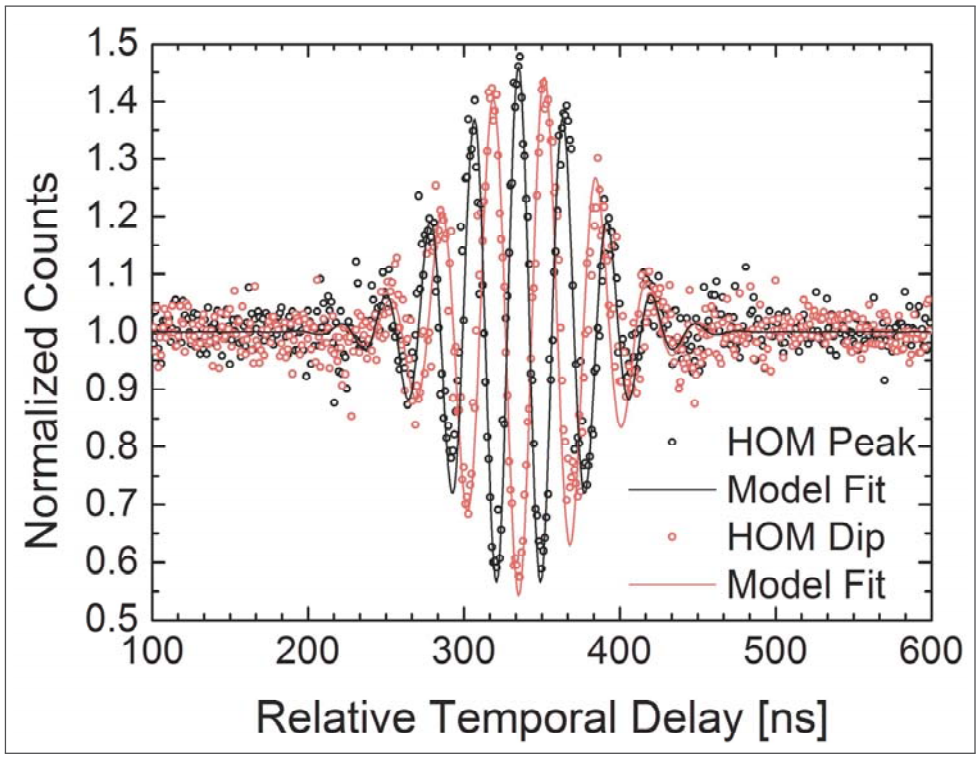

Figure 5.5: Beat pattern modulating the HOM dip (red) and the HOM peak (black) interferogram curves in the case of frequency-displaced wave packets.

The slight difference in the beat frequency between both experiments is due to a small drift in the frequency-locking system which, however undesired, does not overshadows the result which is the beat pattern modulating the HOM peak as expected. We used the model developed in [148] for data-fitting the interferogram with good correspondence. We also assumed gaussian wave packets and assured that the average number of photons per gate μ was kept smaller than the 0.2 limitation of the theoretical model [148].

The experimental results clearly advocate that, from a heralded source point of view, one is able to time tune the heralding event to match the Hong-Ou-Mandel peak or any other region of the interferogram. Conversely, one could also herald a state at the Hong-Ou-Mandel dip. This is important in order to compare the results of $g^{(2)}(0)$ for each case in the light of quantum coherence theory. To conduct the HBT experiment and, thus, experimentally determine the value of $g^{(2)}(0)$, we consider the detector D_g as a heralder for the presence of a photon in spatial mode f: we are interested in determining the multi- to single-photon ratio in this beam conditioned to a detection in D_g.

To perform the Hanburry-Brown and Twiss experiment[2], two SPADs (A

[2]Refer to Appendix 7.16.

and B) are placed at both spatial output modes of another symmetric beam splitter. The input ports of this beam splitter are arranged so that one of them is connected to spatial mode f and the other is left unconnected. The experimental setup is clarified in Fig. 5.6. To eliminate experimental complications due to the frequency-locking loop, we introduce a self-homodyne setup with a single laser source [68]: both frequency-locked lasers are substituted by a single semiconductor CW laser; the output is divided by an optical beam splitter and the coherent states in each arm are uncorrelated by an optical delay line approximately 8-kilometers long to account for the temporal coherence of the source; the independent states are then directed to the modified HOM interferometer which, after the modifications, acts as a heralded source connected to a HBT experiment. The complete setup is depicted in Fig. 5.6. This new setup has the advantages of employing a single laser source and the absence of frequency-locking control which greatly simplifies the experimental apparatus. Other than the fact that the new laser source employed is spectrally narrower when compared to the former frequency-locked lasers, no fundamental changes are made to the experiment.

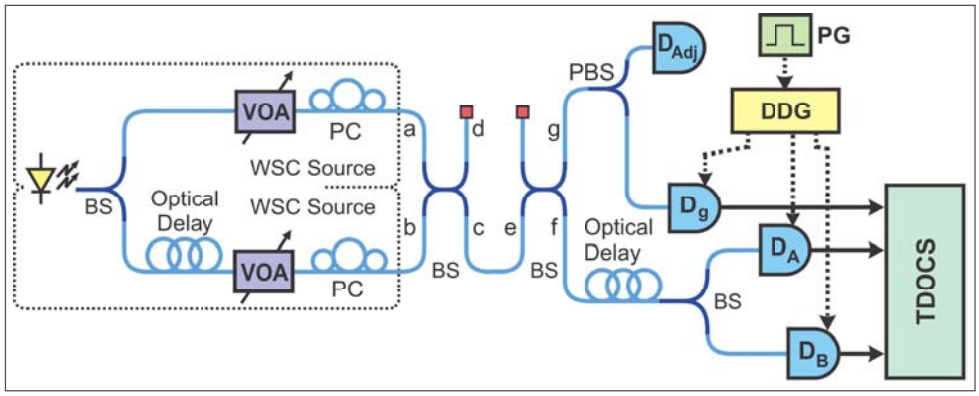

Figure 5.6: Simplified experimental apparatus employing a single laser source in a self-homodyne configuration. The weak coherent states are uncorrelated. The connections necessary for the HBT experiment are depicted: the connection of an additional beam splitter at spatial mode f; and two SPADs (D_A and D_B) at its outputs.

In Fig. 5.7, the results of the HBT experiment are depicted. The value of $g^{(2)}(0)$[3] was calculated for different time-tuned heralding instants covering the whole region of overlapping wave-packets and also outside this region. The experiment was performed for the HOM dip (Fig. 5.7-a) and for the HOM peak(Fig. 5.7-a). For clarity, we plot, for each value of the experimentally determined $g^{(2)}(0)$, the respective accumulated counts on both D_A and D_B

[3]Refer to Appendix 7.16.

conditioned to a delayed detection in g. Note that these counts represent the HOM interferogram between D_g and D_A, and between D_g and D_B, respectively. Upon close inspection of the experimental apparatus depicted in Fig.5.6 for the HBT experiment and in Fig.5.1, one can identify that, apart from the intrinsic optical loss induced by the symmetric beam splitter, the setup is also capable of tracing the HOM interferogram.

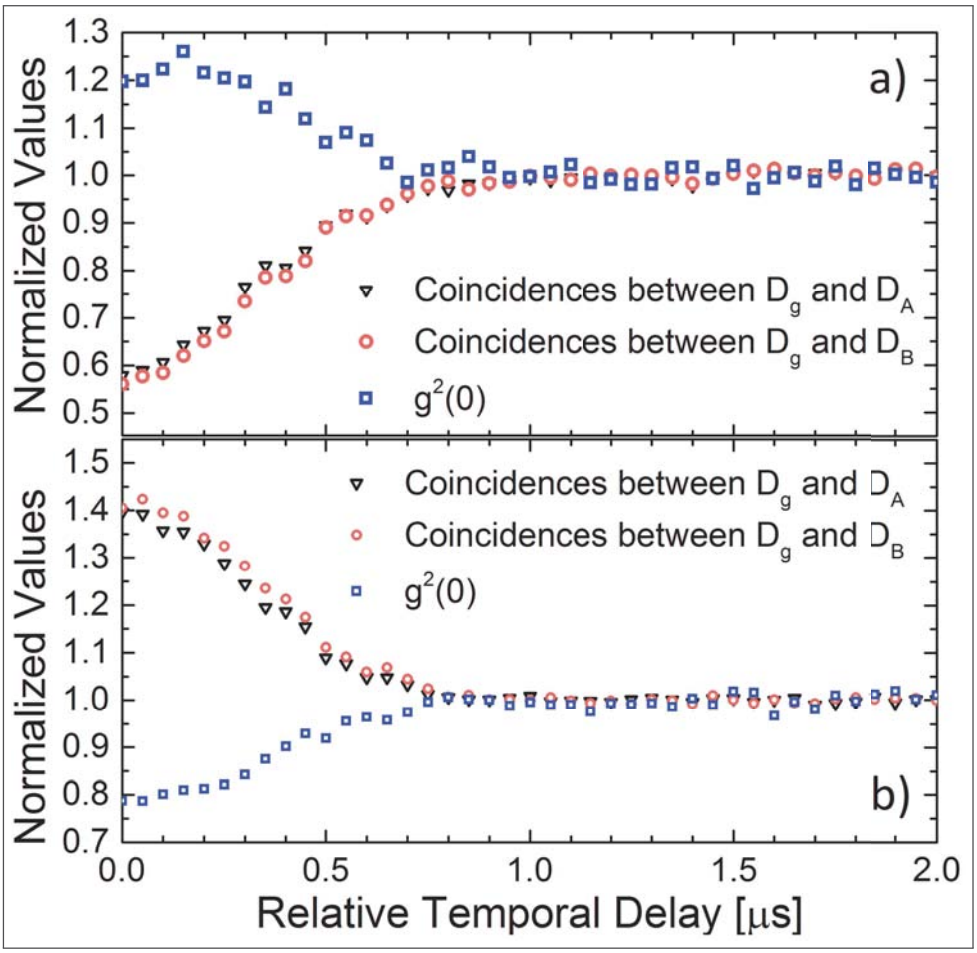

Figure 5.7: Experimentally determined values of $g^{(2)}(0)$ (blue squares) for different time-tuned heralding temporal delays in the HBT. The values are calculated for both the HOM dip (a) and the HOM peak (b), as indicated by the coincidences between D_g and D_A (black triangles) and between D_g and D_B (red circles).

The results clearly indicate a difference in the nature of the states heralded at three distinct regions: the HOM dip; the HOM peak; and the region of distinguishable state in which the wave-packets are not overlapped. As expected, when the states are distinguishable, no variation of $g^{(2)}(0)$ is observed and it is tied to the value of 1 corresponding to states with Poisson photon statistics such as the coherent states. An incoherent mix of coherent states at the input of a beam splitter produce an incoherent mix of coherent

states at the output so $g^{(2)}(0) = 1$ [5]. When the heralding instant matches the HOM dip, on the other hand, we see that the higher probability of states to take on the same path cause the photon statistic of the heralded states to follow a super-Poisson distribution, a result confirmed by $g^{(2)}(0)$ greater than 1. Conversely, in the HOM peak, the states are more likely to take on different output paths so a herald event is likely to announce a light pulse containing at least one photon and, with the condition of weak coherent states satisfied, unlikely to announce a multi-photon pulse. The photon statistics of the heralded states in this case follow a sub-Poisson distribution with $g^{(2)}(0)$ less than 1.

6
Conclusions

Even though we do not attempt to answer the ill-posed question which is rascally dodged right at the beginning of the document ("What is, after all, a photon?"), we attempt to, once again, back the statements which were drawn: quantum optics is a rich and surprising field which allows one to asses purely quantum effects in straightforward linear-optic setups. Linear-optic two-photon interference is capable of putting us closer to the answer – or to *an* answer – to the question we all wish to address.

The spectrum of a photonic wave-packet can be perceived from the analysis of the coincidence events in a Hong-Ou-Mandel interferometer. The so-called Few-Photon Fourier-Transform Spectroscopy offers the means to analysing unknown faint light pulses with high-resolution. Its mathematical modelling is in close correspondence with the experimental results and figures as a simple and resourceful spectral characterization technique [160].

Squeezed states of light which follow a sub-Poisson distribution are especially interesting since they approximate the single-photon condition. The fact that such states can be produced with a simple linear optic setup and a conditioned heralding detection is exciting since it eliminates the need of complicated setups involving non-linear effects with high-energy pump sources. Our claim that the heralding event time-tuned to a coincidence peak after the two-photon interference of classical states at an optical beam splitter can indeed yield states with non-classical photon distribution, such as sub-Poisson, is grounded by the results of $g^{(2)}(0) = 0.78$ for the HOM peak, $g^{(2)}(0) = 1.25$ for the HOM dip, and $g^{(2)}(0) = 1$ when no quantum interference takes place [163].

The Linear-Optic Heralded Photon Source broadens the plethora of resources for quantum communication posing as an alternative low-cost and experimentally-simple source. The all-fiber telecom-compatible design, its sub-poissonian character, and the rather simple setup make it a proper choice for long-distance quantum communication. The performance of the Linear-Optic HPS, evaluated in a simulation of a BB84-like QKD section, reveals that the proposed source outperforms the faint laser source and is highly competitive with the SPDC-based HPS [68].

