Engineering Quantum Communication Systems

Armando N. Pinto[a,c], Álvaro J. Almeida[b,c], Nuno A. Silva[a,c], Nelson J. Muga[a,c] and Luís M. Martins[b,c]

[a]Department of Electronics, Telecommunications and Informatics, University of Aveiro, 3810-193 Aveiro, Portugal
[b]Department of Physics, University of Aveiro, 3810-193 Aveiro, Portugal
[c]Instituto de Telecomunicações, 3810-193 Aveiro, Portugal

ABSTRACT

Quantum communications can provide almost perfect security through the use of quantum laws to detect any possible leak of information. We discuss critical issues in the implementation of quantum communication systems over installed optical fibers. We use stimulated four-wave mixing to generate single photons inside optical fibers, and by tuning the separation between the pump and the signal we adjust the average number of photons per pulse. We report measurements of the source statistics and show that it goes from a thermal to Poisson distribution with the increase of the pump power. We generate entangled photons pairs through spontaneous four-wave mixing. We report results for different type of fibers to approach the maximum value of the Bell inequality. We model the impact of polarization rotation, attenuation and Raman scattering and present optimum configurations to increase the degree of entanglement. We encode information in the photons polarization and assess the use of wavelength and time division multiplexing based control systems to compensate for the random rotation of the polarization during transmission. We show that time division multiplexing systems provide a more robust solution considering the values of PMD of nowadays installed fibers. We evaluate the impact on the quantum channel of co-propagating classical channels, and present guidelines for adding quantum channels to installed WDM optical communication systems without strongly penalizing the performance of the quantum channel. We discuss the process of retrieving information from the photons polarization. We identify the major impairments that limit the speed and distance of the quantum channel. Finally, we model theoretically the QBER and present results of an experimental performance assessment of the system quality through QBER measurements.

Keywords: Quantum Communications, Four-Wave Mixing, Raman Scattering, Single-Photon Source, Photon Statistics, Polarization-Entangled Photon Source, Quantum Bit Error Rate

1. INTRODUCTION

The rapid expansion of the Internet traffic over optical fibers has given rise to a need of secure communication systems. Quantum communications, mainly quantum key distribution (QKD), appears as a natural solution for guarantee perfect security between users of a communication system.[1] The security of these quantum communication systems is based on physical laws, rather than the supposed difficulty of computing certain mathematical problems.[1] In this context, the generation of single and entangled photon pairs already inside optical fibers appears as an important topic for QKD. The four-wave mixing (FWM) process provides a natural solution to create single or entangled photons inside an optical fiber,[2,3] that can be used for implementation of in-fiber QKD systems.

Nowadays the QKD systems have evolved from point-to-point links to optical fiber networks, in a typically wavelength division multiplexing (WDM) architecture.[4] In that scenario, the quantum channel used for QKD

Further author information: (Send correspondence to Armando N. Pinto)
Armando N. Pinto: E-mail: anp@ua.pt; Telephone: +351 234 377 900
Álvaro J. Almeida: E-mail: aalmeida@av.it.pt; Telephone: +351 234 377 900
Nuno A. Silva: E-mail: nasilva@av.it..pt; Telephone: +351 234 377 900
Nelson J. Muga: E-mail: muga@av.it.pt; Telephone: +351 234 377 900
Luís M. Martins: E-mail: lmartins@av.it.pt; Telephone: +351 234 377 900

shares the same optical fiber with several classical optical signals. However, the inter-channel nonlinear effects can potentially degrade the performance of the QKD system, due to the fact that the interactions between the classical signals and the optical fiber will generate in-band noise photons.[4] The knowledge of the impact of those noise photons on the quantum channel is essential to correctly estimate the quantum bit error rate (QBER), due to the fact that, changes in the QBER value are used in several QKD protocols to detect the presence of an eavesdropper on the quantum channel.[1]
The implementation of quantum protocols such the BB84 or B92 can be performed using the polarization of the photons.[1] In that scenario, it is essential that the photons polarization remains the same at fiber input/output. However, the fiber polarization mode dispersion (PMD) may depolarize the photons.[1] In order to avoid that, it is necessary to model and implement polarization control schemes, in order to correctly estimate the different contributions (for instance the polarization decorrelation between the reference and quantum channel) to the total QBER.[5,6]

Efficient generation of photons through FWM process requires the achievement of perfect phase matching condition.[7–11] Due to that restrict condition, most of the work related with FWM has been done around the fiber zero-dispersion frequency. The recent interest on on-chip quantum technologies, such as integrated optical realizations of single photon sources and quantum-correlated photon pairs sources, requires efficient generation of photons over short distances.[12] Recent developments of photonic crystal fibers (PCF) and chalcogenide glass waveguides have enable to produce these structures with high nonlinear coefficient, which is essential to obtain that kind of photon sources over short distances.[13,14] However, those optical waveguides usually present high values of absorption.[14]

In this paper, we present a review of the work that we have been done in the last years, around the FWM process as a source of single and entangled photon pairs in optical fibers, as well the measurement and modelling of the QBER in QKD systems.

This paper contains five sections. In section 2, we present a single photon source based on stimulated FWM in optical fibers. We use that source to encoded information on the polarization of single photons, and present the photon statistics of the source. At the end of the section, we show the impact of the FWM on a quantum channel in a WDM architecture. In section 3, we show the results of the QBER measurements in a system using two nonorthogonal states of polarization (SOPs), in an optical fiber. We also present a theoretical model for QBER estimation in real time polarization-encoded QKD systems with time domain multiplexing (TDM)- and WDM-based polarization control schemes. Section 4 deals with the generation of polarization entangled photon pairs through the spontaneous FWM process inside an optical fiber. We test the degree on entanglement through the analysis of the Clauser, Horne, Shimony, and Holt (CHSH) inequality. It is also presented a model that describes the impact of fiber absorption on the generation of polarization entangled photon pairs through the spontaneous FWM process. Finally, in section 5 we present the main conclusions of this work.

2. QUANTUM COMMUNICATIONS WITH SINGLE PHOTONS

2.1 FWM as a source of single photons

Four-wave mixing is a third-order nonlinear process, and occurs when more than two optical fields (known as pump and signal) are launched into a fiber, giving rise to a new wave (known as idler).[7] During the generation of the idler wave inside the fiber the signal wave is amplified, due to the fact that photons from the pump are annihilated and new photons are created on the signal and idler frequencies.[7] Most of the experiments using the FWM process have been done in a high power regime. However, the FWM process can be obtained in a low power regime, and in that sense only a few photons are generated on the idler wave. The optical power of the idler wave generated inside the fiber is given by[10]

$$P_i(z) = (\gamma P_{\mathrm{p}}(0) z_{\mathrm{eff}})^2 P_{\mathrm{s}}(0) \left| \frac{\sinh(\kappa z)}{kz} \right|^2 \exp\{-\alpha z\}\,, \tag{1}$$

where κ is the parametric gain, and $P_{\mathrm{p}}(0)$ and $P_{\mathrm{s}}(0)$ are the input pump and signal powers, respectively.

