UNIVERSITÀ DI CAMERINO

SCHOOL OF ADVANCED STUDIES

Doctorate course in

Physics

Experimental Study of the Quantum States of Light and Realization of a Quantum Communication Protocol

Cycle XIX

Scientific-Sector FIS/03

PhD Candidate
Alessandro Cerè

Tutor
Prof. Paolo Tombesi

2003/04 – 2005/06

Abstract

I present how to obtain and characterize quantum states of light potentially useful for quantum communication protocols. The control of the frequency correlations, and the bandwidth, of single and paired photons is an essential ingredient in specific quantum applications, from quantum imaging to quantum clock synchronization. I show both theoretical and experimental spectral correlations of pairs of photons generated in non-collinear spontaneous parametric down conversion (SPDC). In the second part of the work, a scheme for quantum key distribution using the two-way LM05 protocol [PRL **94**, 140501 (2005)] and its implementation is presented too. A preliminary transmission test is discussed together with an experimental study for the security of the generated key in presence of noise in the channels. The noise is modulated as to simulate the effect of an eavesdropper.

Contents

Introduction

In this thesis is presented the work of three years of doctorate mostly spent in the recently founded laboratory of Quantum Optics of the University of Camerino. There is a part of the work that cannot be shown that corresponds to the initial set up of the laboratory. Anyway this has been an interesting and formative experience. What there will be in this thesis is the scientific and possibly original contribution to Quantum Optics and Quantum Communication.

In the first part of this thesis I will present the work developed in collaboration with the Quantum inforation Processing Group directed by Prof. Juan Perez Torres at the ICFO-The institute of photonic sciences. It is mainly focused in the control of the kind of correlations between pairs of photons generate in noncollinear down conversion.

In the second part I will present the work developed in Camerino under the supervision of Giovanni Di Giuseppe, Ph.D., and my advisor Prof. Paolo Tombesi. The goal of my research there was the creation of a source of entangled light to be used in the experimental study of Quantum Communication.

Quantum Communication and Quantum Optics have tight connections, one offering the other the mean for real world application and realization. The photon and its interactions with matter is the main subject of Quantum Optics and is also an (almost) ideal carrier for Quantum Information. It is already used for transmitting

classical information, everyone today is aware of the continuously growing network of optical fibers that is replacing the old network based in electrical signal.

The heart of Quantum communication is the Qubit [Schumacher 95], the quantum analogous of the classical bit. The qubit is usually described as a state vector for a two levels quantum system:

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

where α and β are complex coefficients. The photon can easily be seen as physical support for a qubit, its polarization has the correct dimensionality. The peculiarities due to its quantum-mechanical nature allows for a more efficient and more secure communication using qubits, often when is another typically quantum phenomeon is involved, the Entanglement.

Entanglement has proved to be one of the most interesting and peculiar feature of the quantum world. Since its introduction in the seminal work of Einstein, Podolski and Rosen [Einstein 35] as attracted the attention of a large number of physicist. Schrödinger singled out many decades ago that entanglement is "the characteristic trait of quantum mechanics" [Schrödinger 35] and that has been studied extensively in connection with Bell's inequalities [Bell 64, Bell 66]. Entanglement fame grown bigger, outbounding the circle of physicist and epistemologist when in 1982 Feynman proposed a Quantum Computer [Feynman 82], a quantum system based on entanglement that can in principle simulate any other quantum system. When, in 1996, Shor presented [Shor 94] an algorithm that could factorize large number exploiting the entanglement of a system, entanglement was by then a celebrity.

As said, Entanglement is one of the main actors in many quantum communication protocols. The first protocol proposed that in principle can beat the

transmission capacity of classical system was Dense Coding [Bennett 92]. The underlying idea is to use the correlations associated with the entanglement of two qubits to transmit two classical bit of information sending a single qubit. Quantum state are fragile, any interaction with the environment can destroy its coherence. On the other side, the no cloning theorem introduced by Wootters and Zurek [Wootters 82] states the non existence of a quantum machine that can copy with perfect fidelity any quantum state; this limitation comes directly from the principles of quantum mechanics. It is thus impossible to create several copies of the qubit to send. Soon the dense coding was followed by a protocol, the quantum teleportation [Bennet 93]. Transmitting the state of a qubit without degradation is possible via teleportation that expoits a previously shared EPR pair and a classical communication channel. Quantum Teleportation is now a key element in the proposed realization of a Quantum Computer [Knill 01].
The most promising application in the short period for Quantum Communication is the Quantum Cryptography. Initially proposed by Bennet and Brassard[Bennett 84], it bases its security on the no-cloning theorem and allows the generation of a common one-time-use key between the two parties of the communications. The security offered by Quantum Cryptography attracted a lot of interest. The accurate review of Gisin et al. [Gisin 02] reports the many advancement in the practical realization of cryptographic system, from the first tests to the already commercially available on the market quantum boxes.

In the laboratory of Camerino I took part in the realization of a test setup for a novel protocol, the LM05 [Lucamarini 05]. The results of this experiment are not only reported on this thesis but were also published in Physical Review

Letters [Cerè 06].

The work is organized as follows: In chapter 1 is presented the theory of Type-I noncollinear down conversion as a way to control the frequency correlations of the paired photons. In chapter 2 is presented the experimental verification of the theory of chapter 1. It is also shown how the use of a non-Gaussian pump beam produces notable correlation shapes. The study on photons is then shifted from the frequency domain to the polarization one in chapter 3. Here is reported the setup of a source for the generation of polarization entangled photon pair followed by a complete characterization of the state via a tomographic technique.
In chapter 4 I introduce the test system developed for a recently proposed quantum communication protocol. The same test system is used in chapter 5 for studying the effect of noise and for simulating the resistance to an attack from an eavesdropper of the protocol.

Chapter 1

Tailoring of Frequency Correlation of Paired Photons in Noncollinear Down Conversion

A widely used source for quantum light is the Spontaneous Parametric Down Conversion (SPDC).

The control of the characteristics of the quantum light generated is of fundamental importance both for achieving peculiar quantum effects and for practical implementation of quantum communication protocols. An appropriate tailoring of the spectral properties of the entangled two-photon states is often required for efficient information encoding. For example, chromatic dispersion can cause problems for quantum cryptography schemes implemented in optical fibers, when utilizing photon pairs created via SPDC. Therefore, several schemes suitable for transmission over long distances, such as time-bin entanglement, can strongly benefit from frequency engineered, e.g. narrowband-entangled states [Gisin 02].

Several other quantum-optical applications that make use of the frequency entanglement of the two photons can also benefit from such manipulation. In particular, frequency-correlated two-photon states can be used for improving the accuracy of clock synchronization [Giovannetti 01, Giovannetti 02]. Elimination of the strong correlations between the frequencies of the two photons is required for performing linear-optical logic operations [Grice 01, U'Ren 05], suppression of spectral information is crucial for experiments that make use of a portion of the state of two particles [Branning 99], and entangled photons with increased spectral width are needed for enhancing the resolution in quantum optical coherence tomography schemes[Abouraddy 02].

In this chapter I present a theoretical proposal for controlling the frequency correalation of the biphoton generated in noncollinear type-I SPDC via control of the spatial features of the pump beam.

This work was performed in the laboratories of the Quantum Information Group (QIP) directed by prof. Juan Perez Torres at ICFO-The Institute of Photonic Sciences of Barcelona (Spain).

1.1 Theory

SPDC is a non linear optical process in which, when an intense pump laser beam (p) shines a nonlinear crystal, occasionally, one pump photon is down-converted into a pair of lower frequency photons, convectionally labelled signal (s) and idler (i). The generation of the down converted photons is constrained by two conservation laws [Boyd 02]. The energy in the process is conserved. This constraint determines the frequency of the photons. The second constraint is the momentum conservation and defines the geometry of the process. In this chapter I analyze the down

conversion process in the case of non collinear geometry for frequency degenerate Type I generation.

Because of the weak coupling between the fields inside the non-linear crystal, the quantum state of the SPDC radiation can be calculated by using time dependent perturbation theory. To first order, the two-photon state is given by

$$|\psi\rangle = |0,0\rangle - \frac{i}{\hbar}\int_0^\tau \mathrm{dt}\boldsymbol{H}_\mathrm{I}(\mathrm{t})\,|0,0\rangle\,, \tag{1.1}$$

where $|0,0\rangle$ is the vacuum state in the mode i and s, τ is the interaction time and $\boldsymbol{H}_I$ is the effective Hamiltonian in Interaction picture given by [Klyshko 69]:

$$\boldsymbol{H}_I = \varepsilon_0 \int dV \chi^{(2)} \boldsymbol{E}_p^+(\vec{r},t)\boldsymbol{E}_s^-(\vec{r},t)\boldsymbol{E}_i^-(\vec{r},t) + h.c., \tag{1.2}$$

where the integral is performed over the interaction volume. The $\boldsymbol{E}_j^\pm$ are the positive and negative frequency components of the electric field operators associated to the pump, signal and idler photons.

For a paraxial beam propagating along the $\vec{z}$ direction, the positive frequency component can be expanded in plane waves as:

$$\boldsymbol{E}_p^+(\vec{x},z,t) \propto \int d^2q_p \int d\omega_p \xi_p(\vec{q}_p)\xi_\omega(\omega_p)\exp(ik_p z + i\vec{q}_p\cdot\vec{x} - i\omega_p t), \tag{1.3}$$

where k_p is the longitudinal wave number inside the crystal, $\vec{q}_p$ is the transverse wave momentum, ω_p is the angular frequency and $\xi(\vec{q}_p)$ and $xi(\omega_p)$ describe the transverse momentum and the angular frequency distribution of the pump beam at the input face of the non linear crystal, respectively. The previous expression is derived under the assumption of intense pump beam, justifying the classical treatment.

For the idler and signal photons the negative-frequency field operator inside the crystal can be written as:

$$\boldsymbol{E}_j^-(\vec{x}_j,z_j,t) \propto \int d^2q_j \int d\omega_j \exp(-ik_j z_j - i\vec{q}_j\cdot\vec{x}_j + i\omega_j t)\boldsymbol{a}_j^\dagger(\omega_j,\vec{q}_j). \tag{1.4}$$

where ω and $\vec{q}$ denote the frequency and transverse momentum variables for signal (s) and idler (i) photons, respectively. $\boldsymbol{a}^{\dagger}_{\omega_j,\vec{q}_j}$ is the creation operator for a photon in a mode with frequency ω_j and transverse momentum $\vec{q}_j$.

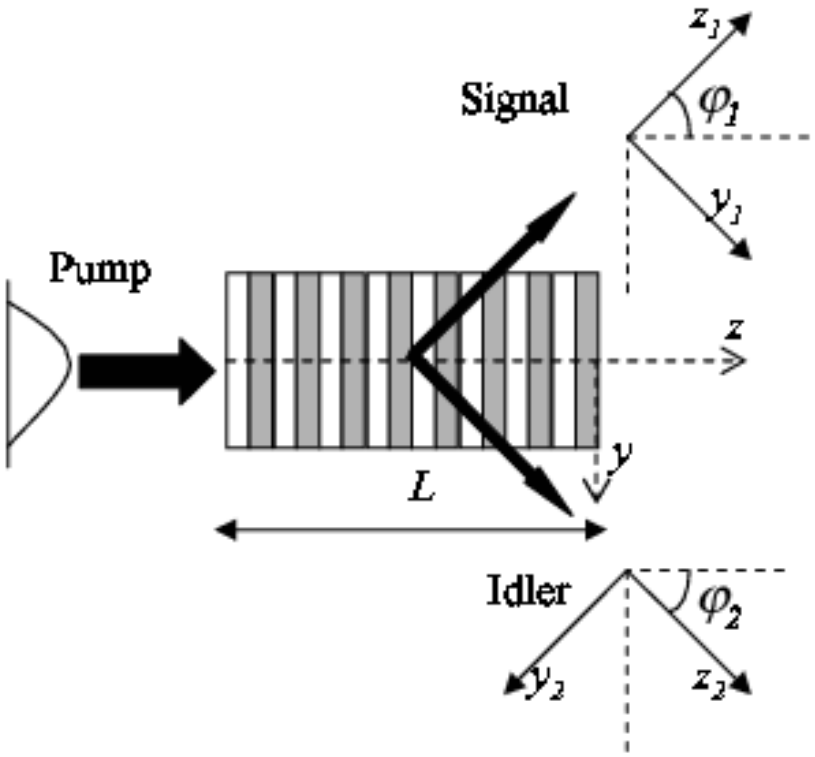


Figure 1.1: *Sketch of the non collinear SPDC geometry, showing the propagation directions of the pump, signal, and idler photons.*

To elucidate the spatial structure of the two-photon state in the noncollinear geometry, we define $x_{1,2} = x$, $y_{1,2} = y\cos\phi_{1,2} + z\sin_{1,2}$, and $z_{1,2} = z\cos\phi_{1,2} - y\sin\phi_{1,2}$, where $\phi_{1,2}$ are the angles formed by the direction of propagation of the pump beam, z, and the direction of propagation of the signal, z_1, and idler photons, z_2, respectively (see Fig.1.1).

Substituting the Pump (Eq. (1.3)), Signal and Idler (Eq.(1.4)) field into the (1.1),

the quantum state of the two-photon is given by:

$$|\psi\rangle = \int d\omega_s \int d\omega_i \int d^2\vec{q}_s \int d^2\vec{q}_i \Phi(\omega_s, \omega_i, \vec{q}_s, \vec{q}_i) \boldsymbol{a}^\dagger_{\omega_s,\vec{q}_s} \boldsymbol{a}^\dagger_{\omega_i,\vec{q}_i} |0,0\rangle \tag{1.5}$$

The function $\Phi(\omega_s, \omega_i, \vec{q}_s, \vec{q}_i)$ in Eq. (1.5) corresponds to the two-photon amplitude or Biphoton. It contains all the information about the frequency and momentum correlations of the two-photon state.

I will examine the case of a crystal of length L, cut for degenerate, non-collinear Type-I SPDC. As it will be shown, this configuration will allow the control of the type of frequency correlations exhibited by the pairs of photons as well as the bandwidth of the single photons. The Biphoton in this case reads [Carrasco 04]:

$$\Phi(\omega_s, \omega_i, \vec{q}_s, \vec{q}_i) = \xi_{\vec{q}}(\vec{q}_{sx} + \vec{q}_{ix}, \Delta_0)\xi_{\omega_p}(\omega_p) F_{pm}(\Delta_k L/2) \exp\{-i\Delta_k L/2\}. \tag{1.6}$$

where $\xi_{\vec{q}}$ and ξ_{ω_p} are functions that describe respectively the transverse momentum distribution and the frequency distribution of the pump already introduced in (1.3). The term Δ_0 comes from the phase matching along the y direction in the transverse plane:

$$\Delta_0 = |\vec{q}_{sy}| \cos\varphi_1 + |\vec{q}_{iy}| \cos\varphi_2 - k_s \sin\varphi_1 - k_i \sin\varphi_2. \tag{1.7}$$

The function $F_{pm}(\Delta_k L/2)$ represents the phase matching conditions inside the crystal [Carrasco 04], there appears the momentum mismatch in the z direction

$$\Delta_k = k_p - k_s \cos\varphi_1 - k_i \cos\varphi_2 - |\vec{q}_{sy}| \sin\varphi_1 - |\vec{q}_{iy}| \sin\varphi_2. \tag{1.8}$$

We are interested in the spectral properties of the SPDC photon pairs, for this we consider $\vec{q}_s{=}\vec{q}_i = 0$ in Eq. (1.6). All the frequency correlations of the photon pairs (except a phase factor) will be given by $|\Phi(\omega_s, \omega_i, \vec{q}_s = 0, \vec{q}_i = 0)|^2$ and its

physics can be better understood defining the new variables $\Omega_j = \omega_j - \omega_j^0$ for the signal ($j = s$), idler ($j = i$) and pump ($j = p$) photons and expanding $k_j(\omega_j)$ in a Taylor series around the central frequencies, ω_j^0, up to first order. With these considerations the joint spectrum can be rewritten as

$$|\Phi(\Omega_s, \Omega_i, \vec{q}_s = 0, \vec{q}_i = 0)|^2 = |\xi_{\vec{q}}(0, \Delta_0^0)\xi_{\omega_p}(\omega_p)F_{pm}(\Delta_k^0 L/2)|^2. \tag{1.9}$$

The momenta mismatches in the previous expression can be connected with frequency:

$$\Delta_0^0 = N_s \sin\varphi(\Omega_i - \Omega_s) \tag{1.10}$$

and

$$\Delta_k^0 = (N_p - N_s \cos\varphi)(\Omega_s + \Omega_i) \tag{1.11}$$

where $N_j \equiv dk_j/d\omega_j$ is the inverse of the group velocity for the signal ($j = s$), idler ($j = i$) and pump ($j = p$) photons when the case of Type-I degenerate SPDC is under consideration.

The key point to understand the control of the frequency correlations of pairs of photons in type-I noncollinear SPDC is in Eq. (1.9). To better visualize the correlation and anticorrelation properties associated with $\Phi(\Omega_s, \Omega_i, \vec{q}_s = 0, \vec{q}_i = 0)$, let us define the variables $\Omega_+ = \Omega_s + \Omega_i$ and $\Omega_- = \Omega_s - \Omega_i$. It is easy to see that Eq. (1.9) can be rewritten as the product of two functions, one in the variable Ω_+ and other in the variable Ω_-:

$$|\Phi(\Omega_+, \Omega_-, \vec{q}_s = 0, \vec{q}_i = 0)|^2 = \left|\xi_{\vec{q}}(0, N_s \sin\varphi\Omega_-)\xi_{\omega_p}(\omega_p)F_{pm}\big((N_p - N_s\cos\varphi)\Omega_+ L/2\big)\right|^2. \tag{1.12}$$

I define the quantity B_+ and B_- as the bandwidth (rms) in the variables Ω_+ and

Ω_- of $\Phi(\Omega_s, \Omega_i, \vec{q}_s = 0, \vec{q}_i = 0)$. The plus term is associated with the frequency correlation of the photons, while the minus term to the frequency anticorrelations. A biphoton is thus defined correlated (anticorrelated) if $B_+ > B_-$ ($B_+ < B_-$). In the case that $B_+ = B_-$ we talk about uncorrelated photons.

The behavior of the biphoton function of Eq. 1.12 in the variable Ω_+ is determined by the phase matching function and the frequency distribution of the pump beam. On the other hand, the dependencies in the variable Ω_- are given by transverse momentum distribution of the pump beam.

Our approach to control the frequency correlations of the SPDC photon pairs consist in manipulate the spatial distribution of the pump, $\xi_{\vec{q}}$ and therefore, engineering in this way the frequency correlations at will. To illustrate this approach mathematically, I start considering that the phase matching function $F_{pm}(\Delta_k^0 L/2) = \mathrm{sinc}(\Delta_k^0 L/2)$ can be approximated by a Gaussian function that has the same width at the $1/e^2$ of the intensity.

$$\mathrm{sinc}(bx) \simeq \exp\left\{-(\alpha b)^2 x^2\right\}, \tag{1.13}$$

with $\alpha = 0.455$.

I also assume a pump beam with an amplitude frequency distribution given by

$$\xi_{\omega_p}(\omega_p) = \exp\left(-\frac{\omega_p^2}{4\sigma_p^2}\right), \tag{1.14}$$

where σ_p is the bandwidth of the pump. Regarding the spatial distribution of the pump beam, I consider a Gaussian beam with a transverse momentum distribution:

$$\xi_{\vec{q}_p}(\vec{q}_p) = \exp\left(-\frac{|\vec{q}_p|^2 W_0^2}{4}\right) \tag{1.15}$$

with W_0 being the beam radius waist of the pump beam. Under these considera-

tion, Eq. (1.12) can be written as

$$|\Phi(\Omega_+,\Omega_-,\vec{q}_s=0,\vec{q}_i=0)|^2 = \exp\left(-\frac{\Omega_+^2}{2\left(T_0^2+(\alpha L)^2\left(N_p-N_s\cos\varphi\right)^2\right)+\frac{1}{B_0^2}}\right)\times \exp\left(-\frac{\Omega_-^2}{2(N_s\sin\varphi W_0)^2+\frac{1}{B_0^2}}\right), \quad (1.16)$$

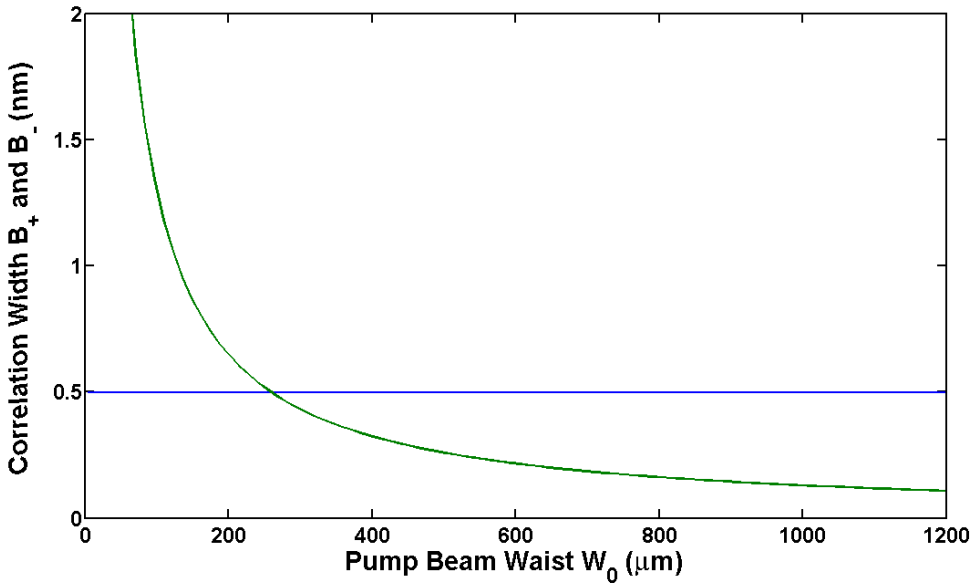


Figure 1.2: *Theoretical values of B_+ (blue) and B_- (green) as function of the pump beam waist W_0 for non collinear SPDC photons. Parameters: the crystal is a $LiIO_3$ 1 mm long, the pump beam has a bandwidth of σ_p =0.258 nm, the selected internal aperture angle is 17°.*

where the term $1/B_0$ takes into account the presence of frequency filters in front of the detectors. These filters are considered as having a Gaussian amplitude distribution of the form $\exp\left\{-\omega_{s,i}^2/(4B_0^2)\right\}$ and being identical for the signal and idler paths.

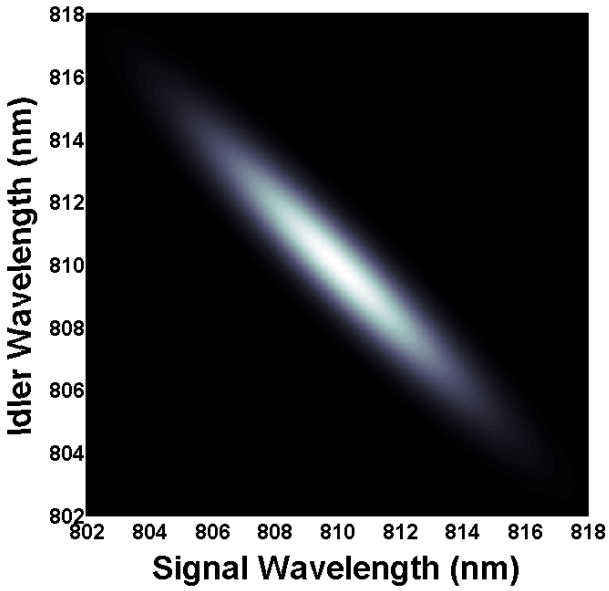


Figure 1.3: *Theoretical joint spectrum for non collinear SPDC photons. Parameters: the crystal is a $LiIO_3$ 1 mm long; the selected internal aperture angle is 17° and the incident pump beam waist is 36 μm.*

It is easy to see how by changing the waists pump, it is possible to get different types of frequency correlations, as evident from Fig. 1.2. In Fig. 1.3, 1.4 and 1.5 we can see the joint spectrum for three different values of the pump waist radius. Fig. 1.3 shows the joint spectrum of frequency anticorrelated photons, Fig. 1.4 corresponds to a circular shape indicating the complete absence of any type of correlations and Fig. 1.5 depicts pairs of photons with correlated frequencies.