6.1 Future Works

A distinct feature of sub-poisson states is that, when they are directed to a Hong-Ou-Mandel interferometer, the visibility of the coincidence dip is higher than 50%. This is related to the higher rate of single-photon to multi-photon pulses when contrasted with classical poisson states which are limited to a 50% visibility. When we mention the fact that sub-poisson states have been heralded in a time-tuned modified Hong-Ou-Mandel interferometer, one of the most immediate concerns is how would the HOM interferogram of such states look like. We know that the visibility is as close to 100% as the sub-Poisson state is close to the ideal single-photon and would expect the linear-optic heralded states to be in between 50% and 100% visibility. Since this is the most exciting prognosis from the results related to the Linear-Optic Heralded Photon source and hereby reported, we leave it as a future work. Not only the HOM interference between two linear-optic heralded states – which requires the development of two linear-optic heralded source – , but also between a linear-optic heralded state and a classical weak coherent state and from states heralded in an SPDC-based source. From the Few-Photon Fourier Transform Spectroscopy point of view, we believe that, once it has been demonstrated that weak coherent state sources can be spectrally characterized, we would wish to spectrally characterize single-photon sources such as SPDC-based Heralded Photon Sources, and quantum dot sources, so we also leave it as a future point of investigation.

7
Appendices

7.1
Electric Field Quantization, Annihilation and Creation Operators and the Quantized Harmonic Oscillator Hamiltonian

The single-mode expression of the electric and magnetic fields, oscillating along the x and y axis inside the cavity, respectively, are given by [5, 140]

$$\begin{aligned} E_x(z,t) &= \left(\frac{2\omega^2}{\epsilon_0\Omega}\right) q(t)\sin(kz), \\ B_y(z,t) &= \left(\frac{\mu_0\epsilon_0}{k}\right)\left(\frac{2\omega^2}{\epsilon_0\Omega}\right) p(t)\cos(kz). \end{aligned} \tag{7.1}$$

The classical field energy, or Hamiltonian, of a single-mode field contained in a cavity which is assumed to have volume Ω is

$$H = \Omega\frac{\langle E\rangle^2 + \langle B\rangle^2}{8\pi}, \tag{7.2}$$

which, using the relation $\langle\sin(\cdot)\rangle^2 = \langle\cos(\cdot)\rangle^2 = 1/2$, yields

$$H = \frac{1}{2}\left(p^2 + \omega^2 q^2\right). \tag{7.3}$$

The variables p and q that represent linear momentum and position, respectively, are canonically conjugate and, therefore, using the correspondence rule, one replaces them by their equivalent $\hat{p}$ and $\hat{q}$ operators [5]. Operators $\hat{p}$ and $\hat{q}$ are Hermitian and obey the commutation relation $[\hat{q},\hat{p}] = i\hbar\hat{I}$. The Hamiltonian, after the replacements, reads

$$\hat{H} = \frac{1}{2}\left(\hat{p}^2 + \omega^2\hat{q}^2\right). \tag{7.4}$$

Writing the commutation relation of annihilation and creation operators in terms of the linear momentum and position operators, for which the

commutation relation is known, yields

$$\begin{aligned}\left[\hat{a},\hat{a}^{\dagger}\right] &= \left[(2\hbar\omega)^{-1/2}(\omega\hat{q}+i\hat{p}),(2\hbar\omega)^{-1/2}(\hat{q}-i\hat{p})\right]\\ &= (2\hbar\omega)^{-1}(-i\omega\hat{q}\hat{p}+i\omega\hat{p}\hat{q}+-i\omega\hat{q}\hat{p}+i\omega\hat{p}\hat{q})\\ &= \frac{-i}{\hbar}[\hat{q},\hat{p}]\\ &= \hat{I}.\end{aligned} \tag{7.5}$$

Now, we express the operators $\hat{p}$ and $\hat{q}$ in terms of the annihilation and creation operators:

$$\begin{aligned}\hat{p} &= \frac{1}{2}\left(\hat{a}-\hat{a}^{\dagger}\right)(2\hbar\omega)^{1/2}i^{-1};\\ \hat{q} &= \frac{1}{2}\left(\hat{a}+\hat{a}^{\dagger}\right)(2\hbar\omega)^{1/2}\omega^{-1}.\end{aligned} \tag{7.6}$$

Taking the square of each operator separately, yields

$$\begin{aligned}\hat{p}^2 &= \left(\frac{1}{2}\left(\hat{a}-\hat{a}^{\dagger}\right)(2\hbar\omega)^{1/2}i^{-1}\right)^2\\ &= -\frac{1}{4}(2\hbar\omega)\left(\hat{a}\hat{a}-\hat{a}\hat{a}^{\dagger}-\hat{a}^{\dagger}\hat{a}+\hat{a}^{\dagger}\hat{a}^{\dagger}\right);\\ \hat{q}^2 &= \left(\frac{1}{2}\left(\hat{a}+\hat{a}^{\dagger}\right)(2\hbar\omega)^{1/2}\omega^{-1}\right)^2\\ &= \frac{1}{4\omega^2}(2\hbar\omega)\left(\hat{a}\hat{a}+\hat{a}\hat{a}^{\dagger}+\hat{a}^{\dagger}\hat{a}+\hat{a}^{\dagger}\hat{a}^{\dagger}\right).\end{aligned} \tag{7.7}$$

Substituting these expressions in the Hamiltonian form

$$\begin{aligned}\frac{1}{2}\left(\hat{p}^2+\omega^2\hat{q}^2\right) &= \frac{\hbar\omega}{2}\left(\hat{a}\hat{a}^{\dagger}+\hat{a}^{\dagger}\hat{a}\right)\\ &= \frac{\hbar\omega}{2}\left(\hat{a}\hat{a}^{\dagger}+\hat{a}^{\dagger}\hat{a}+\hat{a}^{\dagger}\hat{a}-\hat{a}^{\dagger}\hat{a}\right)\\ &= \frac{\hbar\omega}{2}\left(2\hat{a}^{\dagger}\hat{a}+\left[\hat{a},\hat{a}^{\dagger}\right]\right)\\ &= \hbar\omega\left(\hat{a}^{\dagger}\hat{a}+\frac{1}{2}\hat{I}\right),\end{aligned} \tag{7.8}$$

which is the final simplified form of the quantized electric field Hamiltonian operator expressed with annihilation and creation operators. Usually, the identity operator is dropped and one writes $\hbar\omega\left(\hat{a}^{\dagger}\hat{a}+\frac{1}{2}\right)$.

7.2
Effects of the Annihilation and Creation Operators on the Harmonic Oscillator Hamiltonian, Zero-Point Energy, and the Effects of Applying the Annihilation and Creation Operators on Fock States

The commutation relation between the annihilation and creation operators can be used to reduce the number of steps in this particular mathematical development: $\left[\hat{a}, \hat{a}^\dagger\right] = 1 \rightarrow \hat{a}^\dagger\hat{a} = \hat{a}\hat{a}^\dagger - 1$. Let us, then, apply the creation operator to the Hamiltonian of the state of well-define number of photons:

$$\begin{aligned}
\hat{a}^\dagger\left(\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle\right) &= \hat{a}^\dagger E_n |n\rangle \\
\hbar\omega\left(\left(\hat{a}\hat{a}^\dagger - 1\right)\hat{a}^\dagger + \frac{1}{2}\hat{a}^\dagger\right)|n\rangle &= E_n\hat{a}^\dagger|n\rangle \\
\hbar\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)\hat{a}^\dagger|n\rangle &= \left(E_n + \hbar\omega\right)\hat{a}^\dagger|n\rangle \\
\hat{H}\left(\hat{a}^\dagger|n\rangle\right) &= \left(E_n + \hbar\omega\right)\left(\hat{a}^\dagger|n\rangle\right).
\end{aligned} \tag{7.9}$$

The exact same procedure yield the corresponding result when one applies the annihilation operator with the exception that we use the inverse of the above relation derived from the commutator $\hat{a}$ and $\hat{a}^\dagger$, i.e., $\hat{a}\hat{a}^\dagger = \hat{a}^\dagger\hat{a} + 1$:

$$\begin{aligned}
\hat{a}\left(\hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle\right) &= \hat{a}E_n|n\rangle \\
\hbar\omega\left(\left(\hat{a}^\dagger\hat{a} + 1\right)\hat{a} + \frac{1}{2}\hat{a}\right)|n\rangle &= E_n\hat{a}|n\rangle \\
\hbar\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)\hat{a}|n\rangle &= \left(E_n - \hbar\omega\right)\hat{a}|n\rangle \\
\hat{H}\left(\hat{a}|n\rangle\right) &= \left(E_n - \hbar\omega\right)\left(\hat{a}|n\rangle\right).
\end{aligned} \tag{7.10}$$

The zero-point energy, or vacuum energy, is the eigenvalue associated to the vacuum state when operated by the Hamiltonian:

$$\begin{aligned}
H|0\rangle &= \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|0\rangle \\
&= \hbar\omega\hat{a}^\dagger\hat{a}|0\rangle + \frac{\hbar\omega}{2}|0\rangle \\
&= \hbar\omega\hat{a}^\dagger \times 0 + \frac{\hbar\omega}{2}|0\rangle \\
&= \frac{\hbar\omega}{2}|0\rangle,
\end{aligned} \tag{7.11}$$

where we have used the defined relation $\hat{a}|0\rangle = 0$. Starting from $E_0 = \hbar\omega/2$ and knowing that $E_{n+1} = E_n + \hbar\omega$, we find that $E_n = \hbar\omega\left(n + 1/2\right) \forall n \in \mathbb{N}^0$. Going back to the Hamiltonian, we determine the form of the *number of photons*

operator, $\hat{n}$:

$$\begin{aligned} \hat{H}\left|n\right\rangle &= E_n\left|n\right\rangle \\ \hbar\omega\left(\hat{a}^\dagger\hat{a}+\frac{1}{2}\right)\left|n\right\rangle &= \hbar\omega\left(n+\frac{1}{2}\right)\left|n\right\rangle \\ \hat{a}^\dagger\hat{a}\left|n\right\rangle &= n\left|n\right\rangle \\ \hat{n}\left|n\right\rangle &= n\left|n\right\rangle. \end{aligned} \tag{7.12}$$

The number of photons operator is very useful in determining the result of operating the annihilation or creation operator over a state of well-defined number of photons. We know that $\hat{a}^\dagger\left|n\right\rangle = c_n\left|n+1\right\rangle$ and $\hat{a}\left|n\right\rangle = d_n\left|n-1\right\rangle$. Taking the inner product of $\hat{a}\left|n\right\rangle$ with itself yields

$$\left\langle n\right|\hat{a}^\dagger\hat{a}\left|n\right\rangle = \left\langle n\right|\hat{n}\left|n\right\rangle = n. \tag{7.13}$$

At the same time, however,

$$\left(\left\langle n\right|\hat{a}^\dagger\right)\left(\hat{a}\left|n\right\rangle\right) = \left\langle n-1\right|d_n^* d_n\left|n-1\right\rangle = \left|d_n\right|^2 \tag{7.14}$$

so we find $d_n = \sqrt{n}$. We now take the inner product of $\hat{a}^\dagger\left|n\right\rangle$ with itself

$$\left\langle n\right|\hat{a}\hat{a}^\dagger\left|n\right\rangle = \left\langle n\right|\hat{a}^\dagger\hat{a}+1\left|n\right\rangle = \left\langle n\right|\hat{n}+1\left|n\right\rangle = n+1 \tag{7.15}$$

to find that $c_n = \sqrt{n+1}$.

7.3 Time Dependency of the Annihilation and Creation Operators

In the Heisenberg picture, operators evolve in time while the states are time-independent which is in contrast with Schrödinger's interpretation, where the operators are independent of time and the states evolve in time [38, 162, 164]. Therefore, the time-dependence of annihilation and creation operators can be determined by examining Heisenberg's equation for an arbitrary operator A [5],

$$\frac{d\hat{A}}{dt} = \frac{i}{\hbar}\left[\hat{H},\hat{A}\right]. \tag{7.16}$$

Inputting the annihilation operator into Heisenberg's equation yields

$$\begin{aligned}\frac{d\hat{a}}{dt} &= \frac{i}{\hbar}\left[\hbar\omega\left(\hat{a}^{\dagger}\hat{a}+\frac{1}{2}\right),\hat{a}\right]\\ &= i\omega\left(\hat{a}^{\dagger}\hat{a}\hat{a}-\hat{a}\hat{a}^{\dagger}\hat{a}\right)\\ &= i\omega\left(\hat{a}^{\dagger}\hat{a}\hat{a}-\left(1+\hat{a}^{\dagger}\hat{a}\right)\hat{a}\right)\\ &= i\omega\left(\hat{a}^{\dagger}\hat{a}\hat{a}-\hat{a}^{\dagger}\hat{a}\hat{a}-\hat{a}\right)\\ &= -i\omega\hat{a},\end{aligned} \tag{7.17}$$

such that $\hat{a}(t) = \hat{a}(0)\, e^{-i\omega t}$. Analogously, for the creation operator, we have $\hat{a}^{\dagger}(t) = \hat{a}^{\dagger}(0)\, e^{i\omega t}$.