In the single pump configuration, the FWM process is very sensitive to the polarization state of the pump and signal waves. The maximum optical power of the idler wave is obtained in the co-polarized scheme, whereas the

orthogonal leads to a minimum power on the idler field.[7,15] The PMD on the fiber will depolarize the pump and signal fields, and the efficiency of the FWM will decrease. To take into account that decrease on the efficiency due to polarization decorrelation between pump and signal fields, we introduce a new parameter, called effective nonlinear parameter, γ_{eff}, which is dependent on the pump and signal wavelength separation, and can be written as[10]

$$\gamma_{\text{eff}}(\Delta\lambda) = \frac{8\gamma}{9} + \frac{\gamma}{9}\text{sech}\left(\frac{(\Delta\lambda)^{A_0}}{B_0}\right), \tag{2}$$

where A_0 and B_0 are fitting parameters, and $\Delta\lambda = \lambda_p - \lambda_s$. From (2) we can see that increasing $\Delta\lambda$ the γ_{eff} parameter take the value of $8\gamma/9$, which corresponds to a reduction of about 1 dB on the idler power, compared with the co-polarized situation. Using the FWM process, we obtain an variable source of photons per pulse by simple adjusting the spectral separation between pump and signal fields.

The schematics of the experimental setup that we use to implement a single photon source based on the FWM process is presented in Fig. 1(a). It can be seen in Fig. 1(a), path 1, that a pump from a tunable laser

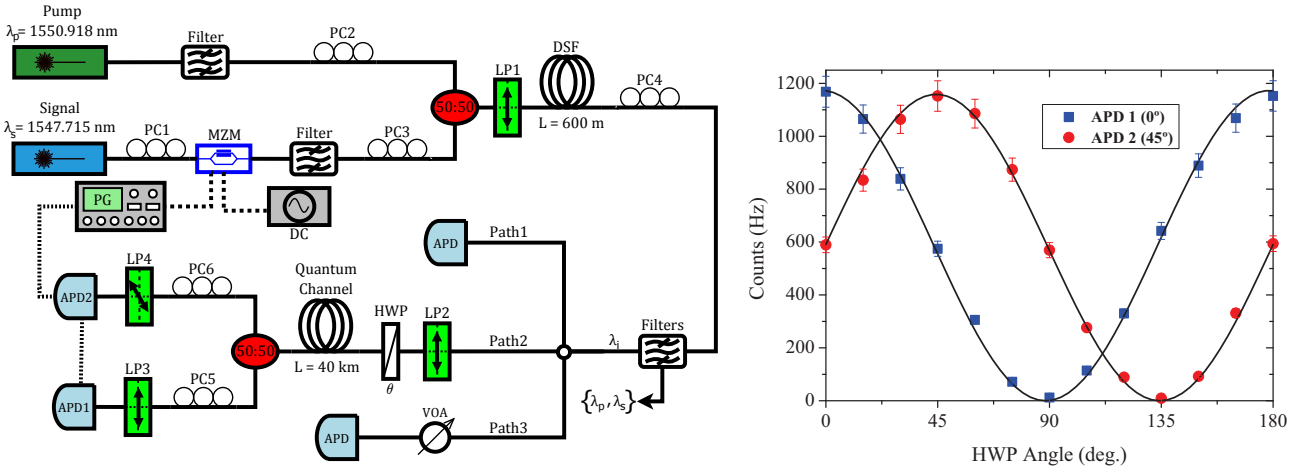


Figure 1. (a): Schematics of the experimental setup used to generate single photons from FWM process, and to encode and transmit that photons through an optical fiber. In (a) PC1-6 – Polarization controllers; MZM – Mach-Zehnder Modulator; DC – Power source; LP1-4 – Linear polarizers; HWP – Half-wave plate; DSF – Dispersion-shifted fiber; VOA – Variable optical attenuator; APD1-2 – Avalanche photodiodes; (b): Experimental results for the photon counts at APD1 and APD2 as a function of the HWP angle, for angles $\theta = 0°$ and $\theta = 45°$, after propagation through a quantum channel with a length equal to 40 km.

source centered at $\lambda_p = 1550.918$ nm, and a signal from and external cavity laser centered at $\lambda_s = 1547.715$ nm are both sent to an optical fiber. The signal wave is modulated with a Mach-Zehnder to obtain pulses with a full width at half maximum of approximately 1 ns and a repetition rate of $f_{\text{rep}} \approx 1.22$ MHz. Both signals are sent co-polarized to a dispersion-shifted fiber (DSF) with a length equal to 600 m and a nonlinear coefficient, $\gamma = 2.3$ W^{-1}km^{-1}. Due to the FWM process, the idler wave is generated inside the DSF. At fiber output the pump and signal photons are suppressed by a cascade of optical filters. The detection is performed with InGaAs/InP avalanche photodiodes (APDs), operating in Geiger mode.

In order to send quantum information, we have used the developed source and we encode information into photons polarization, using the linear polarizer (LP_2) and the half wave plate (HWP), see Fig. 1(a) path 2.[2] At the HWP output we obtain an average number of photons per pulse $\mu \approx 0.2$. After codification, we transmit the photons through a standard single-mode fiber with a length equal to 40 km. At the receiver, photons are detected and the information is extracted from the photons polarization, using the polarization controllers PC_5 and PC_6 as well the linear polarizers LP_3 and LP_4 in path 2 of Fig. 1(a).[2]

From Fig. 1(b) we can see that we can generate single photons with the FWM process, encode information into photons polarization, transmit it through a quantum channel with several kilometers long and decode it

correctly. Results show that, the 45° separation between the nonorthogonal states of polarization is maintained.

2.2 Statistics of the single photon source

In order to characterize the single photon source based on the FWM process, we have used an APD, and the maximum-likelihood estimation (MLE) method to reconstruct the photon number statistics.[16] The APD only gives the number of click or no-click events, and in that sense can be seen as an on/off detector. In that case, the statistics of no-click events from the APD, ρ_n, can be written as[16,17]

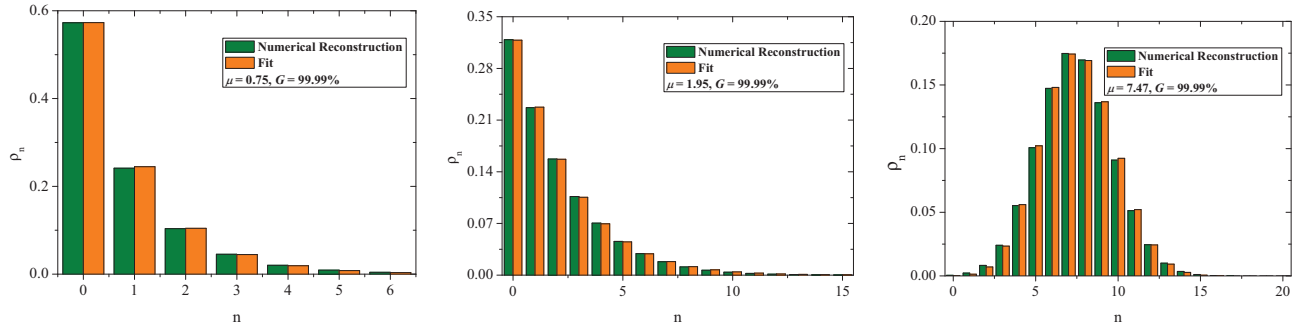
$$\rho_n^{(i+1)} = \frac{\rho_n^{(i)}}{\sum_{j=1}^{K} A_{jn}} \sum_{\nu=1}^{K} f_\nu \frac{A_{\nu n}}{p_\nu^{\text{off}}[\{\rho_n^{(i)}\}]}\,, \tag{3}$$

where $A_{\nu n} = (1-P_{\text{dc}})(1-\eta_\nu)^n$, P_{dc} represents the detector dark count probability, f_ν denotes the experimental frequencies of the no-click events for the efficiency η_ν, and $p_\nu^{\text{off}}[\{\rho_n^{(i)}\}] = (1-P_{\text{dc}})\sum_{n=0}^{N}(1-\eta_\nu)^n\rho_n^{(i)}$ is the no-click probability with quantum efficiency η_ν, obtained from the reconstructed distribution $\{\rho_n^{(i)}\}$.[17]

The experimental setup used was the same as presented in Fig. 1(a), path 3, where we use a variable optical attenuator (VOA) and one APD.