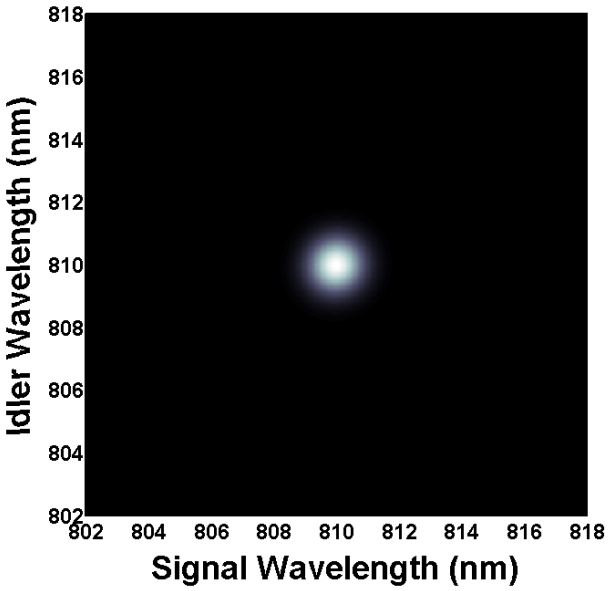


Figure 1.4: *Theoretical joint spectrum for non collinear SPDC photons. Parameters: the crystal is a $LiIO_3$ 1 mm long; the selected internal aperture angle is 17° and the incident pump beam waist is 250 μm.*

1.2 Spatial to Spectral Mapping

Noncollinear SPDC also allows for the generation of paired photons with controllable waveforms [Carrasco 04]. By making use of a specific noncollinear configuration of the parametric interaction, together with specially designed spatial profiles of the pump beam, it is possible to tailor the spectral properties of the two-photon state over a wide range of possibilities. The key point is that the spectral function, Eq. (1.12), contains the pump transverse momentum term $\xi_{\vec{q}}(0, \Delta_0^0)$. Due to the mixing of momentum and frequency conservation rules that governs noncollinear SPDC process, the spatial shape of the pump beam and the frequency spectra of the downconverted photons are related. Let us consider shining a Laguerre-Gauss beam as pump on the nonlinear crystal. The momentum distribution of the pump

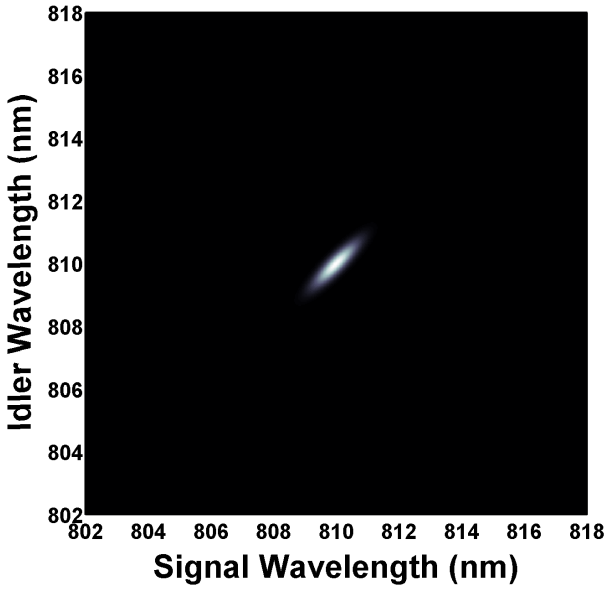


Figure 1.5: *Theoretical joint spectrum for non collinear SPDC photons. Parameters: the crystal is a $LiIO_3$ 1 mm long; the selected internal aperture angle is 17° and the incident pump beam waist is 500 μm.*

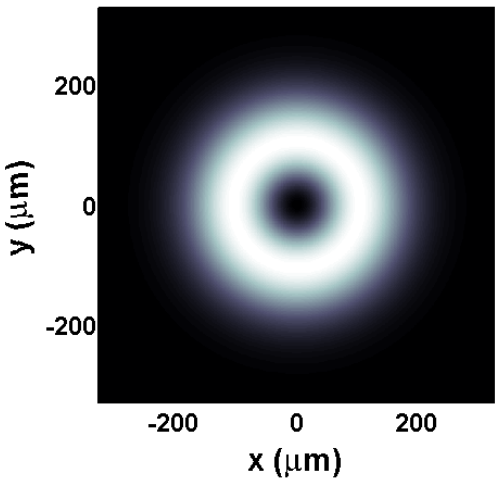
beam with azimuthal index $l = 2$ and radial index $p = 0$ (LG_{02}) writes [Allen 92]:

$$\xi_{\vec{q}}(\Delta_0^0) \propto \frac{\rho_p^2}{w^2}\, e^{-\frac{\rho_p^2}{w^2}}\, e^{2i\phi}, \tag{1.17}$$

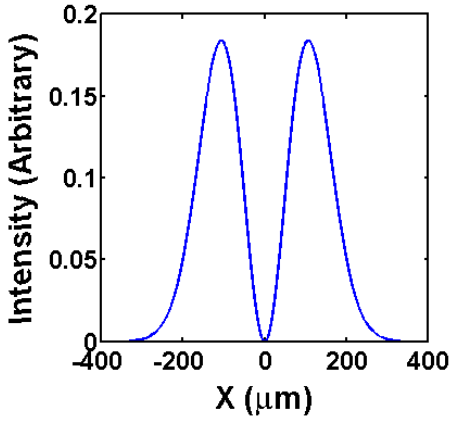
where ρ_p and ϕ_p are cylindrical coordinates in wave number space.

The spatial profile of the pump beam (see Fig. 1.6) gets mapped into the spectral correlations of the SPDC photons allowing tailoring the bandwidth, and in particular, the spectral shape of the generated two-photon states. Inserting the Eq. (1.17) into the Eq. (1.12) results in a non Gaussian shape of the correlation as evident if Fig. 1.7 and in Fig. .

The effect of the spatial pump profile in the spectral function of the photon pairs is then evident. Therefore, one can translate spatial features imprinted in the pump beam into desired spectral profiles of the generated entangled photon



(a) Intensity distribution



(b) Intensity profile

Figure 1.6: *Intensity distribution and profile for a Laguerre-Gauss mode with radial index p=0 and azimuthal index l=2.*

pairs, allowing in this way to obtain the specific forms of the spectral functions.

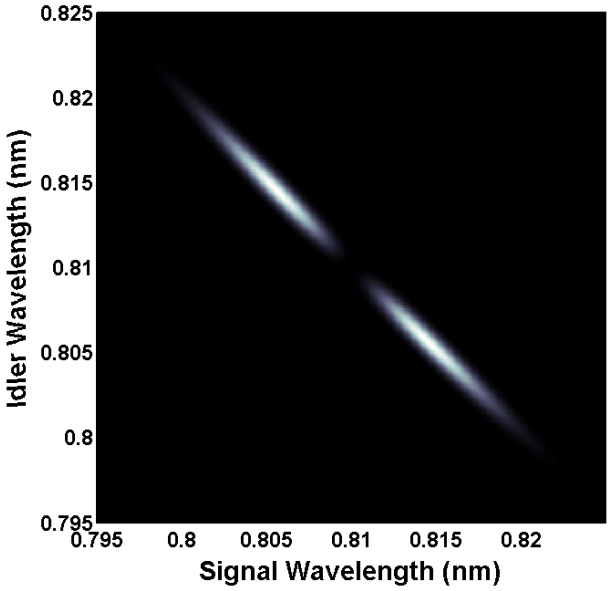
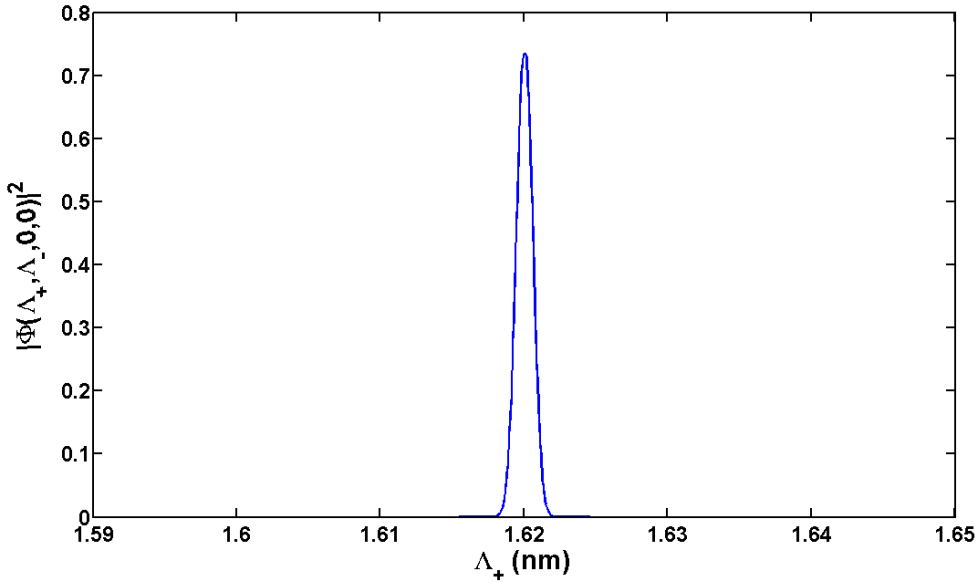
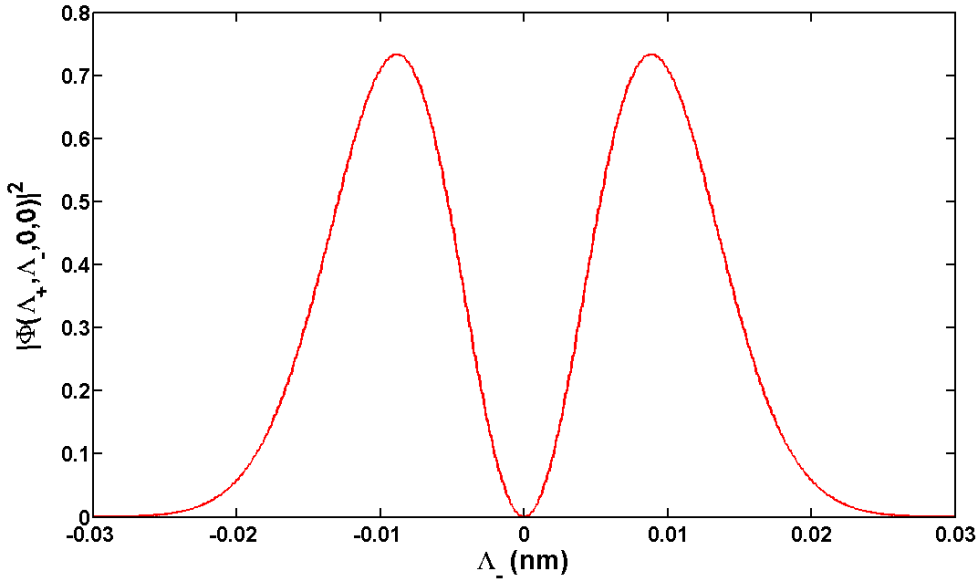


Figure 1.7: *Theoretical joint correlation spectrum for a LG_{02} pump beam. Details of the parameters used: crystal $LiIO_3$, thickness $L = 1$ mm, pump wavelength 405 nm, pump beam waist 150 μm.*



(a) Correlation profile in the Λ_+ direction.



(b) Correlation profile in the Λ_+ direction.

Figure 1.8: *Theoretical profiles of the correlation function calculated with the same parameters as in Fig. 1.7. In the 1.8(b) is evident the difference with a Gaussian distribution.*

Chapter 2

Experimental Control of Frequency Correlation in Type-I Noncollinear Down Conversion

After introducing the underlying theory in chapter 1, in this chapter I present the experimental results achieved in controlling the spectral correlation for a pair of Photons generated via spontaneous parametric down conversion (SPDC) in Type-I noncollinear configuration.

2.1 Experimental Setup

In Fig. 2.1 is depicted the experimental setup used to study the spectral correlation of the biphoton. The crystal used for down conversion is a 1 mm long $LiIO_3$, coated for high transmissivity at 405 nm and 810 nm. The crystal is cut for type-I down conversion, with the optical axis forming an angle of 90°with the input surface. The phase matching conditions give an internal angle of 17.1°for the degenerate case

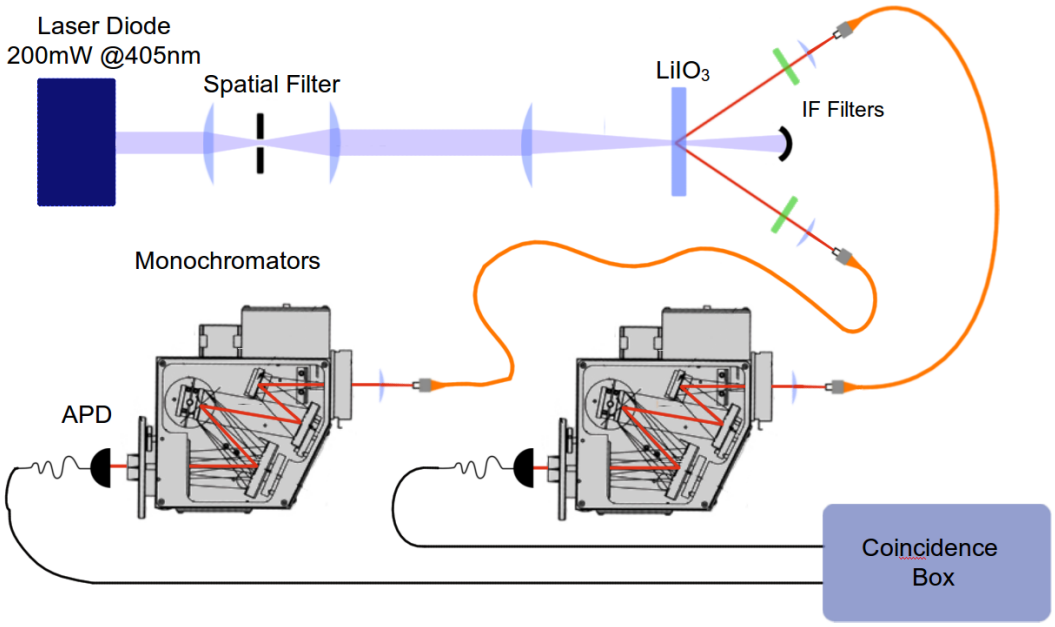


Figure 2.1: *Experimental setup for the study of spectral correlation of Signal and Idler photons in a non-linear Type-I down conversion.*

of Signal and Idler wavelength of $\lambda_s = \lambda_i = 810$ nm for a pump with $\lambda_p = 405$ nm. The pump laser is a CW laser diode (Nichia NDHV220APAE1) emitting at 405 nm and with nominal power of 200 mW. The output mode of the laser needs to be reshaped to obtain a good quality spatial mode thus a spatial filter was built, details will follow in next section. The single photons where detected by two APD single photon detectors.

2.1.1 Monochromators

A key component of the setup are the two monochromators (MC) (see Fig. 2.2). The characterization, alignment and calibration of the monochromators proved to be of crucial importance for the success of the experiment. We used a Hg-Ar

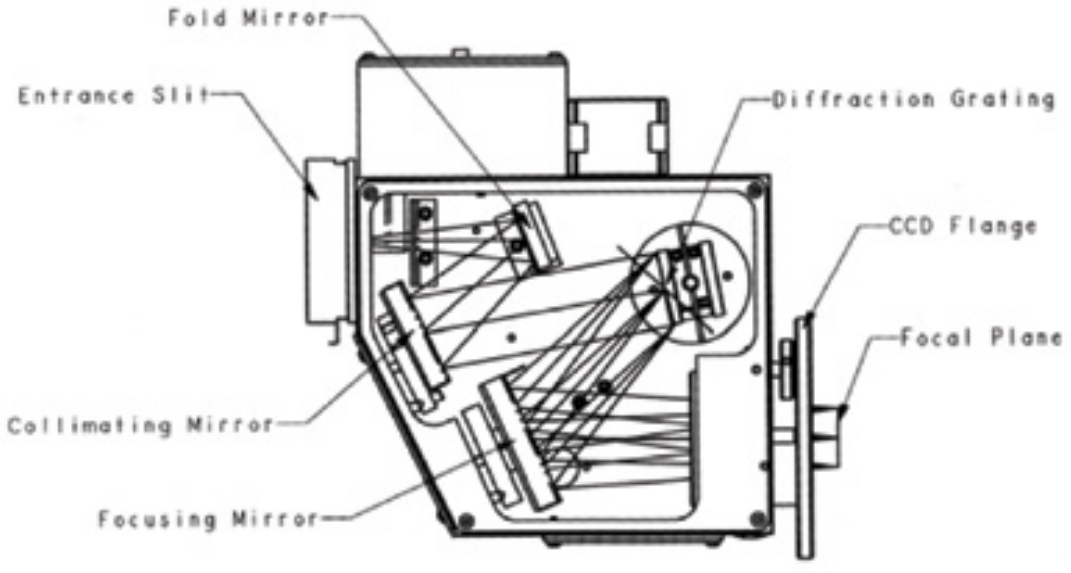


Figure 2.2: *Drawing of the Jobin Yvon MicroHR Czerny-Turner Monochromator. focal length 140 mm, Entrance Aperture Ratio f/3.9. Image from www.jobinyvon.com.*

calibration lamp (Avantes CAL-2000) to carry on a study of the resolution and optimize light collection. A multimode fiber is coupled to the entrance of each monochromator via two lenses: a short focus one (f=11 mm) for initial collimation and a f=50 mm for launching the light into the MC. The bandpass (PB) of a monochromator determines its resolution. The BP is mainly determined by the groove density of the grating and the with of the entrance and exit slits. It is important to realize that there is a tradeoff between resolution and efficiency. The nominal resolution of the monochromator is 0.25 nm. To measure the BP is necessary a mostly monochromatic source. A low-pressure Argon lamp provides the light we needed. It has two lines near the central frequency of interest (810 nm).

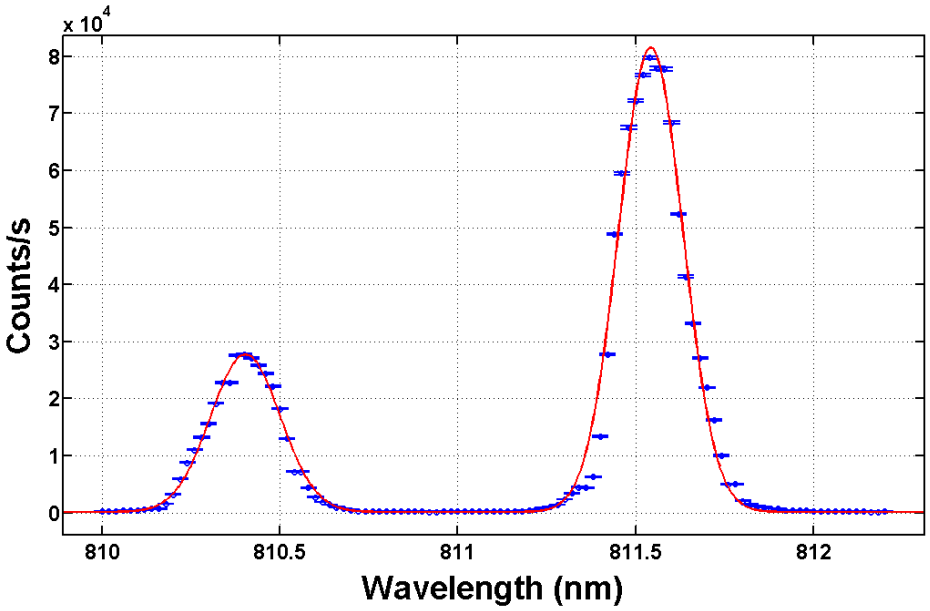


Figure 2.3: *Spectrum of the calibration lamp. Argon has two emission line near 810 nm, exactly one at 810.369 nm and at 811.531 with intensity ratio 1/17.5 between the two lines. The red line is a fit obtained as the sum of two Gaussian peaks:* $I(\lambda) = \frac{\alpha}{1.75} exp\{-\frac{(\lambda-\lambda_1^C)^2}{2\sigma_1^2}\} + \alpha exp\{-\frac{(\lambda-\lambda_2^C)^2}{2\sigma_2^2}\} + \gamma$. *The observed linewidth is the convolution of the real linewidth and the resolution of the monochromator. Parameters of the fit:*

$$\lambda_1^C = 810.403 \pm 0.008 \ nm, \ \sigma_1 = 0.098 \pm 0.01 \ nm$$

$$\lambda_2^C = 811.542 \pm 0.002 \ nm, \ \sigma_2 = 0.090 \pm 0.0028 \ nm$$

$$\gamma = 159\ 300 \pm 1\ 400 \ \ Count/s.$$

In Fig 2.3 is reported a spectrum taken with the monochromator and APD modules. The fitting parameters are used to calculate a function that approximates the real input spectrum. The central wavelength λ_1^C and λ_2^C are used for calibrating the MC. A numerical deconvolution procedure permits to determine the transfer function for the monochromator. It is necessary an Input function to subtract to the measured spectrum. Considering that the line width is much smaller than the

resolution of the monochromator it is reasonable to use a delta function as input:

$$I(\lambda) = \frac{\alpha}{17.5}\delta(\lambda - \lambda_1^C) + \alpha\delta(\lambda - \lambda_2^C). \tag{2.1}$$

It is possible to determine the BP of the monochromator for the given slits

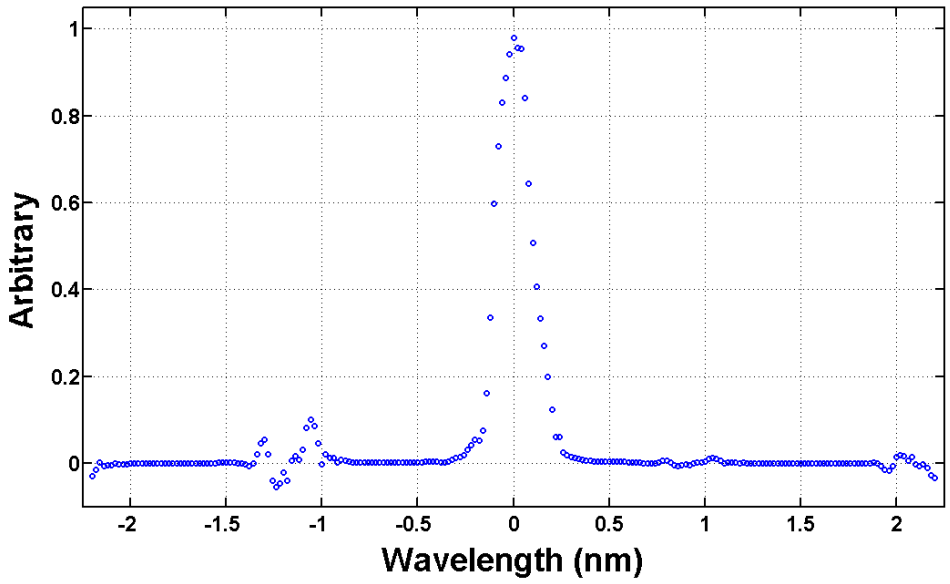


Figure 2.4: *Transmission Function for the monochromator with a both slit aperture set to 50 μm. Missing the information of the input power, the transmission efficiency cannot be calculated. The Full Width Half Maximum is 0.24 nm.*

aperture width via a numerical deconvolution. This procedure was repeated before every measurement to ensure that the two monochromator were well calibrated and had the same BP, so that the system was as much symmetrical as possible.

