Enabling Quantum Communications through Accurate Photons Polarization Control

Álvaro J. Almeida[a,c], Nelson J. Muga[b,c], Nuno A. Silva[b,c], Aleksandar D. Stojanovic[c], Paulo S. André[a,c], Armando N. Pinto[b,c], José Mora[d], and José Capmany[d]

[a]Department of Physics, University of Aveiro, Aveiro, Portugal;
[b]Department of Electronics, Telecommunications and Informatics, University of Aveiro, Aveiro, Portugal;
[c]Instituto de Telecomunicações, Aveiro, Portugal
[d]ITEAM Research Institute, Universitat Politècnica de València, València, Spain

ABSTRACT

The rapid increase on the information sharing around the world, leads to an utmost requirement for capacity and bandwidth. However, the need for security in the transmission and storage of information is also of major importance. The use of quantum technologies provides a practical solution for secure communications systems. Quantum key distribution (QKD) was the first practical application of quantum mechanics, and nowadays it is the most developed one. In order to share secret keys between two parties can be used several methods of encoding. Due to its simplicity, the encoding into polarization is one of the most used. However, when we use optical fibers as transmission channels, the polarization suffers random rotations that may change the state of polarization (SOP) of the light initially sent to the fiber to a new one at the output. Thus, in order to enable real-time communication using this encoding method it is required the use of a dynamic control system. We describe a scheme of transmission of quantum information, which is based in the polarization encoding, and that allows to share secret keys through optical fibers without interruption. The dynamic polarization control system used in such scheme is described, both theoretically and experimentally. Their advantages and limitations for the use in quantum communications are presented and discussed.

Keywords: Control of Polarization, Quantum Communication, Quantum Key Distribution, Dynamic Control

1. INTRODUCTION

Quantum cryptography was born from the idea of Stephen Wiesner to make quantum bank notes. This proposal was rejected for publication at that time, maybe because it was not understood by the editors and referees.[1] However, Stephen Wiesner told his ideas to Charles Bennett, and later, due to a random encounter between Charles Bennett and Gilles Brassard in 1979, they spoked about Wiesner's idea, and from there was born a fruitful collaboration that led the way to quantum cryptography and some other related topics.[1] After several discussions between them, in 1982 Bennett and Brassard published the first paper where the term "quantum cryptography" actually appeared.[2] The publication of Bennett and Brassard's paper triggered the belated publication of Wiesner's original "Conjugate coding", in 1983.[3]

In 1984, the first quantum protocol designed for the use of single photons was proposed, becoming known as BB84.[4] This protocol was experimentally verified in 1989, and the first transmission of quantum information

Further author information: (Send correspondence to Álvaro J. Almeida)
Álvaro J. Almeida: E-mail: aalmeida@av.it.pt, Telephone: +351 234 377 900
Nelson J. Muga: E-mail: muga@av.it.pt, Telephone: +351 234 377 900
Nuno A. Silva: E-mail: nasilva@av.it.pt, Telephone: +351 234 377 900
Aleksandar D. Stojanovic: E-mail: stojanovic@av.it.pt, Telephone: +351 234 377 900
Paulo S. André: E-mail: pandre@av.it.pt, Telephone: +351 234 377 900
Armando N. Pinto: E-mail: anp@ua.pt, Telephone: +351 234 377 900
José Mora: E-mail: jmalmer@iteam.upv.es, Telephone: +34 963 877 000
José Capmany: E-mail: jcapmany@iteam.upv.es, Telephone: +34 963 877 000

was achieved through a distance of 32.5 cm, in a free-space realization.[5] In 1991, Arthur Ekert developed and presented a different way of seeing quantum cryptography, making use of quantum correlations, mainly known as quantum entanglement. From this work has resulted the first quantum protocol for the use of entangled photons, (which is nowadays known as E91[6]). Since those achievements in quantum cryptography were done, new quantum protocols have been proposed, always with the aim of surpassing certain vulnerabilities present in the previous ones.[7–9] For the implementation of all these protocols, several single- and entangled-photon sources were already presented.[10,11] The first experiments were realized using an attenuated laser source.[5,12,13] More recently, the stimulated four-wave mixing (FWM) process was also used to generate a single-photon source,[14] and the spontaneous FWM process was employed to generate entangled photons.[15] Several solutions for codification of the information were already proposed using single or entangled photons, in polarization, phase, frequency and others, having been explored solutions involving either free-space or optical fibers as transmission media.[16] Due to the simplicity of implementation, polarization-based schemes are one of the most used. However, polarization suffers from random rotations inside the optical fiber, which require a dynamic control system for real-time operation purposes.[17,18]