In (3), η_ν is the value of the combined efficiencies of the APD and the VOA. In our algorithm, we set the upper limit to $N = K-1 = 30$, where K is the number of different combined efficiencies considered.

In Fig. 2, we present the reconstructed photon statistics using (3). It can be seen in Fig. 2 that the statistics



(a) (b) (c)

Figure 2. Reconstructed photon statistics obtained from (3) (green bars), and best fits (orange bars). The average number of photons (μ) and the fidelity (G), between the reconstructed statistics and the theoretical distributions, are also presented. The pump power at the input of the fiber was $P_p(0) = 2.63$ mW, and the signal powers at the input of the fiber were $P_s(0) = 0.19$ μW in 2(a), $P_s(0) = 1.29$ μW in 2(b), and $P_s(0) = 7.08$ μW in 2(c).

of the idler wave at DSF output evolves from a thermal statistics, Fig. 2(a), to a Poissonian statistics Fig. 2(c), by simple adjusting the fiber input signal power. In Fig. 2(b) we observe a multithermal statistics with both thermal and coherent photons.

2.3 Impact of FWM in a co-propagating quantum channel

In a WDM architecture, where a quantum channel share the same optical fiber with other classical signals, the FWM and Raman scattering processes create in-band noise photons in the quantum channel. That impairments which occurs inside the fiber can lead to a change on the statistics of the quantum channel used to implementation of the QKD system.[4] The knowledge of the statistics of the quantum channel is essential to correctly estimate the QBER of the QKD system.[1]

The statistical properties of the quantum channel can be assessed by the Mandel's Q parameter[18]

$$Q_Q = \frac{\langle :\hat{N}_Q^2: \rangle - \langle \hat{N}_Q \rangle^2}{\langle \hat{N}_Q \rangle}\,, \tag{4}$$

where $\langle \hat{N}_Q \rangle$ is the expectation value for the dimensionless number operator, and $\langle :\hat{N}_Q^2: \rangle$ is the normally ordered second moment. When $Q_Q = 0$ we obtain a coherent light source, whereas $Q_Q > 0$ or $Q_Q < 0$ determines super-Poissonian or sub-Poissonian statistics of the light, respectively. In (4), the expectation values are given by[11]

$$\langle \hat{N}_Q \rangle = \int_{t_0}^{t_0+T_0} dt \langle \hat{A}_Q^\dagger(L,t) \hat{A}_Q(L,t) \rangle \,, \tag{5a}$$

and

$$\langle : \hat{N}_Q^2 : \rangle = \int_{t_0}^{t_0+T_0} dt \int_{t_0}^{t_0+T_0} dt' \langle \hat{A}_Q^\dagger(L,t) \hat{A}_Q^\dagger(L,t') \hat{A}_Q(L,t') \hat{A}_Q(L,t) \rangle \,. \tag{5b}$$

In (5), T_0 is the detection time window, and $\hat{A}_Q(L,t)$ is the annihilation operator for the quantum channel, given by[11,19]

$$\hat{A}(L,\omega_Q) = \Big(\alpha_Q(L) \hat{A}(0,\omega_Q) + \beta_Q(L) e^{-2i\theta_p} \hat{A}^\dagger(0,\omega_s) + \hat{F}(L,\omega_Q) \Big) \Theta(L) \,, \tag{6}$$

where ω_Q and ω_s are the frequency of the quantum channel and the signal field, respectively, θ_p is the phase of the coherent pump field, $\hat{A}_Q(L,t) = 1/(2\pi) \int d\omega H(\omega) \hat{A}(L,\omega) e^{-i\omega t}$, and $H(\omega)$ is a filter transmission function centered at $\bar{\omega}_Q$ and bandwidth $\Delta\nu$. In (6)

$$\alpha_Q(L) = \Big(\cosh(g(\Omega_{Qp})L) + \frac{i\kappa(\Omega_{Qp})}{2g(\Omega_{Qp})} \sinh((g(\Omega_{Qp})L) \Big) \Phi, \tag{7a}$$

$$\beta_Q(L) = i \frac{\gamma\eta(\Omega_{Qp})}{g(\Omega_{Qp})} A_p^2 \sinh((g(\Omega_{Qp})L) \Phi, \tag{7b}$$

$$\hat{F}(L,\omega_Q) = i \int_0^L \hat{m}(z,\Omega_{Qp}) \Big(A_p e^{-i\theta_p} \alpha_Q(L-z) - A_p^* e^{i\theta_p} \beta_Q(L-z) \Big) dz \,, \tag{7c}$$

where $\Omega_{Qp} = \omega_Q - \omega_p$, $\hat{m}(z,\Omega_{Qp})$ is the Hermitian phase noise operator, k_p is pump propagation constant, γ is fiber nonlinear parameter, and $P_0 = |A_p|^2$ is the input pump power. In (7c), $g(\Omega_{Qp})$ is the parametric gain, $\kappa(\Omega_{Qp})$ is phase-mismatch condition, and $\Phi = \exp\{(-i(k_s - k_Q)/2)L\}$, where k is the propagation constant for the signal field k_s or quantum channel k_Q field.

Figure 3 shows the evolution of the Mandel's Q parameter with wavelength separation between pump and signal fields. Results present in Fig. 3 show that Q_Q is always higher than zero, which means that the statistics of the quantum channel have evolved from Poissonian, at fiber input, to super-Poissonian at fiber output. This is due to the presence of the Raman scattering process inside the fiber, that follows a thermal statistics.

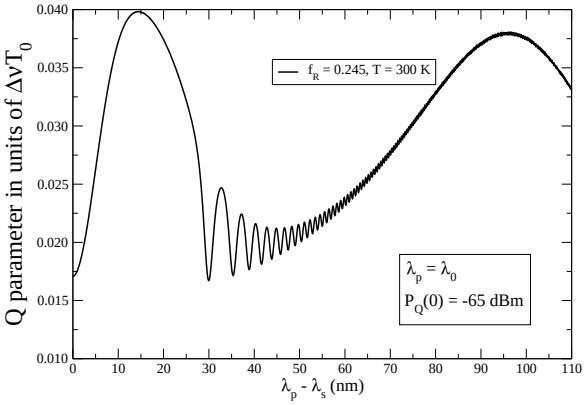


Figure 3. Mandel's Q parameter given by (4) as a function of the wavelength separation between pump and signal waves. We have used the following parameters: $P_p = 10$ dBm, $P_s = -20$ dBm, $\gamma = 2$ W^{-1}/km, zero-dispersion wavelength $\lambda_0 = 1550.92$ nm, third and fourth-order dispersion coefficients at zero-dispersion wavelength $\beta_3 = 0.1$ ps^3/km and $\beta_4 = 10^{-4}$ ps^{-4}/km, respectively, length $L = 2.5$ km, and fiber input pump power on the quantum channel $P_Q(0) = -65$ dBm.

