Orbital Angular Momentum and Polarization in a BB84 Protocol

André Rodrigues
franco.rodrigues@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

October 2019

Abstract

In this work two BB84 protocol implementation solutions and their technical challenges were explored. To study the possibility of employing light's orbital angular momentum (OAM) as a qubit experiments were performed displaying spiral and fork patterns into two spatial light modulators (SLM) to generate and manipulate light's OAM. Computational simulations were made to validate the experimental results using Fourier optics theory and implemented protocol crosstalk matrix is obtained by simulating the tomographic reconstruction. To study the possibility of employing light's polarization as a qubit, optical elements were used to manipulate polarized light. In both solutions a spontaneous parametric down-conversion process was used as a single photon source. The hypothesis of using the angular orbital moment as quantum bit is discarded and the implementation of the spontaneous parametric conversion process is not successful. A detailed explanation is left about the problems encountered throughout the work and possible solutions to solve them.

Keywords: Orbital Angular Momentum (OAM), Spatial Light Modulator (SLM), Laguerre-Gaussian (LG), Spontaneous Parametric Down Conversion (SPDC), Crystal BBO, Quantum Key Distribution Protocol (QKD).

1. Introduction

Nowadays, the society's trust in communication systems depends on the guarantee of content security and privacy (e.g. Shopping Online or Voting via computer) and any new methods or tools to communicate must address this critical factor.

A serious problem, not yet addressed as it should be, is the breakthrough in mathematics and computer sciences (e.g. Quantum Computer [1]) that will completely bypass, in useful time, state-of-the-art encryption methods like the ones used in internet banking transactions. This is because the today's cryptography protocols are designed around the hypothesis that a particular problem cannot be solved efficiently by the available computer power. The trend towards stronger computation devices allows the management of longer keys but also increases the success of breaking keys, which rises another security problem: even with the most advanced security technology and the best-practice methods, data encrypted today can be stored and in the future be decrypted once the technology reaches today's encryption methods.

A solution to this problem is to use the laws of nature as the encryption method here proposed, namely, quantum mechanics to create quantum cryptography links [2]. Quantum cryptography can provide long-term security and concrete evidence of an attempt of eavesdropping just using the theoretically and experimentally tested laws of nature. Understanding the challenges and limitations of inducing angular orbital momentum, generating single photons and implementing this protocol is of utmost importance to, in the future, successfully integrate quantum communications into society.

2. Background

The work developed has an extensive background that requires an introduction. The section will begin by presenting the conceptual aspects that characterize a quantum information protocol, from a qubit in 2.1 to the system crosstalk matrix in 2.2. Only the quantum bit error rate will not be addressed for being out of the work's scope. The Laguerre-Gaussian beams are presented in 2.3 which describes light carrying an orbital angular momentum (OAM). Light's OAM is a quantum aspect that can be generated, manipulated and observed which makes it suitable to be used as a physical qubit. In this implementation, information is sent through air so to describe the propagation of light waves through space, Fourier Optics theory is presented in 2.4 which will also be used in the computational methods to validate the experimental results. By last but not less important, a requirement to implement a quantum key distribu-

tion protocol is the capability of generating single photons. A nonlinear effect process named spontaneous parametric down-conversion is employed and its theretical foundations are presented in 2.5.

2.1. Quantum Bits

The bit is a concept of classical information. Quantum information theory is built upon an analogous concept known as quantum bit or qubit where a state of a quantum system is interpreted as information. Its properties will be introduced by comparing them with those of classical bits and the description will be mathematical although qubits, in every quantum protocol implementation, are physical objects. This mathematical approach allows to construct a quantum information theory that is independent of a specific system created for its implementation. A classical bit has a state, 0 or 1, and a qubit has also a state $|0\rangle$ or $|1\rangle$. The main difference between bits and qubits is that qubits have other states than $|0\rangle$ or $|1\rangle$ which are linear combinations of these states.

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

The α and β are complex numbers but for this discussion considering them real numbers is acceptable but the quantum state $|\psi\rangle$ is a vector in 2-D complex vector space. $|0\rangle$ or $|1\rangle$ are the basis states which form an orthonormal basis.

In a classical system it is possible to determine if a state is 0 or 1 without changing its state. Reading a memory is exactly this. In a qubit such action is not possible and we cannot know the qubit, that is, the values of α and β. When a qubit state is measured we either get $|0\rangle$, with a probability $|\alpha|^2$ or $|1\rangle$ with a probability $|\beta|^2$, where $|\alpha|^2 + |\beta|^2 = 1$. It is important to understand the physical interpretation of these probabilities. Classically, a system with two possible states is always in one of them. We might not know in which one the system is but its certain that it is in one of the states. A qubit is not in one of two states, it is in a continuum of states between $|0\rangle$ and $|1\rangle$ and only when observed, the qubit acquires the state $|0\rangle$ or $|1\rangle$, with their respective probabilities. As an example, a qubit can be in the state

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{2}$$

which means that when we observe the qubit state, half of the time we will get a 0 and 1 in the other half. States like this one are named superpositions. The qubit is in a superposition of $|0\rangle$ and $|1\rangle$ and when it's observed, it collapses to the state $|0\rangle$ or $|1\rangle$.