7.4 Expected Value and Uncertainty of the Electric Field Operator for Fock States

Using the second postulate of quantum mechanics, we can calculate the expected value of the electric field of a state of well-defined number of photons

$$\langle n|\,\hat{E}_x(t)\,|n\rangle = \varepsilon_0\left(\langle n|\,\hat{a}\,|n\rangle + \langle n|\,\hat{a}^{\dagger}\,|n\rangle\right), \tag{7.18}$$

where the time-dependence of the annihilation and creation is left implied. Since $\hat{a}^{\dagger}|n\rangle = \sqrt{n+1}\,|n+1\rangle$ and $\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle$, and due to the orthogonality of Fock states, we find that $\langle n|\,\hat{E}_x(t)\,|n\rangle = 0$. In the case of the expected value of the square of the field, we have

$$\begin{aligned}\langle n|\,\hat{E}_x^2(t)\,|n\rangle &= \varepsilon_0^2\,\langle n|\,\hat{a}^{\dagger}\hat{a}^{\dagger}+\hat{a}^{\dagger}\hat{a}+\hat{a}\hat{a}^{\dagger}+\hat{a}\hat{a}\,|n\rangle\\ &= \varepsilon_0^2\,\langle n|\,\hat{a}^{\dagger}\hat{a}^{\dagger}+\hat{a}\hat{a}+2\hat{a}^{\dagger}\hat{a}+1\,|n\rangle\\ &= \varepsilon_0^2\,(2n+1),\end{aligned} \tag{7.19}$$

where once again we used the relation $\hat{a}\hat{a}^{\dagger} = \hat{a}^{\dagger}\hat{a}+1$ and the orthogonality of Fock states. The uncertainty is calculated as the standard deviation of the observable,

$$\begin{aligned}\Delta\hat{E}_x(t) &= \sqrt{\langle n|\,\hat{E}_x^2(t)\,|n\rangle - \left(\langle n|\,\hat{E}_x(t)\,|n\rangle\right)^2}\\ &= \varepsilon_0^2\,(2n+1).\end{aligned} \tag{7.20}$$

7.5
Coherent States Mathematical Expression

The defined relation $\hat{a}\,|0\rangle = 0$ permits one to rewrite the eigenvalue equation with a change in the summation limits:

$$\begin{aligned}\alpha\,|\alpha\rangle &= \sum_{n=0}^{\infty} c_n \hat{a}\,|n\rangle \\ &= \sum_{n=1}^{\infty} c_n \sqrt{n}\,|n-1\rangle \\ &= \alpha \sum_{n=0}^{\infty} c_n\,|n\rangle\,,\end{aligned} \tag{7.21}$$

where we used the fact that $\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle$. Equaling term by term of the summation, we notice that a generic term can be written, without loss of generality: $c_n = \alpha/n^{-1/2}c_{n-1}$. The coefficient c_n can, therefore, be written as a function of c_0, for which n steps are necessary, so $c_n = \alpha^n\,(n!)^{-1/2}\,c_0$. The expression for the coherent states reads:

$$|\alpha\rangle = \sum_{n=0}^{\infty} c_0 \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{7.22}$$

We enforce the normalization condition over the above expression of the coherent states in order to determine the value of coefficient c_0:

$$\begin{aligned}\langle\alpha|\alpha\rangle &= 1 \\ &= |c_0|^2 \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{\alpha^m}{\sqrt{m!}}\frac{\alpha^n}{\sqrt{m!}}\,\langle m|n\rangle \\ &= |c_0|^2 \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{\sqrt{n!}} \\ &= |c_0|^2 e^{|\alpha|^2}. \\ \Rightarrow c_0 &= e^{-\frac{1}{2}|\alpha|^2}.\end{aligned} \tag{7.23}$$

7.6
Expected Value and Uncertainty of the Electric Field Operator for Coherent States

To calculate the uncertainty over the electric field of coherent states, we employ the same expressions presented in Appendix D but, instead of using the Fock state $|n\rangle$, we use the coherent state $|\alpha\rangle$. We remember that coherent states are eigenstates of the creation and annihilation operators associated to

eigenvalues α^* and α, respectively. The calculation follows:

$$\begin{aligned}\left(\langle\alpha|\,\hat{E}_x\,(t)\,|\alpha\rangle\right)^2 &= \left(\langle\alpha|\,\varepsilon_0\left(\hat{a}+\hat{a}^\dagger\right)|\alpha\rangle\right)^2 \\ &= \varepsilon_0^2\left(\langle\alpha|\,\hat{a}\,|\alpha\rangle + \langle\alpha|\,\hat{a}^\dagger\,|\alpha\rangle\right)^2 \\ &= \varepsilon_0^2\,(\alpha^*+\alpha)^2 \\ &= \varepsilon_0^2\left(\alpha^{*2}+\alpha^2+2|\alpha|^2\right)\end{aligned} \tag{7.24}$$

$$\begin{aligned}\langle\alpha|\,\hat{E}_x^2\,(t)\,|\alpha\rangle &= \langle\alpha|\,\varepsilon_0^2\left(\hat{a}+\hat{a}^\dagger\right)^2|\alpha\rangle \\ &= \varepsilon_0^2\,\langle\alpha|\,\hat{a}^\dagger\hat{a}^\dagger+\hat{a}^\dagger\hat{a}+\hat{a}\hat{a}^\dagger+\hat{a}\hat{a}\,|\alpha\rangle \\ &= \varepsilon_0^2\,\langle\alpha|\,\hat{a}^\dagger\hat{a}^\dagger+\hat{a}\hat{a}+2\hat{a}^\dagger\hat{a}+1\,|\alpha\rangle \\ &= \varepsilon_0^2\left(\alpha^{*2}+\alpha^2+2|\alpha|^2+1\right)\end{aligned} \tag{7.25}$$

$$\begin{aligned}\Delta\hat{E}_x\,(t) &= \sqrt{\langle\alpha|\,\hat{E}_x^2\,(t)\,|\alpha\rangle - \left(\langle\alpha|\,\hat{E}_x\,(t)\,|\alpha\rangle\right)^2} \\ &= \varepsilon_0\end{aligned} \tag{7.26}$$

7.7 Coherent States Photon Distribution

To calculate the probability of finding k photons in a coherent state, it is necessary to project the state $|\alpha\rangle$ over the operator $|k\,\rangle\langle\,k|$: $P_{|\alpha\rangle}\,(k) = \langle\alpha|k\rangle\langle k|\alpha\rangle$ [115]. This is equivalent to taking the modulus squared of the inner product between $\langle k|$ and $|\alpha\rangle$. Using the expression of the linear combination of Fock states to compose the coherent state $|\alpha\rangle$, we write

$$\left|\,\langle k|\alpha\rangle\,\right|^2 = e^{-|\alpha|^2}\sum_n \frac{\alpha^{2n}}{n!}\,\langle k|n\rangle\,. \tag{7.27}$$

Note that the terms of the summation are all equal to zero except when $n = k$ due to the orthogonality property of the Fock state basis. Therefore,

$$P_{|\alpha\rangle}\,(k) = e^{-|\alpha|^2}\frac{\alpha^{2k}}{k!}. \tag{7.28}$$

Setting $\mu = |\alpha|^2$, yields

$$P_{|\alpha\rangle}\,(k) = e^{-\mu}\frac{\mu^k}{k!}, \tag{7.29}$$

which corresponds to a Poisson distribution of parameter μ, the average number of photons occupying the state.

7.8 The Displacement Operator

The Baker-Hausdorff Formula [165, 166] states that when two operators $\hat{A}$ and $\hat{B}$ satisfy both $\left[\hat{A},\hat{B}\right] \neq 0$ and $\left[\hat{A},\left[\hat{A},\hat{B}\right]\right] = \left[\hat{B},\left[\hat{A},\hat{B}\right]\right] = 0$, then the following relation holds:

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}} e^{\hat{B}} e^{-\frac{1}{2}\left[\hat{A},\hat{B}\right]}. \tag{7.30}$$

In the case of annihilation and creation operators, we have $\left[\hat{a},\hat{a}^\dagger\right] = \hat{I}$, so the first condition is satisfied. As for the second, $\left[\hat{a},\hat{I}\right] = \hat{a}\hat{I} - \hat{I}\hat{a} = 0$ and $\left[\hat{a}^\dagger,\hat{I}\right] = \hat{a}^\dagger\hat{I} - \hat{I}\hat{a}^\dagger = 0$, so it is also satisfied. Therefore, the Displacement Operator [132, 167] reads $\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}$. The effect of this operator over the vacuum state is:

$$\begin{aligned}
e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}} |0\rangle &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} \sum_{\ell=0}^{\infty} \frac{\left(-\alpha^*\hat{a}\right)^\ell}{\ell!} |0\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} |0\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} \left(\hat{a}^\dagger\right)^n |0\rangle \\
&= e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \\
&= |\alpha\rangle .
\end{aligned} \tag{7.31}$$

7.9 Coherent States and Beam Splitters

A coherent state can be thought of as a displaced vacuum state in which case the displacement operator plays a fundamental role such that $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$. When the state $|\alpha\rangle$ enters a symmetrical beam splitter, we can employ the Heisenberg picture such that the operators are transformed according to the beam splitter transformation and the states are preserved. We recall that the beam splitter transformation works on the creation operators of each beam splitter input and output mode as

$$\begin{aligned}
\hat{a}_a^\dagger &\xrightarrow{BS} \frac{1}{\sqrt{2}}\left(\hat{a}_c^\dagger + i\hat{a}_d^\dagger\right) \\
\hat{a}_b^\dagger &\xrightarrow{BS} \frac{1}{\sqrt{2}}\left(i\hat{a}_c^\dagger + \hat{a}_d^\dagger\right),
\end{aligned} \tag{7.32}$$

with similar effect on the annihilation operators. We also recall the expression of the displacement operator which displaces the vacuum state on spatial mode a of a beam splitter to create a coherent state: $\hat{D}_a(\alpha) = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha \hat{a}_a^\dagger} e^{-\alpha^* \hat{a}_a}$. The effect of the beam splitter over a coherent state is, thus, described by:

$$\begin{aligned} |\alpha_a, 0_b\rangle = \\ \hat{D}_a(\alpha)\,|0_a, 0_b\rangle = \\ e^{-\frac{1}{2}|\alpha|^2} e^{\alpha \hat{a}_a^\dagger} e^{-\alpha^* \hat{a}_a}\,|0_a, 0_b\rangle \xrightarrow{BS} \\ e^{-\frac{1}{2}|\alpha|^2} e^{\frac{\alpha}{\sqrt{2}}\left(\hat{a}_c^\dagger + i\hat{a}_d^\dagger\right)} e^{\frac{-\alpha^*}{\sqrt{2}}(\hat{a}_c + i\hat{a}_d)}\,|0_c, 0_d\rangle = \\ e^{-\frac{1}{2}|\alpha|^2} e^{\frac{\alpha}{\sqrt{2}}\hat{a}_c^\dagger} e^{\frac{-\alpha^*}{\sqrt{2}}\hat{a}_c} e^{-\frac{1}{2}|\alpha|^2} e^{\frac{i\alpha}{\sqrt{2}}\hat{a}_d^\dagger} e^{\frac{-i\alpha^*}{\sqrt{2}}\hat{a}_d}\,|0_c, 0_d\rangle = \\ \hat{D}_c\left(\tfrac{\alpha}{\sqrt{2}}\right)\hat{D}_d\left(\tfrac{i\alpha}{\sqrt{2}}\right)|0_c, 0_d\rangle = \\ \left|\tfrac{\alpha}{\sqrt{2}}_c, \tfrac{i\alpha}{\sqrt{2}}_d\right\rangle. \end{aligned} \tag{7.33}$$

A coherent state entering a symmetrical beam splitter produces coherent states at both output spatial modes with field intensity obeying the transmissivity and reflectivity of the mirrors such as classical light.