2.1.2 The Pump Laser

The diode is produced by Nichia. For a correct operation it requires a driver for tension and current control and, for improved stability and control over the emitted light frequency, a temperature control is necessary too. The diode was mounted in Temperature Controlled Laser Diode Mounts (Thorlabs TCLDM9) and driven by a compatible controller for both Current and Temperature. The characterization of the diode spectrum was carried on using a monochromator (see sec. 2.1.1). The spatial properties where instead measured using a 7 blades Beam Shaper (Coherent BM-7). The central emission line of the diode depends linearly on temperature. From the datasheets I expected an operation temperature around 15°C. A calibration curve obtained via a monochromator (Fig. 2.5) led to a quite different one. The operation conditions reported in Nichia's datasheet suggest to

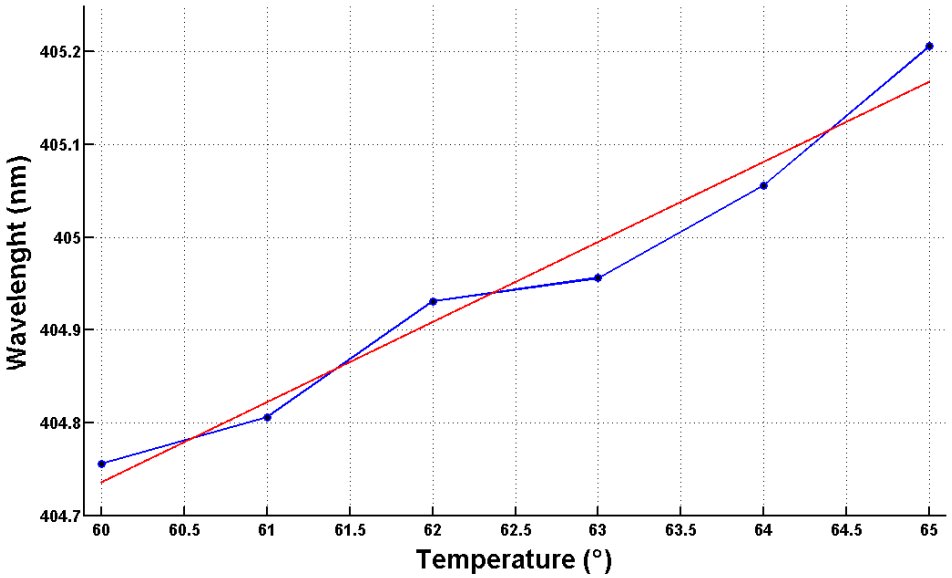


Figure 2.5: *Experimental calibration curve for the Nichia diode. In red the linear regression fit.*

work at room temperature for maximum efficiency and lifetime of the diode. The need for a longer central wavelength pushed us to set the driver control temperature to a quite high value. Humidity conditions seem to affect the emission wavelength as well but was not performed a detailed study in this direction. The temperature was eventually set to 58,4° C giving the spectrum reportred in Fig. 2.6. From

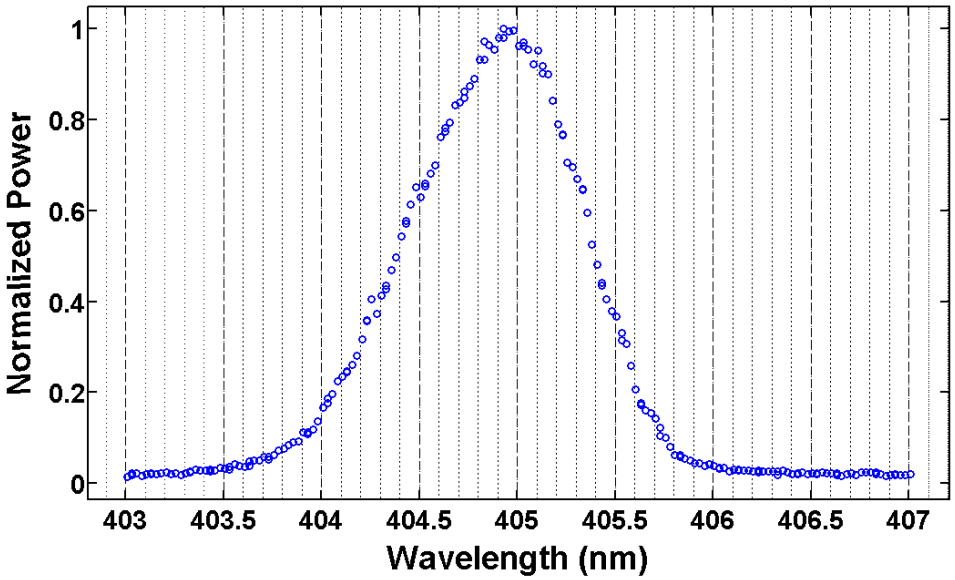


Figure 2.6: *Spectrum of the Nichia diode. Experimental condition: temperature* $T = 58.5°$ *C, current* $I = 280$ *mA. Total measured output power* $P_{LD} = 156$ *mW.*

the spectrum is possible to estimate a bandwidth of $\sigma_{LD} = (0.424 \pm 0.004)nm$. The measured emitted power for this temperature is way lower than the nominal 200 mW and proved to slowly decrease with time. The effect becomes evident after some power-cut the laboratory experienced during the summer months. From an initial power of P_{LD}=156 mW registered in June 2006, the diode emitted only P_{LD}=113 mW as oh January 2007. Also the bandwidth did not stay constant in

time. After an unforeseen powercut the emitted light changed considerably. A new temperature calibration resulted necessary and a new bandwidth of σ_{LD} =0.258 nm was measured.

The emitted light presents a strong ellipticity. The beam divergences reported on the datasheet are 20°for the TE mode and 45°for the TM one. To compensate this difference and obtaining a mode as near as possible to the Gaussian one before entering the spatial filter an anamorphic beam shaping optic (Schäfter+Kirchhoff 5AN-3-V-35) is used. The measured polarization contrast of the laser is 0.00021.

To obtain a good initial spatial Gaussian mode a spatial filter is used. The filter is composed of two short focal length lenses and a pin-hole. The first lens (f=35 mm) focalizes de input beam into the 50μm pin-hole. The light going through the the hole is then collimated by the second lens (f=75 mm). We chose the output lens of the spatial filter to have a longer focal length in order to obtain a quite big pump beam that could be easily focused into smaller modes without a great optical complexity.

Due to the far from being Gaussian nature of the beam after the anamorphic shaper, the spatial filter implies a great loss of power. The maximum transmission we obtained is around 60% while generally the ratio was between 40% and 50%.

Due to the non perfect stability of the spatial emission mode of the Laser Diode, the spatial filter needs continuous adjustment for keeping the power sufficiently high and achieve a good count rate. This also means that before any measurement session it was necessary to fully characterize the beam. To have a better insight on the propagation of the beam and a full determination of its parameters, profiles were taken for different position. During the weeks the spatial parameters changed several times so I report here just one determination as example.

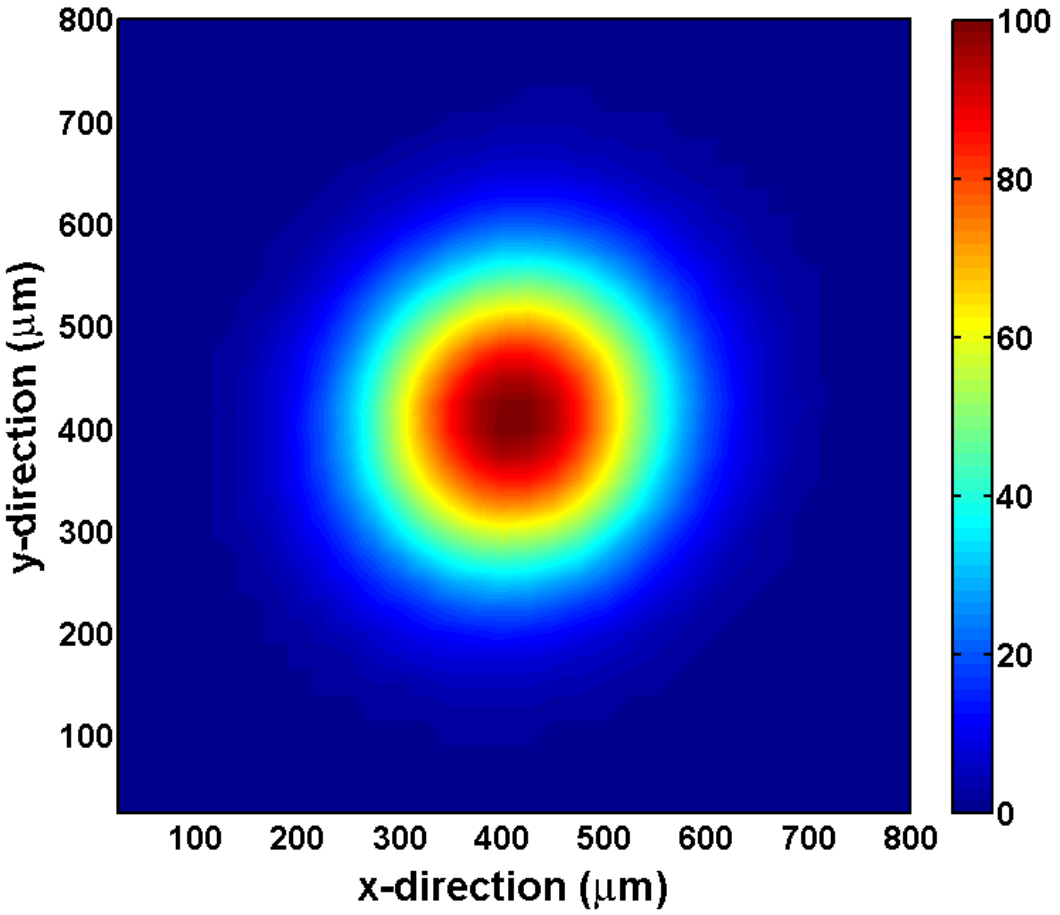


Figure 2.7: *Reconstruction of the Pump Beam after the spatial filter. Data taken via 7-blade Beam Shaper.*

In order to obtain different Pump size standard plano-convex lenses with different folcal lengths were used, except for particularly big size beams, for which a beam expander has been built using least two lenses. The spanned range of beam sizes goes from under 10 μm to almost 2 mm. Always extreme care has been taken for the crystal to be in the Rayleigh range.

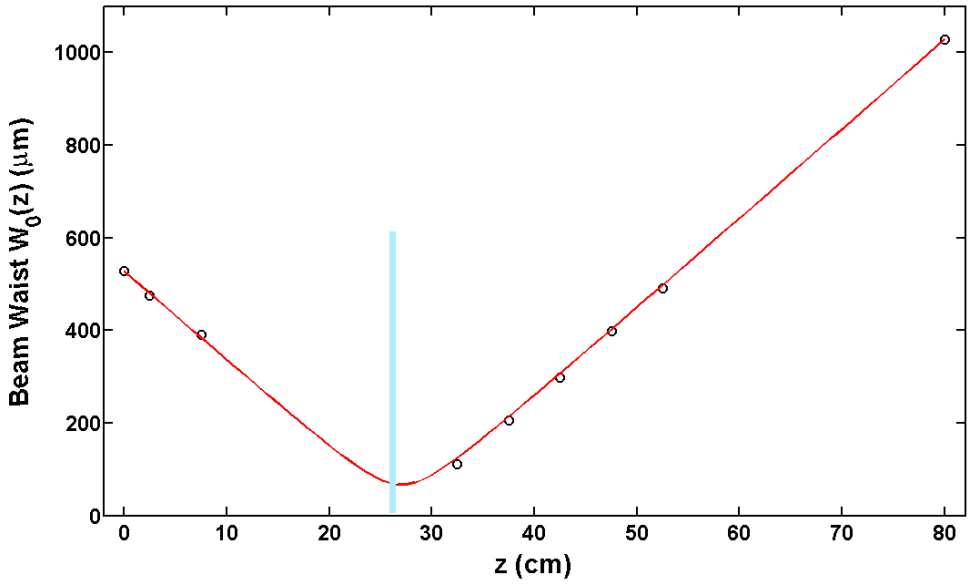


Figure 2.8: *Reconstruction of the Pump Beam after the a 30 cm focusing lens. The beam diameter $W(z)$ is measured at several z positions (black circles). From the first and last point the following parameters are calculated for the beam: beam waist W_0=66.5 μm, Rayleigh range z_R =3,4 cm. In red the profile of the beam with the preceding parameters. The light blue rectangle indicates the position of the crystal.*

2.2 The Down Conversion

The crystal used is a $LiIO_3$, a uniaxial negative material, often used for Spontaneous Parametric Down Conversion experiments (**REFERENCES!!!**). The crystal we used was 1 mm long, type I cut with the optical axis oriented at 90°. The surface were coated for maximum transmittivity at 405 nm and at 810 nm. The phase matching calculation give an output internal angle of 17.1°for degenerate non-collinear down conversion. Due to the high refraction index of this crystal, the aperture angle for the Signal and Idler beams is quite wide, 32°. The

Down Converted photons were collected into optical fibers. During the various stages of the experiment, both single mode and multimode fiber were used. The joint spectrum of the biphoton is affected by the different collection techniques, as proved by data collected. The discussion of the different effects is reported in a later section (see sec. 2.3.1). The light was lunched into the fibers via a short focal length (f=11 mm) lens [Bovino 03]. The efficiency of the down conversion process and the collection of the produced light depends on the focusing of the pump beam [Monken 98]. Before analyzing the spectrum of the DC photons it proved always necessary to optimize the collection of light. The most efficient DC was obtained for a pump size of approximately 30 μm. The recorded single count rate was 500 000 count/s for a coincidence rate of 55 000 coinc/s with a pump of 65 mW and multimode fiber collection. In order to obtain an homogeneous comparison for the different collections and the fluctuating laser power the Quantum Efficiency (QE) was used. QE is defined as

$$QE = \frac{C}{\sqrt{R_s \cdot R_i}}, \tag{2.2}$$

with C being the coincidence rate and $R_{s,i}$ being the single count rate for signal and idler channel. Using single mode fibers was usual to achieve a QE of 6-7%, with peaks of QE=13%. In case of multimode fiber the QE never passed over the 4%.

2.2.1 Electronics and Software

As already said, the photons were detected by two fiber coupled APD single photons detectors. We were interested in recording the singles rate for each channel and especially in the coincidence rate. This required a dedicated acquisition electronics. The electrical signal generated by these two modules was split in two and

sent to a multichannel analyzer (Canberra) and to a time-to-amplitude converter (TAC). One of the detector signal, from now on S_1, served as trigger for the TAC. The second signal was delayed by approx 10 ns via a long coaxial cable. The output signal of the TAC is sent through a single channel analyzer (SCA). The TAC and SCA are set to click for events in a time window of 5 ns after a delay set according the MCA spectrum observed. The single counts and the coincidence clicks generated by the SCA are counted by a computer controlled four channel counter (Quad Counter).

The long measurement times and the high number of monochromator setting for each measure required an almost complete automatization of the data acquisition as well as of the control of the monochromators. All the controls and data acquisition was integrated in various programs created under LabView.

The data analysis, as well as most of the simulations was carried on with Matlab.

2.3 Control of the Frequency Correlation

The initial experimental efforts were addressed to obtain correlated states. The CW nature of the pump make it quite easy to obtain a wide anticorrelation just by focusing the pump beam. The limited bandwidth, together with the phase matching parameters, constraints the correlation. It is thus necessary to expand the beam in order to achieve a "squeezing" of the anticorrelation, as can be interpreted from Eq. (1.12). The main issue to face with a large pump is the decreased coupling efficiency [Bovino 03, see Eq.(7) therein][Monken 98] into the fibers. This reduced count rate sensibly affects the measurement time necessary for obtaining a correlation spectrum.

In Fig. 2.9 is reported a correlation spectrum for near uncorrelated photon. For a

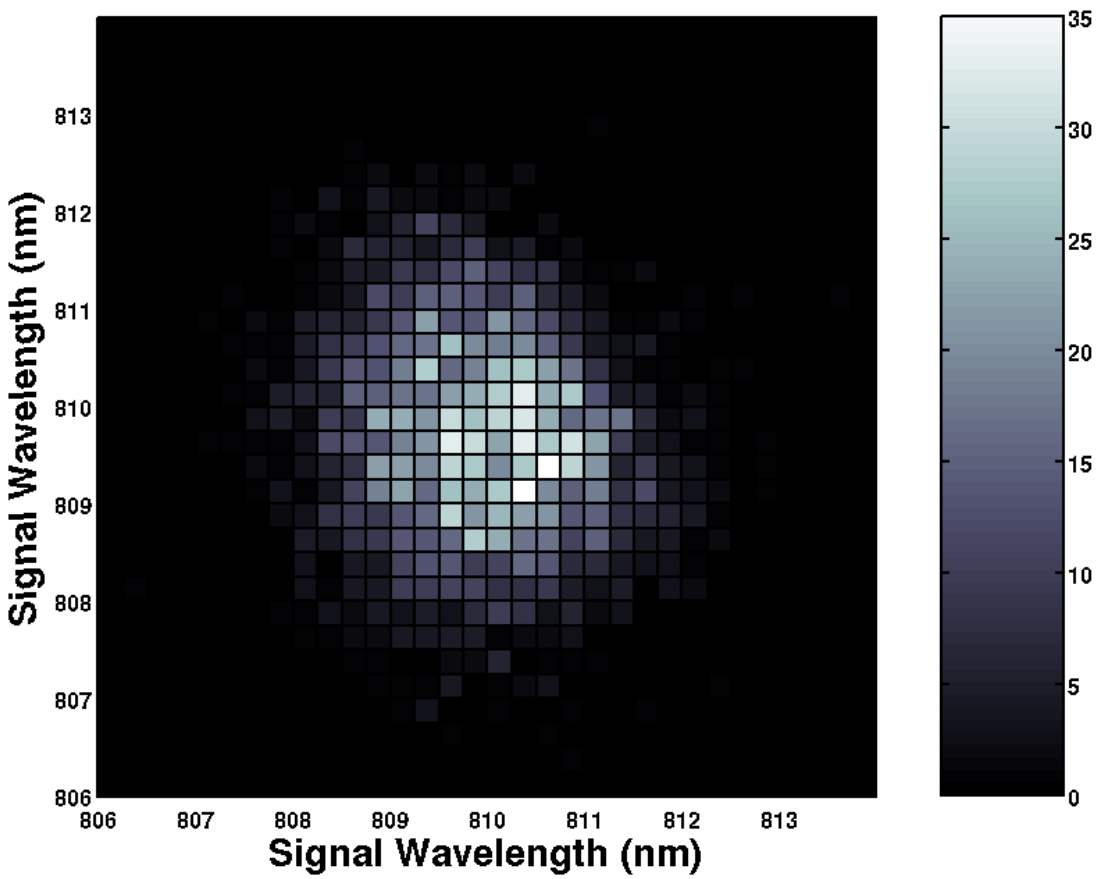


Figure 2.9: *Joint correlation spectrum for the Signal and Idler in a almost uncorrelated case. Pump Bandwidth: σ_p=0.42 nm, Pump Size:W_0=280 μm. The acquisition time was 90 s. From the fit I obtain the following bandwidths: $B_+ = 0.95 \pm 0.11$ nm and $B_- = 1.08 \pm 0.13$ nm.*

pump bandwidth of σ_p=0.42 nm the theory predicts a value for B_+=0.68 nm and, for the measured pump waist W_0=280 nm a B_- =0.46 nm. The experimental results differ from the prediction. A possible explanation is presented is sec. 2.3.1.

As already pointed out, the bandwidth of the Nichia diode laser did not remain stable after a cool down - warm up cycle. The observed trend is a decrease of

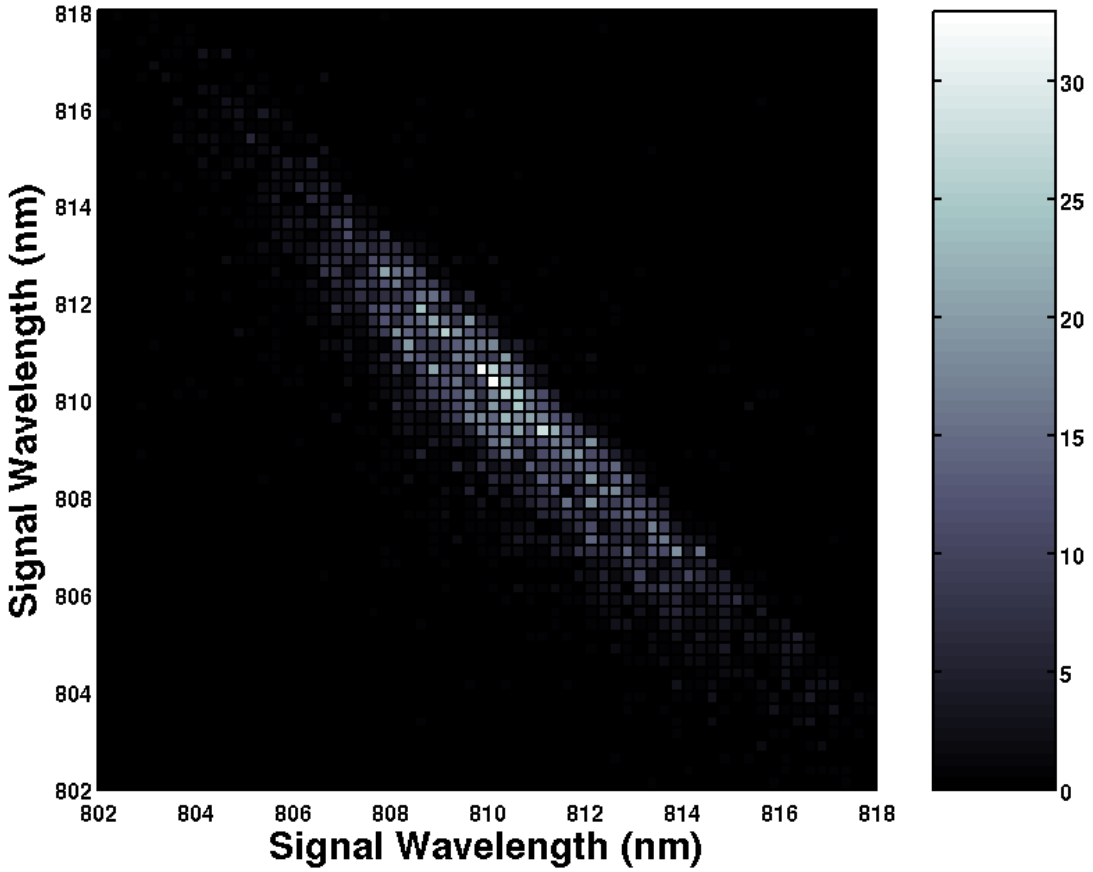


Figure 2.10: *Joint correlation spectrum for the Signal and Idler in the anticorrelated case. Relevant parameters: Pump Bandwidth:* $\sigma_p = 0.337 \pm 0.011$ *nm, Pump Size:30* μ*m. The acquisition time was 50 s. The measured correlation bandwidth are* $B_+ = 0.71 \pm 0.12$ *nm and* $B_- = 3.53 \pm 0.52$ *nm. The* B_+ *agrees with the theoretical value of 0.68 nm. The value of*B_- *is the maximum allowed by the 10 nm FWHM interferencial filter used in front of the collection fibers.*

the bandwidth every time. In Fig. 2.10 is possible to observe that the reduced $\sigma_p = 0.337$ leads to a $B_+ = 0.71$.