2.2. Crosstalk Matrices

To implement a quantum key distribution protocol it is necessary to have two orthonormal bases. Having the base $\{|0\rangle, |1\rangle\}$ where $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ The quantum states of this base are commonly written as $\{|+\rangle, |-\rangle\}$ and when a qubit, in one of these states, is observed with the base set $\{|0\rangle, |1\rangle\}$, the chance of the qubit quantum state collapsing in one of these states is well known. Mathematically $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are mutually unbiased bases. For a set mutually unbiased bases $\{|e_1\rangle, ..., |e_d\rangle\}$ and $\{|f_1\rangle, ..., |f_d\rangle\}$, the square of the magnitude of the inner product between any basis states $|e_j\rangle$ and $|f_k\rangle$ equals the inverse of the dimension d [3]:

$$|\langle e_j|f_k\rangle|^2 = \frac{1}{d}, \forall j, k \in \{0, ..., d-1\}\,. \tag{3}$$

A discrete Fourier transform can be used to find a base which is mutually unbiased to the previous one [4]:

$$|e_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} exp(\frac{i2\pi}{d}.j.k)|f_k\rangle \tag{4}$$

To find out a mutually unbiased base to the set $\{|0\rangle, |1\rangle\}$,where $|0\rangle = |f_0\rangle$, $|1\rangle = |f_1\rangle$ and $d = 2$, equation 4 is used and the base $\{|+\rangle, |-\rangle\}$ is obtained where

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{5}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{6}$$

For the case of a BB84 protocol with the set of bases $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the expected density matrix is presented below is commonly shown as in figure 1. This is the theoretic crosstalk matrix

$$\begin{pmatrix} |\langle -|0\rangle|^2 & |\langle -|1\rangle|^2 & |\langle -|+\rangle|^2 & |\langle -|-\rangle|^2 \\ |\langle +|0\rangle|^2 & |\langle +|1\rangle|^2 & |\langle +|+\rangle|^2 & |\langle +|-\rangle|^2 \\ |\langle 1|0\rangle|^2 & |\langle 1|1\rangle|^2 & |\langle 1|+\rangle|^2 & |\langle 1|-\rangle|^2 \\ |\langle 0|0\rangle|^2 & |\langle 0|1\rangle|^2 & |\langle 0|+\rangle|^2 & |\langle 0|-\rangle|^2 \end{pmatrix}$$

for a BB84 protocol with two ($d = 2$) mutually unbiased bases. A possible implementation with two mutually unbiased bases is using light's polarization as the qubit. Here the $|0\rangle$ would be a photon horizontally polarized or the quantum state $|H\rangle$, $|1\rangle$ the vertical direction or $|V\rangle$, $|+\rangle$ the diagonal direction $|\nearrow\rangle$ and $|-\rangle$ the anti-diagonal direction $|\searrow\rangle$. A qubit has the logical value "0" if the quantum states are $|H\rangle$ or $|\nearrow\rangle$ and has the logical value "1" in the quantum states $|V\rangle$ or $|\searrow\rangle$.

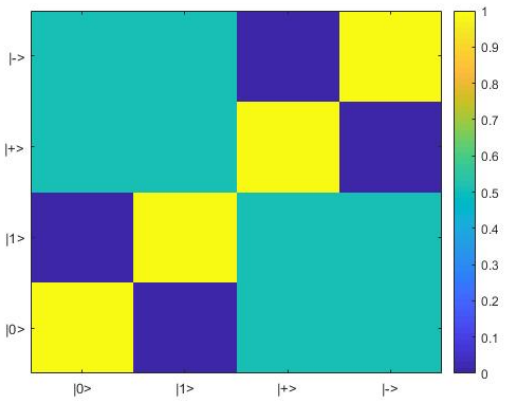

Figure 1: Left Side: Graphical representation of the theoretical crosstalk matrix for an ideal BB84 QKD system with d=2. Right Side: Probability values or magnitude of the inner product between the quantum states.

2.3. Beam Optics

The Gaussian beam is one of the most important solutions to the Helmholtz equation. The optical beam where the OAM will be induced has its characteristics. Light carrying OAM is named the Laguerre-Gaussian beam and its modes are commonly used for optical communications. The Gaussian beam is characterized by three parameters: beam's waist, radius of curvature and phase retardation, presented in equations 7, 8 and 9 where the beam waist at its focus, W_0, is defined by the relation 10 which are functions of z and z_0, the Rayleigh range.

$$W(z) = W_0\sqrt{1+\left(\frac{z}{z_0}\right)^2} \tag{7}$$

$$R(z) = z\left[1+\left(\frac{z_0}{z}\right)^2\right] \tag{8}$$

$$\zeta(z) = \tan^{-1}\frac{z}{z_0} \tag{9}$$

$$W_0 = \sqrt{\frac{\lambda z_0}{\pi}} \tag{10}$$

Another solution to the paraxial Helmholtz equation is the Laguerre-Gaussian beams. This solution comes from writing the paraxial Helmholtz equation in cylindrical coordinates (ρ, ϕ, z) and using the separation of variables technique in ρ and ϕ. The complex amplitude of the Laguerre-Gaussian beam

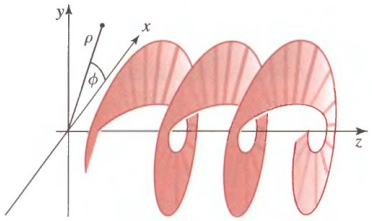

Figure 2: Laguerre-Gaussian beam wavefront [5]

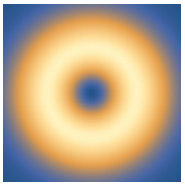

Figure 3: Light carrying OAM Intensity pattern

is written as

$$U_{l,m}(\rho,\phi,z) = A_{l,m}\left[\frac{W_0}{W(z)}\right]\left(\frac{\rho}{W(z)}\right)^l \mathbb{L}_m^l\left(\frac{2\rho^2}{W^2(z)}\right)\exp\left(-\frac{\rho^2}{W^2(z)}\right) \times \exp\left[-jkz - jk\frac{\rho^2}{2R(z)} - jl\phi + j(l+2m+1)\zeta(z)\right] \tag{11}$$

where $\mathbb{L}_m^l(x)$ is the Laguerre polynomial function (In some works l is defined as m and m as p).

$$\mathbb{L}_m^l(x) = \frac{x^{-l}e^x}{m!}\frac{d^m}{dx^m}\frac{x^{l+m}}{e^x}. \tag{12}$$

The intensity pattern of the Laguerre-Gaussian beam only depends on ρ and z so it's circularly symmetric. In the case of $l \neq 0$ the beam carries an orbital angular momentum which translates into intensity pattern with a zero intensity at the center ($\rho = 0$) and a maximum intensity pattern circular shaped as in figure 3. The phase's beam has the same dependence on ρ and z as the Gaussian beam but with an additional linear dependence on the azimuthal angle ϕ. The dependence tilts helically the wavefront along the z direction as seen in figure 2.