7.10 Joint Photon-Detection Probability

The *joint photon-detection probability* is the probability of registering a coincidence event from detectors placed at the output of a symmetric beam splitter fed with two single-photons described by their spatio-temporal mode functions or spatio-temporal wave-packets. By taking the *joint photon-detection probability* expression and the relation between operators $E_c^{(\pm)}(t)$ and $E_d^{(\pm)}(t)$ with the wave-packets of the input photons, one gets

$$\begin{aligned} P_{joint}(t,\tau) = \\ \langle 0|\,\hat{a}_a \hat{a}_b \left[\tfrac{1}{\sqrt{2}}\left(\xi_a^*(t)\,\hat{a}_a^\dagger + i\xi_b^*(t)\,\hat{a}_b^\dagger\right)\right] \\ \left[\tfrac{1}{\sqrt{2}}\left(i\xi_a^*(t+\tau)\,\hat{a}_a^\dagger + \xi_b^*(t+\tau)\,\hat{a}_b^\dagger\right)\right] \\ \left[\tfrac{1}{\sqrt{2}}\left(\xi_a(t+\tau)\,\hat{a}_a + i\xi_b(t+\tau)\,\hat{a}_b\right)\right] \\ \left[\tfrac{1}{\sqrt{2}}\left(i\xi_a(t)\,\hat{a}_a + \xi_b(t)\,\hat{a}_b\right)\right]\hat{a}_b^\dagger \hat{a}_a^\dagger\,|0\rangle. \end{aligned} \tag{7.34}$$

The above expression can be further simplified to:

$$\begin{aligned} P_{joint}(t,\tau) = \\ &\langle 0|\,\hat{a}_a\hat{a}_b \\ &\left(\tfrac{j}{2}\xi_a^*(t)\,\hat{a}_a^\dagger\xi_a^*(t{+}\tau)\,\hat{a}_a^\dagger+\tfrac{1}{2}\xi_a^*(t)\,\hat{a}_a^\dagger\xi_b^*(t{+}\tau)\,\hat{a}_b^\dagger\right. \\ &\left.-\tfrac{1}{2}\xi_b^*(t)\,\hat{a}_b^\dagger\xi_a^*(t{+}\tau)\,\hat{a}_a^\dagger+\tfrac{j}{2}\xi_b^*(t)\,\hat{a}_b^\dagger\xi_b^*(t{+}\tau)\,\hat{a}_b^\dagger\right) \\ &\left(\tfrac{j}{2}\xi_a(t{+}\tau)\,\hat{a}_a^\dagger\xi_a(t)\,\hat{a}_a^\dagger+\tfrac{1}{2}\xi_a(t{+}\tau)\,\hat{a}_a^\dagger\xi_b(t)\,\hat{a}_b^\dagger\right. \\ &\left.-\tfrac{1}{2}\xi_b(t{+}\tau)\,\hat{a}_b^\dagger\xi_a(t)\,\hat{a}_a^\dagger+\tfrac{j}{2}\xi_b(t{+}\tau)\,\hat{a}_b^\dagger\xi_b(t)\right) \\ &\hat{a}_b^\dagger\hat{a}_a^\dagger\,|0\rangle\,. \end{aligned} \tag{7.35}$$

Using the previously defined relation $\langle 0|\,\hat{a}^\dagger = \hat{a}\,|0\rangle = 0$, the expression reduces to

$$\begin{aligned} P_{joint}(t,\tau) = \langle 0|\tfrac{1}{2}\xi_a^*(t)\,\xi_b^*(t{+}\tau) - \tfrac{1}{2}\xi_a^*(t{+}\tau)\,\xi_b^*(t) \\ \tfrac{1}{2}\xi_a(t{+}\tau)\,\xi_b(t) - \tfrac{1}{2}\xi_a(t)\,\xi_b(t{+}\tau)\,|0\rangle\,, \end{aligned} \tag{7.36}$$

and, finally, we arrive at the final expression for the *joint photon-detection probability*:

$$P_{joint}(t,\tau) = \tfrac{1}{4}|\xi_a(t{+}\tau)\,\xi_b(t) - \xi_a(t)\,\xi_b(t{+}\tau)\,|^2. \tag{7.37}$$

7.11 Joint Photon-Detection Proability in the Frequency Domain

We wish to relate the Fourier Transform of the joint photon-detection probability to the spectrum of each light pulse that interacts with the Hong-Ou-Mandel interferometer. The main assumption here is that the spectrum of the input spatio-temporal wave-packets is given by $\phi_i(\omega) = \mathscr{F}\{f_i(t)\}$. Following up from the following equation

$$\begin{aligned} \mathscr{F}\{P_c(\tau)\} = \tfrac{1}{4}(R(\omega)S(\omega) + R(\omega)S(\omega) \\ -[Z(\omega)Z^*(\omega) + Z^*(\omega)Z(\omega)])\,, \end{aligned} \tag{7.38}$$

we must employ a few Fourier Transform properties, specially the ones involving convolution. The first property states the following: $\mathscr{F}\left\{\left|h(t)\right|^2\right\} = H(\omega) * H(\omega)$. This permits us to re-write the first part of the above equation if we remember that $R(\omega)$ is the Fourier Transform of $\left|f_1(t)\right|$ and that $S(\omega)$ is the

Fourier Transform of $\left|f_2(t)\right|$. Its new form will be, thus,

$$\begin{aligned}\mathscr{F}\{P_c(\tau)\} = \tfrac{1}{4}\,(\phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega) + \phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega)) \\ -(Z(\omega)Z^*(\omega) + Z^*(\omega)Z(\omega))\,.\end{aligned} \tag{7.39}$$

The second and last property we wish to employ states the following: $\mathscr{F}\{h_1(t)h_2^*(t)\} = H_1(\omega) * H_2^*(\omega)$. We can now re-write the second part of the equation if we remember that $Z(\omega)$ is the Fourier Transform of $f_1(t)f_2^*(t)$, to find:

$$\begin{aligned}\mathscr{F}\{P_c(\tau)\} = \tfrac{1}{4}(\phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega) + \phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega)) \\ -(\phi_1(\omega) * \phi_2^*(\omega) \cdot \phi_1^*(\omega) * \phi_2(\omega) + \phi_1^*(\omega) * \phi_2(\omega) \cdot \phi_1(\omega) * \phi_2^*(\omega))\,.\end{aligned} \tag{7.40}$$

We arrange the final equation in a simpler form which yields

$$\begin{aligned}\mathscr{F}\{P_c(\tau)\} = \tfrac{1}{2}[\phi_1(\omega) * \phi_1(\omega) \cdot \phi_2(\omega) * \phi_2(\omega) \\ -\phi_1(\omega) * \phi_2^*(\omega) \cdot \phi_1^*(\omega) * \phi_2(\omega)]\,.\end{aligned} \tag{7.41}$$

7.12 No-Cloning Theorem

The No-Cloning Theorem [36,37] states that no non-orthogonal quantum system can be duplicated due to the intrinsic loss of information during a measurement. Take the normalized states $|H\rangle$ and $|45^o\rangle$, for instance, which are non-orthogonal, i.e., $\langle H|45^o\rangle \neq 0$, and a supposedly quantum cloning machine which operates as follows

$$\begin{aligned}|H\rangle\,|blanck\rangle\,|machine\rangle \rightarrow |H\rangle\,|H\rangle\,|machine_0\rangle \\ |45^o\rangle\,|blanck\rangle\,|machine\rangle \rightarrow |45^o\rangle\,|45^o\rangle\,|machine_1\rangle\end{aligned} \tag{7.42}$$

where *blanck* is an initial state of a particle which, after the machine's operation, becomes the cloned state. This operation must be unitary and should preserve the inner product, or $\langle H|45^o\rangle = \langle H|45^o\rangle\,\langle H|45^o\rangle\,\langle machine_0|machine_1\rangle$ which is only possible when $\langle H|45^o\rangle = 0$ (the two states are orthogonal) or when $\langle H|45^o\rangle = 1$ (the two states are indistinguishable) [168]. Both conditions, however, lead to contradictions. The first one contradicts the very first assumption of non-orthogonality between the two states. The second renders this system useless for communication since, with indistinguishable states, no information can be transmitted. Making use of non-orthogonal states and the unavoidable modification of the original quantum state after measurements, it is possible to devise Quantum Cryptography protocols that, instead of depending on computation hardness, base their security on the laws of physics.

7.13 The BB84 Quantum Key Distribution Protocol

The first protocol for Quantum Cryptography, or Quantum Key Distribution, was proposed in 1984 by Bennet and Brassard [39]. The protocol involves two parties, Alice and Bob, who wish to communicate privately over an untrusted channel. If Alice and Bob previously shared a random binary key which had never been used, they could use it to encrypt and decrypt the message with mathematically proved security. The *One-Time Pad* protocol [169], to which we are referring, is secure given that the above mentioned conditions are respected, namely: the key is perfectly random; and the key is only used once. The goal of the BB84 protocol is to allow for Bob and Alice to simultaneously create a shared binary key whenever the need for secure communication arises. Instead of transmitting the message itself through a quantum channel, it aims on establishing a new key for classical perfectly secure communication. For their distinct characteristics, protocols of such ilk are called Quantum Key Distribution protocols.

The feature of QKD protocols that causes it to surpass classical cryptography protocols such as the RSA [170] is that the key distribution protocol is grounded on the No-Cloning Theorem and allows for the communicating parties to identify possible eavesdroppers which intend to gain information of the key by measuring the quantum states that are being transmitted. For that, a two-step protocol has been devised where quantum states are transmitted and measured (quantum step) and the results of such measurements are communicated by classical means (classical step). After the results are compared by the two parties either one of two possible outcomes is reached: the quantum key distribution has been successful and Alice and Bob can employ their mutual key to communicate securely using the *One-Time Pad*; or an eavesdropper has been identified and the quantum channel is compromised, therefore the mutual key is to be discarded and re-generated.

The protocol initializes with Alice sending bits encoded on quantum states to Bob which measures the states; this is step 1, the *quantum step*. For long-haul quantum key distribution, the quantum channel is usually chosen as an optical fiber and the transmitted quantum state as a physical property of a photon such as polarization, phase, or time-bin, since photons experience low loss inside an optical fiber. Alice prepares each qubit in a single-photon state, according to a random choice between four states that form two pairs of orthogonal states in canonically conjugated bases in a bi-dimensional Hilbert space. Considering polarization states encoding, the bases may be sorted from the rectilinear basis (composed by horizontal and vertical states of

polarization) or the diagonal basis (composed by diagonal and anti-diagonal states of polarization). Bob randomly chooses the measurement basis for each incoming qubit and has a deterministic or probabilistic result according to the overlap between his own and Alice's chosen bases.

Bob's typical detection apparatus for polarization qubits includes a HWP to change the measurement basis, a polarizing beams plitter (PBS) and two G-APDs. To choose between measuring on the rectilinear or diagonal bases Bob sets the HWP to 0^o or 22.5^o, respectively. If Alice's and Bob's bases match, the photon is routed to a deterministic spatial mode and is delivered to the G-APD corresponding to the transmitted qubit. Otherwise, it becomes a superposition of the PBSs eigenstates and the photon randomly emerges at one output spatial mode, which can then be detected with an G-APD. During the basis reconciliation in the post-processing round, Alice and Bob communicate though an authenticated channel and select only the time-slots when their bases have agreed. The conjunction of both Alice's and Bob's random decisions produces the key, so neither parties can decide which key will result from the protocol. It is worth noting that only the time slots corresponding to a measurement result are considered, as in practice neither all pulses sent by Alice contain photons – due to imperfect photon sources – nor all received pulses can be detected by Bob – due to imperfect detectors, and channel and component loss.

How the No-Cloning Theorem assures the security of the protocol becomes clear when we introduce a third party, Eve, which wishes to spy on the transmission between Alice and Bob. A straightforward approach for Eve, is to mimic Bob's own performance, from the point of view of Alice, and to mimic Alice's own performance, from the point of view of Bob; this is called the *intercept-resend* strategy: Eve measures the states sent by Alice in one of the two possible basis like Bob would and resends a state corresponding to her measurement result. With this strategy, Eve will get the right basis in about half of the cases and the re-transmission to Bob will be successful. However, the intervention can be noticed on the other half of the cases where Bob and Alice get uncorrelated results and here is where step 2, the *classical step*, steps up. After removing the cases in which Alice and Bob used incompatible basis, they perform an error assessment by sacrificing some of the bits in their string. If the error rate is higher than the expected when taking into account the communicating link's characteristics (attenuation, dispersion), it means the states have been tempered with. In that case, the whole compromised key is discarded and the protocol initializes once again. Evidently, the key distribution will only be successful if no eavesdropper is detected and, until then, no rel-

evant data is transmitted. Assuming that no eavesdropper was detected, Alice and Bob share a common binary key which can be used in order to communicate secretly using the *One-Time Pad* Protocol. All subsequent transmissions must be preceded by another QKD run since the binary key should only be used once.

7.14 Attacks on the BB84

Quantum key distribution [35] benefits from the laws of quantum physics to provide absolutely secure communication [171] between two communicating parties (Alice and Bob), even if imperfect devices are used [161,172,173]. Imperfections on the equipment used in a QKD system can be related to sources that emit multi-photon pulses which enable the photon-number splitting attack [35]. Clever solutions based on fundamental principles were used to overcome such imperfections, as in the decoy states method [44], which enable a more efficient use of imperfect photon sources – more specifically weak coherent states with moderate multi-photon probability – for QKD. Recently a critical point was recognized: back-doors may be open in some physical devices comprising the QKD system, specially the single-photon detector (SPD). The flaws may be explored by an eavesdropper for side-channel attacks [48,50,50–58,174–176], which can jeopardize the security of the protocol.

These quantum hacking attacks are interventions caused by Eve from the outside of Bob's station by high-jacking the detection apparatus – whose response can be predicted in some degree or even manipulated. In all cases, the attacks make it possible for an eavesdropper to gain information without being noticed, i.e., achieving a critically high mutual information with Alice and Bob without exceeding the upper threshold of the quantum bit error rate (QBER). The hacking schemes basically aim on two key points: exploring the imperfect nature of the SPD – efficiency mismatched-based attacks [48,50,55] – or externally forcing a deterministic result on the detection equipment – bright-light based attacks [51–54,56,174]. Different countermeasures to avoid detector-aimed quantum hacking attacks have been presented [47,48,50,50–58,174–178] however, despite being effective for the proposed specific end, i.e., closing a specific back-door, the solutions have no guarantees of being final, in the sense that the vulnerabilities depend on the physical implementation of the devices and the deployment of the systems. The counter-measures give, in the best case, ad-hoc protection over some class of attacks.