Before going on showing the analytical study of the correlation with the pump

beam waist diameter it is necessary to understand why we were not able to reduce the width of the correlation function along the Λ_+ direction as predicted by the theory and, especially why we never obtained a B_- smaller than B_+.

2.3.1 Light Collection Theory

In the theoretical model developed in chapter 1, the condition $\vec{q}_s = \vec{q}_i = 0$ is imposed in order to observed the spectral characteristics of the pairs of photons. In the experiment this condition is generally approximated by placing small pinholes in front of detectors that are placed far away from the crystal [Pittman 96]. An alternative approach is to collect the signal and idler photons by using single mode fibers in such a way the the signal mode and the idler mode are projected into the mode of the fiber [Bovino 03, Andrews 04, Castelletto 05, Dragan 04, Kurtsiefer 01]. This last approach was the one used in the experiment.
To consider the effect of collecting various $\vec{q}_s$ and $\vec{q}_i$ because of the projection into a finite mode, we rewrite the joint spectrum as

$$G^2_{proje}(\omega_s, \omega_i) = \left| \int \mathrm{d}\tilde{\mathrm{q}}_\mathrm{s} \int \mathrm{d}\tilde{\mathrm{q}}_\mathrm{i} \Phi(\omega_\mathrm{s}, \omega_\mathrm{i}, \tilde{\mathrm{q}}_\mathrm{s}, \tilde{\mathrm{q}}_\mathrm{i}) \mathrm{U}_0(\tilde{\mathrm{q}}_\mathrm{s}) \mathrm{U}_0(\tilde{\mathrm{q}}_\mathrm{i}) \right|^2 , \tag{2.3}$$

where $U_0(\vec{q}_j) = exp\{-|\vec{q}_j|^2 \tilde{w}_s/4\}$ represents the mode into which the signal and idler radiation are being projected and $\tilde{w}_s$ is the radius of the mode of the single mode fiber.

Define $Q_{x+} = q_{sx} + q_{ix}$, $Q_{y+} = q_{sy} + q_{iy}$, $Q_{x-} = q_{sx} - q_{ix}$ and $Q_{y-} = q_{sy} - q_{iy}$,

Eq. (2.3) can be rewritten as

$$
\begin{aligned}
G^2_{proje}(\Omega_s,\Omega_i) \sim \\
& e^{-\frac{\Omega_+^2}{2}\left(T_0^2+(\alpha L)^2(N_p-N_s\cos\varphi)^2+\frac{1}{2B_0^2}\right)}\times \\
& e^{-\frac{\Omega_-^2}{2}\left((N_s\sin\varphi W_0)^2+\frac{1}{2B_0^2}\right)}\times \\
& \left|\int \mathrm{dQ_{x+}} \mathrm{e}^{-\left(\mathrm{Q_{x+}^2}(\frac{\mathrm{W_0^2}}{4}+\frac{\tilde{\mathrm{w}}_\mathrm{s}}{8})\right)}\times\right. \\
& \int \mathrm{dQ_{x-}} \mathrm{e}^{-\left(\mathrm{Q_{x-}^2}(\frac{\tilde{\mathrm{w}}_\mathrm{s}}{8})\right)}\times \\
& \int \mathrm{dQ_{y+}} \mathrm{e}^{-\left(\mathrm{Q_{y+}^2}(\frac{(\mathrm{W_0}\cos\varphi)^2}{4}+\frac{\tilde{\mathrm{w}}_\mathrm{s}}{8})\right)} \mathrm{e}^{\mathrm{Q_{y+}}\frac{\mathrm{W_0^2}}{2}\cos\varphi\sin\varphi\mathrm{N_s}\Omega_-}\times \\
& \left.\int \mathrm{dQ_{y-}} \mathrm{e}^{-\mathrm{Q_{y-}^2}\left(\frac{\tilde{\mathrm{w}}_\mathrm{s}}{8}+\frac{(\alpha\mathrm{L}\sin\varphi)^2}{4}\right)} \mathrm{e}^{\mathrm{Q_{y-}}\left(\frac{(\alpha\mathrm{L})^2\sin\varphi\{\mathrm{N_p}-\mathrm{N_s}\cos\varphi\}\Omega_+^2}{4}+\mathrm{i}\frac{\mathrm{L}\sin\varphi}{2}\right)}\right|^2 .
\end{aligned}
\tag{2.4}
$$

After performing the integrals in Eq. (2.4) we obtain

$$
\begin{aligned}
G^2_{proje}(\Omega_s,\Omega_i) \sim \\
& exp\left\{-\frac{\Omega_+^2}{2}\left(T_0^2+(\alpha L)^2(N_p-N_s\cos\varphi)^2+\frac{1}{2B_0^2}-\frac{(\alpha L)^2(N_p-N_s\cos\varphi)^2\sin^2\varphi}{(\alpha L\sin\varphi)^2+\frac{w_s^2}{2}}\right)\right\}\times \\
& exp\left\{-\frac{\Omega_-^2}{2}\left((N_s\sin\varphi W_0)^2+\frac{1}{2B_0^2}-\frac{(N_s\sin\varphi\cos\varphi W_0^2)^2}{(\cos\varphi W_0)^2+\frac{w_s^2}{2}}\right)\right\},
\end{aligned}
\tag{2.5}
$$

from where we get that the widths B_+ and B_- (defined as the standard deviation) in the variables Ω_+ and Ω_- are given by

$$
B_+ = \left(T_0^2+\frac{(\alpha L)^2(N_p-N_s\cos\varphi)^2}{1+2(\frac{\alpha L}{\tilde{w}_s^2})}+\frac{1}{2B_0^2}\right)^{-\frac{1}{2}} \tag{2.6}
$$

and

$$B_- = \left((N_s \sin\varphi\, W_0)^2 \frac{\frac{\tilde{w}_s^2}{2}}{(\cos\varphi\, W_0)^2 + \frac{\tilde{w}_s^2}{2}} + \frac{1}{2B_0^2} \right)^{-\frac{1}{2}} \tag{2.7}$$

In Fig. 2.11 is reported the systematic study of the correlation as a function of

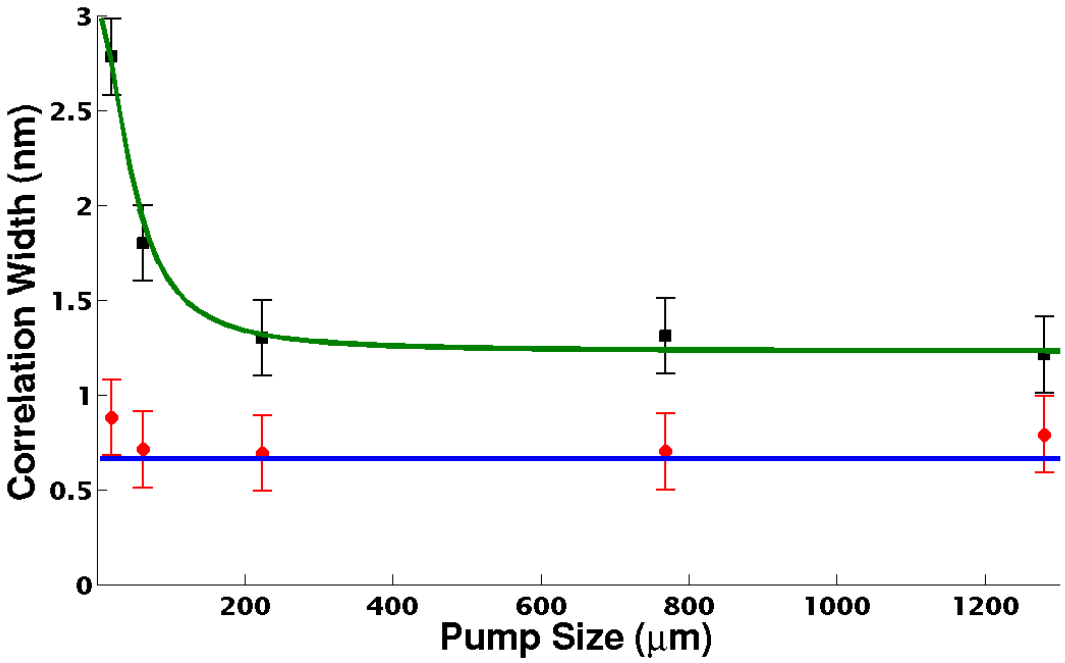


Figure 2.11: *Correlation (B_+, black squares) and Anticorrelation (B_-, red circles) of the spectral correlation as a function of the Pump beam waist (W_0). The Continuous lines represent the theoretical predictions with the free parameter W_s (sec. 2.3.1) set to 130μm. In blue the curve for B_+, in green the one for B_-.*

the pump beam waist. The superimposed solid lines are calculated from Eqs. 2.6 and 2.7 for a collection mode beam waist $\tilde{w}_s = 130$ μm. Comparing this graphic with the one of Fig. 1.2 we observe that the anticorrelation bandwidth B_- never crosses the B_+ for that value of $\tilde{w}_s$.

2.4 Spatial to Spectral Mapping

The same setup presented in section 3.1 can be easily extended to experimentally test the theory presented in section 1.2.

In order to obtain the necessary spatial (and thus momentum) profile for the pump beam we used a "fork" computer generated hologram [Arlt 98, Mair 01]. The QIP has a good tradition of generation of those holograms for mode conversion (citare GABI) for visible and infrared light on plastic support. Unfortunately the plastic film presents an high absorption coefficient for UV light. It has been necessary to use some commercial holograms prepared on glass support. In Fig. 2.12 is shown a photo taken via a CCD camera of the Spatial profile of the generated non-Gaussian beam. The intensity of this beam less than 40% of the initial Gaussian beam. This loss is mainly due to the diffraction nature of the interference effect that generate the vortex.

The pump beam is focused on the crystal. A beam waist of ~ 17 μm as been estimated. After shining the beam on the crystal the down converted radiation is collected at the same aperture angle of section by multimode fibers. We adopted multimode fibers for collecting as much light as possible. This choice, in principle, should not affect the correlation: as shown in section 2.3.1, for such a small pump size the collected $\Delta\vec{q}$ does not affect the anticorrelation.

Due to the reduced pump intensity a lower count rate was expected. The data acquisition program was modified to scan the joint correlation plane in the Λ_+ and Λ_- direction, reducing the total measurement time.

Up to now the best obtained measure in shown in Fig. 2.13. Observing it is possible

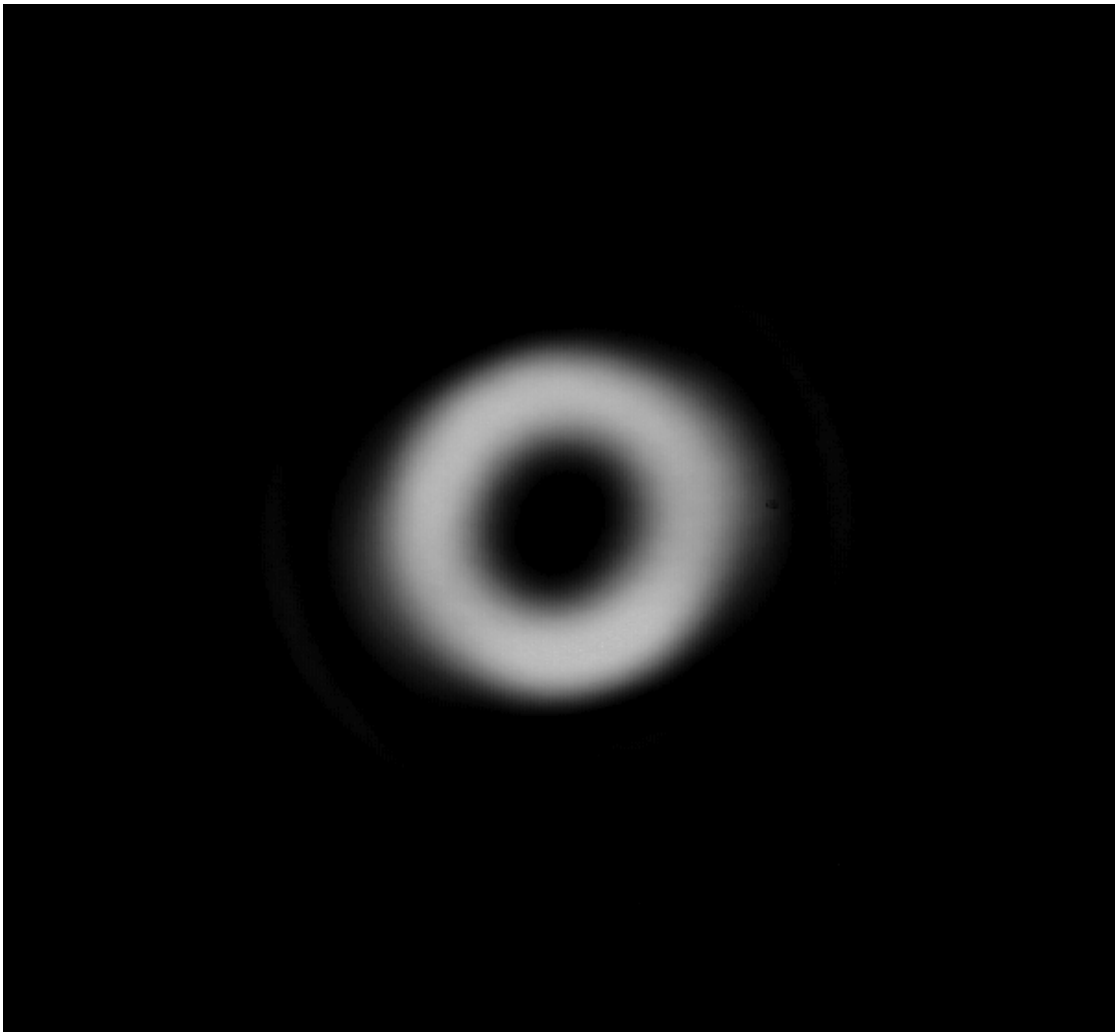


Figure 2.12: *Image of the transverse profile of the Pump Beam Diffracted by the computer generated hologram. The image has been captured via an high sensitivity CCD camera. It is evident the hole in the middle, distinctive of the higher order Laguerre-Gaussian modes. The characteristics of the hologram allows for the generation of intense LG_{02} modes.*

to note the presence of two separate peaks. This shape differs significantly from the one obtained in the case of a Gaussian pump beam (e.g. Fig. 2.10).

To observe in a clearer way the shape of the correlation function, in Fig. 2.14 are

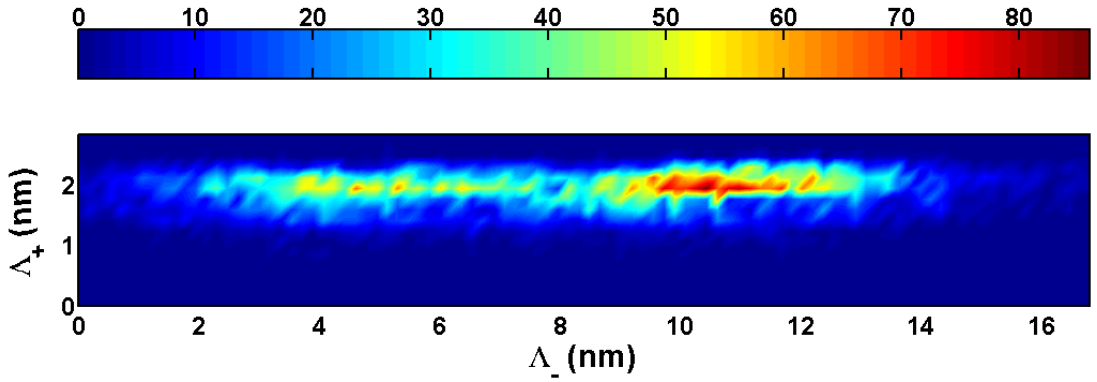


Figure 2.13: *Joint correlation spectrum obtained for a LG_{02} pump beam. The acquisition time is 100 s; the step of the monochromators was set to 0.25 nm*

reported the profiles of the correlation along the Λ_+ and Λ_- directions.

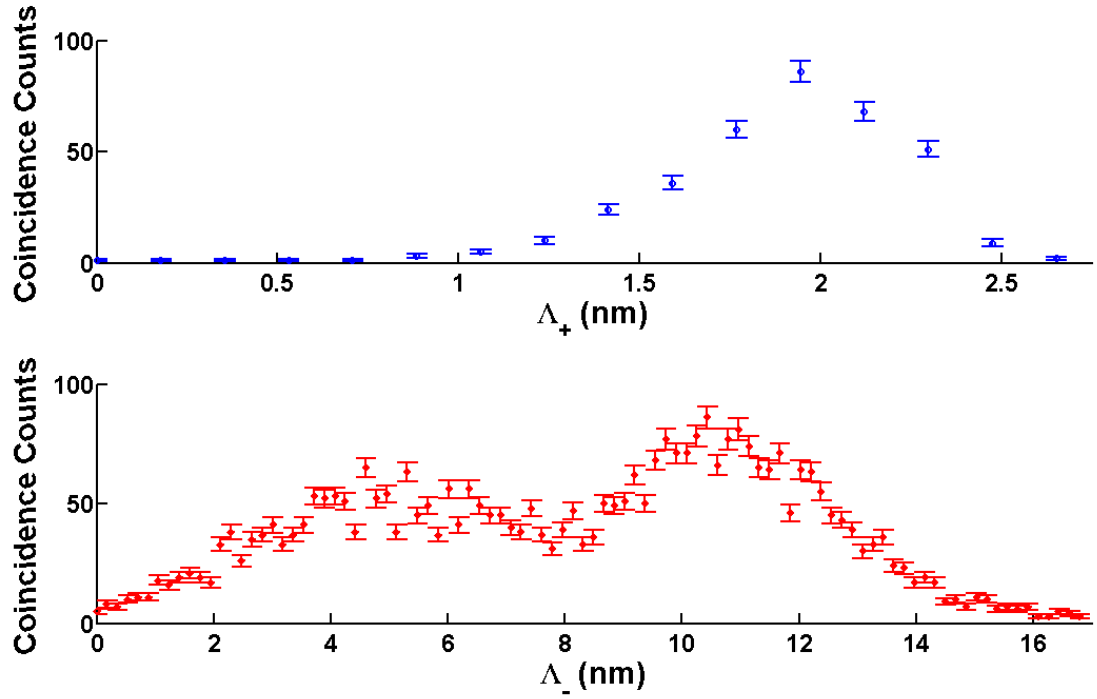


Figure 2.14: *Profiles of the Correlation function for a LG_{02} pump beam. In the lower graph it is evident the depression in the middle of curve.*

In this chapter were presented the experimental results achieved in the control of the correlation of paired photons achieved by a carefull control of the pump beam waist. The anticorrelated and uncorrelated pairs have been demostrated to be feasibles. Work is still in progress for obtaining correlated pairs, concentrating mainy in the collection parameters. An easier way for obtaining correlated photons is to use a pump with a broader spectrum.

Chapter 3

Polarization Entanglement: Generation and Characterization

In this chapter is presented the generation and study of a bipartite state that exhibits entanglement in the polarization space. This state will prove a usefull tool for study

Many theoretical and experimental works have been produced over the years dealing with bipartite system entanglement detection, manipulations and exploitation. The entanglement between the two system can be detected in various degrees of freedom. The particular appeal of the polarization entangled photons is the I will present here the characterization of the polarization entanglement . Various "indicators" have been proposed for detecting entanglement and here two of them are presented. As first test, in the experimental work I used the CHSH [Clauser 69] version of the Bell inequalities [Bell 64] for checking the entanglement of the generated photon pair. Having in mind the possible study of channel dechoerence I needed a measurement of bipartite entanglement that could work for pure states as for mixed ones. In the case of a bipartite 2-qubit system,

a usefull and practically meaningfull measure is the *entanglement of formation* (EF) [Wootters 98]. Experimentally for obtaining the EF was necessary to implement complete tomography of the state [James 01, White 99], a powerfull technique that can also be extended for a complete characterization of a complete quantum process [Poyatos 97, Chuang 97, Chuang 00]. Some preliminary measurements were performed for the characterization of the polarization dechoerence introduced by single mode and multimode fibers.

3.1 The Source of Entangled Photons

The photons used for the generating the polarization bipartite state are generated by a type II non collinear down-conversion process.

A UV pump beam impinges on a 1.5 mm thick BBO crystal forming an angle of

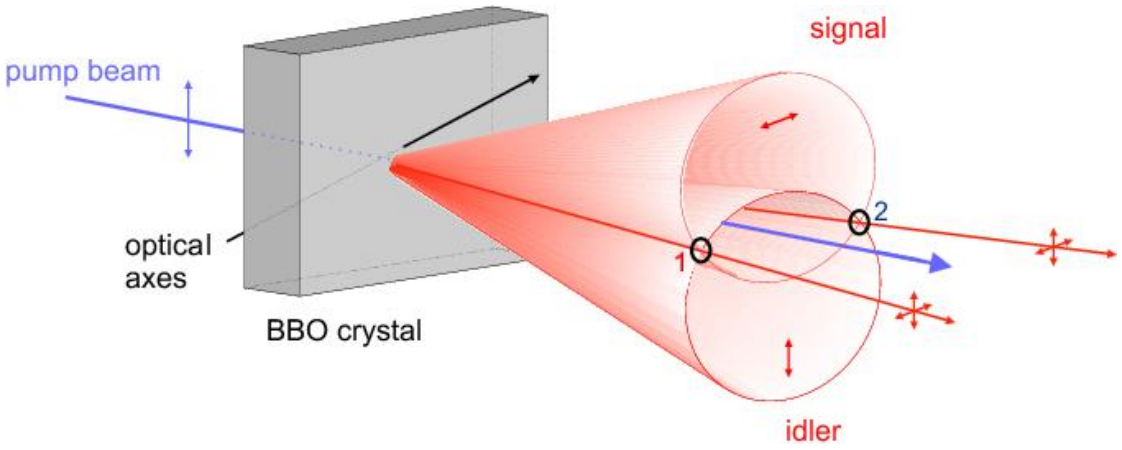


Figure 3.1: *Drawing of the Type-II down conversion process.*

$\sim 43°$ with the optical axis. The pump laser is a laser diode (Coherent Compass 405) with central emission wavelength $\lambda = 406.5$ nm, a bandwidth of $\Delta\lambda = 0.9$ nm

and a nominal power of 25 mW.

Selecting the intersection of the ordinary propagating light cone (Signal, horizontal polarization) and the extraordinary one (Idler, vertical polarization) through a pair of pinholes is possible to observe a superposition of the Signal and Idler amplitude. The angular aperture of the two beams is determined by the phase matching condition [Boyd 02]. For this wavelength and this crystal the calculated aperture angle is $\sim 4°$ [Rubin 96].