We review the basics of polarization-encoding schemes used in quantum communications, briefly discussing single-photon sources and detectors, mutual information shared between Alice and Bob, and between Alice and Eve. Next, we present dynamic polarization controllers and characterize one of them in terms of its use in quantum communication schemes. The dynamic polarization controller is characterized both theoretically and experimentally. Its advantages and limitations are also discussed.

2. QUANTUM COMMUNICATIONS BASED ON POLARIZATION-ENCODING

The first experimental realization of QKD was performed in 1989, using a free-space channel and polarization-encoding for BB84 protocol.[5] The scheme of the experimental setup used in that experiment is shown in Fig. 1. On Alice's side, the photon pulses were generated using a light-emitting diode (LED). After that they were

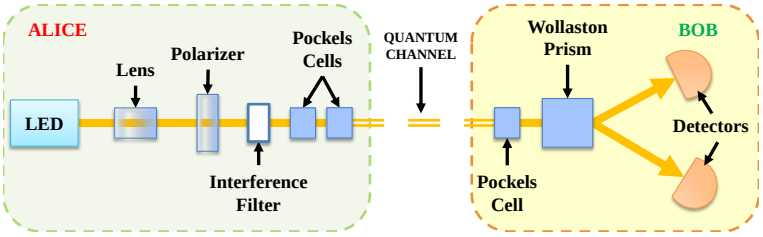

Figure 1. Scheme of the first QKD experiment, in free-space (adapted from[5]).

attenuated using an interference filter and polarized using a polarizer. The encoding of qubits in the photon's polarization was performed through the use of Pockels cells. The encoded qubits were transmitted through a free-space path of 32.5 cm. On Bob's side, the choice of the basis was performed using another Pockels cell, and the analysis of the polarizations was performed using a Wollaston prism. The detection was carried out by photomultipliers.

Using an optical fiber as a quantum channel, the group from the University of Geneva have achieved quantum communication through more than 1 km, using the experimental setup shown in Fig. 2. The BB84 protocol was

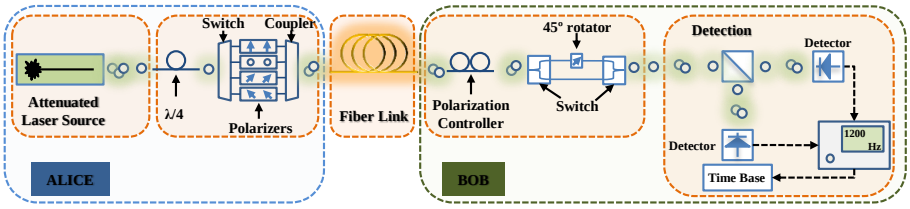

Figure 2. Schematics of the first QKD experiment, in optical fibers (adapted from[12]).

also implemented. Alice setup was composed of a laser at 800 nm that generated attenuated pulses. The photons