2.4. Fourier Optics

Fourier optics describe the propagation of light waves based on harmonic analysis, more commonly known as Fourier transform which can be used to relate spatial coordinates and spatial frequencies. A complex function $f(x, y)$ with x and y representing the spatial coordinates in a plane can be written as a sum of harmonic functions of x and y with the form $\mathcal{F}(v_x, v_y)exp(-j2\pi(v_x x + v_y y))$ with $\mathcal{F}(v_x, v_y)$ being the complex amplitude and v_x and v_y the spatial frequencies. The relation between the spatial

and the spatial frequency domain is written as

$$\mathcal{F}(v_x, v_y) = \iint_{-\infty}^{+\infty} U(x,y) exp(-2\pi i(v_x x + v_y y)) dxdy \quad (13)$$

One of its most useful results is the Fresnel Diffraction Approximation which is a valid approximation under the Fresnel regime which is applied to the propagation of waves in the near field. This near field is specified by the Fresnel number F given by $F = \frac{a^2}{L\lambda}$ where a is the size of the aperture that in our case is the laser source aperture, L the distance between the laser aperture and the plane where the light is projected and λ the wavelength. When $F > 1$ the diffracted wave is considered to be in the near field and the Fresnel Diffraction Approximation presented in equation 15 can be used. This result can be interpreted as a convolution in which the wave function, $U^{in}(x_A, y_A)$, shape is modified by $h(x,y)$, the Fresnel Diffraction Impulse and it is an accurate approximation to small diffraction angles.

$$h(x,y) = \frac{exp(ikz)}{i\lambda z} exp[\frac{ik}{2z}(x^2 + y^2)] \quad (14)$$

$$U^{out}(x_B, y_B) =$$

$$\iint_{-\infty}^{+\infty} U^{in}(x_A, y_A).h(x_B - x_A, y_B - y_A) dx_A dy_B = \mathrm{U}^{in}(x_A, y_A) * h(x_A, y_A) \quad (15)$$

2.5. Spontaneous Parametric Down-Conversion

Quantum optics experiments use entangled photon pairs, which usually are created in a nonlinear crystal by a process named spontaneous parametric-down-conversion (SPDC), an optical nonlinear effect. SPDC-based systems have been exploited as a basis for entangled-photons schemes. Entanglement between these photons can be achieved by exploiting temporal [6], spectral [7] , polarization [8], linear momentum [9] and OAM [10] degrees of freedom although SPDC can also be used in the implementation of probabilistic heralded single-photon sources.

It is often explained as a quantum-mechanical decay process, in which the incident photons traveling through an optically nonlinear crystal create, probabilistically, pairs of lower-energy photons. Since the signal and the idler are generated in pairs, the detection of one of them implies the presence of the other. Idler and signal photons are radiated within two distinct cones tangent or partially overlapped as in figure 9. The incident optical field is the pump beam (pulsed or continuous) and the other two are the signal and idler beams. In this process, the incident light, with frequency w_{pump}, interacts with matter in such a way that as to leave the quantum state of the material unchanged. As a consequence, there can be no transfer of energy, momentum, or angular momentum between the optical field and the physical system. Energy is conserved (i.e. frequency-matching condition (equation 16)) among the incident photons.

$$w_{pump} = w_{idler} + w_{signal} \quad (16)$$

The emission efficiency is the highest when the fields are coherent over the full length of the crystal and the phase-matching condition (equation 17) between the three wave vectors is satisfied where $k_\alpha = n_\alpha k_0 = n_\alpha \frac{w_\alpha}{c_0}$ with $\alpha = pump, signal, idler$, w_α is the beam's frequency and n_α the wavelength refraction index of the nonlinear crystal. This means that a good phase correlation between the interacting waves is preserved along the propagation direction where for maximum conversion efficiency, $\Delta\vec{k} = 0$.

$$\vec{k}_{pump} = \vec{k}_{idler} + \vec{k}_{signal} + \Delta\vec{k} = 0 \quad (17)$$

3. Implementation

Implementing a BB84 QKD protocol using light's OAM [11] with a low cost solution requires to explore if this solution efficiently induces and nullifies an OAM mode. This issue will be addressed by simulating the OAM modulation setup in MATLAB R2018b and tracking the light's phase and intensity wave front profiles through out the simulation to obtain the implentation's quantum tomography. The computational aspects are presented in the 3.1 and the experimental setup is presented in 3.2. In 3.3 the spontaneous parametric down-conversion process is presented.

3.1. Computational Simulations

In this section, are presented methods are presented necessary to validate the experimental observations. The simulation generates two outputs. The first output is how the beam's intensity and phase profiles evolve through space after being modulated by a phase mask displayed on a SLM. The second output or the validation result is the cross-talk matrix between the several modulated and demodulated OAM modes which is the attempt to simulate the whole setup to verify if the experimental setup can be integrated into a BB84 protocol. The first step of this process is to generate a beam with an intensity profile described by a Gaussian distribution. The mask pattern is the phase component and it is multiplied by the intensity field profile as in equation 18.

$$U^{in}(x_1, y_1) = GuassianBeam_{IntensityProfile} \cdot e^{i.SLMPhaseMaskProfile} \quad (18)$$

In the next step the Matlab bi-dimensional fast Fourier function, fft2, is applied to the input field, $U^{in}(x_1, y_1)$, as in equation 15 and its multiplied by

the Fourier transform of h, the Fresnel diffraction approximation impulse. Equations 15 and 14 are simplified using the Fourier convolution theorem as shown in equation 19, where $H(f_x, f_y)$ is the Fourier transform of $h(x_1, y_1)$ as shown is equation 20. The propagated field, at a distance $z01$, is obtained by the Matlab's inverse fast Fourier transform algorithm ifft2 of the convolution as in the equation 19.