3. QUANTUM BIT ERROR RATE

The QBER is the parameter used to quantify the amount of errors present in QKD systems. The total QBER is the sum of several different contributions, likewise the intrinsic fiber birefringence, the non ideal polarization isolation of some components, or other sources related with SOP control scheme. The QBER can be defined as the ratio between the wrong detections and total detections. In terms of rates we have[1]

$$\mathrm{QBER} = \frac{N_{\mathrm{wrong}}}{N_{\mathrm{right}} + N_{\mathrm{wrong}}} = \frac{R_{\mathrm{error}}}{R_{\mathrm{sift}} + R_{\mathrm{error}}} \approx \frac{R_{\mathrm{error}}}{R_{\mathrm{sift}}}, \tag{8}$$

where R_{error} represents the rate of error and R_{sift} is the rate of the sifted key. Note that due to the incompatible choice of bases by Alice and Bob $R_{\mathrm{sift}} = 1/2R_{\mathrm{raw}}$, where R_{raw} is the rate corresponding to the raw key.

3.1 QBER measurements without SOP control

As stated above, the photon's SOP evolution is highly dependent on the environmental conditions and on the physical characteristics of the optical channel, in particular PMD.[7] In general, the SOP evolution has a random behavior in time and frequency domains.[20,21]

In order to assess the impact of the random SOP evolution in the QBER, we have implemented the setup presented in Fig. 4. That setup corresponds to a QKD system using two nonorthogonal SOPs. We have used an attenuated laser source to generate single photons, and encoded a sequence of random bits into polarization. An external laser was used to trigger the avalanche photodiodes. A microcontroller is used to send the sequence and to measure the QBER.

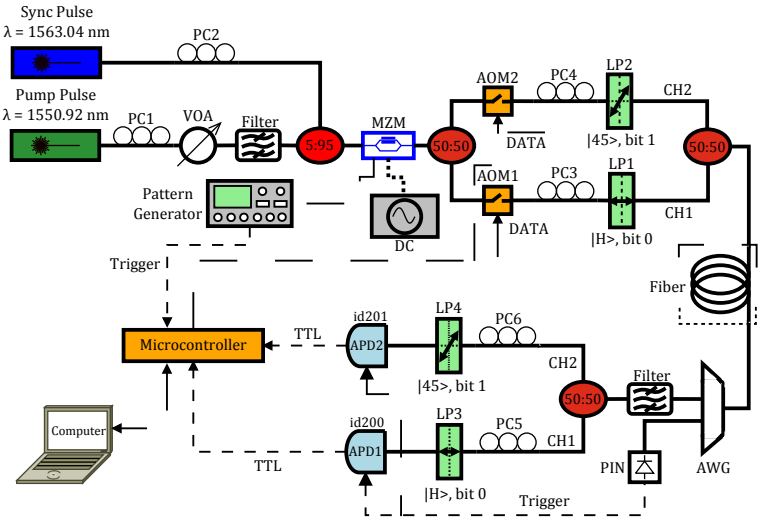


Figure 4. Setup used to perform QBER measurements of a QKD systems using two nonorthogonal SOPs. PC1-6 – Polarization controllers; VOA – Variable optical attenuator; MZM – Mach-Zehnder Modulator; DC – Power source; AOM1-2 – Acousto-optic modulators; LP1-4 – Linear polarizers; AWG – Arrayed-wavelength grating; APD1-2 – Avalanche photodiodes.

Figure 5 shows the QBER time evolution of the QKD system represented in Fig. 4 for two different scenarios. The first one corresponds to a QBER measurement in back-to-back configuration, where Alice and Bob are separated by one meter of optical fiber. In this case, the QBER presents a linear increment along the time, reaching a value of approximately 8% after 12 hours of continuous running. Notice that our system has an initial QBER of QBER(t=0)= 5%. In the second scenario, we have increased the fiber length to 20 km. In contrast with the previous case, the QBER presents now a random evolution along the time. A maximum QBER value of approximately 40% is observed after 9 hours of transmission.

The results presented in Fig. 5 show that the SOP drift can seriously affect the performance of polarization-encoded QKD systems. In order to make this kind of encoding feasible, random polarization drifts should

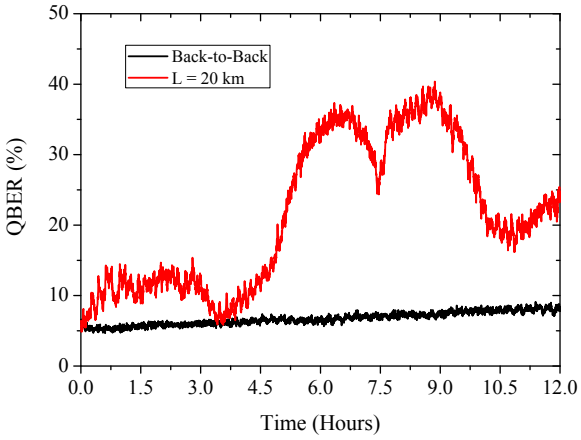


Figure 5. Experimental results for the QBER as a function of time, for a back-to-back configuration and after propagation through a single-mode fiber with a length equal to 20 km.

be compensated. These polarization changes cannot be reversed using traditional polarization controllers.[22] Indeed, active and efficient polarization control schemes, using feedback algorithms, are required. If the effects of polarization dependent losses (PDL) are negligible, the relation between the SOP at the fiber input and at the fiber output is unitary.[23] This means that the SOP changes can be reversed by compensating two non-orthogonal SOPs.[23–25] The SOP control system can be implemented by multiplexing the two non-orthogonal reference signals with the quantum information into the time or frequency domains (see Fig. 6). An active

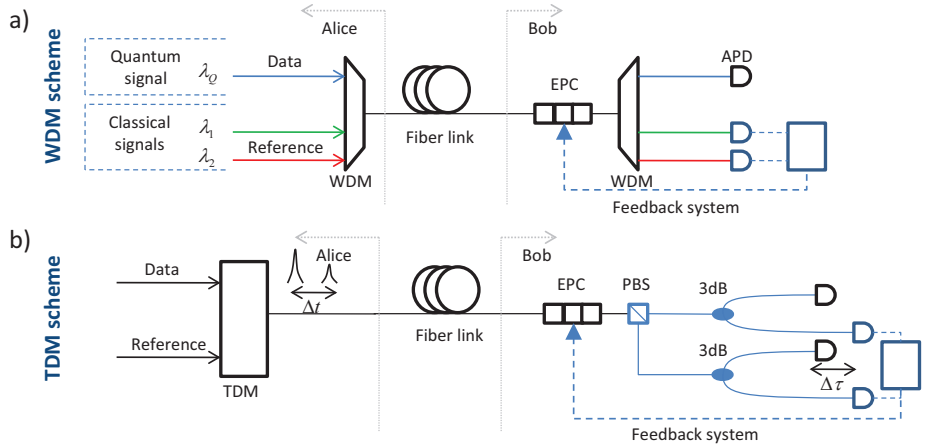


Figure 6. Schematic representation of WDM- and TDM-based dynamic polarization control schemes for polarization-encoded QKD systems in optical fibers: a) – WDM-based SOP control scheme, two nonorthogonal classical signals at different wavelengths are used as reference signals; b) – TDM-based SOP control scheme, data and reference pulses are multiplexed in the time domain. EPC – Electronic polarization controller, and PBS – Polarization beam splitter.