The traditional single-photon detector (SPD) used in QKD systems is composed of a cooled InGaAs avalanche photodiode (APD) operated in

gated Geiger mode and an avalanche quenching circuit [15, 35, 179, 180]. When reversely polarized above the breakdown threshold – during short time windows – the device becomes single-photon sensitive, so impinging weak light may trigger a self-sustained avalanche. With the end of the gate, the over-voltage bias is reduced and the macroscopic burst current is quenched to reset the single-photon sensitivity. A discriminator circuit creates a formatted voltage pulse that indicates the occurrence of a photon count. APD-based single-photon detectors are usually not photon number resolving, i.e., they cannot discriminate between a single-photon or multi-photon optical pulse and emit an identical formatted voltage pulse in both cases. Apart the traditional commercial devices, different gating and quenching schemes can also be used with APDs to construct enhanced devices [181, 182] and even photon number resolving detectors [152].

The Geiger mode makes the SPD sensitive to a single photon during the gate time due to the high electronic gain provided by the operational point above the breakdown voltage. However, when biased with lower voltage, the APD works in linear mode, as is usual in telecommunication applications. Therefore, if the bias voltage is brought below the breakdown, the device no longer detects single-photons. This behaviour can be explored by Eve to disable Bob's detectors. Of course, this strategy alone gives no information to Eve, but can be combined with other ruses, as to manipulate Bob's results as we will see. During this blinding attack, the eavesdropper sends strong light to enforce a current flow, which can alter the threshold breakdown value [54, 177, 178]. The excess voltage applied to the APD to enable Geiger mode is no longer sufficient and the detector becomes blind to single-photon detection. Even when operating with low bias voltage (in the case of free-running operation or outside a detection window in gated mode), the SPD may trigger an avalanche when under attack if a sufficiently strong pulse is received [57, 58]. Assuming an interception-resend strategy, Eve measures each qubit sent by Alice in a random basis and prepares a faked state to send to Bob according to the result obtained. If Bob's basis choice matches Eve's, the strong pulse is routed to the corresponding detector, forcing an avalanche with unity probability, and Eve knows that their results are correlated. However, if their bases disagree, the pulse is split and half the power is delivered to each of Bob's detectors. As this half-power pulse is not sufficient to trigger an avalanche, no detection event takes place. The ruse renders all valid results obtained by Bob correlated to Eve's, who then acquires high knowledge of the key. This strategy may be used standalone as in the aftergate attack [53], or combined to the blinding scheme, causing no critical quantum bit error rate (QBER) increase [57, 58],

as Bob's SPDs never click in the absence of a faked state.

Each SPD operating in gated mode has its own time-dependent efficiency curve. This means that the device is usually more efficient in one temporal position relative to the other, due to asymmetries or to temporal mismatch. Eve can explore a mismatch between the two efficiency curves to launch an attack by manipulating, for example, the time of arrival of the qubits relative to the gate windows. A faked states strategy may be employed [53,55,57,58,174], which makes the detection events of Bob more probable to occur at a certain detector according to the delay imposed by Eve. Another example is the time-shift attack [50], in which there is no interception at all by Eve, but only a bi-stable random (but known by Eve) delay change in the qubit's time-of-flight. By manipulating the optical path, Eve can position the optical pulse in a region of the gate window that increases the probability of a detection occurring in one or other SPD, allowing the eavesdropper to infer (part of) the key without even increasing the QBER. The drawback of this strategy is the reduction of the net detection efficiency of Bob's apparatus that must be compensated by Eve. It is assumed, however, that Eve can replace the link by a more transparent one, or can teleport the states from Alice's output to Bob's entrance.

7.15 The Ekert Protocol and The Measurement-Device Independent QKD Protocol

EPR sources, or entangled state sources, take their name after Einstein's acclaimed article in which the completeness of quantum mechanics is contested: the scarcely well interpreted phenomenon of entanglement is directed into a trail of thought that leads to either abandoning the notions of physical reality or concluding that an underlying model must govern quantum mechanics [183]. An entangled system, which mathematically takes on a relatively simple definition "a state which is not separable and, therefore, cannot be written as a tensor product", has been the source of a physical conundrum since John Bell showed how one could experimentally demonstrate, in 1964, that indeed quantum mechanics is complete and it is our view of the physical reality that must be seen from another perspective (which usually involves giving up the notion of *locality*) [184]. Among other aspects of Bell's proof, there is the mathematical demonstration that entangled states violate a special kind of inequality, the Bell-CHSH Inequality [185]. The violation of this inequality can, in principle, be experimentally verified and, since it depends on the entanglement of a bi-partite system, the verification fails whenever the states

are tempered with: entanglement is a delicate and subtle condition and the fact that the violation has been violated is proof that the entanglement has been preserved.

In 1991, Arthur Ekert proposed a means of employing EPR sources in quantum cryptography [40]. Suppose that, instead of sending states one to another such as in the BB84 protocol, Alice and Bob receive, each, a part of a bi-partite entangled state and attempt to verify the violation of the Bell-CHSH Inequality: they would be sure no eavesdropper assessed the transmitting quantum state; not only that but they would be sure that the entangled source itself is truly entangled. The verification step must be, as in the BB84, a completely classical step and, throughout this step, Alice and Bob keep the information regarding the states for which the inequality was violated; attributing bit values to the basis information is straightforward and results in a shared key between the two parties.

Only recently, however, the violation of the Bell-CHSH Inequality has been truly verified, since it involves closing experimental loopholes intrinsic to usual measurement apparatuses [186]. Violating the inequality, however, is still a matter of concern from an practical point of view and its implementation on large scale quantum key distribution is far from secured. The Measurement-Device Independent Quantum Key Distribution, on the other hand, is immediately applicable and eliminates the concern over the fact that the measurement apparatus is far from the idealized in theoretical QKD [60]. The protocol can be thought of as a *time-reversed* Ekert Protocol where, instead of measuring entangled states sent from an intermediate EPR source, Alice and Bob send states which are measured in an intermediate facility. Usually, the middle-man is called Charlie and its duty is to realized a projection measurement with the states sent from Alice and Bob, a Bell-State Projection in a Bell-state analyzer (BSA). The BSA is used to project two-photon states (each half of which is sent by Alice and Bob) onto maximally entangled bi-partite states (usually denominated Bell States) [60, 61]. The idea behind a Bell-State Projection is to determine which Bell state would have given origin to the two previously uncorrelated photon pulses sent by Alice and Bob. Upon a positive projection, Charlie announces the result through a classical channel to the communicating parties which, with knowledge of their state, can deduce which state had been prepared by the other party so that the specific projection occurred. The important part is that, with the information from the projection alone, one is not possible to determine neither of the states sent either by Alice and Bob. Note also, that nothing protects Alice and Bob from a cold truth: Eve could be mimicking Charlie. That, however, is completely acceptable since, either way,

Eve will not be able to assess the key shared by Alice and Bob. Since, therefore, the measurement apparatus is completely free to be hacked and could, in principle, be Eve's, the protocol is called Measurement-Device Independent.

7.16 The Hanburry-Brown and Twiss Experiment and the Second-Order Temporal Correlation Function at Zero Time

As we have seen before, quantum interference phenomena are explained in the light o the quantum theory of coherence. In particular, a light source's statistical properties can be analyzed [140, 141]. Throughout this document, the light source can either relate to the output of the Linear-Optic Heralded Photon Source (Chapter 4) or to the heralded states time tuned to the HOM *peak* (Chapter 5). In the experiment of Hanburry Brown and Twiss [134], two detectors are placed at the output ports of a beam splitter and the coincidences are taken as a function of the delay between the temporal modes as depicted in Fig. 7.1.

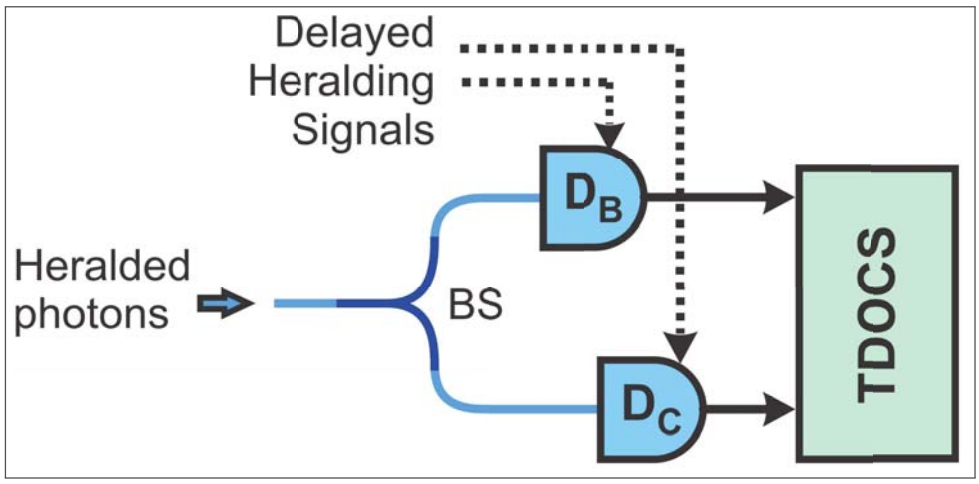

Figure 7.1: Experimental setup for the Hanbury-Brown and Twiss Analyzer. TDOCS: Time-Delay-Offset Coincidence Station.

In a heralded source context, as is our own, the detectors are gated whenever a heralding event occurs, i.e., the detections from the *heralder* detector trigger both detectors (say A and B) and the coincidence events are recorded. The value of $g^{(2)}(0)$, the second-order temporal autocorrelation function at zero time, can be experimentally calculated from the rates of detections in each detector (D_A and D_B), and the rate of coincidence events D_{AB} as [68, 83]

$$g^{(2)}(0) = \frac{D_{AB}}{D_A D_B}. \tag{7.43}$$

For negligible dark count probability and assuming the single-photon detection probability of detectors A and B are given by η_A and η_B, a detection event can be triggered by a single- or multi-photon pulse, so we can write

$$D_{A,B} = \frac{P_s \eta_{A,B}}{2} + \left(\eta_{A,B} - \frac{\eta_{A,B}^2}{4}\right) P_m. \tag{7.44}$$

The second-order temporal autocorrelation function indicates whether the photons in an optical beam are *bunched* ($g^{(2)}(0) > g^{(2)}(\tau)$), *antibunched* ($g^{(2)}(0) < g^{(2)}(\tau)$), or randomly distributed ($g^{(2)}(0) = g^{(2)}(\tau)$) [139]. Also, by inspecting the value of $g^{(2)}(0)$ calculated from Eq. 7.43, one is able to determine the ratio between multi- and single-photon pulses in the beam: when the value drops below 1, the ratio surpasses that of a coherent field and the beam is said to be follow *sub-Poisson* statistics [135, 139]. This result alone may also impart information regarding the antibunched nature of the photons: $g^{(2)}(0) < 1$ implies $g^{(2)}(0) < g^{(2)}(\tau)$ and, therefore, antibunching [139]. The relation between sub-Poisson statistics and antibunching, however, is subtle, since one can have a field with Poisson, or even super-Poisson, statistics which exhibits antibunching even though the converse does not apply [139].

7.17 Joint Photon-Detection Probability – Modified Hong-Ou-Mandel Interferometer

The *joint photon-detection probability* for the modified Hong-Ou-Mandel interferometer can be calculated through the following expression:

$$\begin{aligned} &P_{joint}(t,\tau) = g_{f,g}(t, t+\tau) = \\ &\langle 0|\, \hat{a}_a \hat{a}_b \hat{E}_f^{(-)}(t) \hat{E}_g^{(-)}(t+\tau) \hat{E}_f^{(+)}(t+\tau) \hat{E}_g^{(+)}(t) \hat{a}_b^\dagger \hat{a}_a^\dagger \,|0\rangle . \end{aligned} \tag{7.45}$$

We use Eq.5.8 which relates the electric field operators at modes f and g to the electric field operators at modes a and b to write

$$\begin{aligned} &P_{joint}(t,\tau) = \\ &\quad \langle 0|\, \hat{a}_a \hat{a}_b \tfrac{i}{2} \left(\hat{E}_a^{(-)}(t) + i\hat{E}_b^{(-)}(t)\right) + \tfrac{1}{\sqrt{2}} \hat{E}_e^{(-)}(t) \\ &\quad \tfrac{1}{2} \left(\hat{E}_a^{(-)}(t+\tau) + i\hat{E}_b^{(-)}(t+\tau)\right) + \tfrac{i}{\sqrt{2}} \hat{E}_e^{(-)}(t+\tau) \\ &\quad \tfrac{i}{2} \left(\hat{E}_a^{(+)}(t+\tau) + i\hat{E}_b^{(+)}(t+\tau)\right) + \tfrac{1}{\sqrt{2}} \hat{E}_e^{(+)}(t+\tau) \\ &\quad \tfrac{1}{2} \left(\hat{E}_a^{(+)}(t) + i\hat{E}_b^{(+)}(t)\right) + \tfrac{i}{\sqrt{2}} \hat{E}_e^{(+)}(t)\, \hat{a}_b^\dagger \hat{a}_a^\dagger \,|0\rangle . \end{aligned} \tag{7.46}$$