$$U^{out}(x_B, y_B) = \mathcal{F}^{-1}\left\{\mathcal{F}\left\{U^{in}(x_A, y_A)\right\}.H(f_{xA}, f_{yA})\right\} \tag{19}$$

$$H(f_{xA}, f_{yA}) = exp(ikz).exp[-i\pi\lambda z(f_{x_A}^2 + f_{y_A}^2)] \tag{20}$$

The procedure is then repeated to calculate the effect of a second modulation, by another SLM, on the light's intensity and phase wave front patterns after being propagated by a distance of $z02$. A simulation for a modulation with a $l = 8$ spiral mask for a 0.6π and 2π phase-shift SLM is presented in figure 4. A small efficiency fails to create a pure ring and instead points of maximum intensity spawn around the center of the image. It seems that a SLM with this limitation fails to fully create a OAM mode leaving an unmodulated component in the center but as the phase shift capacity increases, the intensity pattern acquires the shape of a ring. Looking at the phase patterns when the propagation distance exceeds the Rayleigh range, $z_0 = 794\ mm$, the radius of curvature increases, a spiral pattern starts to appear at the center of the phase wave-front and a ripple effect starts to appear in intensity pattern. These results are similar to the ones obtained in the articles [12], [13] and [14] using also the angular spectrum propagation method with the Fresnel approximation.

In the demodulation simulation, masks with symmetrical topological charges are displayed in each SLM and the demodulation results are shown in figure 5. The expected result is the recovery of the initial Gaussian beam when phase masks with symmetrical l values are displayed on each SLM. With a 2π phase retardation for a distance $z01 = 10\ mm$ the original beam is recovered as expected but for $z01 = 100\ mm$ and $z01 = 1000\ mm$ the ring shape reappears. The field size increases with increasing the propagation distance and in this case the beam waist becomes to large, compared to the physical phase mask display to be affected by it, and in this situation, the second SLM just acts as a modulator to an unmodulated component from a poor modulated beam by a SLM with a small phase retardation. For an phase retardation of 0.6π this effect originates an intensity pattern as if the beam was being modulated and not the inverse. Lowering the efficiency also makes us observe a Gaussian beam after demodulation at $z01 = 10\ mm$ (figure 5-Down Left) but that is because the beam is never fully modulated by the first SLM so there's no OAM mode to demodulate. This results are not enough to conclude if the system can be implemented with our technical constrains but necessary to simulate the crosstalk matrices.

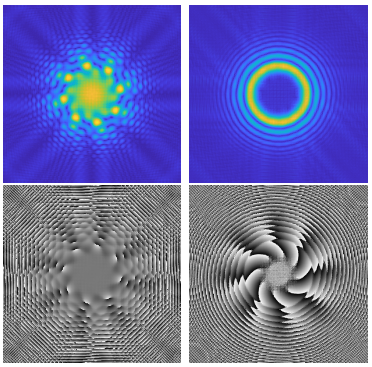

Figure 4: OAM Modulation with topological Charge $l = 8$ with $z01 = z02 = 1000\ mm$. Up Left: 0.6π Modulation Intensity Pattern. Down Left: 0.6π Modulation Phase Pattern. Up Right: 2π Modulation Intensity Pattern. Down Right: 2π Modulation Phase Pattern

The crosstalk matrix values are obtained by integrating the product of the intensity pattern, after being modulated by a spiral mask with topological value n and demodulated by one with topological value m, by a filter matrix that acts like an aperture. If a 5-pixel aperture is chosen then only the matrix values around the center within a 5-pixel range will count to the integration. Using a 5-pixel aperture value translates into using an aperture with a radius of, approximately, 1.8% of the beam waist $w(z)$, which results on a crosstalk matrix as in figure 7-Left. Increasing the aperture size to 18% (50 pixels), will reduce the gap between the intensity measured with masks with symmetrical topological charges and all the other combinations, which results on a crosstalk matrix as in figure 7-Right.

3.2. Experimental Implementation

The SLM used in this work is a Liquid Crystalon Silicon Twisted Nematic Spatial Light Modulator SDE1024 by Cambridge Correlators. At 633 nm a 0.6π phase delay its achievable when using a 2π phase mask display. An important issue to be analysed is that if this phase delay is enough to create a set of basis to use in a BB84 protocol. Two setups were implemented. One to modulate the incident beam and another to demodulate the incident beam. The setups are very similar and are shown in figure 8. In both cases, a 633 nm signal wavelength Uniphase 1125 HeNe laser, with a 5 mW optical power and a 1.2 mm beam diameter, it's used.

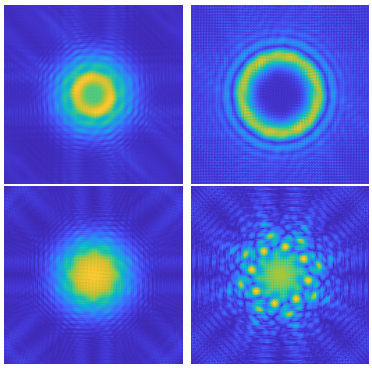

Figure 5: OAM Modulation with topological charge $l = 8$ with $z02 = 1000\ mm$. Up Left: 2π Phase-Shit Intensity Pattern at $z01 = 10\ mm$. Up Right: 2π Phase-Shit Intensity Pattern at $z01 = 1000\ mm$. Down Left: 0.6π Phase-Shit Intensity Pattern at $z01 = 10\ mm$. Down Right: 0.6π Phase-Shit Intensity Pattern at $z01 = 1000\ mm$.

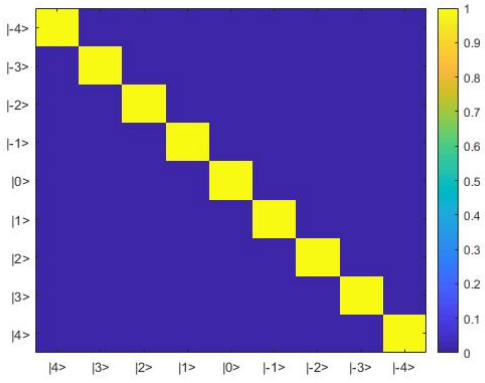

Figure 6: Graphical representation of the theoretical crosstalk matrix for an ideal BB84 QKD system with d=1. Probability values or magnitude of the inner product between the quantum states are described by the color scale inserted in the right side.