The polarization state of the biphoton is not pure (and completely entangled) as desired. The timing information provided by the different group velocities experienced by the different polarizations [Kwiat 95] and the wide spectral width of the pump beam ($\Delta\lambda = 0.9nm$) affects the degree of entanglement of the pairs of photon, as in the case of a pulsed pump [Grice 97, Keller 97]. To recover a full polarization entanglement it is necessary delete the timing information and to obtain a totally symmetrical spectrum [Di Giuseppe 97]. There are several techniques for solving the spectral issues. The simplest one is narrow filtering [Rarity 95, Zukowski 95]. An alternative approach is the use of an interferometer to obtain a complete separation between the spectral inforation and the polarization, achieving an highly entangled state [Kim 03b]. We decided to adopt this last technique for generating polarization entangled state. The output state of the crystal, after the two pinholes, can be generally described as [Grice 97, Kim 03a]:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \iint \mathrm{d}\omega_\mathrm{s}\mathrm{d}\omega_\mathrm{i} \left[\mathrm{F}_{\mathrm{s1,i2}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{h}}_1^\dagger(\omega_\mathrm{s})\hat{\mathrm{v}}_2^\dagger(\omega_\mathrm{i}) + \mathrm{e}^{\mathrm{i}\phi}\mathrm{F}_{\mathrm{i1,s2}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{v}}_1^\dagger(\omega_\mathrm{i})\hat{\mathrm{h}}_2^\dagger(\omega_\mathrm{s})\right]|0\rangle\,. \tag{3.1}$$

where the creation operators $\hat{h}_{1,2}^\dagger$ and $\hat{v}_{1,2}^\dagger$ stands for the creations of photons in the horizontal and vertical modes 1 and 2 defined by the pinholes and $F_{s1,i2}(\omega_s,\omega_i)$ is the normalized biphoton function [Grice 97].

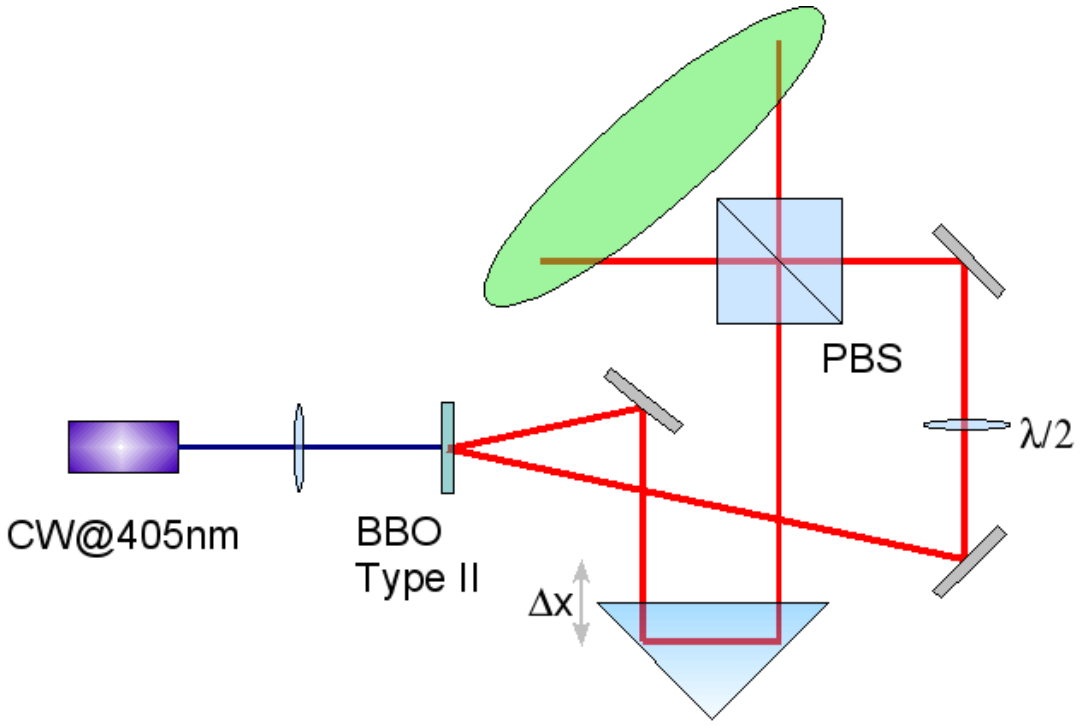


Figure 3.2: *Schematics of the interferometer used for recovering full entanglement. The Trombone is moved via an electronically controlled translational stage.*

The half wave plate inserted on the path labelled 2 is oriented with the fast axis forming an angle of 45° with the vertical. This flips the horizontal and vertical polarizations according to the transformation:

$$\hat{h}_2^\dagger(\omega_s) \rightarrow \hat{v}_2^\dagger(\omega_s) \tag{3.2}$$

$$\hat{v}_2^\dagger(\omega_i) \rightarrow -\hat{h}_2^\dagger(\omega_i). \tag{3.3}$$

The new state after the waveplate thus reads:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \iint \mathrm{d}\omega_\mathrm{s}\mathrm{d}\omega_\mathrm{i} \left[\mathrm{F}_{\mathrm{s1,i2}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{h}}_1^\dagger(\omega_\mathrm{s})\hat{\mathrm{h}}_2^\dagger(\omega_\mathrm{i}) - \mathrm{e}^{\mathrm{i}\phi}\mathrm{F}_{\mathrm{i1,s2}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{v}}_1^\dagger(\omega_\mathrm{i})\hat{\mathrm{v}}_2^\dagger(\omega_\mathrm{s})\right]|0\rangle\,. \tag{3.4}$$

The photons are now sent to the two input faces of a polarization beam splitter (PBS, Fig. 3.3). Even if not shown here, a good temporal and spatial overlap in the PBS is necessary for the Interference to occur. The spatial overlap requires a generally good alignment of the whole system and is also achieved with the help of a HeNe laser used for simulating the path of the downconverted photons.
The temporal overlap is controlled changing the length of the path number 2 via a moving trombone. The action of the PBS on polarization is to transmit the horizontal one and to reflect the vertical one. In the creation operator formalism introduced before it is summarized as:

$$\hat{h}_1^\dagger = \hat{h}_3^\dagger; \tag{3.5}$$

$$\hat{v}_1^\dagger = i\hat{v}_4^\dagger; \tag{3.6}$$

$$\hat{h}_2^\dagger = \hat{h}_4^\dagger; \tag{3.7}$$

$$\hat{v}_2^\dagger = i\hat{v}_3^\dagger. \tag{3.8}$$

Another relevant effect of the PBS is to permutate the indices of the spectral function of the biphoton to account the different paths taken by H and V polarized photons. When the two arms of the interferometer are equal, the state at the output of the PBS is:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \iint \mathrm{d}\omega_\mathrm{s}\mathrm{d}\omega_\mathrm{i} \left[\mathrm{F}_{\mathrm{s1,i2}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{h}}_3^\dagger(\omega_\mathrm{s})\hat{\mathrm{h}}_4^\dagger(\omega_\mathrm{i}) - \mathrm{e}^{\mathrm{i}\phi}\mathrm{F}_{\mathrm{s2,i1}}(\omega_\mathrm{s},\omega_\mathrm{i})\hat{\mathrm{v}}_4^\dagger(\omega_\mathrm{i})\hat{\mathrm{v}}_3^\dagger(\omega_\mathrm{s})\right]|0\rangle\,. \tag{3.9}$$

It is interesting to note how in output 3 there will always be a signal photon, while in output 4 there will always be an idler photon; it is possible to drop the indices for the mode propagation in the spectral amplitude. The amplitude interference between the vertical and horizontal modes is thus not affected by the

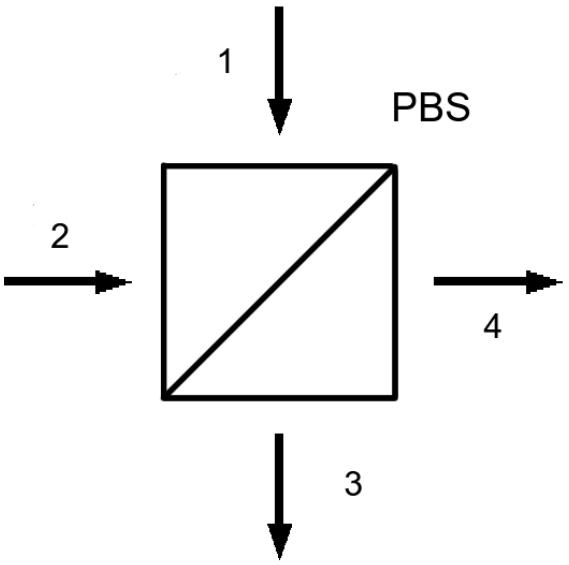


Figure 3.3: *Schematic of the inputs and outputs of a Polarizing Beam Splitter (PBS).*

non separability of $F(\omega_s, \omega_i)$ in a signal and an idler part because there is no mixing anymore between the polarization and the frequency. A distinctive sign of a polarization-entangled state is that if the pair of photons are directed to detectors preceded by polarizers, the coincidence rate will vary sinusoidally with either the sum or difference of the polarizer angles. The general polarizer state with the axis forming an angle θ with the horizontal reads:

$$|\theta_j\rangle = \left(\cos\theta_j \hat{h}_j^\dagger + \sin\theta_j \hat{v}_j^\dagger\right)|0\rangle\,. \tag{3.10}$$

The measured rate of coincidence is given by:

$$R(\theta_3,\theta_4) \propto \left|{}_3\langle\theta_3|{}_4\langle\theta_4|\,|\psi\rangle\right|^2 = \left|\iint \mathrm{d}\omega_\mathrm{s}\mathrm{d}\omega_\mathrm{i}\mathrm{F}(\omega_\mathrm{s},\omega_\mathrm{i})\mathrm{e}^{\mathrm{i}\phi}\left[\cos\phi\cos(\theta_3-\theta_4) - \mathrm{i}\sin\phi\cos(\theta_3+\theta_4)\right]\right|^2 . \tag{3.11}$$

Setting $\phi = \pi/2$ and using the normalization property of the biphoton spectral function the coincidence rate becomes:

$$R(\theta_3, \theta_4) \propto \left|\cos(\theta_3 + \theta_4)\right|^2, \tag{3.12}$$

as expected for the entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|H\rangle\,|H\rangle - |V\rangle\,|V\rangle\big). \tag{3.13}$$

When the two arms of the interferometer are not equal, the output state of the PBS is not anymore fully entangled. When the difference in the arrival time of the two photons on the PBS is greater than the coherence time of the biphoton the output state is a totally mixed state formed by the incoherent superposition of the $|H\rangle_1\,|H\rangle_2$ and $|V\rangle_1\,|V\rangle_2$ states. The associated density matrix thus reads:

$$\begin{aligned} \rho_{mixed} &= \frac{1}{2}\left(\rho_H + \rho_V\right) = \\ &= \frac{1}{4}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{3.14}$$

3.2 Source Characterization

In order to obtain the good temporal superposition, one arm of the interferometer is equipped with a moving trombone to change its length. The two output modes of the PBS are launched [Bovino 03] into single mode fibers at 800 nm (Thorlabs

P1-830A-FC) through a couple of interference filters (IF) centered at 810 nm and a bandwidth of 40 nm, which are used to reduce the background light. The fibers terminate onto the sensible area of two APD modules with quantum efficiency $\sim 70\%$ at 810 nm. The recorded single count rate is 12 000 count/s for the two channels, for a coincidence rate of 1 000 coinc/s.

Between the PBS and the fibers a system formed by an half waveplate and a Glenn-Laser (GL) polarizer is inserted on both arms. The Glenn-Laser polarizers axis are set to select the $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ state. The half waveplate rotation change the direction of the polarizer.

To find the correct position of the trombone, all the waveplates for both arms are removed. The state $|\psi\rangle$ is then projected onto the state $|D\rangle_1 |D\rangle_2$. From the Eq. 3.12, in case of perfect superposition the coincidence rate should be count rate should drop to zero. In Fig. 3.4 is reported the coincidence rate for different position of the trombone. When the two paths are equal a second order interference effect [Hong 87] occurs between the two paths. The result is a Hong-Ou-Mandel like dip. From the width of this dip is possible to estimate the coherence time of the biphoton [Hong 87, Carrasco 06]. The measured coherence time is $\tau \approx 130$ fs.

Once that that the correct delay was set the half waveplates where inserted. Fixing the one in arm 3 and rotating the one in arm 4 gives the oscillatory pattern, as predicted by the Eq. 3.12. It is reported in Fig. 3.5. The visibility of this pattern is sufficiently high for assuming the purity of the state and its high degree of entanglement.

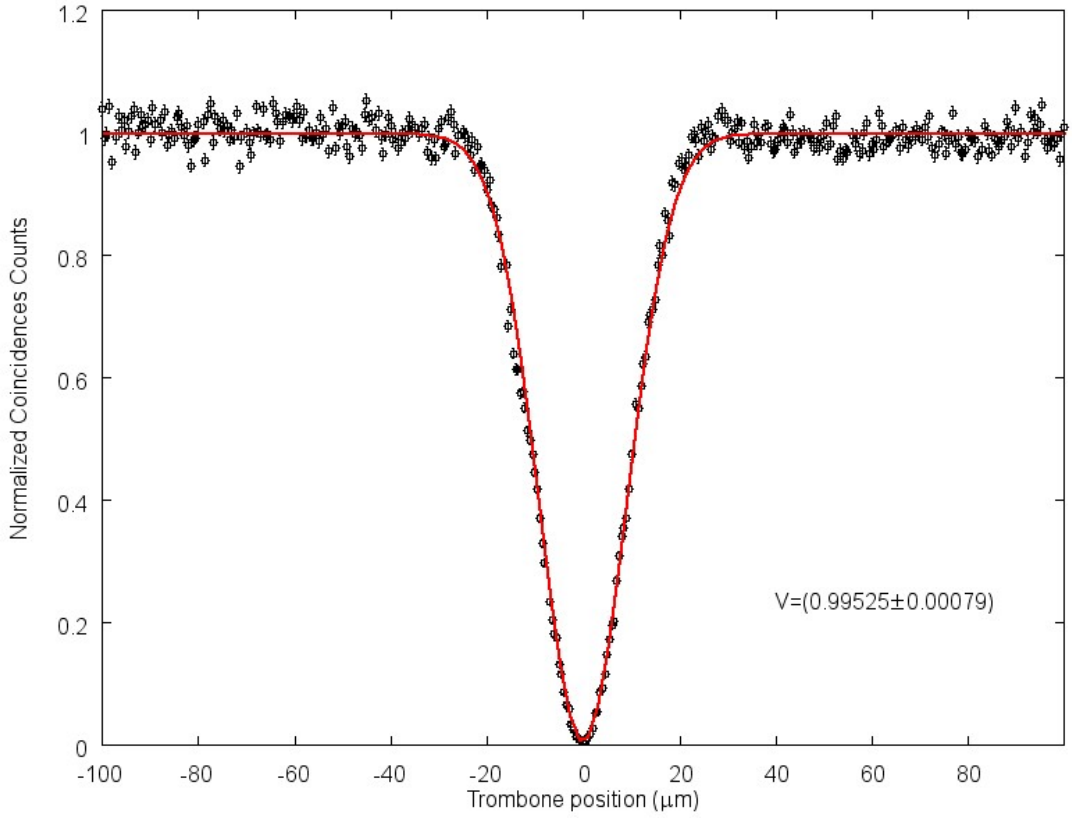


Figure 3.4: *Interference pattern given by the record of the coincidence in selecting the state $|\nearrow\rangle$ in both arm 1 and 2 of the interferometer. In red a Gaussian fit. The observed visibility is 0.995±0.001. The width of the dip gives an estimation on the coherence time of the downconverted photons $\tau_c \approx 130$ fs [Hong 87].*

3.3 Bell Inequality

The dip in the coincidence counts is not sufficient to assert that the generated state is a fully entangled one [Kim 03a]. A distinctive indication of the presence of entanglement is the violation of a class of inequalities, generally know as Bell's inequality [Bell 66, Clauser 69, De Caro 94, Aspect 02]. For the case of polarization entangled photons is necessary to test the correlation between the two photons

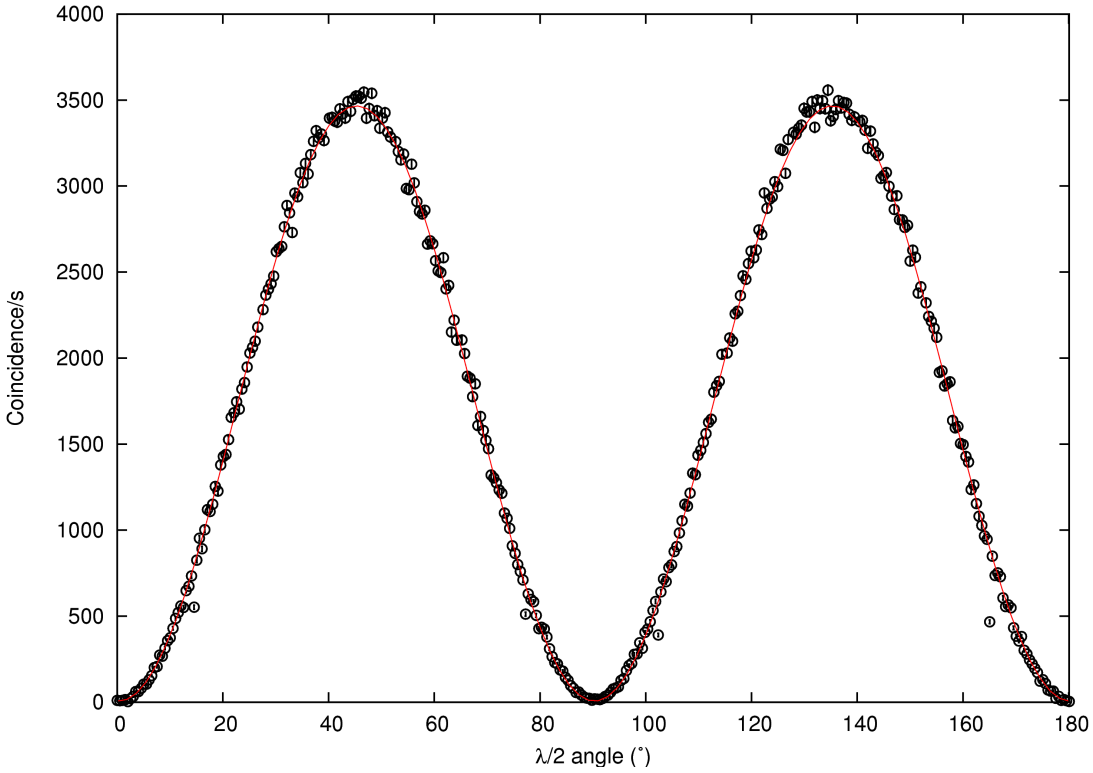


Figure 3.5: *Fixing the waveplate on one output arm of interferometer and rotating the half waveplate on the other arm, the registered coincidence show the polarization contrast originating from the interference. In case of out of interference paths length there would be no oscillation. The observed visibility is 0.997±0.002.*

measured in different basis.

For the following I will indicate with a and b the direction of the two polarization analyzer and with '+" and '−' the two possible outcomes. For polarizers with only one output is useful to define the '−' result as the '+' outcome for a perpendicular orientation of the same polarizer. Following the review work of Aspect [Aspect 02], I define a Bell operator for testing the CHSH inequality [Clauser 69] with a fixed angular relation between the various measurement directions. I define the angle η

as the angle formed by the two analyzer:

$$\eta = (a, b) = (b, a') = (a', b'). \tag{3.15}$$

I can now define the correlation operator for two polarization direction a and b as function of the coincidence rates $R_{i,j}(\alpha, \beta)$:

$$E(a, b) = \Big(R_{++}(a, b) + R_{--}(a, b) - R_{+-}(a, b) - R_{+-}(a, b) \Big) / \sum_{ij} R_{ij}(a, b), \tag{3.16}$$

The Bell operator for the angle η eventually takes the form:

$$\boldsymbol{S}(\eta) = E(a, b) - E(a, b') + E(a', b) + E(a', b'). \tag{3.17}$$

Experimentally, the operator corresponds to a set of four measurement for every correlation $E(\alpha, \beta)$. In total, sixteen measurement are necessary for obtaining the value for $\boldsymbol{S}(\eta)$.

The quantum mechanical expression for the coincidence rate $R_{ij}(a, b)$

$$R_{ij}(a, b) \propto | \langle i|_a \langle j|_b |\psi\rangle |^2 \tag{3.18}$$

also gives indication on how to measure it in our setup: The waveplates are rotated, determining the measurement directions a, a', b and b'.

It can be easily shown that the maximum value for $S(\eta)$ occurs for $\eta = \pi/8$ that corresponds to setting the waveplates axes in the directions

$$\begin{aligned} a &\rightarrow 0^o \\ a' &\rightarrow 45^o \end{aligned}$$

for the first half waveplate and

$$\begin{aligned} b &\rightarrow 22.5^o \\ b' &\rightarrow 67.5^o \end{aligned}$$

for the second one. Using Glenn-Laser polarizer that presents only one output is necessary to consider also the orthogonal angle for every configuration for measuring also the '−' outcome. When the two arms of the interferometer are balanced, i.e. in the minimum of the dip of Fig. 3.4, the violation of the classical limit was maximal. Classically the maximum value for the S(η) is 2. The maximum mea-

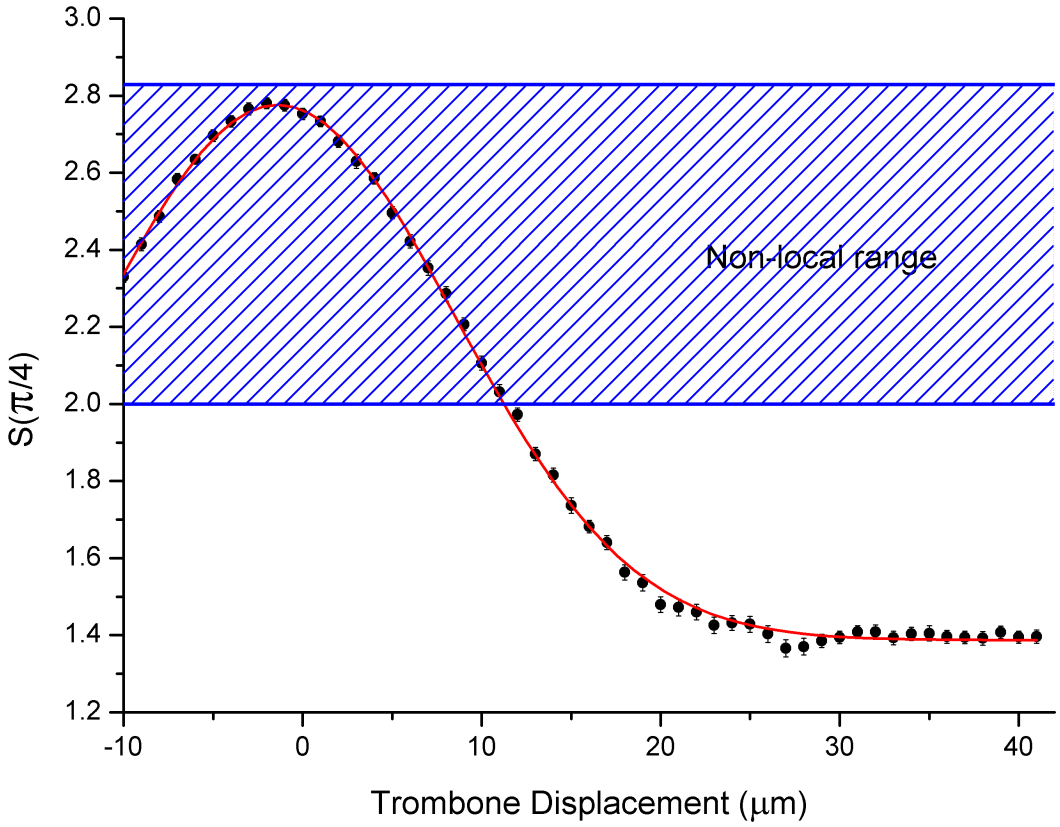


Figure 3.6: *Value of the Bell operator for different values of the trombone position. In blue area corresponding to non-local correlation. The maximum violations corresponds to a maximum entangled state.*

sured $S(\pi/2) = 2,7981 \pm 0.0078$, a value that violate the Bell inequality of over 98 standard deviations. This is an other confirmation of the purity of the generated state. The $S(\pi/2)$ was also measured for different position of the trombone. The

reduced temporal overlap between the wavepackets reduce the interference thus reducing the purity of the state. It is evident in Fig. 3.6 how a small displacement bring the produced state out of the quantum region back to the classical one.