full polarization control scheme using two classical signals at different wavelengths has already been reported in literature.[26] Using an improved WDM control scheme, the same authors demonstrated a QKD system over 16 km of optical fiber.[5] The SOP control can also be performed using the same wavelength for both reference and data signals, and in such case the system should be able to alternate between data communication and the reference signals (TDM-based SOP control scheme). Following that technique, a method and device for readjusting the polarization drift in the QKD systems was already patented.[25] These setups can be implemented using classical signals,[25] where a switch alternates between the transmission of polarization-encoded signals and the SOP control system, or using pulses with a low mean number of photons per pulse.[27,28] An incremental real-time polarization control scheme where the reference and signal pulses are time delayed has already been

reported in literature.[29] These systems assure a continuous transmission of quantum data information with real-time polarization control. A maximum transmission distance of 50 km is reported.

In the next two subsections, we present a theoretical model for QBER estimation in polarization-encoded QKD systems with WDM- and TDM-based polarization control schemes. In both cases, we analyze the different contributions to the total QBER.

3.2 WDM-based SOP control scheme

As refereed in the introduction, WDM-based SOP control schemes use two reference pulses with different wavelengths. The correlation between the SOP of two signals depends on its wavelength separation. As much closer the wavelengths are, as stronger the correlation presented by the SOP. The degree of correlation between two Stokes vectors, at different frequencies, can be characterized by the respective frequency autocorrelation function ACF. This correlation function can be used to calculate the QBER expression for this kind of SOP control schemes[6]

$$\begin{aligned}\mathrm{QBER} &= \mathrm{QBER}_{\mathrm{fACF}} + \mathrm{QBER}_{\mathrm{dc}} \\ &= \frac{1-\exp\left(-\langle\Delta\tau^2\rangle\Delta\omega^2/3\right)}{3-\exp\left(-\langle\Delta\tau^2\rangle\Delta\omega^2/3\right)+P_{\mathrm{dc}}/(\langle n\rangle t_{\mathrm{link}})} + \frac{P_{\mathrm{dc}}}{\langle n\rangle t_{\mathrm{link}}[3-\exp\left(-\langle\Delta\tau^2\rangle\Delta\omega^2/3\right)]+P_{\mathrm{dc}}},\end{aligned} \tag{9}$$

where P_{dc} is the dark count probability, $\langle n\rangle$ is the mean number of photons per pulse, t_{link} is the transmission efficiency, $\langle\Delta\tau^2\rangle$ is the mean square differential group delay (related with the fiber PMD coefficient D_p through $\langle\Delta\tau^2\rangle = D_p^2 z$) and $\Delta\omega$ is the frequency separation between the two reference pulses.

Equation (9) shows that for long distances (note that $\langle\Delta\tau^2\rangle$ increases linearly with the distance) the polarization decorrelation between the reference signals induces an increment of the QBER. In order to avoid this QBER increment, narrow wavelength separations are required.

3.3 TDM-based SOP control schemes

For SOP control systems with reference signals multiplexed in the time domain, the main contributions to the total QBER are the time decorrelation between reference and data SOPs ($\mathrm{QBER}_{\mathrm{tACF}}$), the feedback SOP control system limitations ($\mathrm{QBER}_{\mathrm{SOP}}$), the leakage of photons from the reference pulse to the data gate ($\mathrm{QBER}_{\mathrm{leak}}$), the detector afterpulse probability ($\mathrm{QBER}_{\mathrm{af}}$), and the dark counts ($\mathrm{QBER}_{\mathrm{dc}}$). The expression for the total QBER can be written as[6]

$$\begin{aligned}\mathrm{QBER} =& \mathrm{QBER}_{\mathrm{tACF}} + \mathrm{QBER}_{\mathrm{SOP}} + \mathrm{QBER}_{\mathrm{leak}} + \mathrm{QBER}_{\mathrm{af}} + \mathrm{QBER}_{\mathrm{dc}} \\ =& \frac{1}{4} - \frac{1}{4}\exp\left[\frac{-3\omega^2 D_p^2 z\,|T_{\mathrm{rep}}-\Delta t|}{2t_0}\right] + 1 - \cos^2\left[\frac{1}{2}\Theta(1-\exp(-gT_{\mathrm{rep}}))\right] \\ &+ \frac{1}{2}\frac{\langle n_r\rangle A}{\langle n\rangle} + \frac{\langle n_r\rangle P_{\mathrm{af}}}{\langle n\rangle\eta_{\mathrm{det}}} + \frac{1}{2}\frac{P_{\mathrm{dc}} n_{\mathrm{det}}}{\langle n\rangle t_{\mathrm{link}}\eta_{\mathrm{det}}},\end{aligned} \tag{10}$$

where T_{rep} is the inverse of the pulse rate (f_{rep}), Δt is the temporal separation between the reference and data pulses, t_0 represents the drift time of the index difference between the fast and slow fiber axes, Θ and g are parameters related with the feedback SOP control,[6] η_{det} is the quantum detector efficiency, P_{af} is the afterpulse probability, $\langle n_g\rangle = A\langle n_r\rangle$ is the mean number of reference photons per pulse leaked to the data detector gate, with $\langle n_r\rangle$ being the mean number of reference photons per pulse, and the parameter A the fraction of photons that are leakage to the wrong detector.

Some contributions to the QBER in (10) depend on the propagation distance. In the case of $\mathrm{QBER}_{\mathrm{dc}}$, it occurs because the detector dark counts are constant, whereas R_{sift} decreases with t_{link}. The contribution due to the pulse leakage, $\mathrm{QBER}_{\mathrm{leak}}$, is dependent on the propagation distance, since for narrow pulses chromatic dispersion can induce pulse broadening. With that, and since the reference signal is also present in the data arm, the probability of photons be detected into the data detector, A, increases. Since the typical drift time t_d is dependent on the PMD, the $\mathrm{QBER}_{\mathrm{tACF}}$ will increase with the distance. Concerning the frequency, we

observe that only $\mathrm{QBER_{leak}}$ and $\mathrm{QBER_{dc}}$ are frequency independent. On the other hand, both $\mathrm{QBER_{SOP}}$ and $\mathrm{QBER_{tACF}}$ contributions decrease with the frequency. In the first case, that occurs because as more photons are received at the SOP controller system, smaller will be the deviations from the target SOP at the EPC output. In the second case, the QBER contribution decreases because as higher the frequency is, smaller will be the separation between the reference and data pulses, which means a stronger correlation between their SOP.

The models presented in (9) and (10) show that the decorrelation between the reference and data signals is the fundamental impairment in the implementation of WDM-based SOP control schemes. This makes mandatory the use of low PMD fibers in order to achieve large distances with a low QBER. In the TDM-based SOP control scheme, we have identified some limitative technical aspects, likewise the single-photon detector dark counts, the afterpulse detections or the feedback SOP control system performance. However, our results show that for long distances fiber losses are the major impairment, presenting a main contribution to the total QBER.