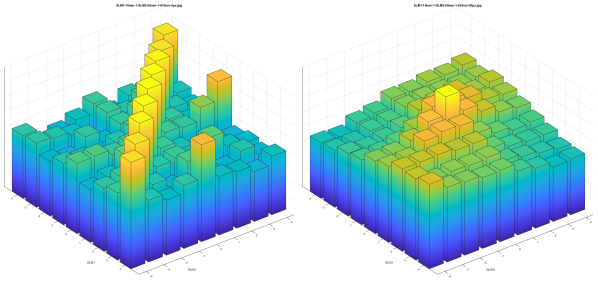

Figure 7: Left: CrossTalk Matrix SLM1-2π z01=10 mm SLM2-2π z02=50 mm Aperture-5 Pixels. Right:CrossTalk Matrix SLM1-2π z01=10 mm SLM2-2π z02=50 mm Aperture-50 Pixels

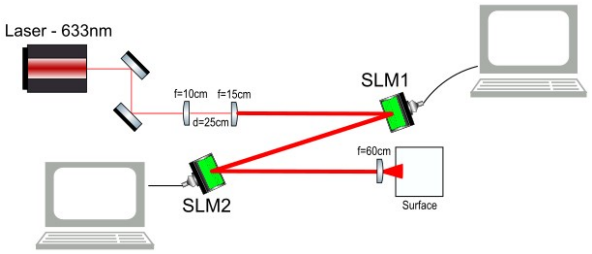

Figure 8: OAM Modulation setup with one SLM and Demodulation setup with two SLMs.

3.3. Noncollinear spontaneous parametric down-conversion

The crystal employed is birefringent i.e. the material has a refractive index that depends on the light's polarization and propagation direction. For most of birefringent crystals the refraction index depends on the angle of propagation with the crystal axes [15]. A wave orthogonally polarized to the crystal optical axis is named ordinary wave and one parallel is named extraordinary wave. A ordinary wave will sense a refraction index, n_o, different from a extraordinary wave, n_e. In our case the crystal generates a type 1 SPDC and to achieve the ideal phase matching the highest frequency wave is polarized parallel to the direction with the lowest refractive index [5], which is n_e and illustrated in figure 9. In figure 9 we can see that the signal beam and idler beam are generated as ordinary waves which are always perpendicular to the optical axis. This means that their refractive index, n_0 is independent of θ and only depends of w. The same can't be said about the pump beam. It is polarized to be an extraordinary wave which makes its refractive index n_e dependent of θ and w. The second characteristic of SPDC is that $w_{signal} = w_{idler} = w$, which allows to write, with equation 16, the relation

$$\begin{aligned} n_3.w_{pump} &= n_1.w_{idler} + n_2.w_{signal} \Leftrightarrow \\ n_e(\theta, 2w).2w &= n_o(w).w + n_o(w).w \Leftrightarrow \\ n_e(\theta, 2w) &= n_o(w) \end{aligned}$$

which means that the phase match is obtained by rotating the crystal over the plane $x0y$ to find the ideal θ whose value makes the refractive index of the pump beam, $n_e(\theta, \lambda = 405\ nm)$ the same as the refractive index of the signal and idler beams, $n_o(\lambda = 810\ nm)$, and when this condition is met, $\Delta\vec{k} = 0$. Regarding the direction of the generated photons, the phase-matching conditions can be tuned so that the signal and idler photons wave vectors point away from the direction of the pump vector with a angle δ. In that case the process is named noncollinear SPDC. Non-collinear downconversion allows us to spatially filter the pump from the generated modes without any additional optical

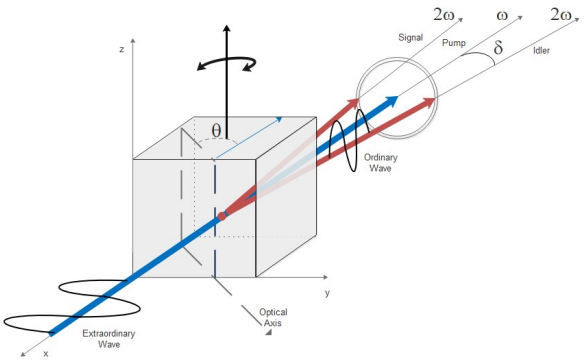

Figure 9: Spontaneous Parametric Down Conversion Type 1

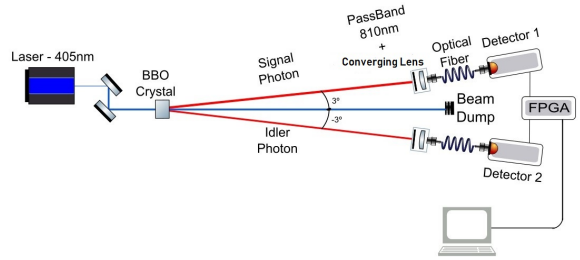

Figure 10: Schematic SPDC Implementation Setup

components. To implement the SPDC process, as in figure 10, a BBO crystal supplied by Newlight Photonics was used. The half opening angle δ between the signal/idler and pump beam is around 3º; the angle between the crystal surface and it's optical axis is $\theta = 29.3$º; the parametric down-conversion requires a pump beam with a $\lambda = 405\ nm$ and generates photon pairs with $\lambda = 810\ nm$; its dimensions are $5 \times 5 \times 3\ mm^3$.

4. Results

4.1. Modulation and Demodulation Patterns

Four modulation patterns were registered in figure 11, where the simulated patterns are also presented. The experimental results are in agreement with the simulated patterns but once again, it's necessary to find balance between modulation efficiency and light intensity. Using a film polarizer increases the modulation efficiency but will attenuate the beam's intensity. Not using a film polarizer allows the light, perpendicular to the largest SLM display side, to be reflected poorly modulated, which is considered noise or unwanted reflectivity. In figure 12 the difference is quite clear in the intensity pattern.