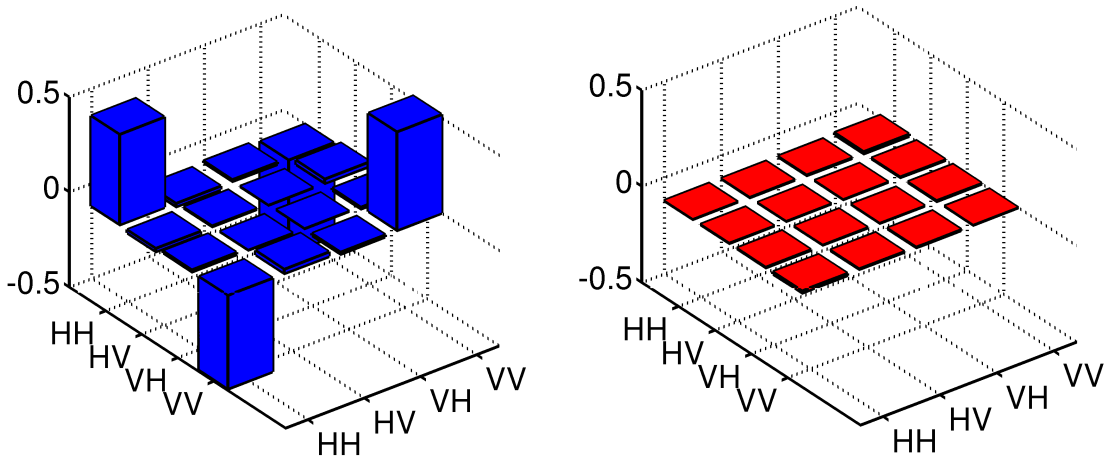
3.4 Tomography of the Entangled State

Quantum Tomography [James 01] is a technique that allows to reconstruct the full density matrix of a quantum state. Due to the limitation in the measurement [Peres 93, Wootters 82] is necessary to dispose of many copies of the state to reconstruct it.

For characterization of the polarization state of the biphoton I followed the procedure depicted in the work of James et al. [James 01], implementing the sequence of polarization measuremet via the rotation of two set of half and quarter waveplates in front of the Glenn-Laser polarizers. To have a complete description of the state is necessary to perform sixteen measurements. Often the tomographically measured matrices often fail to be positive semidefinite, especially when measuring low-entropy states. To avoid this problem the obtained density matrix describes a physical state a maximum likelihood numerical procedure has been implemented.

The measured density matrix for the output state is reported in Fig. 3.7. The presence of high peaks out of the main diagonal in the real part is a distinctive sign of entanglement. From the Density matrix is possible to measure many useful quantities. The measured entanglement of formation [Wootters 98] is 0.989 ± 0.005.

In this chapter I presented the entangled state source setup in the laboratory of quantum optics. The generated entangled state was used as source for a cryp-



(a) Real Part (b) Imaginary Part

Figure 3.7: *Density Matrix for the output state of the Interferometer.*

tographic system, as presented in the next chapter.

Chapter 4

Realization of a Quantum Communication Protocol

One of the most attractive application of quantum mechanics is the secret sharing of random data between two or more users. Since the seminal works by Bennett and Brassard [Bennett 84] and Ekert [Ekert 91] the Quantum Cryptography (QC) developed into a promising field of research for near-future technology, and both theoretical and experimental work has been done in order to prove its security and feasibility (see [Gisin 02] and references therein). QC allows for the generation of a secret random key between two legitimate parties, traditionally called Alice and Bob. The key is then used to make the information traveling on a public channel unintelligible to any unauthorized party (Eve).

In this chapter I present the experimental test of a quantum communication protocol suitable both for direct communication of plain text messages and Quantum Key Distribution (QKD) that does not employ entanglement, specifically the one described in Ref. [Lucamarini 05] (LM05).

4.1 The Lucamarini-Mancini Protocol

In 2002 Boström and Felbinger introduced [Boström 02] a protocol for QKD and *quasisecure* [1] direct communication exploiting the the properties of two ways quantum protocols and. They named it "Ping-Pong" (PP) protocol from the pictorial metaphor of the information carrier bouncing back and forth between the two users. The use of entanglement, the absence of basis reconciliation, typical of the one-way protocols and the separated procedures for security verification and key generation are the distinctive features of the PP. In this protocol entanglement is exploited to attain a deterministic transmission of information allowing for a number of new tasks besides QKD such as direct communication (DC) [Beige 02] and quantumLetter dialogue [Ba An 04]. Unfortunately, PP was proved to be not secure [Cai 03, Wójcik 03]. In 2005 Lucamarini and Mancini [Lucamarini 05] presented a new protocol (LM05), inspired by Boström and Felbinger's one, of which does not share the same weakness but allows essentially all the kind of communication provided by PP. The LM05 is a two way quantum protocol but does not relay on entanglement for security.

The communication begins when Bob prepares a qubit in one of a four states alphabet: $|0\rangle$, $|1\rangle$ (the Pauli $\boldsymbol{Z}$ eigenstates), $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (Pauli $\boldsymbol{X}$ eigenstates), and sends it to his counterpart Alice. For every run, Alice has two operation to apply randomly on the state. With probability c she projects the received qubit a basis chosen at random between $\{|0\rangle, |1\rangle\}$

[1] From [Boström 02]:"an eavesdropper is able to gain a small amount of message information before being detected". This means that the two users can establish a channel for direct communication in which the presence of the eavesdropper can be promptly detected.

and $\{|+\rangle, |-\rangle\}$ (*Control Mode* or CM); with probability $1-c$ she encodes a bit (*Encoding Mode* or EM). The encoding is realized applying the identity operator $\boldsymbol{I}$ for '0' or $i\boldsymbol{Y} = \boldsymbol{Z}\boldsymbol{X}$ for '1'. Notice that $i\boldsymbol{Y}$ acts as spin flip for all the states in the alphabet:

$$i\boldsymbol{Y}\left(|0\rangle, |1\rangle\right) = \left(-|1\rangle, |0\rangle\right); \tag{4.1}$$

$$i\boldsymbol{Y}\left(|+\rangle, |-\rangle\right) = \left(-|-\rangle, |+\rangle\right); \tag{4.2}$$

. The parameter $c \in [0,1]$ enters in the security test for the communication and can, in principle, be set to a value that maximize the efficiency of the overall protocol [Lucamarini 05] according the noise present on the channels.
Alice can now send the qubit back to Bob who measures it in the same basis he prepared it. In case of an EM run Bob deterministically infer Alice's operation from the eventual flipping of the received qubit. As public declaration of the CM runs from Alice permits the security check of the channels. Via a public debate, Alice and Bob performs a double control, which includes two single tests on the quantum channel, each of which is equivalent to that performed in the one-way BB84 [Bennett 84, Gisin 02, Ekert 91]. It is possible to calculate a quantum bit error rate (QBER) for the two channel. A complete prove of the security for the protocol is presented in the original work of Lucamarini and Mancini [Lucamarini 05].

4.2 Experimental Setup

In fig. 4.1 is represented the experimental setup used for initial test of the protocol and later used also for noise studies (section 5). The protocol is realized

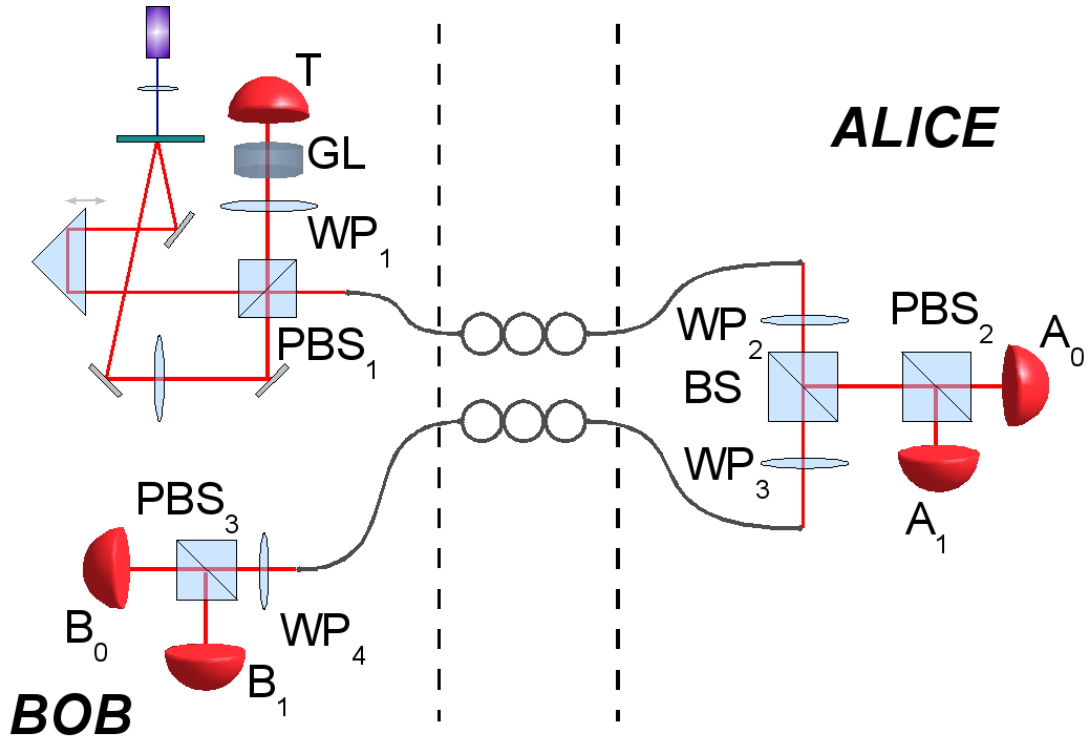


Figure 4.1: *Schematic picture of the experimental setup.*

encoding the qubit in the polarization degree of freedom of optical photons. The four state we used belongs to the equator of the Bloch sphere, i.e. the linear polarization subspace: horizontal ($|\leftrightarrow\rangle$), vertical ($|\updownarrow\rangle$), diagonal ($|\nearrow\rangle$)and its orthogonal state ($|\nwarrow\rangle$).The photons necessary for communication were generated with the technique described in section 3.1. A non-local preparation exploiting the entanglement of the source is applied to generate the necessary polarization states. The use of entangled photons is not necessary for the protocol itself but in the case of this experimental realization has several advantages. The first one is the the use of coincidence counts opposed to single counts: the use of one photon of the pair as trigger for the whole communication system reduces the noise signal. Moreover, this system could be easily extended to a totally random

state preparation using only linear optics components.

The output state of the interferometer can be accurately described in the polarization space as [Kim 03b]:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|\leftrightarrow\rangle_1 |\leftrightarrow\rangle_2 - |\updownarrow\rangle_1 |\updownarrow\rangle_2\big). \tag{4.3}$$

To prepare the qubit to send to Alice, one of the output mode (from now on labelled 1) of the interferometer is measured to obtain a non-local preparation of the state in the other mode (labelled 2). This can be easily described in terms of density matrix:

$$\rho_{12}^{(2)} = |\psi\rangle\langle\psi| = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}. \tag{4.4}$$

The measurement on channel 1 is represented by the projector $\boldsymbol{P}_1$, which is one of $\{|\leftrightarrow\rangle\langle\leftrightarrow|, |\updownarrow\rangle\langle\updownarrow|, |\nearrow\rangle\langle\nearrow|, |\nwarrow\rangle\langle\nwarrow|\}$. The reduced state for mode 2 then reads:

$$\rho_2^{(1)} = \mathrm{Tr}_1\big[\rho_{12}^{(2)}\,(\boldsymbol{P}_1 \otimes \boldsymbol{I}_2)\big]. \tag{4.5}$$

The projector is realized via an half waveplate and a Glen Laser (GL) polarizer. It is possible to control the preparation process at Bob's side through the rotation of the waveplate; I indicate with α the angle formed by the fast axis and the horizontal. The following angles encode the corresponding states:

State	α
$\|\leftrightarrow\rangle$	-22.5°
$\|\updownarrow\rangle$	22.5°
$\|\nearrow\rangle$	45°
$\|\nwarrow\rangle$	0°

In order to improve the resistance of the state to the natural degradation of the entanglement the photons are filtered by a pair of interference filters centered at 810 nm and with a bandwidth of 40 nm. This reduces the count rate but improves the values of the various QBERs, reducing the background light. The singlet count rate for the source is 12 000 cps, coincidence count rate is 1 000 cps.

The prepared photon is launched into a single mode fiber at 810 nm and sent to Alice. For this test setup the fiber used is 5 m long. For compensating polarization rotations, the fiber passes through a manual fiber polarization controller (Thorlabs FPC-562). Before every experimental runs the controller is aligned so that polarization contrast is at least 98% for both the $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ basis and the $\{|\nearrow\rangle, |\nwarrow\rangle\}$ one. This contrast is easily measured through the polarizing beam splitter PBS_2 and the waveplate WP_2.

When the photon reaches Alice's side a 50/50 beam splitter (BS_A) provide a passive random switch between CM runs and EM runs with equal probabilities, i.e. determining a value for $c = 0.5$.

Encoding mode

For the message mode is necessary to realize the $\boldsymbol{I}$ and the $i\boldsymbol{Y}$ Pauli operators. Laying all the states on the equator of the Bloch sphere, two half waveplates (WP_2 and WP_3 in Fig. 4.1) with properly aligned axis suffice to our needs.

For implementing the Identity, the optical axes of the two waveplates must be parallel or orthogonal (an eventual phase has no importance for the rest of the protocol); for the flipping operator $i\boldsymbol{Y}$ the optical axis must form an angle of 45°. It is worth noting that it is not necessary to define any specific direction in space and that only the relative angle of the waveplates axes is important and the rotation of only one between WP_2 and WP_3 is sufficient to switch from $\boldsymbol{I}$ to $i\boldsymbol{Y}$ and

viceversa.

After passing through the two waveplates the photon travels back to Bob through a second 5m long fiber equipped with manual fiber polarization controller too. This backward fiber pads, as the forward ones, are aligned in order to achieve a good fidelity between the input and output polarization.

Control Mode

There is a CM run every time that a photon is reflected by the 50/50 beam splitter BS_A. Working with single photons, it is rather hard to project a photon without destroying it. To compensate for the lack of an easy projection technique, a destructive measurement plus the injection of a photon with definite polarization was implemented as a turnaround.

Rotating the WP_2, Alice can choose which basis to analyze with a polarizing beam splitter (PBS_2). When the fast axis of WP_2 is parallel to the vertical, the PBS measures in the $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ basis, when the axis form an angle of 22.5°, the polarizer separates the states belonging to the $\{|\nearrow\rangle, |\nwarrow\rangle\}$ one. The output modes of PBS_2 are coupled into multimode fibers that bring the light onto the sensible surface of two APD. The counts get recorded for subsequent estimation of the QBER associated with the first channel.

An initial estimation of the channel QBER comes from the alignment procedure of the forward fiber. From the polarization contrast is possible to estimate the QBER for this channel. Defining the polarization contrast for a curve of the type shown in Fig. 4.2 as

$$V = \frac{C_{max} - C_{min}}{C_{max}}, \tag{4.6}$$

the QBER of the setup is

$$QBER = \frac{1 - V}{2}. \tag{4.7}$$

To complete the control mode, Alice injects an attenuated light pulse of definite

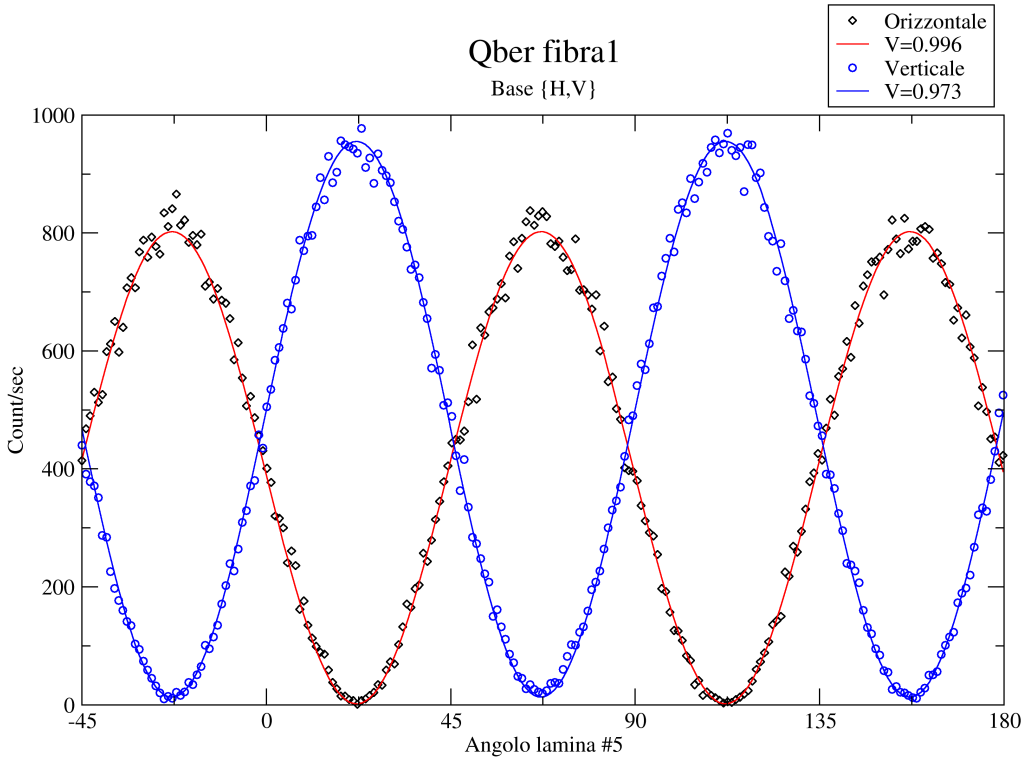


Figure 4.2:

polarization with a wavelength of 810 nm in the BS_A. This pulse is generated by a pulsed diode laser (Picoquant PDL 808 "Sepia") emitting at 810 nm and with a repetition rate of 80 MHz. The output of this laser is coupled into a multimode fiber and attenuated by a series of almost orthogonal polarizer, achieving an average number of photons per pulse of $\mu = (1.20 \pm 0.05)10^{-3}$.

Before being injected in the beam splitter, a polarizer ensure the vertical polarization of the light. The polarization of the photons sent by Alice can be rotated using the second half waveplate (WP_3) to obtain all the four state necessary starting from the vertical one provided by the laser diode.

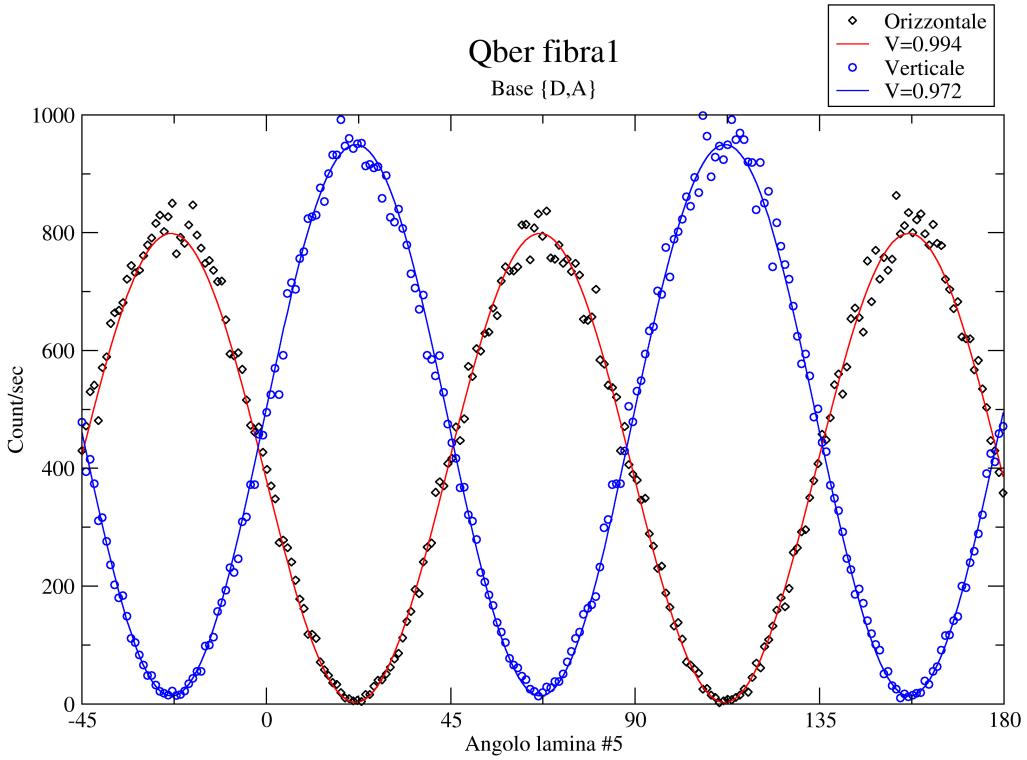


Figure 4.3:

The evident drawback of this system is the lack of contextuality, i.e. the CM and the EM cannot not run at the same time. Being a proof of principle experiment, we were interested in a system that could measure all the QBERS as easily as possible. For realizing the complete CM it would be necessary to synchronize the pulsed laser with the trigger signal and to work on its bandwidth to make it as close as possible to that of the down converted photons, all tasks that can be better accomplished with light at 1550 nm, where the full power of fiber integrated technologies could be exploited.

The photons sent by Alice are eventually polarization-analyzed at Bob's side by a half waveplate (WP_4) and a polarizing beam splitter (PBS_3). The WP_4 is set so

that the photons are measured in the same basis as they were originally prepared by Bob. Two multimode fibers are aligned with the output of the PBS collect the photons and transmit them to two APD modules. Correlation with the prepared qubits polarization transforms to logical bits. In case the two polarization are the same the bit is '0', in case there was a flip the bit is '1'. In the case of a complete protocol realization, from the raw data obtained by Bob must be removed all the runs corresponding to CM runs whose value is necessary for testing the security of the backward channel. In our case, the light from the diode was used to measure the polarization contrast for the backward fiber and estimating the associated QBER (see Fig 4.3).