It is now a matter of substituting the electric field expression in terms of the input spatio-temporal wave-packets. Since we are now dealing with an extra input mode represented by the letter e, we also introduce a spatio-temporal

wave-packet for this mode such that $\hat{E}_e^{(-)}(t) = \xi_e^*(t)\,\hat{a}_e^\dagger$. The expression after the mentioned substitutions reads:

$$\begin{aligned}
&P_{joint}(t,\tau) = \\
&\quad\langle 0|\,\hat{a}_a\hat{a}_b \\
&\qquad\Big(\tfrac{j}{4}\xi_a^*(t)\,\hat{a}_a^\dagger\xi_a^*(t{+}\tau)\,\hat{a}_a^\dagger - \tfrac{1}{4}\xi_a^*(t)\,\hat{a}_a^\dagger\xi_b^*(t{+}\tau)\,\hat{a}_b^\dagger \\
&\qquad+\tfrac{j}{2\sqrt{2}}\xi_a^*(t)\,\hat{a}_a^\dagger\xi_e^*(t{+}\tau)\,\hat{a}_e^\dagger - \tfrac{1}{4}\xi_b^*(t)\,\hat{a}_b^\dagger\xi_a^*(t{+}\tau)\,\hat{a}_a^\dagger \\
&\qquad-\tfrac{j}{4}\xi_b^*(t)\,\hat{a}_b^\dagger\xi_b^*(t{+}\tau)\,\hat{a}_b^\dagger - \tfrac{1}{2\sqrt{2}}\xi_b^*(t)\,\hat{a}_b^\dagger\xi_e^*(t{+}\tau)\,\hat{a}_e^\dagger \\
&\qquad+\tfrac{1}{2\sqrt{2}}\xi_e^*(t)\,\hat{a}_e^\dagger\xi_a^*(t{+}\tau)\,\hat{a}_a^\dagger + \tfrac{j}{2\sqrt{2}}\xi_e^*(t)\,\hat{a}_e^\dagger\xi_b^*(t{+}\tau)\,\hat{a}_b^\dagger \\
&\qquad+\tfrac{1}{2}\xi_e^*(t)\,\hat{a}_e^\dagger\xi_e^*(t{+}\tau)\,\hat{a}_e^\dagger\Big)\Big(\tfrac{j}{4}\xi_a(t{+}\tau)\,\hat{a}_a^\dagger\xi_a(t)\,\hat{a}_a^\dagger \\
&\qquad-\tfrac{1}{4}\xi_a(t{+}\tau)\,\hat{a}_a^\dagger\xi_b(t)\,\hat{a}_b^\dagger + \tfrac{j}{2\sqrt{2}}\xi_a(t{+}\tau)\,\hat{a}_a^\dagger\xi_e(t)\,\hat{a}_e^\dagger \\
&\qquad-\tfrac{1}{4}\xi_b(t{+}\tau)\,\hat{a}_b^\dagger\xi_a(t)\,\hat{a}_a^\dagger - \tfrac{j}{4}\xi_b(t{+}\tau)\,\hat{a}_b^\dagger\xi_b(t) \\
&\qquad-\tfrac{1}{2\sqrt{2}}\xi_b(t{+}\tau)\,\hat{a}_b^\dagger\xi_e(t)\,\hat{a}_e^\dagger + \tfrac{1}{2\sqrt{2}}\xi_e(t{+}\tau)\,\hat{a}_e^\dagger\xi_a(t)\,\hat{a}_a^\dagger \\
&\qquad+\tfrac{j}{2\sqrt{2}}\xi_e(t{+}\tau)\,\hat{a}_e^\dagger\xi_b(t)\,\hat{a}_b^\dagger + \tfrac{1}{2}\xi_e(t{+}\tau)\,\hat{a}_e^\dagger\xi_e(t)\,\hat{a}_e^\dagger\Big) \\
&\qquad\qquad\hat{a}_b^\dagger\hat{a}_a^\dagger\,|0\rangle\,.
\end{aligned} \tag{7.47}$$

Using the previously defined relation $\langle 0|\,\hat{a}^\dagger = \hat{a}\,|0\rangle = 0$, the expression reduces to

$$\begin{aligned}
P_{joint}(t,\tau) = \langle 0|\Big(&-\tfrac{1}{4}\xi_a^*(t)\,\xi_b^*(t{+}\tau) - \tfrac{1}{4}\xi_a^*(t{+}\tau)\,\xi_b^*(t)\Big) \\
&\Big(-\tfrac{1}{4}\xi_a(t{+}\tau)\,\xi_b(t) - \tfrac{1}{4}\xi_a(t)\,\xi_b(t{+}\tau)\Big)\,|0\rangle\,,
\end{aligned} \tag{7.48}$$

and, finally, we arrive at the final expression for the *joint photon-detection probability* in the modified Hong-Ou-Mandel interferometer:

$$P_{joint}(t,\tau) = \tfrac{1}{16}|\xi_a(t{+}\tau)\,\xi_b(t) + \tfrac{1}{2}\xi_a(t)\,\xi_b(t{+}\tau)\,|^2. \tag{7.49}$$

7.18 Publications

In this appendix, the published, submitted and accepted (in case of conference) papers related to this work are listed.

One paper was published in Journal of Optical Society of America - B in 2015. This is: *Spectral Characterization of Weak Coherent State Sources Based on Two-Photon Interference* [148]. It is a first approach to the Few-Photon Fourier Transform Spectroscopy method and makes use of a self-homodyne

setup instead of two independent laser sources.

One paper was published in Journal of Selected Topics of Quantum Electronics in 2015. This is: *Safeguarding Quantum Key Distribution Through Detection Randomization* [59]. It addresses the main classes of attacks on the BB84 and proposes an elegant counter-measure to both simultaneously.

One paper was published in Physical Review A in 2015. This is *Linear-Optic Heralded Photon Source* [68]. In this paper, we present the contents of Chapter 4.

One paper has been accepted and is about to be published in Optics Letters in 2016. This is *Few-Photon Heterodyne Spectroscopy* [160]. The Few-Photon Fourier Transform Spectroscopy is presented in this paper.

The three first papers have also been submitted to conferences in a short form and have been presented in QCrypt2014-Paris [148] and in QCrypt2015-Tokyo [59, 68].

The paper *Sub-Poisson States Heralded at a Hong-Ou-Mandel Peak* [163], which reports the results of Chapter 5, was first conceived with a different name (*Photon Antibunching and Hong-Ou-Mandel Peak*) which evoked a few controversies and, thus, was rejected by Physical Review Letters. After its revision, it finally got its present name and has been submitted to Optics Letters and is currently under review.

Short versions of [160] and [163] have been submitted to the *International Conference on Quantum Communication, Measurement and Computing* (QCMC2016) and are currently under review.

Bibliography

[1] A. Muthukrishnan, M. O. Scully, and M. S. Zubairy, *The concept of the photon – revisited*, **Optics & Photonics News**, 2003.

[2] A. Zajonc, *Light reconsidered*, **Optics & Photonics News**, 2003.

[3] P. A. M. Dirac, *The Quantum Theory of the Emission and Absorption of Radiation*, **Proceedings of the Royal Society of London A**, 1927.

[4] E. Fermi, *Quantum Theory of Radiation*, **Reviews of Modern Physics**, 1932.

[5] C. C. Gerry and P. L. Knight, **Introductory Quantum Optics**. Cambridge University Press, second ed., 2005.

[6] M. Born and E. Wolf, **Principles of Optics**. Pergamon Press Ltd., 1970.

[7] Z.-Y. J. Ou, **Multi-Photon Quantum Interference**. Springer, first ed., 2006.

[8] H. Hertz, *Ueber einen Einfluss des ultravioletten Lichtes auf die electrische Entladung*, **Annalen der Physik**, vol. 267, no. 8, pp. 983–1000, 1887.

[9] A. Einstein, *Über einem die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt*, **Annalen der Physik**, vol. 4, 1905.

[10] D. Renker, *Geiger-mode avalanche photodiodes, history, properties and problems*, **Nuclear Instruments and Methods in Physics Research Section A**, vol. 567, no. 1, pp. 48–56, 2006.

[11] B. Lubsandorzhiev, *On the history of photomultiplier tube invention*, **Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment**, vol. 567, no. 1, pp. 236 – 238, 2006.

[12] C. Kittel, **Introduction to solid state physics**. Wiley, 2005.

[13] R. J. McIntyre, *The distribution of gains in uniformly multiplying avalanche photodiodes: Theory*, **Electron Devices, IEEE Transactions on**, vol. 19, no. 6, pp. 703–713, 1972.

[14] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D. MacSween, R. J. McIntyre, C. Trottier, and P. P. Webb, *Photon counting techniques with silicon avalanche photodiodes*, **Applied Optics**, vol. 32, no. 21, pp. 3894–3900, 1993.

[15] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, *Avalanche photodiodes and quenching circuits for single-photon detection*, **Applied optics**, vol. 35, no. 12, pp. 1956–1976, 1996.

[16] B. F. Aull, A. H. Loomis, D. J. Young, R. M. Heinrichs, B. J. Felton, P. J. Daniels, and D. J. Landers, *Geiger-mode avalanche photodiodes for three-dimensional imaging*, **Lincoln Laboratory Journal**, vol. 13, no. 2, pp. 335–349, 2002.

[17] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, *Evolution and prospects for single-photon avalanche diodes and quenching circuits*, **Journal of Modern Optics**, vol. 51, no. 9-10, pp. 1267–1288, 2004.

[18] G. Buller and R. Collins, *Single-photon generation and detection*, **Meas. Sci. Technol**, vol. 21, no. 1, p. 012002, 2010.

[19] R. G. Brown, K. D. Ridley, and J. G. Rarity, *Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching*, **Applied Optics**, vol. 25, no. 22, pp. 4122–4126, 1986.

[20] P. Antognetti, S. Cova, and A. Longoni, *A study of the operation and performances of an avalanche diode as a single-photon detector* in **Proceedings of the Second ISPRA Nuclear Electronics Symposium**, 1975.

[21] S. Cova, A. Longoni, and A. Andreoni, *Towards picosecond resolution with single-photon*, **Rev. Sci. Instrum**, vol. 52, no. 3, 1981.

[22] N. Otte, *The Silicon Photomultiplier – A new device for High Energy Physics, Astroparticle Physics, Industrial and Medical Applications* in **Proceedings to SNIC Symposium (SLAC, Stanford, 2006)**, 2006.

[23] A. Lacaita, F. Zappa, S. Cova, and P. Lovati, *Single-photon detection beyond 1 μm: performance of commercially available InGaAs-InP detectors*, **Applied Optics**, vol. 35, no. 16, pp. 2986–2996, 1996.

[24] P. A. Hiskett, G. S. Buller, A. Y. Loudon, J. M. Smith, I. Gontijo, A. C. Walker, P. D. Townsend, and M. J. Robertson, *Performance and design of InGaAs-InP photodiodes for single-photon counting at 1.55 μm*, **Applied Optics**, vol. 39, no. 36, pp. 6818–6829, 2000.

[25] J. C. Campbell, A. Dentai, W. Holden, and B. Kasper, *High-performance avalanche photodiode with separate absorption grading and multiplication regions*, **Electronics Letters**, vol. 19, no. 20, pp. 818–820, 1983.

[26] S. Pellegrini, R. E. Warburton, L. J. J. Tan, J. S. Ng, A. B. Krysa, K. Groom, J. P. R. David, S. Cova, M. J. Robertson, and G. S. Buller, *Design and performance of an InGaAs-InP single-photon avalanche diode detector*, **IEEE J. Quantum Electronics**, vol. 42, 2006.

[27] M. A. Itzler, R. Ben-Michael, C.-F. Hsu, K. Slomkowski, A. Tosi, S. Cova, F. Zappa, and R. Ispasoiu, *Single photon avalanche diodes (SPADs) for 1.5 μ m photon counting applications*, **Journal of Modern Optics**, vol. 54, no. 2-3, pp. 283–304, 2007.

[28] R. Warburton, M. Itzler, and G. S. Buller, *Improved free-running InGaAs/InP single-photon avalanche diode detectors operating at room temperature*, **Electronics letters**, vol. 45, no. 19, pp. 996–997, 2009.

[29] N. Namekata, S. Sasamori, and S. Inoue, *800 MHz single-photon detection at 1550-nm using an InGaAs-InP avalanche photodiode operated with a sine wave gating*, **Optics Express**, vol. 14, no. 21, pp. 10043–10049, 2006.

[30] N. Namekata, S. Adachi, and S. Inoue, *1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs-InP avalanche photodiode*, **Optics express**, vol. 17, no. 8, pp. 6275–6282, 2009.

[31] R. T. Thew, D. Stucki, J. D. Gautier, H. Zbinden, and A. Rochas, *Free-running InGaAs-InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths*, **Applied Physics Letters**, vol. 91, 2007.

[32] R. E. Warburton, M. Itzler, and G. S. Buller, *Free-running, room temperature operation of an InGaAs-InP single-photon avalanche diode*, **Applied Physics Letters**, vol. 94, no. 7, p. 071116, 2009.

[33] G. Buller, R. Warburton, S. Pellegrini, J. Ng, J. David, L. Tan, A. Krysa, and S. Cova, *Single-photon avalanche diode detectors for quantum key distribution*, **Optoelectronics, IET**, vol. 1, no. 6, pp. 249–254, 2007.