The demodulation follows the setup in figure 8-Bottom and the expected result would be the recovery of the Gaussian beam previously modulated although with this set up a new problem appears. The incident beam in the first SLM is divided in several overlapped components. The first reflection order light from the first SLM is divided in two parts: the partial modulated component seen as the points of light around the center of the intensity pattern and the unmodulated component, result of the SLM's reflectivity, seen as the Gaussian beam in the center of the intensity pattern. The second SLM will affect each component. The modulated component will be partially demodulated which results in a Gaussian beam and in a partial undemodulated component seen as a less intense set of points around the center. The unmodulated component will be divided as the incident beam was divided on the first SLM: a partial modulated component and a reflected unmodulated component. Part of the unmodulated reflected light from the first SLM, due to reflectivity, will now be modulated by the second SLM and reflected again unmodulated. The final projection will have these five components overlapped but their relative intensities are not the same for all the components. The components due to reflectivity have much less intensity and with an adequate CMOS camera these relative intensities can be measured. It is possible, at eyesight, to observe some demodulation of the initial modulated component and in figure 13 the result of demodulating an OAM with $l = 8$ is presented. Cunha [16] confirms that result using a FWS CCD to evaluate the front wave intensity pattern after the demodulation attempt.

Due to lack of appropriate optical and measurement equipment at the time of this work the experimental quantum tomography process, to evaluate if the system was capable of being implemented in a BB84 protocol, was not performed and by so, only the simulation results will be discussed. A viable setup to be used in a quantum communication protocol would have a crosstalk matrix similar to the one in figure 7-Left which is similar to crosstalk matrices from successful setups like [17] and [18]. In these crosstalk matrices, the bars represent the light's intensity measured by an aperture after the demodulation. As expected, when phase masks with symmetrical topological charges are used the beam is correctly demodulated and any other phase mask combination does not totally recover the Gaussian beam pattern as it can be observed also in figure 7-Left. For larger distances the second SLM will just act as another modulator, makes the demodulation inefficient. After an extensive inspection, simulating the system by changing the distances and apertures within a large range of values, the conclusion is that it isn't possible to mount a setup capable of produce results like the ones in 7-Left. The SLM simply can't modulate and demodulate the beam to a point where only using symmetrical phase masks the Gaussian beam is totally recovered. Testing all the logical parameter

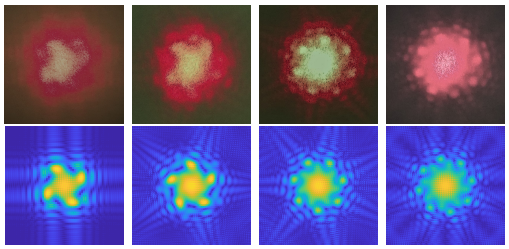

Figure 11: Intensity Patterns Observed and Simulated for $z01 = 2000\ mm$

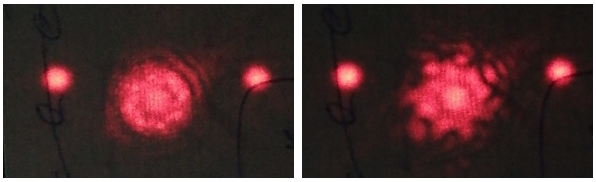

Figure 12: Pattern intensity of Perpendicular: Left and Parallel: Right polarized light with the SLM's longest side.

values with a maximum phase delay of 0.6π results in an almost homogeneous pattern, as is shown in figure 7-Right, which is not the intended pattern. Only with a 2π phase delay it is possible to tune the parameters to obtain a configuration suitable to a BB84 protocol.

4.2. Noncollinear spontaneous parametric down-conversion Implementation

Only one beam was spatially detected with $60000 \sim 80000 \pm 2000$ so it was registered how the counts changed with several parameters. Changing the pump intensity between 5 mW and 20 mW did not change the number of counts as explained in [19]. Tilting the crystal by changing the angle θ to 29.05 ± 0.15^{o}, as in figure 9, made the number of counts drop to $4000 \sim 7000$ due to the crystal no longer being under the phase-matching conditions. Slightly moving the lens system support, about 1 mm, orthogonally to the single photons path or rotating the threaded kinematic mount screws by one revolution made the counts drop to background noise values.

It was estimated that the single photons horizontal beam width was around 0.1 mm near the crystal.

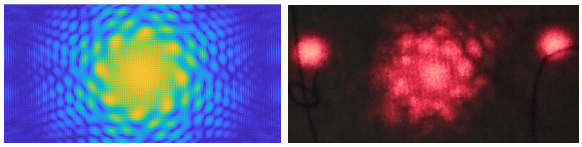

Figure 13: Demodulation with spiral phase $l = 8$ on the first SLM and $l = -8$ on the second SLM. Left: Simulation Result. Right: Experiment Result.

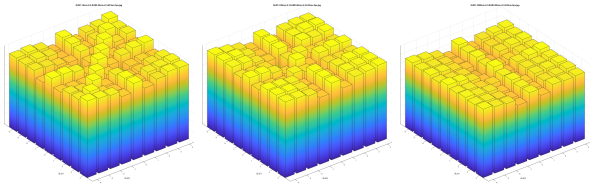

Figure 14: Cross-Talk Matrices with a 0.6π phase shift capacity, z02=50 mm and Left: z01=10 mm, Middle: z01=100 mm, Right: z01=1000 mm

This value was obtained by suspending a 0.1 mm thick cotton thread between the crystal and the detector but very close to the first crystal. It was observed that the counts lowered to values around 10000 cps. The same test was made near the lens system and the values measured were around 40000 cps although it can't be concluded that the waist increases with the propagation distance due to the cotton thread not blocking as many single photons as it did near the crystal. This difference in the number of counts can be due to a diffraction effect created by the cotton thread. The beam width value is just indicative but is in accordance with the literature. Gabriel Molina-Terriza in [20] using a 25 mW 405 nm pump beam with a 0.5 mm waist, scanned the idler beam along two different orthogonal directions. In the x transverse dimension the beam spatial shape is described having a Gaussian shape with a beam width $w_x = 0.120\ mm$ and $w_y = 0.180\ mm$. A film polarizer, vertically oriented, was placed in the single photons path and the counts lowered to around 50000 cps but rotating the film polarizer by 90°, to only allow horizontal polarized light pass by, lowered the counts to 30000 cps. On one hand is an expected result because the single photons are generated vertically polarized but by the other hand the counts with the film polarizer perpendicular to the light's polarization are not as low as expected, which would be around background noise values. The last parameter measured was the deflection angle between the pump beam and the photon source which was around 2.8°. This value was also measured with a ruler with a minimum scale of 1 mm so it is just an indicative value.