were circularly polarized using an $\lambda/4$ waveplate. After that, photons were sent to one of four linear polarizers, set at 0°, 45°, 90° and 135°, which were randomly chosen through the use of an electro-optical switch, passing through a passive coupler, and being sent through an optical fiber. Since the polarization is changing over transmission through the fiber, a fiber-optic polarization controller was used to re-align the state of polarization. In order to choose the detection basis, another electro-optic switch system was used, where one arm is 45° to the other. The detection of photons was performed using single-photon counters, and the recording of the states of polarization was achieved through the use of a time base. As described in,[13] polarization suffers from several limitations, which change it randomly during transmission. First, a topological problem related to the parallel transport of a vector along a curve. When the path taken by the light in an optical fiber is three dimensional its polarization is rotated by an angle related to Berry's phase.[19] The second difficulty arises from the intrinsic birefringence of an optical fiber. The third problem is related to the polarization mode dispersion (PMD), which is due to different velocities in the two axes of the fiber (slow and fast). The last problem is related to polarization-dependent losses (PDL) in optical fiber components. In order to overcome these problems, the use of polarization controllers is the more simple solution. Initially, the use of manual polarization controllers[20] was enough to demonstrate new ideas. However, in order to implement real-time working systems, the use of electronic polarization controllers (EPCs) provides a feasible solution.

A general scheme for a QKD system in optical fibers, using a polarization controller to compensate for polarization rotations, is shown in Fig. 3. From Fig. 3 we can see the various stages of a polarization-encoding

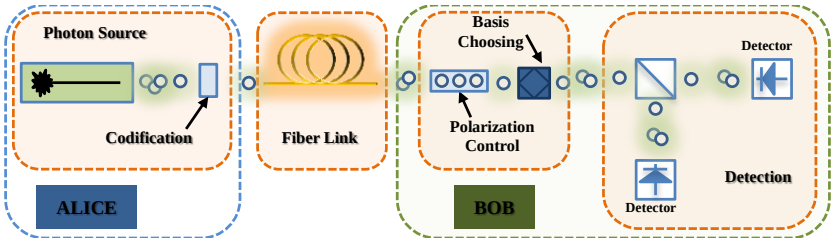

Figure 3. General scheme for QKD in optical fibers using a polarization controller to compensate for polarization rotations.

scheme for quantum cryptography. This includes a photon source and photon's encoding on Alice's side. Next, after the transmission channel, on Bob's side we should have a polarization control device, followed by the basis choosing one, and finally the analysis of polarizations, which can be performed using a polarization-beam splitter (PBS), and single-photon detectors.

First implementations used manual polarization control, which allowed the demonstration of their feasibility. More recently, a few experimental demonstrations used EPCs, which allowed continuous run of QKD systems.[17,18]

In order to implement QKD is necessary to generate single photons, as carriers of information. However, the assembling of a true single-photon source is a really challenging task. To overcome that difficulty, the so-called probabilistic single-photon sources can be used. Two ways to obtain a probabilistic single-photon source are from an attenuated laser and from the four-wave mixing process. The photons generated through an attenuated laser follow a Poissonian statistics,[16,21] and in the four-wave mixing source photons present different statistics, changing from thermal to Poissonian, depending on the average number of photons per pulse generated.[22,23] Several other types of photon sources were already presented and are discussed in.[11]

On the detection side, there are also several single-photon detectors which can be used.[11] Depending on the ability to discriminate the number of photons in a pulse, single-photon detectors can be divided into non-photon-number-resolving and photon-number-resolving detectors.[11] Since the task of discriminating the number of photons is very difficult, non-photon-number-resolving detectors are the most commonly used. Several non-photon-number-resolving detectors are already commercially available.[24] However, these detectors still offer a very low quantum efficiency, the dark-count rate can be considerably improved, as the timing jitter. Anyway, these detectors have allowed the demonstration of many physical and mathematical theories, and will help solving many breakthroughs in quantum cryptography. Future research should come up with better detectors.

On the channel side, and since an eavesdropper can be present in any node of a quantum network, the amount of information that it can obtain can also be estimated. Thus, we can determine the mutual information shared between Alice and Bob, $I_{\rm AB}$, and between Alice and Eve, $I_{\rm AE}$.