[34] A. Tosi, A. D. Mora, F. Zappa, and S. Cova, *Single-photon avalanche diodes for the near-infrared range: detector and circuit issues*, **Journal of Modern Optics**, vol. 56, no. 2-3, pp. 299–308, 2009.

[35] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, **Rev. Mod. Phys.**, vol. 74, pp. 145–195, 2002.

[36] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, **Nature**, vol. 299, no. 5886, pp. 802–803, 1982.

[37] D. Dieks, *Communication by EPR devices*, **Physics Letters A**, vol. 92, no. 6, pp. 271–272, 1982.

[38] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik*, **Zeitschrift für Physik**, vol. 43, no. 3-4, pp. 172–198, 1927.

[39] H. Bennett Ch and G. Brassard, *Quantum cryptography: public key distribution and coin tossing Int* in **Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)**, pp. 175–9, 1984.

[40] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, **Physical Review Letters**, vol. 67, no. 6, p. 661, 1991.

[41] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, **Physical Review Letters**, vol. 68, no. 21, p. 3121, 1992.

[42] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states*, **Physical Review Letters**, vol. 81, no. 14, p. 3018, 1998.

[43] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, **Phys. Rev. Lett.**, vol. 91, p. 057901, 2003.

[44] X.-B. Wang, *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography*, **Phys. Rev. Lett.**, vol. 94, p. 230503, 2005.

[45] H.-K. Lo, H. F. Chau, and M. Ardehali, *Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*, **J. Cryptology**, vol. 18, pp. 133–165, 2005.

[46] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Practical decoy state for quantum key distribution*, **Phys. Rev. A**, vol. 72, p. 012326, 2005.

[47] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, *Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems*, **Optics Express**, vol. 20, no. 17, pp. 18911–18924, 2012.

[48] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems*, **Physical Review A**, vol. 74, no. 2, p. 022313, 2006.

[49] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Time-shift attack in practical quantum cryptosystem*, **Quantum Inf. Comput.**, vol. 7, pp. 073–082, 2007.

[50] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, **Physical Review A**, vol. 78, no. 4, p. 042333, 2008.

[51] V. Makarov, *Controlling passively quenched single photon detectors by bright light*, **New Journal of Physics**, vol. 11, no. 6, p. 065003, 2009.

[52] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, *Controlling an actively-quenched single photon detector with bright light*, **Optics Express**, vol. 19, no. 23, pp. 23590–23600, 2011.

[53] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, *After-gate attack on a quantum cryptosystem*, **New Journal of Physics**, vol. 13, no. 1, p. 013043, 2011.

[54] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Thermal blinding of gated detectors in quantum cryptography*, **Optics Express**, vol. 18, no. 26, pp. 27938–27954, 2010.

[55] V. Makarov* and D. R. Hjelme, *Faked states attack on quantum cryptosystems*, **Journal of Modern Optics**, vol. 52, no. 5, pp. 691–705, 2005.

[56] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, *Quantum eavesdropping without interception: an attack exploiting the*

dead time of single-photon detectors, **New Journal of Physics**, vol. 13, no. 7, p. 073024, 2011.

[57] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination*, **Nature Photonics**, vol. 4, no. 10, pp. 686–689, 2010.

[58] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, **Nature Communications**, vol. 2, p. 349, 2011.

[59] T. Ferreira da Silva, G. C. Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, *Safeguarding Quantum Key Distribution through Detection Randomization*, **Selected Topics in Quantum Electronics, IEEE Journal of**, vol. 21, no. 3, pp. 1–9, 2015.

[60] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution*, **Physical Review Letters**, vol. 108, no. 13, p. 130503, 2012.

[61] T. Ferreira da Silva, D. Vitoreti, G. Xavier, G. do Amaral, G. Temporão, and J. von der Weid, *Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits*, **Physical Review A**, vol. 88, no. 5, p. 052303, 2013.

[62] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, *et al.*, *Experimental measurement-device-independent quantum key distribution*, **Physical Review Letters**, vol. 111, no. 13, p. 130502, 2013.

[63] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, *Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution*, **Physical Review Letters**, vol. 112, no. 19, p. 190503, 2014.

[64] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, *Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks*, **Physical Review Letters**, vol. 111, no. 13, p. 130501, 2013.

[65] S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, *A photonic quantum information interface*, **Nature**, vol. 437, pp. 116–120, 2005.

[66] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, **Nature**, vol. 409, pp. 46–52, 2001.

[67] N. Gisin and R. Thew, *Quantum communication*, **Nature Photon.**, vol. 1, pp. 165–171, 2007.

[68] T. Ferreira da Silva, G. C. Amaral, G. P. Temporão, and J. P. von der Weid, *Linear-optic heralded photon source*, **Physical Review A**, vol. 92, no. 3, p. 033855, 2015.

[69] B. E. A. Saleh and M. C. Teich, **Fundamentals of Photonics**. John Wiley & Sons, Inc, 2007.

[70] B. Lounis and M. Orrit, *Single-photon sources*, **Reports on Progress in Physics**, vol. 68, no. 5, p. 1129, 2005.

[71] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental quantum cryptography*, **Journal of Cryptology**, vol. 5, no. 1, pp. 3–28, 1992.

[72] P. A. Hiskett, D. Rosenberg, C. Peterson, R. Hughes, S. Nam, A. Lita, A. Miller, and J. Nordholt, *Long-distance quantum key distribution in optical fibre*, **New Journal of Physics**, vol. 8, no. 9, p. 193, 2006.

[73] V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, *Passive optical network approach to gigahertz-clocked multiuser quantum key distribution*, **Quantum Electronics, IEEE Journal of**, vol. 43, no. 2, pp. 130–138, 2007.

[74] C. Gobby, Z. Yuan, and A. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, **Applied Physics Letters**, vol. 84, no. 19, pp. 3762–3764, 2004.

[75] P. A. Hiskett, G. Bonfrate, G. S. Buller, and P. D. Townsend, *Eighty kilometre transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm*, **Journal of Modern Optics**, vol. 48, no. 13, pp. 1957–1966, 2001.

[76] P. D. Townsend, A. Ougazzaden, and P. Tapster, *Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel*, **Electronics Letters**, vol. 29, no. 14, pp. 1291–1293, 1993.

[77] P. Michler, A. Imamoğlu, M. Mason, P. Carson, G. Strouse, and S. Buratto, *Quantum correlation among photons from a single quantum dot at room temperature*, **Nature**, vol. 406, no. 6799, pp. 968–970, 2000.

[78] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, *Triggered single photons from a quantum dot*, **Physical Review Letters**, vol. 86, no. 8, p. 1502, 2001.

[79] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, *Single-photon generation with InAs quantum dots*, **New Journal of Physics**, vol. 6, no. 1, p. 89, 2004.

[80] D. Bimberg, E. Stock, A. Lochmann, A. Schliwa, W. Unrau, M. Münnix, S. Rodt, A. Toropov, A. Bakarov, A. Kalagin, *et al.*, *Quantum dots for single and entangled photon emitters* in **OPTO**, pp. 76100G–76100G, International Society for Optics and Photonics, 2010.

[81] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, *New High-Intensity Source of Polarization-Entangled Photon Pairs*, **Phys. Rev. Lett.**, vol. 75, pp. 4337–4341, 1995.

[82] C. K. Hong and L. Mandel, *Experimental realization of a localized one-photon state*, **Phys. Rev. Lett.**, vol. 56, pp. 58–60, 1986.

[83] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, *High-quality asynchronous heralded single-photon source at telecom wavelength*, **New J. Phys.**, vol. 93, p. 070503, 2004.

[84] M. Halder, A. Beveratos, R. Thew, C. Jorel, H. Zbinden, and N. Gisin, *High coherence photon pair source for quantum communication*, **New J. Phys**, vol. 10, p. 023027, 2008.

[85] Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, *Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source*, **Phys. Rev. Lett.**, vol. 100, p. 090501, 2008.

[86] E. Pomarico, B. Sanguinetti, T. Guerreiro, R. Thew, and H. Zbinden, *MHz rate and efficient synchronous heralding of single photons at telecom wavelengths*, **Opt. Express**, vol. 20, pp. 23846–23855, 2012.

[87] L. A. Ngah, O. Alibart, L. Labonté, V. D'Auria, and S. Tanzilli, *Ultra-fast heralded single photon source based on telecom technology*, **Laser & Photonics Reviews**, vol. 9, no. 2, pp. L1–L5, 2015.

[88] M. Fiorentino, P. Voss, J. Sharping, and P. Kumar, *All-fiber photon-pair source for quantum communications*, **Photon. Techn. Lett.**, vol. 14, pp. 983–985, 2002.

[89] J. Rarity, J. Fulconis, J. Duligall, W. Wadsworth, and P. Russell, *Photonic crystal fiber source of correlated photon pairs*, **Opt. Express**, vol. 13, pp. 534–544, 2005.

[90] C. K. Hong and L. Mandel, *Theory of parametric frequency down conversion of light*, **Phys. Rev. A**, vol. 31, pp. 2409–2418, 1985.

[91] M. H. Rubin, D. N. Klyshko, Y. Shih, and A. Sergienko, *Theory of two-photon entanglement in type-II optical parametric down-conversion*, **Physical Review A**, vol. 50, no. 6, p. 5122, 1994.

[92] S. Tanzilli, A. Martin, F. Kaiser, M. P. De Micheli, O. Alibart, and D. B. Ostrowsky, *On the genesis and evolution of integrated quantum optics*, **Laser & Photonics Reviews**, vol. 6, no. 1, pp. 115–143, 2012.

[93] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, *High-performance guided-wave asynchronous heralded single-photon source*, **Optics letters**, vol. 30, no. 12, pp. 1539–1541, 2005.

[94] P. Aboussouan, O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, *High-visibility two-photon interference at a telecom wavelength using picosecond-regime separated sources*, **Physical Review A**, vol. 81, no. 2, p. 021801, 2010.

[95] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, *Multiphoton entanglement and interferometry*, **Rev. Mod. Phys.**, vol. 84, pp. 777–838, 2012.

[96] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, *Long-Distance Bell-State Analysis of Fully Independent Polarization Weak Coherent States*, **J. Lightwave Technol.**, vol. 31, pp. 2881–2887, 2013.

[97] J. Armstrong, N. Bloembergen, J. Ducuing, and P. Pershan, *Interactions between light waves in a nonlinear dielectric*, **Physical Review**, vol. 127, no. 6, p. 1918, 1962.

[98] E. A. Watson and G. M. Morris, *Comparison of infrared upconversion methods for photon-limited imaging*, **Journal of Applied Physics**, vol. 67, no. 10, pp. 6075–6084, 1990.

[99] M. A. Albota and F. N. Wong, *Efficient single-photon counting at 1.55 μm by means of frequency upconversion*, **Optics Letters**, vol. 29, no. 13, pp. 1449–1451, 2004.

[100] H. Pan, H. Dong, H. Zeng, and W. Lu, *Efficient single-photon counting at 1.55 mum by intracavity frequency upconversion in a unidirectional ring laser*, **Applied Physics Letters**, vol. 89, no. 19, p. 1108, 2006.

[101] E. Diamanti, H. Takesue, C. Langrock, M. Fejer, and Y. Yamamoto, *100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors*, **Optics Express**, vol. 14, no. 26, pp. 13073–13082, 2006.

[102] A. Shields, M. O'sullivan, I. Farrer, D. Ritchie, R. Hogg, M. Leadbeater, C. Norman, and M. Pepper, *Detection of single photons using a field-effect transistor gated by a layer of quantum dots*, **Applied Physics Letters**, vol. 76, no. 25, pp. 3673–3675, 2000.

[103] B. Kardynal, A. Shields, M. O'Sullivan, N. Beattie, I. Farrer, D. Ritchie, and K. Cooper, *Detection of single photons using a field effect transistor with a layer of quantum dots*, **Measurement Science and Technology**, vol. 13, no. 11, p. 1721, 2002.

[104] B. Kardynal, S. Hees, A. Shields, C. Nicoll, I. Farrer, and D. Ritchie, *Photon number resolving detector based on a quantum dot field effect transistor*, **Applied Physics Letters**, vol. 90, no. 18, p. 1114, 2007.

[105] M. Rowe, E. Gansen, M. Greene, R. Hadfield, T. Harvey, M. Su, S. Nam, R. Mirin, and D. Rosenberg, *Single-photon detection using a quantum dot optically gated field-effect transistor with high internal quantum efficiency*, **Applied Physics Letters**, vol. 89, no. 25, p. 253505, 2006.

[106] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, *Noise-free high-efficiency photon-number-resolving detectors*, **Physical Review A**, vol. 71, no. 6, p. 061803, 2005.

[107] W. Meissner and R. Ochsenfeld, *Ein neuer effekt bei eintritt der supraleitfähigkeit*, **Naturwissenschaften**, vol. 21, no. 44, pp. 787–788, 1933.

[108] J. Bardeen, L. N. Cooper, and J. R. Schrieffer, *Theory of superconductivity*, **Physical Review**, vol. 108, no. 5, p. 1175, 1957.

[109] J. R. Schrieffer and M. Tinkham, *Superconductivity*, **Rev. Mod. Phys.**, vol. 71, pp. S313–S317, 1999.