4. GENERATION OF ENTANGLED PHOTON PAIRS IN OPTICAL FIBERS

In optical fibers, the spontaneous FWM process can be used to create polarization entangled states through a fiber loop.[30] The fiber loop gives rise to two co-polarized FWM processes, one clockwise (CW) and other counterclockwise (CCW), creating a polarization entangled Bell state of $|\Phi^{\pm}\rangle = (|H\rangle_s|H\rangle_i \pm |V\rangle_s|V\rangle_i)/\sqrt{2}$, where H and V denote horizontal and vertical linear polarizations, respectively.[31]

4.1 Evaluation of the CHSH parameter using FWM in a fiber loop

The CHSH inequality is a special type of Bell's inequality. By evaluating its value its possible to verify the generation of entangled photon pairs. In order to generate polarization entangled photon pairs in optical fibers, it can be used the spontaneous FWM process. A schematics of the experimental setup used to generate polarization entangled photon pairs, and consequently to verify the violation of CHSH inequality is presented in Fig. 7.

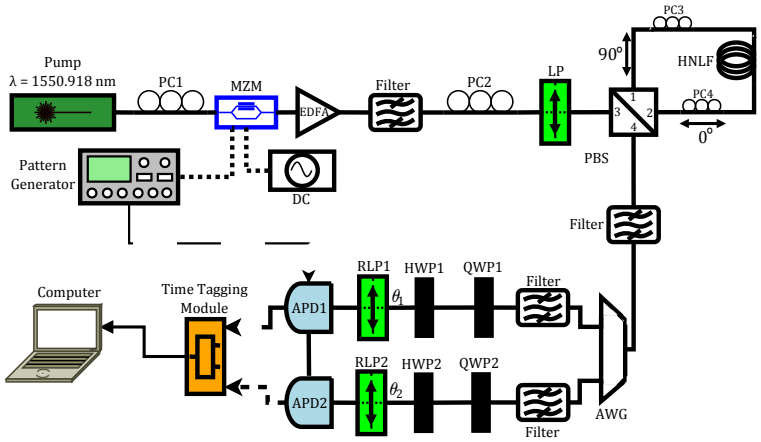


Figure 7. Schematics of the experimental setup used to generate polarization entangled photon pairs in a highly nonlinear fiber. PC1-4 – Polarization controllers; MZM – Mach-Zehnder Modulator; DC – Power source; EDFA – Erbium-doped fiber amplifier; LP – Linear polarizer; PBS – Polarization beam splitter; HNLF – Highly nonlinear fiber; AWG – Arrayed-wavelength grating; QWP1-2 – Quarter-wave plates; HWP1-2 – Half-wave plates; RLP1-2 – Rotating linear polarizers; APD1-2 – Avalanche photodiodes.

In Fig. 7, a pump pulse is sent to a Sagnac fiber loop, where polarization entangled photon pairs are generated, and then detected using two APDs. To verify the violation of CHSH inequality through the value of the parameter $\mathcal{S}(0)$, we measured the coincidence rate for 16 combinations of the polarizer settings (θ_1 = -45°, 0°, 45°, 90° and θ_2 = -22.5°, 22.5°, 67.5°, 112.5°).[32] The parameter $\mathcal{S}(0)$ is defined as[33]

$$\mathcal{S}(0) = |E(\theta_1, \theta_2) - E(\theta_1, \theta_2') + E(\theta_1', \theta_2) + E(\theta_1', \theta_2')|\,, \tag{11}$$

where E are the expectancy values. A violation of the CHSH inequality happens when $\mathcal{S}(0) > 2$.

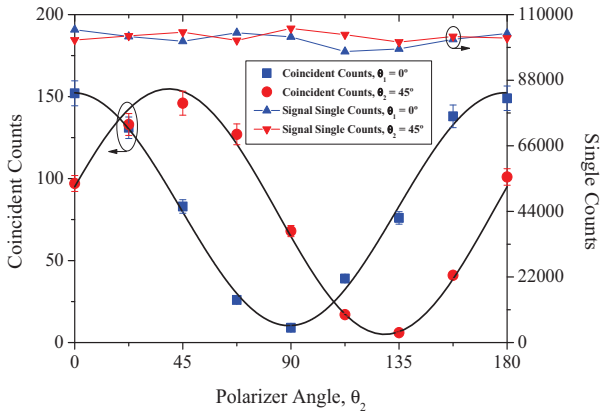


Figure 8. Coincident and single counts as a function of the linear polarizer angle, θ_2, when $\theta_1 = 0°$ and $45°$. The solid curve is a sinusoidal fit to the experimental data.

In Fig. 8, we show coincident and single counts obtained when $\theta_1 = 0°$ and $45°$, and θ_2 is varied. The results for the other angles of θ_1 and θ_2 are similar.

The results for the coincident counts show that our source produces polarization entangled photon pairs with a visibility greater than 86%. From the values that we measured, we obtained a parameter $\mathcal{S}(0) = 2.470 \pm 0.173$, when accidental coincidences were subtracted. From this result we can conclude that the CHSH inequality was violated by 2.7 standard deviations, and entangled photon pairs were successfully generated through the spontaneous FWM source.

4.2 Impact of fiber loss on the CHSH parameter

Recent developments of PCF and chalcogenide glass waveguides have enable to produce these structures with high nonlinear coefficient, which is essential to obtain that kind of photon sources over short distances. However, those optical waveguides usually present high values of absorption.[13,14]

The quantum version of the nonlinear Schrödinger equation in optical fibers in the frequency domain is given by[34,35]

$$\frac{\partial \hat{A}_j(z,\omega)}{\partial z} = i\sum_k \tilde{R}^{(1)}_{jk}(\omega)\hat{A}_k(z,\omega) + \frac{i\hbar\omega_0}{(2\pi)^2}\sum_{klm}\iint d\omega_1 d\omega_2 \tilde{R}^{(3)}_{jklm}(\omega_2-\omega_1)\hat{A}^\dagger_l(z,\omega_1)\hat{A}_m(z,\omega_2)\hat{A}_k(z,\omega+\omega_1-\omega_2)$$
$$+ \frac{i\sqrt{\hbar\omega_0}}{2\pi}\sum_k \int d\omega_1 \hat{m}_{jk}(z,\omega-\omega_1)\hat{A}_k(z,\omega_1) + \hat{l}_j(z,\omega), \tag{12}$$

where $j,k,l,m = x$ or y, $\tilde{R}^{(1)}_{jk}(\omega)$ is the linear response function and $\tilde{R}^{(3)}_{jklm}(\Omega)$ is the third-order nonlinear response function of the optical fiber. In (12), $\hat{m}_{jk}(z,\Omega)$ is the noise operator due to the presence of a phonon reservoir, and $\hat{l}_j(z,\omega)$ represents the photon absorption reservoir.[19,34,35]

The evolution of the signal and idler annihilation operators at a given distance L in the fiber are given by[34,36]

$$\hat{A}_u(L) = \mu_u(L,0)\hat{A}_u(0) + \nu_u(L,0)\hat{A}^\dagger_v(0) + \hat{N}(L,\omega_u) + \int_0^L dz\left(\hat{l}(z,\omega_u)\mu_u(L,z) + \hat{l}^\dagger(z,\omega_v)\nu_u(L,z)\right), \tag{13}$$

where $u \neq v = s$ or i and represent the signal and idler fields, $\hat{N}(L,\omega_u)$ is the Raman noise operator given by

$$\hat{N}(L,\omega_u) = i\int_0^L \hat{m}(z,\Omega_{up})\Big(\bar{A}_p(z)\mu_u(L,z) - \bar{A}^*_p(z)\nu_u(L,z)\Big)dz. \tag{14}$$