The mutual information between Alice and Bob in BB84 protocol is given by,

$$I_{\rm AB} = 1 + \left[{\rm QBER}\log_2({\rm QBER}) + (1-{\rm QBER})\log_2(1-{\rm QBER})\right], \tag{1}$$

which is the same for B92 protocol.[16] The QBER parameter is the quantum-bit error rate, and is described as,

$${\rm QBER} = p_{\rm opt} + \frac{p_{\rm dark}}{2t_{\rm link}\eta\mu}, \tag{2}$$

where $p_{\rm opt} = (1 - V/2)$, with V being the visibility, $p_{\rm dark}$ is the dark count probability of the single-photon detectors, $t_{\rm link} = 10^{-\alpha L/10}$, with α being the fiber losses [dB/km], and L the fiber length [km], and η is the quantum efficiency of the single-photon detectors.[16]

The general formula for the mutual information between Alice and Eve can be written as,

$$I_{\rm AE} = 1 - h(x), \tag{3}$$

where x corresponds to Eve's measurement error, and

$$h(x) = x\log_2\left(\frac{1}{x}\right) + (1-x)\log_2\left(\frac{1}{1-x}\right). \tag{4}$$

For BB84 protocol, assuming optimal individual attack strategy, the parameter x is given by,[25]

$$x = \frac{1}{2} - \sqrt{{\rm QBER}(1-{\rm QBER})}. \tag{5}$$

For B92 protocol we assume that Eve has unlimited technological resources. At the same time, since the angle of the encoding bases, α, is a continuous parameter, we are choosing it to be 45° in order to maximize Eve's knowledge about transmitted qubits. We are choosing $\alpha = 45°$, since if $\alpha = 0°$ we are not able the estimate the error rate precisely, and if $\alpha = 90°$ the system is extremely sensitive to noise. Using optimal individual strategy, the parameter x in B92 is written as,[26]

$$x = \frac{1 - \sqrt{1 - (1 - |{\rm QBER}|)^2}}{2}. \tag{6}$$

In Fig. 4, we show the mutual information between Alice and Bob and between Alice and Eve as a function of the channel transmission length and the QBER, both for BB84 and B92 quantum protocols. The parameters

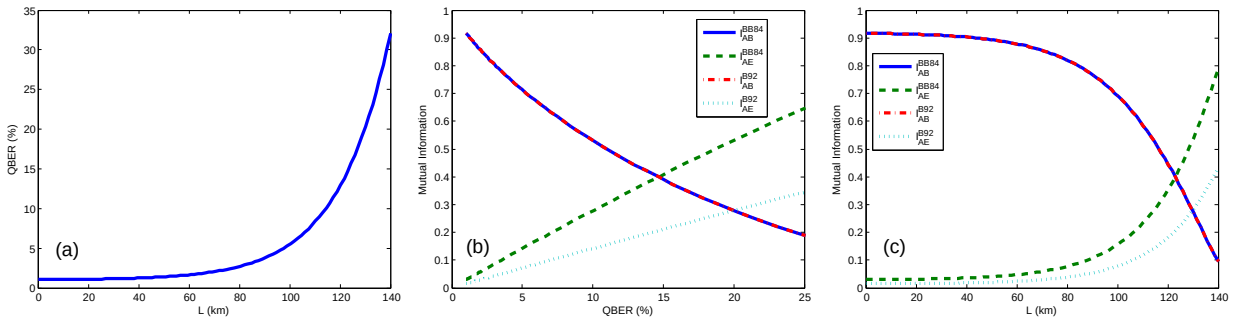

Figure 4. (a) QBER as a function of the fiber length; and mutual information between Alice and Bob and between Alice and Eve as a function (a) of the QBER and (b) the channel transmission length.

used to plot Fig. 4 are shown in Table 1.

Table 1. Parameters used to plot Fig. 4.

Parameter	Value
μ	0.1
α	0.21
η	0.07
p_{dark}	5×10^{-6}
V	0.98

As we can see from Fig. 4(a), the measured QBER exponentially increases with the channel length. That result is very intuitive, since the main contribution to QBER comes from the properties of transmission media (its channel length). On the other hand, the mutual information between Alice and Bob, I_{AB} decreases with QBER, due to the fact that if the QBER is higher, less is the information that Bob get after his measurement. Also, the mutual information between Alice and Bob, I_{AE} increases with QBER, since the higher QBER indicates that EVE has stolen more information. This is illustrated on Fig. 4(a). Finally, the dependency of mutual information from channel length, shown in Fig. 4(c), is the simple consequence of Fig. 4(a) and Fig. 4(b).