[110] J. G. Bednorz and K. A. Müller, *Possible highT c superconductivity in the Ba- La- Cu- O system*, **Zeitschrift für Physik B Condensed Matter**, vol. 64, no. 2, pp. 189–193, 1986.

[111] M. E. Huber, P. Neil, R. G. Benson, D. Burns, A. M. Corey, C. S. Flynn, Y. Kitaygorodskaya, O. Massihzadeh, J. M. Martinis, G. Hilton, *et al.*, *DC SQUID series array amplifiers with 120 MHz bandwidth (corrected)*, **Applied Superconductivity, IEEE Transactions on**, vol. 11, no. 2, pp. 4048–4053, 2001.

[112] D. Koelle, R. Kleiner, F. Ludwig, E. Dantsker, and J. Clarke, *High-transition-temperature superconducting quantum interference devices*, **Reviews of Modern Physics**, vol. 71, no. 3, p. 631, 1999.

[113] Y. S. Greenberg, *Application of superconducting quantum interference devices to nuclear magnetic resonance*, **Reviews of Modern Physics**, vol. 70, no. 1, p. 175, 1998.

[114] M. A. Nielsen and I. L. Chuang, **Quantum Computation and Quantum Information**. Cambridge University Press, 2000.

[115] C. Kubrusly, **Elements of Operator Theory**. Birkhäuser, 2001.

[116] V. Vedral, **Introduction to Quantum Information Science**. Oxford University Press, 2006.

[117] J. Von Neumann, **Mathematical foundations of quantum mechanics**. No. 2, Princeton university press, 1955.

[118] G. B. Arfken, **Mathematical methods for physicists**. Academic press, 2013.

[119] R. Loudon, **The quantum theory of light**. Oxford university press, 2000.

[120] I. Abram, *Quantum theory of light propagation: Linear medium*, **Physical Review A**, vol. 35, no. 11, p. 4661, 1987.

[121] L. Knöll, W. Vogel, and D.-G. Welsch, *Action of passive, lossless optical systems in quantum optics*, **Physical Review A**, vol. 36, no. 8, p. 3803, 1987.

[122] P. D. Drummond, *Electromagnetic quantization in dispersive inhomogeneous nonlinear dielectrics*, **Physical Review A**, vol. 42, no. 11, p. 6845, 1990.

[123] R. J. Glauber and M. Lewenstein, *Quantum optics of dielectric media*, **Physical Review A**, vol. 43, no. 1, p. 467, 1991.

[124] L. Knöll and D.-G. Welsch, *QED of resonators in quantum optics*, **Progress in quantum electronics**, vol. 16, no. 3, pp. 135–182, 1992.

[125] H. Khosravi and R. Loudon, *Vacuum field fluctuations and spontaneous emission in a dielectric slab* in **Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences**, vol. 436, pp. 373–389, 1992.

[126] B. Huttner and S. M. Barnett, *Quantization of the electromagnetic field in dielectrics*, **Physical Review A**, vol. 46, no. 7, p. 4306, 1992.

[127] S. Dutra and G. Nienhuis, *Derivation of a Hamiltonian for photon decay in a cavity*, **Journal of Optics B: Quantum and Semiclassical Optics**, vol. 2, no. 5, p. 584, 2000.

[128] C. Viviescas and G. Hackenbroich, *Field quantization for open optical cavities*, **Physical Review A**, vol. 67, no. 1, p. 013805, 2003.

[129] S. Scheel and S. Y. Buhmann, *Macroscopic quantum electrodynamics – concepts and applications*, **Acta Phys. Slovaca**, vol. 58, no. 5, pp. 675–809, 2008.

[130] T. G. Philbin, *Canonical quantization of macroscopic electromagnetism*, **New Journal of Physics**, vol. 12, no. 12, p. 123008, 2010.

[131] T. M. Barlow, R. Bennett, and A. Beige, *A master equation for a two-sided optical cavity*, **Journal of modern optics**, vol. 62, no. sup2, pp. S11–S20, 2015.

[132] R. J. Glauber, *Coherent and Incoherent States of the Radiation Field*, **Phys. Rev.**, vol. 131, pp. 2766–2788, 1963.

[133] G. I. Taylor, *Interference Fringes with Feeble Light*, **Proceedings of the Cambridge Philosophiical Society**, vol. 15, pp. 114–115, 1909.

[134] R. Hanbury Brown and R. Q. Twiss, *A Test of a New Type of Stellar Interferometer on Sirius*, **Nature**, vol. 178, pp. 1046–1048, 1956.

[135] T. Jeltes, J. M. McNamara, W. Hogervorst, W. Vassen, V. Krachmalnicoff, M. Schellekens, A. Perrin, H. Chang, D. Boiron, A. Aspect, and C. I. Westbrook, *Comparison of the Hanbury Brown–Twiss effect for bosons and fermions*, **Nature**, vol. 445, no. 7126, pp. 402–405, 2007.

[136] P. Grangier, G. Roger, and A. Aspect, *Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences*, **EPL (Europhysics Letters)**, vol. 1, no. 4, p. 173, 1986.

[137] H. J. Kimble, M. Dagenais, and L. Mandel, *Photon antibunching in resonance fluorescence*, **Physical Review Letters**, vol. 39, no. 11, p. 691, 1977.

[138] J. G. Rarity, P. R. Tapster, and R. Loudon, *Non-classical interference between independent sources*, **Journal of Optics B: Quantum and Semiclassical Optics**, vol. 7, p. S171, 2005.

[139] L. Davidovich, *Sub-Poissonian processes in quantum optics*, **Reviews of Modern Physics**, vol. 68, no. 1, p. 127, 1996.

[140] L. Mandel and E. Wolf, **Optical coherence and quantum optics**. Cambridge university press, 1995.

[141] R. J. Glauber, *The Quantum Theory of Optical Coherence*, **Phys. Rev.**, vol. 130, pp. 2529–2539, 1963.

[142] U. Fano, *Quantum theory of interference effects in the mixing of light from phase-independent sources*, **American Journal of Physics**, vol. 29, no. 8, pp. 539–545, 1961.

[143] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference*, **Phys. Rev. Lett.**, vol. 59, pp. 2044–2046, 1987.

[144] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, *Observation of a "quantum eraser": A revival of coherence in a two-photon interference experiment*, **Phys. Rev. A**, vol. 45, pp. 7729–7739, 1992.

[145] T. B. Pittman, D. V. Strekalov, A. Migdall, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, *Can Two-Photon Interference be Considered*

the Interference of Two Photons?, **Phys. Rev. Lett.**, vol. 77, pp. 1917–1920, 1996.

[146] K. J. Resch, K. L. Pregnell, R. Prevedel, A. Gilchrist, G. J. Pryde, J. L. O'Brien, and A. G. White, *Time-Reversal and Super-Resolving Phase Measurements*, **Phys. Rev. Lett.**, vol. 98, p. 223601, 2007.

[147] P. A. M. Dirac, **The Principles of Quantum Mechanics**. Oxford University Press, fourth ed., 1930.

[148] T. Ferreira da Silva, G. C. Amaral, D. Vitoreti, G. P. Temporão, and J. P. von der Weid, *Spectral characterization of weak coherent state sources based on two-photon interference*, **J. Opt. Soc. Am. B**, vol. 19, pp. 716–723, 2015.

[149] T. Legero, T. Wilk, A. Kuhn, and G. Rempe, *Time-Resolved Two-Photon Quantum Interference*, **Appl. Phys. B**, vol. 77, pp. 797–802, 2003.

[150] V. Vedral, **Modern foundations of quantum optics**. Imperial College Press, 2005.

[151] A. Peres, **Quantum theory: concepts and methods**. Springer Science & Business Media, 2006.

[152] B. Kardynał, Z. Yuan, and A. Shields, *An avalanche‐ photodiode-based photon-number-resolving detector*, **Nature photonics**, vol. 2, no. 7, pp. 425–428, 2008.

[153] G. C. Amaral, **FPGA Applications on Photon Detection Systems**. M.S. thesis, Dept. Elect. Eng., PUC-Rio Univ., Rio de Janeiro, RJ, Brazil, 2014.

[154] X. Ma, C.-H. F. Fung, and M. Razavi, *Statistical fluctuation analysis for measurement-device-independent quantum key distribution*, **Physical Review A**, vol. 86, no. 5, p. 052305, 2012.

[155] Stanford Research Systems, *DG645 – Digital Delay and Pulse Generator (4 or 8 channels)* - `http://www.thinksrs.com/downloads/PDFs/Catalog/DG645c.pdf`. Accessed: 2016-02-05.

[156] K. Wang, vol. 39, no. 18, p. R293, 2006.

[157] N. Wiener, **Extrapolation, interpolation, and smoothing of stationary time series**, vol. 2. MIT press Cambridge, MA, 1949.

[158] G. P. Agrawal, **Fiber-Optic Communication Systems**. John Wiley & Sons, second ed., 2002.

[159] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, *Quantum Beat of Two Single Photons*, **Phys. Rev. Lett.**, vol. 93, p. 070503, 2004.

[160] G. C. Amaral, T. Ferreira da Silva, G. P. Temporão, and J. P. von der Weid, *Few-Photon Spectroscopy*, **Optics Letters**, vol. –, no. –, pp. –, 2015.

[161] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices*, **Quantum Inf. Comput.**, vol. 4, pp. 325–360, 2004.

[162] J. J. Sakurai, **Modern quantum mechanics**. Addison-Wesley Pub. Co, revised ed., 1994.

[163] G. C. Amaral, F. Calliari, T. Ferreira da Silva, G. P. Temporão, and J. P. von der Weid, *Sub-Poisson States Heralded at a Hong-Ou-Mandel Interference Peak*, **ArXiV**, 2016.

[164] E. Schrödinger, *An undulatory theory of the mechanics of atoms and molecules*, **Physical Review**, vol. 28, no. 6, p. 1049, 1926.

[165] H. F. Baker, *Alternants and continuous groups*, **Proceedings of the London Mathematical Society**, vol. 2, no. 1, pp. 24–47, 1905.

[166] F. Hausdorff, *Die symbolische Exponentialformel in der Gruppentheorie*, **Ber. Verh. Kgl. S. chs. Ges. Wiss. Leipzig., Math.-phys. Kl.**, vol. 58, pp. 19–48, 1906.

[167] J. R. Klauder, *Continuous-Representation Theory. II. Generalized Relation between Quantum and Classical Dynamics*, **Journal of Mathematical Physics**, vol. 4, no. 8, pp. 1058–1073, 1963.

[168] D. Bouwmeester, A. Ekert, A. Zeilinger, *et al.*, **The physics of quantum information**, vol. 3. Springer, Berlin, 2000.

[169] Vernam, Gilbert S, , *Secret signaling system* 1919. US Patent 1,310,719.

[170] Rivest, Ronald L and Shamir, Adi and Adleman, Leonard M, , *Cryptographic communications system and method* 1983. US Patent 4,405,829.

[171] H.-K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, **science**, vol. 283, no. 5410, pp. 2050–2056, 1999.

[172] N. Lütkenhaus, *Security against individual attacks for realistic quantum key distribution*, **Physical Review A**, vol. 61, no. 5, p. 052304, 2000.

[173] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, **Reviews of modern physics**, vol. 81, no. 3, p. 1301, 2009.

[174] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, *Superlinear threshold detectors in quantum cryptography*, **Physical Review A**, vol. 84, no. 3, p. 032320, 2011.

[175] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, *Experimentally faking the violation of Bell's inequalities*, **Physical Review Letters**, vol. 107, no. 17, p. 170404, 2011.

[176] Q. Liu, A. Lamas-Linares, C. Kurtsiefer, J. Skaar, V. Makarov, and I. Gerhardt, *A universal setup for active control of a single-photon detector*, **Review of Scientific Instruments**, vol. 85, no. 1, p. 013108, 2014.

[177] Z. Yuan, J. Dynes, and A. Shields, *Avoiding the blinding attack in QKD*, **Nature Photonics**, vol. 4, no. 12, pp. 800–801, 2010.

[178] Z. Yuan, J. Dynes, and A. Shields, *Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography*, **Applied physics letters**, vol. 98, no. 23, p. 231104, 2011.

[179] R. H. Hadfield, *Single-photon detectors for optical quantum information applications*, **Nature photonics**, vol. 3, no. 12, pp. 696–705, 2009.

[180] M. Eisaman, J. Fan, A. Migdall, and S. Polyakov, *Invited review article: Single-photon sources and detectors*, **Review of Scientific Instruments**, vol. 82, no. 7, p. 071101, 2011.

[181] Z. Yuan, B. Kardynal, A. Sharpe, and A. Shields, *High speed single photon detection in the near infrared*, **Applied Physics Letters**, vol. 91, p. 041114, 2007.

[182] N. Namekata, S. Adachi, and S. Inoue, *Ultra-low-noise sinusoidally gated avalanche photodiode for high-speed single-photon detection at telecommunication wavelengths*, **Photonics Technology Letters, IEEE**, vol. 22, no. 8, pp. 529–531, 2010.

[183] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, **Physical review**, vol. 47, no. 10, p. 777, 1935.

[184] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, **Physics**, vol. 1, 1964.

[185] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, **Physical review letters**, vol. 23, no. 15, p. 880, 1969.

[186] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, **Nature**, vol. 526, no. 7575, pp. 682–686, 2015.