In (14), $\bar{A}_p(z)$ is the the classical pump field, such that $P_x(z) = |\bar{A}_p(z)|^2$ represents the pump power, given by

$$\bar{A}_p(z) = \bar{A}_p(0)\exp\left\{(i\beta_p z + \gamma P_x(0)z_e) - \frac{\alpha_p}{2}z\right\}, \tag{15}$$

where z_e is the fiber effective length, and α_p is the pump loss coefficient. In (13)[34,36]

$$\mu_s(L,z) = e^{p(L,z,\omega_s)} \sum_{n=0} s_n(z) L_e^n(z), \tag{16a}$$

with $s_0 = 1$ and $a_0^* = 0$,

$$\nu_i(L,z) = e^{p(L,z,\omega_i)} \sum_{n=0} a_n(z) L_e^n(z), \tag{16b}$$

with and $s_0 = 1$ and $a_0^* = 0$.

The function ν_s is the same series as μ_s except that the initial condition is $s_0 = 0$ and $a_0^* = 1$. The function μ_i is the same series as ν_i except that the initial condition is $s_0 = 0$ and $a_0^* = 1$. In (16), $L_e(z) = (1 - \exp\{-\alpha_p(L-z)\})/\alpha_p$, and

$$p(L,z,\omega_u) = -\frac{\alpha_s + \alpha_i + 2i\Delta\beta}{4}(L-z) + i\left(\beta_u(L-z) + \gamma P_x(0) L_e(z)\right), \tag{17}$$

where $\Delta\beta$ is the phase-matching condition.

According with[19] the CHSH parameter $\mathcal{S}(\tau)$ is given by

$$\mathcal{S}(\tau) = 2\sqrt{2}\,\frac{G^{(2)}_{(si)}(\tau) - \mathcal{I}_i(L,t)\mathcal{I}_s(L,t+\tau)}{G^{(2)}_{(si)}(\tau) + \mathcal{I}_i(L,t)\mathcal{I}_s(L,t+\tau)} \leq 2, \tag{18}$$

where $\mathcal{I}_u(L,\tau) = \langle \hat{A}_u^\dagger(L,\tau)\hat{A}_u(L,\tau)\rangle$ is the signal or idler photon flux, and

$$G^{(2)}_{(si)}(\tau) = \langle \hat{A}_i^\dagger(L,t)\hat{A}_s^\dagger(L,t+\tau)\hat{A}_s(L,t+\tau)\hat{A}_i(L,t)\rangle, \tag{19}$$

is the cross correlation function between signal and idler fields.

Figure 9 shows the evolution of the $\mathcal{S}(0)$ parameter as a function of the ratio of signal to idler photon-fluxes $\mathcal{I}_s(L,0)/\mathcal{I}_i(L,0)$. The idler, $\alpha_{\bar{i}}$, and signal, $\alpha_{\bar{s}}$, fiber loss coefficients varies between 0 and 100 dB/km. It can be seen in Fig. 9 that, a strong violation of the CHSH inequality is obtained for high values of both signal and idler loss coefficients, where $\mathcal{I}_s(L,0)/\mathcal{I}_i(L,0) \ll 1$. Results also show that, if the signal loss is almost negligible and the idler loss is very high, we obtain $\mathcal{I}_s(L,0)/\mathcal{I}_i(L,0) > 1$, and it is not observed a violation of the CHSH inequality. From Fig. 9, we can see that a maximum on $\mathcal{S}(0)$ value happens when $\mathcal{I}_s(L,0)/\mathcal{I}_i(L,0)$ lies between 0.5 and 0.75, in a regime with high losses on the signal field.

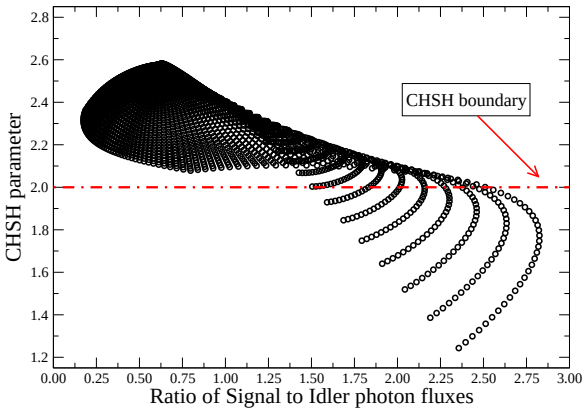


Figure 9. CHSH parameter, $\mathcal{S}(0)$, given by (18) as a function of the ratio $\mathcal{I}_s(L,0)/\mathcal{I}_i(L,0)$. The signal and idler loss coefficients, α_s and α_i, varies between 0 and 100 dB/km. The fiber parameters used are $\gamma = 95$ W^{-1}km^{-1}, zero-dispersion wavelength $\lambda_0 = \lambda_p = 1257.45$ nm, $\Delta\beta = 0$, $\alpha_p = 37$ dB/km, $T = 300$ K, $\gamma P_x(0) z_e = 0.25$, and $\Omega_{sp}/(2\pi) = 3$ (THz).

5. CONCLUSIONS

In summary, we presented our recent results on quantum communications. We presented a single photon source based on FWM process, and we statistical characterize that source of photons. We show that the statistics of the source evolves from thermal to Poissonian by adjusting the fiber input power. We use that source to encode information on the polarization state of the photons. We also present experimental results for the measurement of the QBER, and we show that without a polarization control scheme the QBER rapidly grows until 40%. It was also presented a theoretical model that compares WDM-with TDM-based polarization control schemes. Results show that the TDM scheme offers a better solution to compensation of random polarization rotations that photons suffers during the evolution on the fiber. Finally, we use the spontaneous FWM process and implement a source of polarization entangled photon pairs. We test the CHSH inequality and we obtain $\mathcal{S}(0) = 2.470 \pm 0.173$, when accidental coincidences were subtracted. The CHSH inequality was violated by 2.7 standard deviations. We also model the impact of fiber absorption on the generation rate of polarization entangled photon pairs, and we show that high loss regimes give rise to a strong violation of the CHSH inequality.

ACKNOWLEDGMENTS

This work was supported in part by the FCT - Fundação para a Ciência e a Tecnologia, through the PhD Grants SFRH/BD/79482/2011, SFRH/BD/63958/2009, and the Post-Doc Grant SFRH/BPD/77286/2011, by the FCT and European Union FEDER - Fundo Europeu de Desenvolvimento Regional, through project PTDC/EEA-TEL/103402/2008 (QuantPrivTel), and by the FCT and the Instituto de Telecomunicações, under the PEst-OE/EEI/LA0008/2011 program, project "P-Quantum".

REFERENCES

[1] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Rev. Mod. Phys.* **74**(1), 145–195 (2002).

[2] Almeida, A. J., Silva, N. A., Muga, N. J., and Pinto, A. N., "Single-photon source using stimulated FWM in optical fibers for quantum communication," *International Conference on Applications of Optics and Photonics* **8001**(1), 80013W, SPIE (2011).