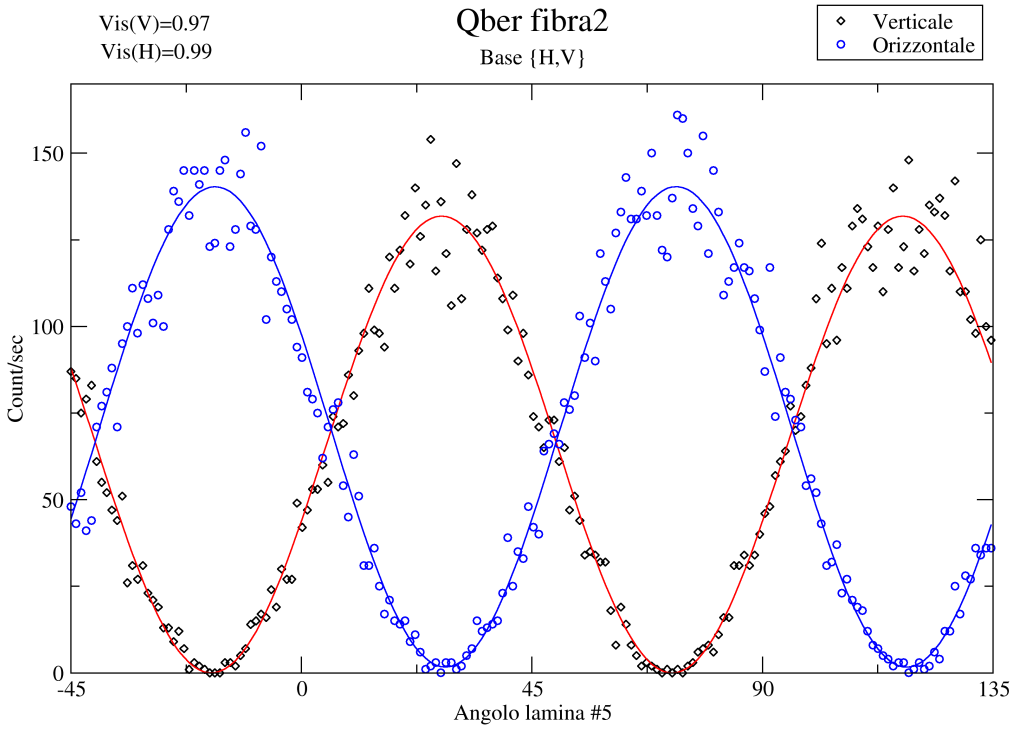


Figure 4.4:

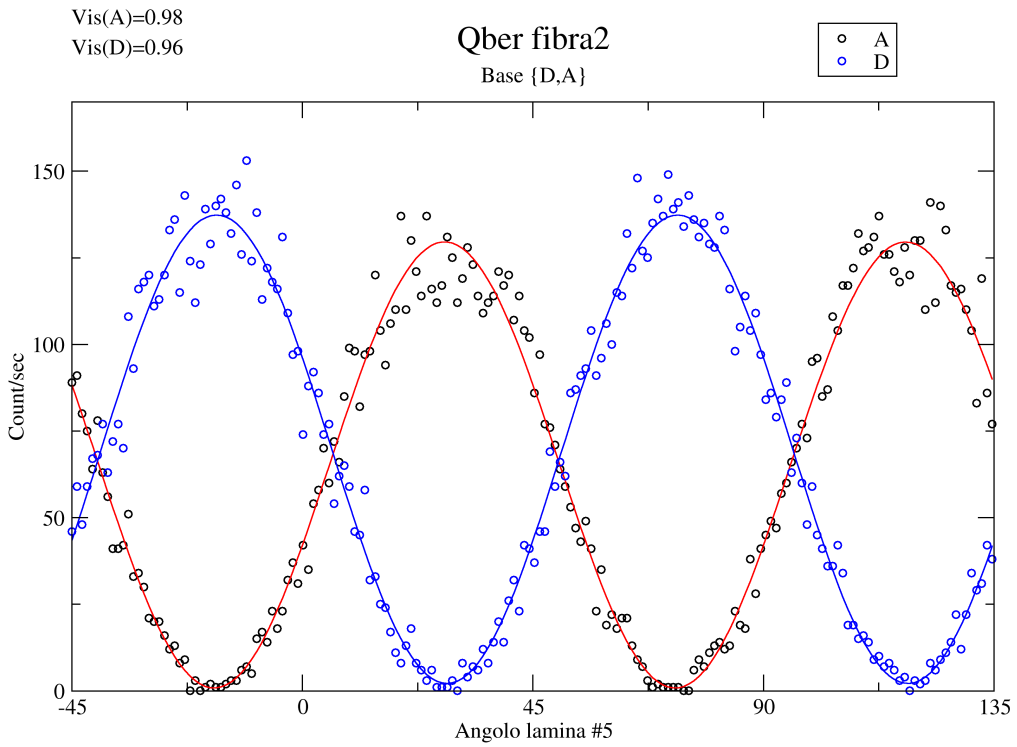


Figure 4.5:

4.3 The Communication test

After the alignment of the fiber the communication test was run. The EM and the CM were run separately, with the CM further split in two separate session, one for the first fiber and one for the second. The fibers proved to remain stable for quite long periods ($\sim 4h$), enough for several runs after the alignment. In figure 4.6 is reported a graphical representation of a communication test.

The test was run separately for every one of the four possible input state, $|\leftrightarrow\rangle$,

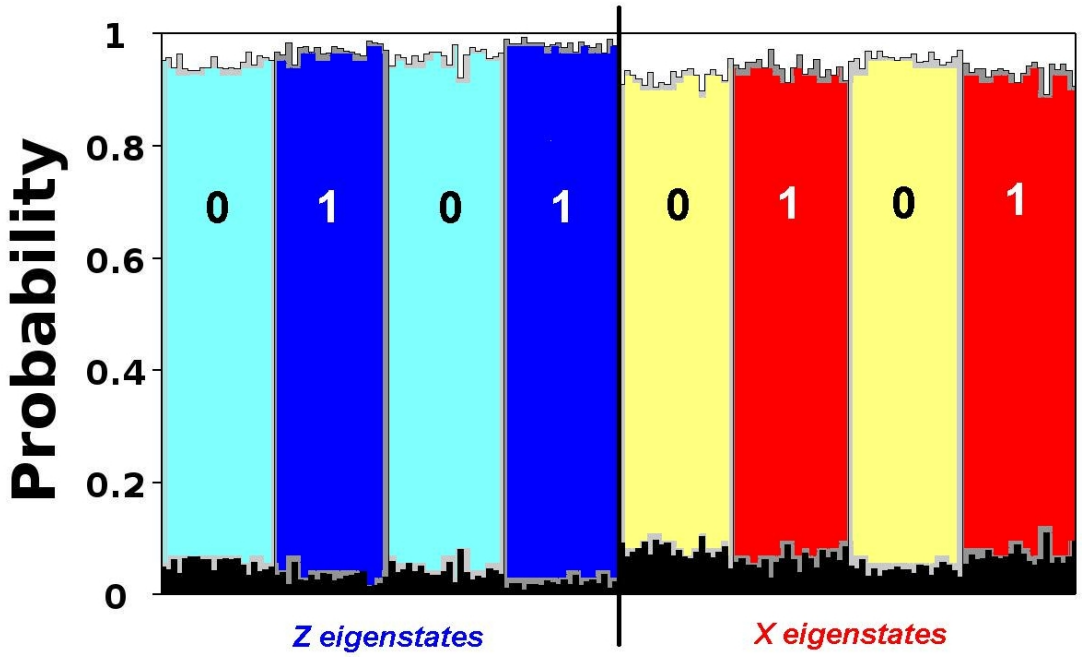


Figure 4.6: *Communication Test for the Message Mode of the LM05. On the left the test for the **Z** eigenstates, in light blue the coincidence counts corresponding to logical '0', i.e. H_T-H_B or V_T-V_B coincidence, in dark blue the coincidence counts for the logical '1', i.e. H_T-V_B or V_T-H_B coincidence; on the right the test for the **X** eigenstates. In black the QBER rate.*

$|\updownarrow\rangle$, $|\nearrow\rangle$ and $|\nwarrow\rangle$. After travelling the whole setup, two coincidence count rates between the trigger detector and the B_0 and B_1 (all at Bob's side) are recorded. With the basis for the measurement being the same of the encoding, the two detectors B_0 and B_1 can be directly associated to the logical value '0' and '1' respectively. In fact, when at Alice side the Identity operator is applied all the photons should be transmitted into B_0. The coincidence rate registered on the other detectors is thus an estimation of the total QBER of the system for that

state via the formula:

$$Q_T^{\boldsymbol{I}}(\text{`0'}) = \frac{R_1}{R_1 + R_0}, \tag{4.8}$$

where $R_{0,1}$ is the rate of coincidence between $B_{0,1}$ and the trigger detector.

When Alice encodes a '1' applying the $i\boldsymbol{Y}$, the photon polarization is switched, so that it gets ways reflected into B_1. This time, the rate at B_0 is the numerator of (4.8). The QBER for that prepared state is thus the average between the two measured QBER. The same procedure was repeated for the three remaining input state reported in the plot of Fig. 4.6. Different regions correspond to the different state preparation and Alice's encoding; all the eight configuration of interest are reported. The final QBER is the average of this eight values. The best value we obtained for Q_T is $(4.05 \pm 0.22)\ 10^{-2}$.

This quantity is not necessary for the security of the protocol but gives an idea on the performances of the setup and will prove useful in the rest of this work for estimating the mutual information between Alice and Bob.

During the CM runs, two BB84 [Bennett 84] are effectively performed, one for every channel, but with all the exchanged states used for QBER estimation. We define two quantities, q_1 and q_2, one for each channel, corresponding to the QBERs of those channels [Gisin 02]:

$$q_{1,2} = \frac{R_{\text{wrong}}}{R_{\text{wrong}} + R_{\text{right}}}. \tag{4.9}$$

For the security of the protocol is sufficient to measure q_1 and q_2 [Lucamarini 05] but the use of the three QBER (Q_T, q_1 and q_2) will permit the study of the behavior of a communication system under a certain class of attacks. This is presented in the next chapter.

In this chapter the LM05 protocol has been presented together with a test implementation. Even if the experimental setup used is not yet able to perform a complete generation of a key, the presented measurement witness its potential feasibility.

Chapter 5

Simulation of Individual Inchoerent Eavesdropping on the LM05 Protocol via Controlled Noise

In the years, several eavesdropping strategies of limited generality have been defined [Lütkenhaus 96, Biham 97b, Biham 97a, Gisin 02] and analyzed. Of particular interest is the assumption that Eve attaches independent probes to each qubit and measures her probes one after the other. This class of attack is called the *individual* or *incoherent attack* (IIA). The interest in this class of attacks resides in its few technology requirements (compared especially to the collective attacks, which requires the long storage of qubit). There are indications that the security threshold of 2-way QKD can overcome that of 1-way QC. One of these is that LM05 results secure against IIA regardless of the noise caused on the channel by this kind

of eavesdropping [Lucamarini 05]; on the other side BB84 results secure against individual attacks only if the noise threshold is lower than 15% [Fuchs 97] [Gisin 02, Sec. VI E]. In this section is prsented the theory for understanding the IIA and their experimental simulation performed on the test setup presented in the previous chapter.

5.1 Individual Inchoerent Attack

In the IIA, Eve prepares two sets of ancillae ε, η and makes them interact with the qubit: the ε's on the forward path and the η's on the backward one, after Alice's encoding stage. By a proper measure of her two sets of ancillae, Eve can gain information over the transmitted message performed by Alice and extract information about the key.

There are two mutually exclusive interactions that minimize Eve's noise on the channel while maximizing her gain, corresponding to the two bases ($\boldsymbol{Z}$ and $\boldsymbol{X}$) of Bob's preparation, and which I indicate with the superscript $\mathbb{Z}$:

$$\begin{aligned} &|0\rangle|\varepsilon\rangle \rightarrow |0\rangle|\varepsilon_0^{\mathbb{Z}}\rangle; \\ &|+\rangle|\varepsilon\rangle \rightarrow |+\rangle|\varepsilon_+^{\mathbb{Z}}\rangle + |-\rangle|\varepsilon_-^{\mathbb{Z}}\rangle \\ &; |1\rangle|\varepsilon\rangle \rightarrow |1\rangle|\varepsilon_1^{\mathbb{Z}}\rangle \\ &; |-\rangle|\varepsilon\rangle \rightarrow |+\rangle|\varepsilon_-^{\mathbb{Z}}\rangle + |-\rangle|\varepsilon_+^{\mathbb{Z}}\rangle; \end{aligned} \tag{5.1}$$

and $\mathbb{X}$:

$$\begin{aligned} &|+\rangle|\varepsilon\rangle \rightarrow |+\rangle|\varepsilon_+^{\mathbb{X}}\rangle; \\ &|0\rangle|\varepsilon\rangle \rightarrow |0\rangle|\varepsilon_0^{\mathbb{X}}\rangle + |1\rangle|\varepsilon_1^{\mathbb{X}}\rangle; \\ &|-\rangle|\varepsilon\rangle \rightarrow |-\rangle|\varepsilon_-^{\mathbb{X}}\rangle; \\ &|1\rangle|\varepsilon\rangle \rightarrow |0\rangle|\varepsilon_1^{\mathbb{X}}\rangle + |1\rangle|\varepsilon_0^{\mathbb{X}}\rangle; \end{aligned} \tag{5.2}$$

where have been introduced the states $\left|\varepsilon^{\mathbb{Z}}_{0,1}\right\rangle$, $|\varepsilon^{\mathbb{X}}_{+,-}\rangle$, $|\varepsilon^{\mathbb{Z}}_{+,-}\rangle = \left(|\varepsilon^{\mathbb{Z}}_{0}\rangle \pm |\varepsilon^{\mathbb{Z}}_{1}\rangle\right)/2$ and $|\varepsilon^{\mathbb{X}}_{0,1}\rangle = \left(|\varepsilon^{\mathbb{X}}_{+}\rangle \pm |\varepsilon^{\mathbb{X}}_{-}\rangle\right)/2$.

The states $|\varepsilon^{\mathbb{Z}}_{0,1}\rangle$ and $|\varepsilon^{\mathbb{X}}_{+,-}\rangle$ are normalized and non orthogonal:

$$\begin{aligned} \langle\varepsilon^{\mathbb{Z}}_{0,1}|\varepsilon^{\mathbb{Z}}_{1,0}\rangle &= \cos\phi^{\mathbb{Z}}_{\varepsilon} \\ \langle\varepsilon^{\mathbb{X}}_{+,-}|\varepsilon^{\mathbb{X}}_{-,+}\rangle &= \cos\phi^{\mathbb{X}}_{\varepsilon} \end{aligned} \qquad \text{with} \quad \phi^{\mathbb{Z},\mathbb{X}}_{\varepsilon} \in [0, \pi/2]. \tag{5.3}$$

The same derivation holds for backward propagation with η's ancillae in the place of ϵ's.

If Eve chooses the $\mathbb{Z}$-attack, corresponding to the transformations of Eqs.(5.1), she introduces no noise on the channel when Bob prepares the eigenstates of the Z-basis but creates disturbance in the conjugate basis X; the same argument applies for the $\mathbb{X}$-attack, Eqs.(5.2). Notice that the absence of a public basis revelation in LM05 prevents Eve from doing always the right choice between Eqs.(5.1) and (5.2).

In the frame of IIA, an explicit functional relation among the three abovementioned QBERs, q_1, q_2 and Q_{AB}, can be found. Let us begin with the expression of q_{1z} and q_{1x} as functions of the angles $\phi^{\mathbb{Z}}_{\varepsilon}, \phi^{\mathbb{X}}_{\varepsilon}$ chosen by Eve on the forward path:

$$q_{1z} = \left(1 - \cos\phi^{\mathbb{X}}_{\varepsilon}\right)/2 \tag{5.4}$$

$$q_{1x} = \left(1 - \cos\phi^{\mathbb{Z}}_{\varepsilon}\right)/2. \tag{5.5}$$

Through these relations is possible to guess Eve's angles $\phi^{\mathbb{X}}_{\varepsilon}, \phi^{\mathbb{Z}}_{\varepsilon}$ from the measurable quantities q_{1z}, q_{1x}, respectively. Analogous results (with angles $\phi^{\mathbb{X}}_{\eta}$ and $\phi^{\mathbb{Z}}_{\eta}$) hold for the partial QBERs q_{2z} and q_{2x} of the backward channel.

The expression of the total QBER Q_{AB} can be derived as the average probability that Alice and Bob find an error on the complete 2-way travel of the photon during the EM [Lucamarini 05]. The final expression as function of the measurable

partial QBERs, q_1 and q_2, is $(i = x, z)$:

$$Q_{ABi} \quad = \quad q_{1i} + q_{2i} - 2q_{1i}\, q_{2i}. \tag{5.6}$$

To ensure the security it is necessary to compare the mutual information shared by Alice and Bob, I_{AB}, with the one possessed by Eve.
It is known [Csiszár 78] that a secret key can be safely distilled with only unidirectional classical communication if the condition

$$I_{AB} \geq \min[I_{AE}, I_{BE}] \tag{5.7}$$

is accomplished. It is useful now to define the binary entropy

$$h(x) = x\, \log_2(x) + (1 - x)\, \log_2(1 - x). \tag{5.8}$$

The average Alice-Bob mutual information is then given by:

$$\bar{\mathrm{I}}_{AB} = \left(I_{ABz} + I_{ABx}\right)/2 \tag{5.9}$$

where

$$I_{ABi} = 1 - h\left(Q_{ABi}\right) \quad \text{with } i = (x, z). \tag{5.10}$$

In the LM05, for IIA the mutual information between Bob and Eve I_{BE} results always less than I_{AB} [Lucamarini 05], For the Security of the protocol is thus sufficient to concentrate on the mutual inforation between Alice and Eve.

The mutual information between Alice and Eve can be evaluated from $Q_{AE}^{\mathbb{Z},\mathbb{X}}$, defined as the error rate between Eve's guesses on Alice's encoding and Alice's real encoding. This quantity can be estimated from the measurements of the single channels QBERs q_1 and q_2, supposing that all the noise introduced in the channel is due to the interaction between the legitimate carrier and Eve's ancillae.

Considering the probability to correctly distinguish between two non-orthogonal states [Peres 93], in case of Eve's $\mathbb{Z}$-attack, Eq.(5.1), $Q^{\mathbb{Z}}_{AE}$ reads:

$$Q^{\mathbb{Z}}_{AE} = \frac{1}{2} - 2\sqrt{q_{1x}q_{2x}\,(1-q_{1x})\,(1-q_{2x})}. \tag{5.11}$$

A symmetrical result holds for $Q^{\mathbb{X}}_{AE}$. It is worth noting that the QBERs $Q^{\mathbb{Z},\mathbb{X}}_{AE}$ result independent of initial basis preparation and depend only on non-orthogonality of Eve's ancillae, i.e. on Eve's choice of the angles $\phi^{\mathbb{Z}}_{\varepsilon}, \phi^{\mathbb{Z}}_{\eta}$.
The average Alice-Eve mutual information is given by

$$\overline{I}_{AE} = (I^{\mathbb{Z}}_{AE} + I^{\mathbb{X}}_{AE})/2 \tag{5.12}$$

where $I^{\mathbb{Z},\mathbb{X}}_{AE} = 1 - h(Q^{\mathbb{Z},\mathbb{X}}_{AE})$.

An expression for the mutual QBER between Bob and Eve, Q_{BE}, can be derived in terms of Q_{AB} and Q_{AE} using the relation [Lucamarini 05]

$$Q_{BE} = Q_{AB} + Q_{AE} - 2Q_{AB}\cdot Q_{AE}. \tag{5.13}$$

The average mutual information between Bob and Eve is then expressed as:

$$\overline{I}_{BE} = (I^{\mathbb{Z}}_{BEz} + I^{\mathbb{Z}}_{BEx} + I^{\mathbb{X}}_{BEx} + I^{\mathbb{X}}_{BEz})/4\,, \tag{5.14}$$

where $I^{(\mathbb{Z},\mathbb{X})}_{BEi} = 1 - h(Q^{\mathbb{Z},\mathbb{X}}_{BEi})$, with $i = (x, z)$.

5.2 Experimental Eavesdropping Simulation

The idea of simulating an eavesdropping on this protocol was suggested by an attentive observations of eq. (5.6). This relation is suitable for direct experimental verification since the QBER on the left side and those on the right side are measured through independent processes, i.e. respectively during EM and CM runs

of the LM05 protocols. Even more interesting, the Mutual Informations that can be estimated by those QBERs (see previous section) can be compared and the effective security of the LM05 protocol under IIA can be verified. To simulate the presence of an eavesdropper we inserted a controlled noise on the channels to generate the same effect caused by an eavesdropper'saction equal the one described in Eqs. (5.1) and (5.2). Consider the following unitary transformation:

$$\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\varepsilon}} = \cos\phi^{\mathbb{Z}}_{\varepsilon}\,\boldsymbol{I} + i\sin\phi^{\mathbb{Z}}_{\varepsilon}\,\boldsymbol{Z}, \tag{5.15}$$

where $\phi^{\mathbb{Z}}_{\varepsilon}$ is the same angle defined for the Eve's $\mathbb{Z}$-attack in Eq. (5.3). If Bob's initial state is an eigenstate of the X-basis, we observe that under the action of $\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\varepsilon}/2}$ they are flipped with probability

$$P_{flip} = \sin^2\left(\phi^{z}_{\varepsilon}/2\right) = \left(1-\cos\phi^{z}_{\varepsilon}\right)/2, \tag{5.16}$$

equal to the expression of $q^{\mathbb{Z}}_{1x}$ in Eq.(5.4). Therefore the unitary transformation $\boldsymbol{U}^{\mathbb{Z}}_{\phi^{z}_{\varepsilon}/2}$ determines on the forward channel the same effect as Eve's $\mathbb{Z}$ attack. An analogous result is true for the backward path. To evaluate the total QBER Q_{AB}, we must consider the transformations on the X-states for the forward and backward channel, $\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\varepsilon}/2}$ and $\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\eta}/2}$, and both Alice's encoding operations, $\boldsymbol{I}$ and $i\,\boldsymbol{Y}$. This way leads to this two expression:

$$Q^{\mathbb{Z}}_{ABx}(\boldsymbol{I}) = \sin^2(\phi^{\mathbb{Z}}_{\varepsilon}/2 + \phi^{\mathbb{Z}}_{\eta}/2) \tag{5.17}$$

and

$$Q^{\mathbb{Z}}_{ABx}(i\,\boldsymbol{Y}) = \sin^2(\phi^{\mathbb{Z}}_{\varepsilon}/2 - \phi^{\mathbb{Z}}_{\eta}/2). \tag{5.18}$$

This quantities depend on Alice's transformation, but the average between them is not:

$$\overline{Q}^{\mathbb{Z}}_{ABx} = (1-\cos\phi^{\mathbb{Z}}_{\varepsilon}\cos\phi^{\mathbb{Z}}_{\eta})/2, \tag{5.19}$$

exactly equal to Eq.(5.6) after expressing the partial QBERs through Eqs. (5.4). The action of the eavesdropping is simulated by the two polarization controlling pads on the fibers connecting Alice and Bob's sides. The $\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\varepsilon}/2}$ is achieved aligning the pads so that the propagation along the fiber almost does not disturb the states $|H\rangle$ and $|V\rangle$ (eigenstates of the $\boldsymbol{Z}$ operator), while the $|D\rangle$ and $|A\rangle$ states (eigenstates of the $\boldsymbol{X}$ operator) are affected. To complete the simulation of the attack, the return fiber has to be set symmetrically (or anti-symmetrically). Experimentally this is achieved checking the polarization state of the photons after a whole trip. For the anti-symmetric case Alice's waveplates WP_2 and WP_3 axes are set parallel, i.e. they act as the identity operator. To obtain an high degree of fidelity is necessary that

$$\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\eta}/2} = \left(\boldsymbol{U}^{\mathbb{Z}}_{\phi^{\mathbb{Z}}_{\varepsilon}/2}\right)^{-1}, \tag{5.20}$$

so that the evolution is described as:

$$\boldsymbol{Z}^{F2}_{\theta}\boldsymbol{I}_{A}\boldsymbol{Z}^{F1}_{\theta}\,|\psi\rangle = |\psi\rangle\,. \tag{5.21}$$

The intrinsic structure of the pads does not allow an high precision in the alignment, while it gives a good stability figure.

After the two fibers are aligned, we measured both q_1 and q_2. We experimentally verified this relation by measuring independently all the QBERs Q_{ABi}, q_{1i} and q_{2i}.