Further work is required to detect the second single photon beam although it is important to show how the setup would be integrated in the BB84 QKD protocol shown in figure 15. For the case of the BB84 protocol with light's polarization, the set of bases $\{|H\rangle, |V\rangle, |+\rangle, |-\rangle\}$ is used, which corresponds to use the light's horizontal, vertical, diagonal and anti-diagonal polarization as the qubit. The logic value "0" corresponds to photon be prepared in the states $|H\rangle$ or $|\nearrow\rangle$ and the logic value

"1" to the states $|V\rangle$ or $|\searrow\rangle$. In this setup, the detection of the beam identified as "signal photon" is used to identify when the idler photon is created. Only simultaneous detections within a time interval, commonly named coincidences, in detector 1 and detector 2 or 3 will be considered as it is the away to be sure that what Bob is detecting is for sure the idler photon. The idler photon is always generated in the $|V\rangle$ state and when it is reflected by two mirrors it maintains that state. Alice controls an optical device capable of shifting the polarization direction of linearly polarized light. With it, Alice prepares the idler photon in one of the 2 bases. Bob also has an half-wave plate, so he decides on which base he detects the photon. Let's suppose that Alice and Bob use the same base. Alice sends the photon in the state $|H\rangle$ and Bob sets the half-wave plate so that incoming horizontally polarized photons do not suffer any polarization direction shift. The photons will pass by the half-wave plate and will pass by a polarizing beam splitter. A polarizing beam splitter divides incident unpolarized light into two orthogonally polarized beams. In our case, the beam splitter is mounted to divide light into $|V\rangle$ and $|H\rangle$ states. The horizontal component is transmitted to the detector 2 and the vertical component is reflected to the detector 3. So for the case of a qubit prepared in the $|H\rangle$ state and observed with the $\{|H\rangle, |V\rangle\}$ basis set, it is certain that Bob will detect the photon in detector 2. In the end, Alice and Bob communicate classically to know what bases each one used to prepare and measure the idler photon. If the bases were the same then Bob knows that the measure done is correct. For the case of different bases, if Alice sends the $|H\rangle$ state and Bob uses the wrong base, the photon state, after the half-wave plate will be in the base $\{|\nearrow\rangle, |\searrow\rangle\}$. When the photon hits the beam splitter, there will be a 50% probability of being transmitted and other 50% of being transmitted. Bob, in this case, must discard this measurement because the chance of the value being correct is 50%. Physically, because the beam splitter works differently for horizontal and vertical polarizations, when the photon polarization is a linear combination of these two polarizations, the beam splitter observes the photon polarization and collapses the photon to into one of the states $\{|H\rangle, |V\rangle\}$. From a vectorial point of view, a vector $\overrightarrow{D}$ is the sum of an horizontal vector $\overrightarrow{H}$ with a vertical vector $\overrightarrow{V}$ where $|\overrightarrow{H}| = |\overrightarrow{D}|Cos(\theta)$ and $|\overrightarrow{V}| = |\overrightarrow{D}|Sin(\theta)$. So when a photon with a polarization orientation $|\overrightarrow{D}|$ passes through a beam splitter, prepared to separate a beam horizontal $|\overrightarrow{H}|$ and vertical $|\overrightarrow{V}|$ polarization components, it will be observed and will collapse into a horizontal polarization state $|H\rangle$ with a $Cos^2(\theta)$ probability or into a vertical polarization state $|V\rangle$ with a $Sin^2(\theta)$ probability.

The goal was to characterize this system and understand how it could be optimized so that its crosstalk matrix would be as similar as possible to theoretic one. A true implementation would not be possible because the half-wave plates are prepared mechanically, which means each state would take around 5 seconds to prepare. This corresponds to have a QKD rate of 0.2 b/s. Electro-optic devices, with a very low response time, capable of manipulating the light's polarization can achieve high QKD rates and are capable of delivering sustainable, real-time secure keys continuously at rates exceeding 10 Mb/s [21].

5. Conclusions

Two BB84 QKD protocol implementation solutions and their technical challenges were explored. A solution aimed to employ light's OAM as the qubit. Experiments were performed displaying spiral patterns into two SLMs to generate and manipulate light's OAM. Computational simulations were made to validate the experimental results using Fourier optics theory and to obtain the implemented protocol crosstalk matrix by tomographic reconstruction. By simulating the light's intensity patterns modulated by spiral mask patterns displayed on the SLM and simulating the protocol crosstalk matrix, it was shown that a device with a minimum of 2π phase retardation is required to generate and manipulate a photon carrying OAM capable of being employed as a qubit in this quantum protocol implementation.

The other solution aimed to employ light's polarization as the qubit, by the use of optical elements to manipulate polarized light. In both solutions a single photon generation process was required and a spontaneous parametric down-conversion source was used. The SPDC was not fully assembled and it was not possible to implement the protocol with polarized light. Implementing the SPDC process in a dark room with no light sources and using an Electron Multiplying CCD camera would have made possible to correctly generate, detect and image the single photons. From here two possible works can be developed. An OAM BB84 protocol with a suitable SLM and a phase-sensor camera (CMOS SPAD) to obtain much more solid experimental measurements. The other work is to implement the BB84 protocol at long distances or via underwater. Several challenges related to turbulence would need to be addressed but it is the natural step in the development of a free-space communication system.