[3] Almeida, A., Carneiro, S., Silva, N., Muga, N., and Pinto, A., "Polarization-entangled photon pairs using spontaneous four-wave mixing in a fiber loop," in [*EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE*], 1 –4 (april 2011).

[4] Peters, N. A., Toliver, P., Chapuran, T. E., Runser, R. J., McNown, S. R., Peterson, C. G., Rosenberg, D., Dallmann, N., Hughes, R. J., McCabe, K. P., Nordholt, J. E., and Tyagi, K. T., "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New Journal of Physics* **11**(4), 045012 (2009).

[5] Xavier, G. B., Walenta, N., de Faria, G. V., Temporão, G. P., Gisin, N., Zbinden, H., and von der Weid, J. P., "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," *New J. Phys.* **11**(4), 045015 (2009).

[6] Muga, N. J., Mário F. S. Ferreira, and Pinto, A. N., "QBER estimation in QKD systems with polarization encoding," *IEEE/OSA J. Lightwave Technol.* **29**(3), 355–361 (2011).

[7] Agrawal, G. P., [*Nonlinear Fiber Optics, 3rd ed.*], Academic Press, San Diego, USA (2001).

[8] Silva, N., Muga, N., and Pinto, A., "Influence of the stimulated Raman scattering on the four-wave mixing process in birefringent fibers," *Lightwave Technology, Journal of* **27**(22), 4979–4988 (2009).

[9] Silva, N. A., Muga, N. J., and Pinto, A. N., "Evolution of first-order sidebands from multiple FWM processes in HiBi optical fibers," *Optics Communications* **284**(13), 3408 – 3415 (2011).

[10] Silva, N. A., Muga, N. J., and Pinto, A. N., "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *Quantum Electronics, IEEE Journal of* **46**(3), 285–291 (2010).

[11] Silva, N. A., Almeida, A. J., and Pinto, A. N., "Interference in a quantum channel due to classical four-wave mixing in optical fibers," *Quantum Electronics, IEEE Journal of* **48**, 472 –479 (april 2012).

[12] Politi, A., Cryan, M. J., Rarity, J. G., Yu, S., and O'Brien, J. L., "Silica-on-silicon waveguide quantum circuits," *Science* **320**(5876), 646–649 (2008).

[13] NKT Photonics, "NL-PM-750 data sheet." http://www.nktphotonics.com/files/files/NL-PM-750-090612.pdf.

[14] Gai, X., Wang, R. P., Xiong, C., Steel, M. J., Eggleton, B. J., and Luther-Davies, B., "Near-zero anomalous dispersion $Ge_{11.5}As_{24}Se_{64.5}$ glass nanowires for correlated photon pair generation: design and analysis," *Opt. Express* **20**, 776–786 (Jan 2012).

[15] Lin, Q. and Agrawal, G. P., "Vector theory of four-wave mixing: polarization effects in fiber-optic parametric amplifiers," *J. Opt. Soc. Am. B* **21**, 1216–1224 (Jun 2004).

[16] Zambra, G., Andreoni, A., Bondani, M., Gramegna, M., Genovese, M., Brida, G., Rossi, A., and Paris, M. G., "Experimental Reconstruction of Photon Statistics without Photon Counting," *Physical Review Letters* **95**, 063602 (Aug. 2005).

[17] Álvaro J. Almeida, Silva, N. A., André, P. S., and Pinto, A. N., "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal," *Optics Communications* (0), – (2012).

[18] Mandel, L. and Wolf, E., [*Optical coherence and quantum optics*], Cambridge University Press, New York, first ed. (1995).

[19] Lin, Q., Yaman, F., and Agrawal, G. P., "Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization," *Phys. Rev. A* **75**(2), 023803 (2007).

[20] Karlsson, M., Brentel, J., and Andrekson, P., "Long-term measurement of PMD and polarization drift in installed fibers," *IEEE/OSA J. Lightwave Technol.* **18**, 941–951 (Jul. 2000).

[21] Zbinden, H., Gisin, N., Huttner, B., Muller, A., and Tittel, W., "Practical aspects of quantum cryptographic key distribution," *J. Cryptology* **13**, 207–220 (Dec. 2000).

[22] Muga, N. J., Pinto, A. N., Ferreira, M., and da Rocha, J. R. F., "Uniform polarization scattering with fiber-coil based polarization controllers," *IEEE/OSA J. Lightwave Technol.* **24**(11), 3932–3943 (2006).

[23] Huttner, B., Muller, A., Gautier, J. D., Zbinden, H., and Gisin, N., "Unambiguous quantum measurement of nonorthogonal states," *Phys. Rev. A* **54**, 3783–3789 (Nov. 1996).

[24] Martinelli, M., Martelli, P., and Pietralunga, S. M., "Polarization stabilization in optical communications systems," *IEEE/OSA J. Lightwave Technol.* **24**(11), 4172–4183 (2006).

[25] Poppe, A., "Method and device for readjusting a polarization drift," *United States Patent, no. US2008/0310856 A1* (Dec. 2008).

[26] Xavier, G. B., de Faria, G. V., ao, G. P. T., and von der Weid, J. P., "Full polarization control for fiber optical quantum communication systems using polarization encoding," *Opt. Express* **16**(3), 1867–1873 (2008).

[27] Chen, J., Wu, G., Li, Y., Wu, E., and Zeng, H., "Active polarization stabilization in optical fibers suitable for quantum key distribution," *Opt. Express* **15**(26), 17928–17936 (2007).

[28] Cheng-Zhi, P., Jun, Z., Dong, Y., Wei-Bo, G., Huai-Xin, M., Yin, H., Zeng, H.-P., Tao, Y., Xiang-Bin, W., and Jian-Wei, P., "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.* **98**, 010505 (Jan. 2007).

[29] Chen, J., Wu, G., Xu, L., Gu, X., Wu, E., and Zeng, H., "Stable quantum key distribution with active polarization control based on time-division multiplexing," *New J. Phys.* **11**(6), 17928–17936 (2009).

[30] Chen, J., Altepeter, J. B., and Kumar, P., "Quantum-state engineering using nonlinear optical sagnac loops," *New Journal of Physics* **10**(12), 123019 (2008).

[31] Takesue, H. and Inoue, K., "Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop," *Phys. Rev. A* **70**, 031802 (2004).

[32] Clauser, J. F., Horne, M. A., Shimony, A., and Holt, R. A., "Proposed Experiment to Test Local Hidden-Variable Theories," *Physical Review Letters* **23**, 880–884 (Oct. 1969).

[33] Aspect, A., Grangier, P., and Roger, G., "Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities," *Physical Review Letters* **49**, 91–94 (July 1982).

[34] Voss, P. L. and Kumar, P., "Raman-effect induced noise limits on $\chi^{(3)}$ parametric amplifiers and wavelength converters," *Journal of Optics B: Quantum and Semiclassical Optics* **6**(8), S762 (2004).

[35] Drummond, P. D. and Corney, J. F., "Quantum noise in optical fibers. I. Stochastic equations," *J. Opt. Soc. Am. B* **18**(2), 139–152 (2001).

[36] Silva, N. and Pinto, A., "Role of absorption on the generation of quantum-correlated photon pairs through FWM," Submitted to: Quantum Electronics, IEEE Journal of (2012).