3. DYNAMIC POLARIZATION CONTROL

As we have said in previous section, the control of polarization in real time can be performed through the use of an EPC. This type of controller has the advantage of enabling programming. Despite the few options available on market, for example,[27] we chose PolaRITE III$^{\text{TM}}$, from General Photonics to do our tests.[28] This type of controller comprises a fiber squeezer that rotates around the optical fiber and applies a pressure on it, to produce a linear birefringence. In fact, the retardation of the waveplates varies with the pressure. The scheme of this type of controller can be seen in Fig. 5.

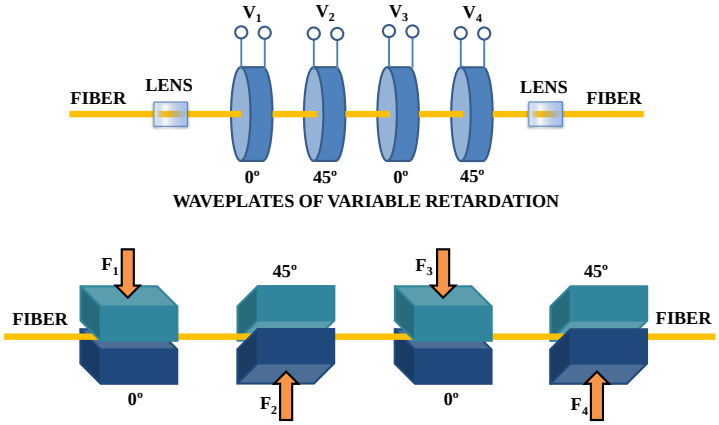

Figure 5. Scheme of PolaRITE III$^{\text{TM}}$ (adapted from[29]).

In order to characterize the EPC, we have determined the variation of its waveplates as a function of the applied voltage, by using the experimental setup shown in Fig. 6. The experimental setup is composed of a laser, a manual polarization controller (PC-1), two linear polarizers (LP-1 and LP-2), and a power meter. Between the two LPs we inserted the EPC, which can be controlled through a computer that runs a LabVIEW$^{\text{TM}}$ program in order to set the voltage of the waveplates.

We started by setting the angle of LP-1 and LP-2 as 0°, and changed the voltage from 0 to 4095 bits (this scale has a correspondence from 0 to 150 V), registering the output power. Next, we kept LP-2 at 0°, set LP-1 to 45° and performed the same measurements. The behavior of each waveplate is shown in Fig. 7. Regarding Fig. 7, a periodic behavior can be observed for each waveplate. This means that we can set a limited range for

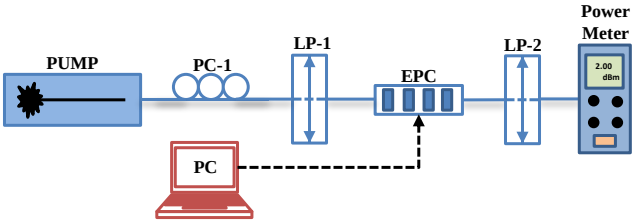

Figure 6. Scheme of experimental setup used to measure the variation of the waveplates as a function of the voltage.

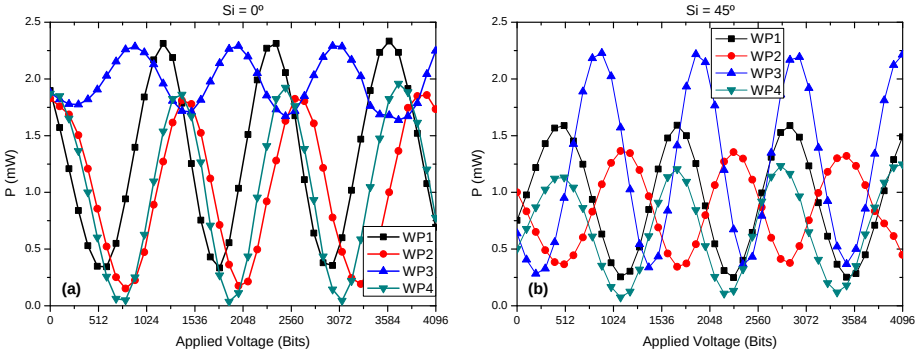

Figure 7. Waveplate behavior as a function of the applied voltage, for (a) LP-1 = 0° and (b) LP-1 = 45°. The LP-2 = 0° for both figures. The step used was 100 bits.