Acknowledgements

The author would like to thank Instituto de Telecomunicações (IT) and Instituto Superior de Engenharia de Lisboa (ISEL) for providing the equipment and the installations for this work.

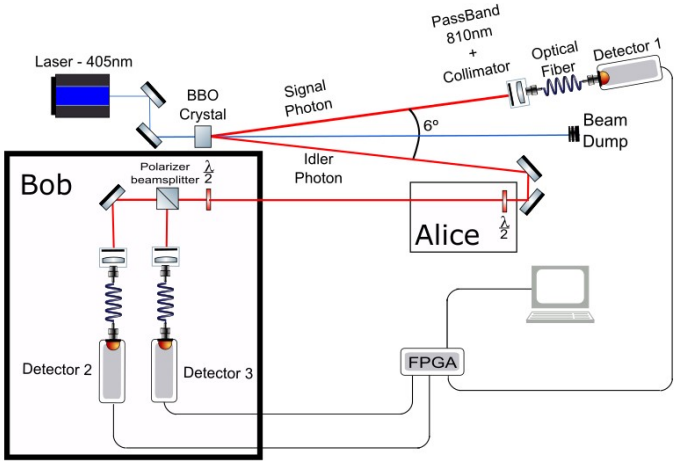

Figure 15: Schematic of BB84 QKD Protocol Setup

References

[1] F. Jazaeri, A. Beckers, A. Tajalli, and J.-M. Sallese. A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics. *arXiv e-prints*, 2019.

[2] A. Shenoy H., A. Pathak, and R. Srikanth. Quantum cryptography: key distribution and beyond. *arXiv e-prints*, 2018.

[3] Ingemar Bengtsson. Three Ways to Look at Mutually Unbiased Bases. 2007.

[4] Vincenzo D'Ambrosio, Filippo Cardano, Ebrahim Karimi, Eleonora Nagali, Enrico Santamato, Lorenzo Marrucci, and Fabio Sciarrino. Test of mutually unbiased bases for six-dimensional photonic quantum systems. *Scientific reports*, 2013.

[5] Bahaa E A Saleh and Malvin Carl Teich. *Fundamentals of photonics; 2nd ed.* Wiley, 2007.

[6] Kutlu Kutluer, Emanuele Distante, Bernardo Casabone, Stefano Duranti, M Mazzera, and Hugues de Riedmatten. Time entanglement between a photon and a spin wave in a multimode solid-state quantum memory. 2019.

[7] C K. Law, Ian Walmsley, and J H. Eberly. Continuous frequency entanglement: Effective finite hilbert space and entropy control. *Physical review letters*, 2000.

[8] T E. Kiess, Yanhua Shih, Alexander Sergienko, and C O. Alley. Einstein-podolsky-rosen-bohm experiment using pairs of light quanta produced by type-ii parametric down-conversion. 1994.

[9] John C Howell, Ryan Bennink, Sean Bentley, and Robert Boyd. Realization of the einstein-podolsky-rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion. *Physical review letters*, 2004.

[10] Jonathan Leach, Barry Jack, Jacquiline Romero, Anand Jha, Alison Yao, Sonja Franke-Arnold, David Ireland, Robert Boyd, Stephen M Barnett, and Miles Padgett. Quantum correlations in optical angle-orbital angular momentum variables. *Science (New York, N.Y.)*, 2010.

[11] G Bennett, Charles H. Brassard. Proceedings of ieee international conference on computers, systems and signal processing, pp. 175-179. 1984.

[12] Zhang Gongjian, Zhang Man, and Zhao Yang. Wave front control with slm and simulation of light wave diffraction. *Opt. Express*, 2018.

[13] Doohwan Lee, Hirofumi Sasaki, Hiroyuki Fukumoto, Yasunori Yagi, and Takashi Shimizu. An evaluation of orbital angular momentum multiplexing technology. *Applied Sciences*, 2019.

[14] Xiaohang Dong, Hengyi Sun, Zhuo Li, Xinlei Chen, and Baijie Xu. Generation of ultra-wideband multi-mode vortex waves based on monolayer reflective metasurface. *Progress In Electromagnetics Research M*, 2019.

[15] D. A. Kleinman. Nonlinear dielectric polarization in optical media. *Phys. Rev.*, 1962.

[16] André Madeira Bastos da Cunha. Study of photons orbital angular momentum for optical communications. Master's thesis, Instituto Superior Técnico, 2015.

[17] Frédéric Bouchard, Khabat Heshami, Duncan England, Robert Fickler, Robert W. Boyd, Berthold-Georg Englert, Luis L. Sánchez-Soto, and Ebrahim Karimi. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum*, 2018.

[18] Frédéric Bouchard, Alicia Sit, Felix Hufnagel, Aazad Abbas, Yingwen Zhang, Khabat Heshami, Robert Fickler, Christoph Marquardt, Gerd Leuchs, Robert w. Boyd, and Ebrahim Karimi. Quantum cryptography with twisted photons through an outdoor underwater channel. *Opt. Express*, 2018.

[19] Ryan S. Bennink, Yun Liu, D. Duncan Earl, and Warren P. Grice. Spatial distinguishability of photons produced by spontaneous parametric down-conversion with a focused pump. 2006.

[20] Gabriel Molina-Terriza, Stefano Minardi, Yana Deyanova, Clara Osorio, Martin Hendrych, and Juan Torres. Control of the shape of the spatial mode function of photons generated in noncollinear spontaneous parametric down-conversion. *Phys. Rev. A*, 2005.

[21] Zhiliang Yuan, Alan Plews, Ririka Takahashi, Kazuaki Doi, Winci Tam, Andrew Sharpe, Alexand er Dixon, Evan Lavelle, James Dynes, Akira Murakami, Mamko Kujiraoka, Marco Lucamarini, Yoshimichi Tanizawa, Hideaki Sato, and Andrew J. Shields. 10-Mb/s Quantum Key Distribution. 2018.