5.3 Experimental Results

In Fig. 5.1 is reported the experimental test of Eq. (5.6). In the x-axes is reportred the estimated value of Q_{AB} from the direct measuring of q_{1i} and q_{2i} and averaged over all the initial states; in the y-axes the mean value Q^{m}_{AB} of the measured Q_{ABi} obtained from the Q_T as measured in a communication test similar as the one

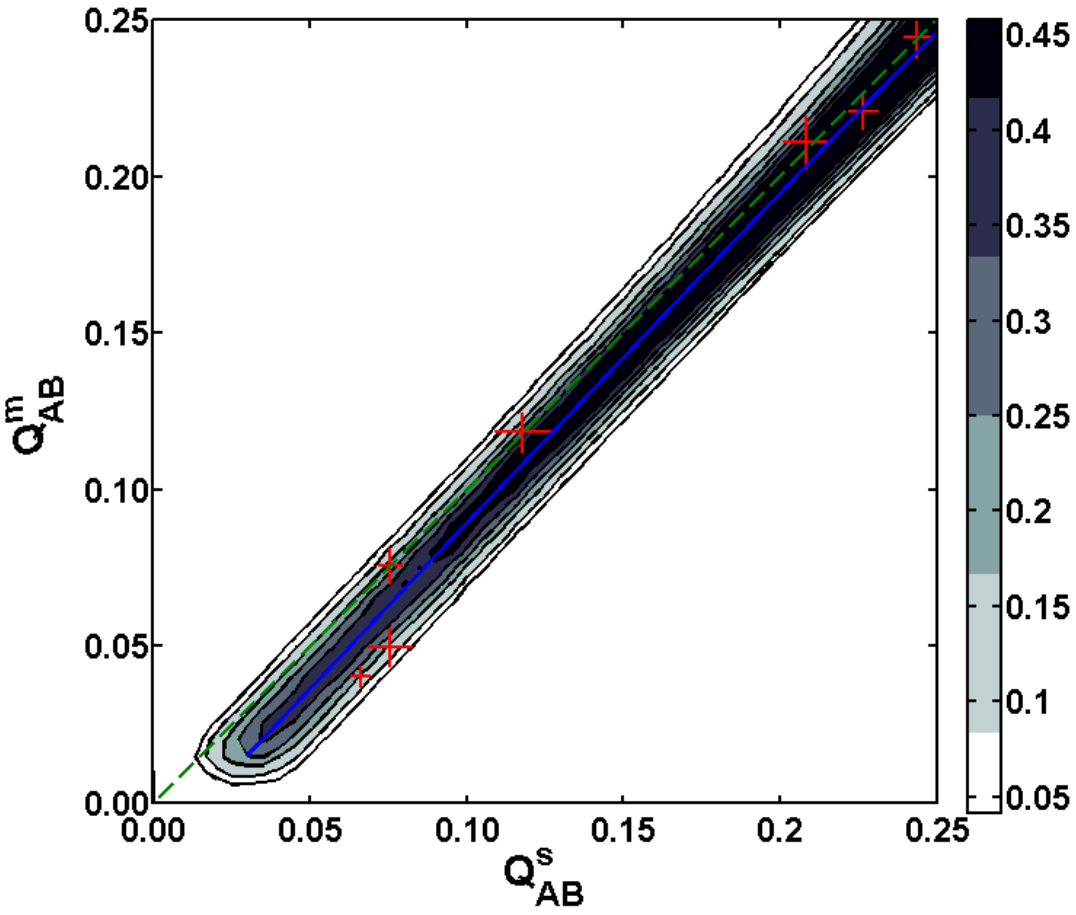


Figure 5.1: *Measured values of Q^m_{AB} in function of Q^s_{AB}, evaluated as explained in the text. The experimental data are reported as crosses with arms size equal to the estimated errors. The dashed-line represents the prediction of Eq. 5.6. The solid-line is the expected relation in the case of an apparatus in which 'noise' transformations in the wrong bases happen with probability* 0.015 *and a background errors in the QBER equal to* 0.03.

presented in section 4.3.

The main source of errors in our setup is the polarization evolution during its

propagation along the fibers. The Eq. (5.6) as to be modified to account all the possible errors in the alignment of the pads and also for accounting for background noise that leads to an homogeneous QBER, that is independent on the basis.
The presence of undesired contributions due to $\boldsymbol{Y}, \boldsymbol{X}$ operators during the simulated $\mathbb{Z}$-attack are taken into account through a parameter Δ, which quantifies the distance from a perfect realization of the unitary transformation of Eq.(5.15). A second parameter ξ has been introduced to account for the background noise in the detection. These effects have been included in a Montecarlo simulation[1]. In Fig. 5.1 the contour plot shows the result for for $N_t = 5 \times 10^5$ simulated trials for a $\mathbb{Z}$ attack with a uniform random choice of the Eve's angles ϕ_J in the range $[-\pi/4, \pi/4]$ ($J = F$ for the forward journey, $J = B$ for the backward one). The coefficient Δ varies in the range $[0, 0.03]$, and background correction coefficient is randomly chosen in the range $[0, 0.06]$. The counter plot represents the probability evaluated from the number of trials in the bins, equally spaced with area 0.005x0.005, divided by the total number of events N_t and normalized to the maximum value of the probability. The region at higher probability around QBER 0.25 is due to how the distribution of the QBER is affected by the uniformly random choice of the unitary transformation and noise parameters.

In Fig. 5.2 are plotted the curves of mutual information I according to Eqs.(5.9), (5.12) and (5.14) as function of the quantity Q^s_{AB}, already defined. We report in the same figure experimental, numerical and theoretical values. The solid lines represent our best fit of the experimental data, and draw the behavior of a perfect eavesdropping simulation. It is worthy of note the almost perfect intersection of these lines for $\bar{I}_{AB}$,$\bar{I}_{AE}$ and the theoretical (dashed)

[1]This simulation is mainly due to Gianni Di Giuseppe.

line at $Q^s_{AB} \simeq 19\%$, corresponding to the $\simeq 23\%$ of detection probability in Ref. [Lucamarini 05]. Furthermore the curve for $\bar{I}_{BE}$ is always below that for $\bar{I}_{AB}$, implying the security of the scheme against IIA regardless of the noise on the channel. Notice that the lower $\bar{I}_{AE}$ and $\bar{I}_{BE}$ the safer is the protocol, since the intersection points move towards the right. In turn this demonstrates the optimality of the eavesdropping described by Eqs.(5.1) and (5.2).

In conclusion, in this chapter I presented the experimental test of the security of a quantum communication protocol measuring the mutual information shared by the legitimate parties of the communication and the maximum accessible information for an eavesdropper. The particular two-way nature of the LM05 protocol allowed for a direct access to these mutual information through independent measures in a way that was never presented before.

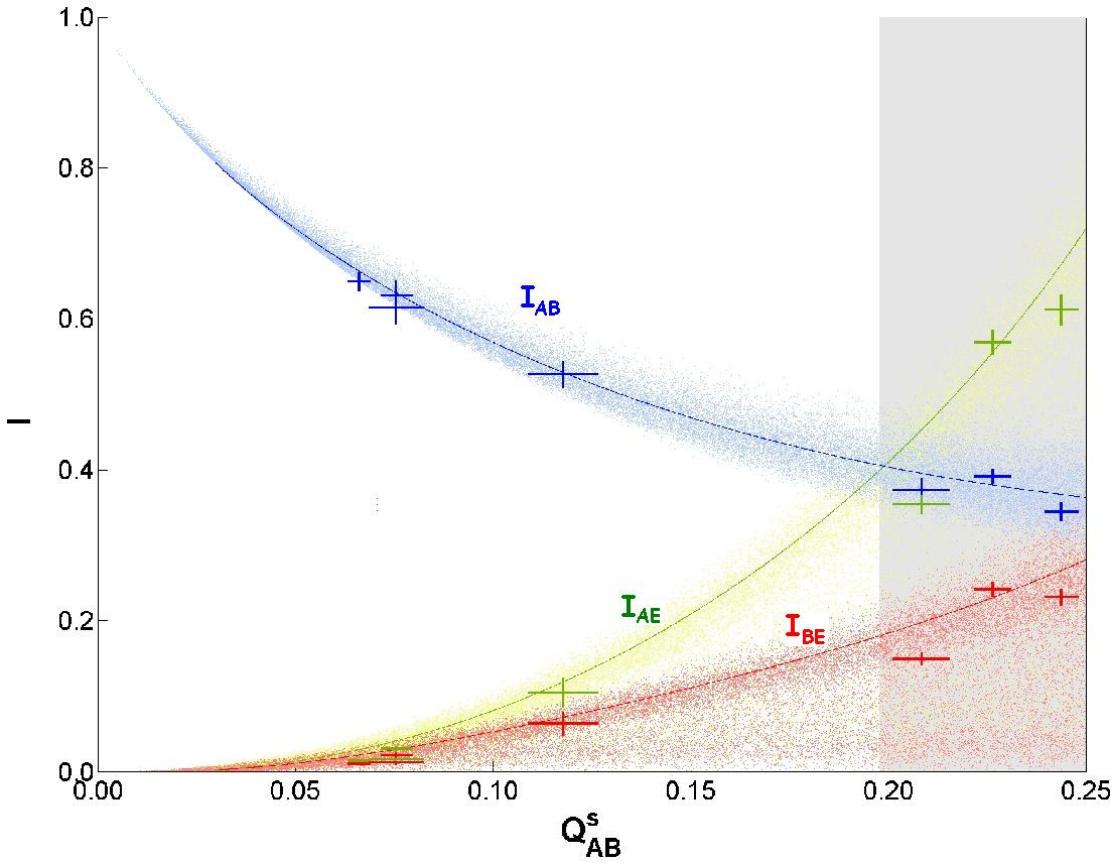


Figure 5.2: *Mutual information as function of the QBER* $\mathrm{Q}^{\mathrm{s}}_{\mathrm{AB}}$ *. The experimental points are reported with their statistical errors as crossed-rectangles* ($\bar{I}_{AB}$)*, white-crossed-rectangles* ($\bar{I}_{AE}$) *and gray-crossed-rectangles* ($\bar{I}_{BE}$)*. The solid lines are the mutual information with* $\Delta = 0.015$ *and* $\xi = 0.03$*. Results of* $N_t = 5 \times 10^5$ *simulated trials with the same parameters used for Fig.5.1 are reported. The asymmetric imperfection of the two channels cause the gray area below the lines* I_{AE}*,* I_{BE}*.*

Bibliography

[Abouraddy 02] Ayman F. Abouraddy, Magued B. Nasr, Bahaa E. A. Saleh, Alexander V. Sergienko & Malvin C. Teich. *Quantum-optical coherence tomography with dispersion cancellation.* Phys. Rev. A, vol. 65, no. 5, page 053817, May 2002.

[Allen 92] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw & J. P. Woerdman. *Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser mode.* Phys. Rev. A, vol. 45, no. 11, pages 8185–8189, June 1992.

[Andrews 04] R. Andrews, E. R. Pike & Sarben Sarkar. *Optimal coupling of entangled photons into single-mode optical fibers.* Optics Express, vol. 12, pages 3264–3269, 2004.

[Arlt 98] J. Arlt, K. Dholakia, L. Allen & M. J. Padgett. *The production of multiringed Laguerre-Gaussian modes by computer-generated holograms.* J. Mod. Opt., vol. 45, no. 6, pages 1231–1237, June 1998.

[Aspect 02] Alain Aspect. Quantum [un]speakables - from bell to quantum information, chapitre 9, pages 119–154. Springer, 2002.

[Ba An 04] Nguyen Ba An. *Quantum dialogue.* Physics Letters A, vol. 328, page 6, 2004.

[Beige 02] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer & Harald Weinfurter. *Secure communication with a publicly known key.* ACTA PHYS.POL.A, vol. 101, page 357, 2002.

[Bell 64] J. S. Bell. *On the Einstein Podolsky Rosen Paradox.* Physics, vol. 1, page 195, 1964.

[Bell 66] John S. Bell. *On the Problem of Hidden Variables in Quantum Mechanics.* Rev. Mod. Phys., vol. 38, no. 3, pages 447–452, Jul 1966.

[Bennet 93] Charles H. Bennet, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres & William K. Wooters. *Teleporting an Unknown Quantum State via Dual Classical and Einstei-Podolsky-Rosen Channels.* Phys. Rev. Lett., vol. 70, no. 13, page 1895, March 1993.

[Bennett 84] C. H. Bennett & G. Brassard. *Quantum Cryptography: Public-Key Distribution and Coin Tossing.* In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pages 175–179, Bangalore, India, December 1984. IEEE.

[Bennett 92] Charles H. Bennett & Stephen J. Wiesner. *Communication via One- andTwoParticle Operators on Einstein-Podolsky-Rosen States.* Phys. Rev. Lett., vol. 69, no. 20, page 2881, November 1992.

[Biham 97a] Eli Biham & Tal Mor. *Bounds on Information and the Security of Quantum Cryptography.* Phys. Rev. Lett., vol. 79, no. 20, pages 4034–4037, Nov 1997.

[Biham 97b] Eli Biham & Tal Mor. *Security of Quantum Cryptography against Collective Attacks.* Phys. Rev. Lett., vol. 78, no. 11, pages 2256–2259, Mar 1997.

[Boström 02] Kim Boström & Timo Felbinger. *Deterministic Secure Direct Communication Using Entanglement.* Phys. Rev. Lett., vol. 89, no. 18, page 187902, 2002.

[Bovino 03] Fabio Antonio Bovino, Pietro Varisco, Anna Maria Colla, Giuseppe Castagnoli, Giovanni Di Giuseppe & Alexander V. Sergienko. *Effective fiber-coupling of entangled photons for quantum communication.* Opt. Comm., vol. 227, page 343, November 2003.

[Boyd 02] Robert W. Boyd. Nonlinear optics. Academic Press, 2002.

[Branning 99] D. Branning, W. P. Grice, R. Erdmann & I. A. Walmsley. *Engineering the Indistinguishability and Entanglement of Two Photons.* Phys. Rev. Lett., vol. 83, no. 5, pages 955–958, Aug 1999.

[Cai 03] Qing-yu Cai. *The "Ping-Pong" Protocol Can Be Attacked without Eavesdropping.* Phys. Rev. Lett., vol. 91, no. 10, page 109801, September 2003.

[Carrasco 04] Silvia Carrasco, Juan P. Torres, Lluis Torner, Alexander Sergienko, Bahaa E. A. Saleh & Malvin C. Teich. *Spatial-*

to-spectral mapping in spontaneous parametric down-conversion. Phys. Rev. A, vol. 70, no. 4, page 043817, 2004.

[Carrasco 06] Silvia Carrasco, Alexander V. Sergienko, Bahaa E. A. Saleh, Malvin C. Teich, Juan P. Torres & Lluis Torner. *Spectral engineering of entangled two-photon states.* Physical Review A (Atomic, Molecular, and Optical Physics), vol. 73, no. 6, page 063802, 2006.

[Castelletto 05] Stefania Castelletto, Ivo Pietro Degiovanni, Giampiero Furno, Valentina Schettini, Alan Migdall & Michael Ware. *Two-Photon Mode Preparation and Matching Efficiency: Definition, Measurement, and Optimization.* IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, vol. 54, no. 2, page 890, April 2005.

[Cerè 06] Alessandro Cerè, Marco Lucamarini, Giovanni Di Giuseppe & Paolo Tombesi. *Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise.* Phys. Rev. Lett., vol. 96, no. 20, page 200501, May 2006.

[Chuang 97] I. L. Chuang & M. A. Nielsen. J. Mod. Opt., vol. 44, page 2455, 1997.

[Chuang 00] I. L. Chuang & M. A. Nielsen. Quantum computation and quantum information. Cambridge University Press, 2000.

[Clauser 69] John F. Clauser, Michael A. Horne, Abner Shimony & Richard A. Holt. *Proposed Experiment to Test Local Hidden-Variable The-*

ories. Phys. Rev. Lett., vol. 23, no. 15, pages 880–884, October 1969.

[Csiszár 78] Csiszár & Körner. IEEE Transactions on Information Theory, vol. IT-24, page 339, 1978.

[De Caro 94] Liberato De Caro & Augusto Garuccio. *Reliability of Bell-inequality measurements using polarization correlations in parametric-down-conversion photon sources.* Phys. Rev. A, vol. 50, no. 4, pages R2803–R2805, 1994.

[Di Giuseppe 97] G. Di Giuseppe, L. Haiberger, F. De Martini & A. V. Sergienko. *Quantum interference and indistinguishability with femtosecond pulses.* Phys. Rev. A, vol. 56, no. 1, page 21, July 1997.

[Dragan 04] Andrzej Dragan. *Efficient fiber coupling of down-conversion photon pairs.* Phys. Rev. A, vol. 70, no. 5, page 053814, Nov 2004.

[Einstein 35] A. Einstein, B. Podolsky & N. Rosen. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev., vol. 47, no. 10, pages 777–780, May 1935.

[Ekert 91] Artur K. Ekert. *Quantum Cryptography Based on Bell's Theorem.* Phys. Rev. Lett., vol. 67, no. 6, page 661, Aug 1991.

[Feynman 82] R.P. Feynman. *Simulating physics with computers.* Int. J. of Theor. Phys., vol. 22, 1982.

[Fuchs 97] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu & Asher Peres. *Optimal eavesdropping in quantum*

cryptography. I. Information bound and optimal strategy. Phys. Rev. A, vol. 56, page 1163, 1997.

[Giovannetti 01] Vittorio Giovannetti, Seth Lloyd & Lorenzo Maccone. *Quantum-enhanced positioning and clock synchronization.* Nature, vol. 412, page 417, 2001.

[Giovannetti 02] Vittorio Giovannetti, Lorenzo Maccone, Jeffrey H. Shapiro & Franco N. C. Wong. *Generating Entangled Two-Photon States with Coincident Frequencies.* Phys. Rev. Lett., vol. 88, no. 18, page 183602, Apr 2002.

[Gisin 02] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel & Hugo Zbinden. *Quantum cryptography.* Rev. of Mod. Phys., vol. 74, page 145, Jan 2002.

[Grice 97] W. P. Grice & I. A. Walmsley. *Spectral information and distinguishability in type-II down-conversion with a broadband pump.* Phys. Rev. A, vol. 56, no. 2, page 1627, August 1997.

[Grice 01] W. P. Grice, A. B. U'Ren & I. A. Walmsley. *Eliminating frequency and space-time correlations in multiphoton states.* Phys. Rev. A, vol. 64, no. 6, page 063815, Nov 2001.

[Hong 87] C. K. Hong, Z. Y. Ou & L. Mandel. *Measurement of Subpicosecond Time Intervals Between Two Photons by Interference.* Phys. Rev. Lett., vol. 59, page 2044, 1987.

[James 01] Daniel F. V. James, Paul G. Kwiat, William J. Munro & Andrew G. White. *Measurement of qubits*. Phys. Rev. A, vol. 64, no. 5, page 052312, 2001.

[Keller 97] Timothy E. Keller & Morton H. Rubin. *Theory of two-photon entanglement for spontaneous parametric down-conversion driven by a narrow pump pulse*. Phys. Rev. A, vol. 56, no. 2, pages 1534–1541, Aug 1997.

[Kim 03a] Yoon-Ho Kim & Warren P. Grice. *Reliability of the beam-splitter-based Bell-state measurement*. Phys. Rev. A, vol. 68, no. 6, page 062305, 2003.

[Kim 03b] Yoon-Ho Kim, Sergei P. Kulik, Maria V. Chekhova, Warren P. Grice & Yanhua Shih. *Experimental Entanglement Concentration And Universal Bell-State Synthesizer*. Phys. Rev. A, vol. 67, no. 1, page 010301, 2003.

[Klyshko 69] D. N. Klyshko. Sov. Phys. JETP, vol. 28, page 522, 1969.

[Knill 01] E. Knill, R. Laflamme & G. J. Milburn. *A scheme for efficient quantum computation with linear optics*. Nature, vol. 409, page 46, January 2001.

[Kurtsiefer 01] Christian Kurtsiefer, Markus Oberparleiter & Harald Weinfurter. *High-efficiency entangled photon pair collection in type-II parametric fluorescence*. Phys. Rev. A, vol. 64, no. 2, page 023802, August 2001.

[Kwiat 95] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko & Yanhua Shih. *New High-Intensity Source of Polarization-Entangled Photon Pairs.* Phys. Rev. Lett., vol. 75, no. 24, pages 4337–4341, December 1995.

[Lucamarini 05] Marco Lucamarini & Stefano Mancini. *Secure Deterministic Communication without Entanglement.* Phys. Rev. Lett., vol. 94, no. 14, page 140501, 2005.

[Lütkenhaus 96] Norbert Lütkenhaus. *Security against eavesdropping in quantum cryptography.* Phys. Rev. A, vol. 54, no. 1, page 97, Jul 1996.

[Mair 01] Alois Mair, Alipasha Vaziri, Gregor Weihs & Anton Zeilinger. *Entanglement of the orbital angular momentum states of photons.* Nature, vol. 412, pages 313–316, July 2001.

[Monken 98] C. H. Monken, P. H. Souto Ribeiro & S. Pádua. *Optimizing the photon pair collection efficiency: A step toward a loophole-free Bell's inequalities experiment.* Phys. Rev. A, vol. 57, no. 4, pages R2267–R2269, Apr 1998.

[Peres 93] A. Peres. Quantum theory: Concepts and methods. Kluwer Academic Publishers, 1993.

[Pittman 96] T. B. Pittman, D. V. Strekalov, D. N. Klyshko, M. H. Rubin, A. V. Sergienko & Y. H. Shih. *Two-photon geometric optics.* Phys. Rev. A, vol. 53, no. 4, pages 2804–2815, Apr 1996.

[Poyatos 97] J. F. Poyatos, J. I. Cirac & P. Zoller. *Complete Characterization of a Quantum Process: The Two-Bit Quantum Gate*. Phys. Rev. Lett., vol. 78, no. 2, pages 390–393, Jan 1997.

[Rarity 95] J. Rarity. Ann. N.Y. Acad. Sci., vol. 755, page 624, 1995.

[Rubin 96] Morton H. Rubin. *Transverse correlation in optical spontaneous parametric down-conversion*. Phys. Rev. A, vol. 54, no. 6, pages 5349–5360, December 1996.

[Schrödinger 35] E. Schrödinger. Proc. Cambridge Philos. Soc., vol. 31, page 555, 1935.

[Schumacher 95] Benjamin Schumacher. *Quantum coding*. Phys. Rev. A, vol. 51, no. 4, pages 2738–2747, Apr 1995.

[Shor 94] P. W. Shor. *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. In Proceedings of the 35th Annual Symposium on Fundation of Computer Science, pages 124–134, Los Alamos, CA, 1994. IEEE Computer Society Press.

[U'Ren 05] A. B. U'Ren, C. Silberhorn, K. Banaszek, I. A. Walmsley, R. Erdmann, W. P. Grice & M. G. Raymer. *Generation of Pure-State Single-Photon Wavepackets by Conditional Preparation Based on Spontaneous Parametric Downconversion*. Laser Physics, vol. 15, no. 1, page 146161, 2005.

[White 99] Andrew G. White, Daniel F. V. James, Philippe H. Eberhard & Paul G. Kwiat. *Nonmaximally Entangled States: Produc-*

tion, Characterization, and Utilization. Phys. Rev. Lett., vol. 83, no. 16, pages 3103–3107, Oct 1999.

[Wójcik 03] Antoni Wójcik. *Eavesdropping on the "Ping-Pong" Quantum Communication Protocol.* Phys. Rev. Lett., vol. 90, no. 15, page 157901, April 2003.

[Wootters 82] W. K. Wootters & W. H. Zurek. *A single quantum cannot be cloned.* Nature, vol. 299, pages 802–803, October 1982.

[Wootters 98] William K. Wootters. *Entanglement of Formation of an Arbitrary State of Two Qubits.* Phys. Rev. Lett., vol. 80, no. 10, pages 2245–2248, March 1998.

[Zukowski 95] M. Zukowski, A. Zeilinger & H. Weinfurter. Ann. N.Y. Acad. Sci., vol. 755, page 91, 1995.