control, instead of using all the scale, from 0 to 4095 bits, which will allow us to increase the working speed. In other words, we can use only $1/4^{th}$ of the scale to achieve polarization control efficiency.

From the behavior of the waveplates we can induce a simplified equation,

$$P = \frac{A}{2}\left[1 + \cos(2\alpha)\cos(\tfrac{7}{2}(\beta - V))\right], \tag{7}$$

where A is the amplitude, α is the ellipticity of the state of polarization (SOP), β is the orientation of the semi-major axis of the ellipse, and V is the applied voltage in the waveplates of the EPC. The variation of the waveplates as a function of the applied voltage is shown in Fig. 8. In Fig. 9 is shown the waveplates behavior as

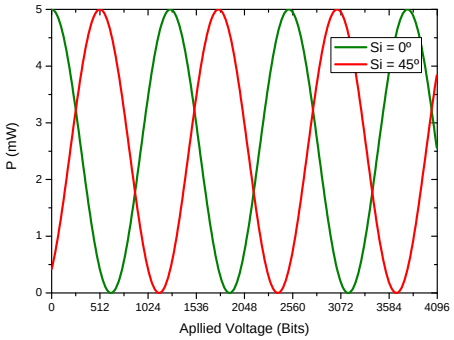

Figure 8. Theoretical behavior for the waveplates as a function of the applied voltage, obtained from Eq. (7).

a function of the applied voltage and the fit using Eq. (7).

Although these devices have their main applications in classical communications, they can also be used for quantum communications, where the number of photons involved is very small. The use of such devices was shown for example in.[17,18] As main advantages of the Polarite III^{TM} EPC, we have the plug and play versatility, the low insertion loss and low cost, the small size, or wavelength insensitivity. As main limitation, PolaRITE

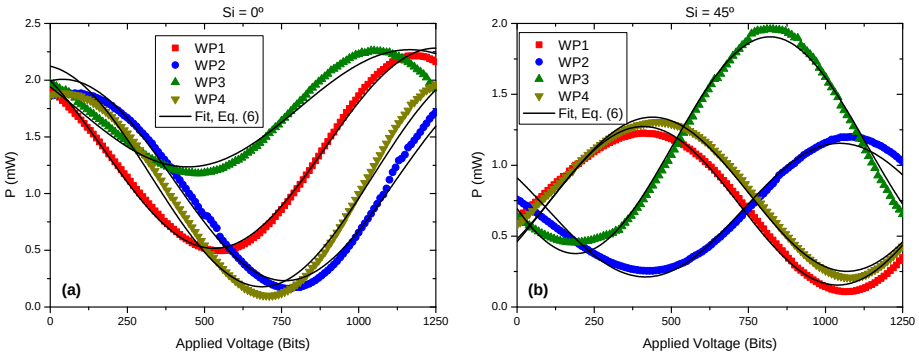

Figure 9. Waveplate behavior as a function of the applied voltage, for (a) LP-1 = 0° and (b) LP-1 = 45°. The LP-2 = 0° for both figures. The step used was 10 bits.

III^{TM} has a relatively high response time, of about 65 μs, which corresponds to only a few kHz, of repetition rate. However, other types of EPCs, as the one from EOSPACE Inc.,[30] allows to achieve tens of MHz, depending on the quality of programming.

4. CONCLUSIONS

Since its proposal (29 years ago), QKD have achieved great maturity and also some very important and prolific results. Only 5 years after the theoretical proposal, QKD was first demonstrated in free-space, and 4 years later in optical fibers. Meanwhile, numerous protocols were proposed, and QKD has even reached commercial level. On photons generation and detection, several proposals were already presented and demonstrated. In order to achieve continuous operation on polarization-encoding-based QKD, two methods were already presented, and good results were demonstrated. The use of EPCs provides a simple solution, which can be used as a plug and play scheme. In this work, we characterized PolaRITE III^{TM} EPC in terms of the behavior of its waveplates, both theoretically and experimentally. EPCs present several advantages, such as low insertion loss or wavelength insensitivity, and may allow also an high repetition rate. On their limitations, some of them present low repetition rate, and need high level programming in order to achieve a proper repetition rate. Nonetheless, polarization-encoding schemes are still up to date, and may allow a good performance with the aim to achieve the global quantum network.

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 and SFRH/BD/63958/2009, the Post Doctoral Grant SFRH/BPD/77286/2011, and by the FCT and the European Union, EU-FEDER - Fundo Europeu de Desenvolvimento Regional, through project PTDC/EEA-TEL/103402/2008 (QuantPrivTel), by the FCT and the Instituto de Telecomunicações, under the PEst-OE/EEI/LA0008/2011 program, project 'P-Quantum', and by the Conselho de Reitores das Universidades Portuguesas (CRUP) project 'Ação Integrada E 91/12'. The authors also thank Eng. João Prata, from the Instituto de Telecomunicações, Aveiro, for the help in the assembling of the EPC.

REFERENCES

[1] Brassard, G., "Brief History of Quantum Cryptography: A Personal Perspective," in [*Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop on*], 19–23 (Oct. 2005).

[2] Bennett, C. H., Brassad, G., Breidbard, S., and Wiesner, S., "Quantum Cryptography, or Unforgeable Subway Tokens," in [*Advances in Cryptology: Proceedings of CRYPTO '82*], 267–275 (1982).

[3] Wiesner, S., "Conjugate coding," *written circa 1970 and later published in Sigact News* **15**(1), 78–88 (1983).

[4] Bennett, C. H. and Brassad, G., "Quantum cryptography: Public-key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* , 175–179 (Dec. 1984).

[5] Bennett, C. H. and Brassad, G., "The dawn of a new era for quantum cryptography: The experimental prototype is working!," *Sigact News* **20**(4), 78–82 (1989).

[6] Ekert, A. K., "Quantum cryptography based on Bell's theorem," *Physical Review Letters* **67**, 661–663 (Aug. 1991).

[7] Huttner, B., Imoto, N., Gisin, N., and Mor, T., "Quantum cryptography with coherent states," *Physical Review Letters* **51**, 1863–1869 (Mar. 1995).

[8] Bruß, D., "Optimal Eavesdropping in Quantum Cryptography with Six States," *Physical Review Letters* **81**, 3018–3021 (Oct. 1998).

[9] Hwang, W.-Y., "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Physical Review Letters* **91**, 057901 (Aug. 2003).

[10] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K., "Quantum entanglement," *Reviews of Modern Physics* **81**, 865–942 (Apr. 2009).

[11] Eisaman, M. D., Fan, J., Migdall, A., and Polyakov, S. V., "Invited Review Article: Single-photon sources and detectors," *Review of Scientific Instruments* **82**, 071101 (July 2011).

[12] Muller, A., Breguet, J., and Gisin, N., "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km," *Europhysics Letters* **23**, 383–388 (Aug. 1993).

[13] Breguet, J., Muller, A., and Gisin, N., "Quantum Cryptography with Polarized Photons in Optical Fibres: Experiment and Practical Limits," *Journal of Modern Optics* **41**, 2405–2412 (Dec. 1994).

[14] Almeida, Á. J., Silva, N. A., Muga, N. J., and Pinto, A. N., "Single-Photon Source Using Stimulated FWM in Optical Fibers for Quantum Communication," in [*Proc. SPIE 8001*], 80013W (May 3, 2011).

[15] Almeida, A. J., Carneiro, S. R., Silva, N. A., Muga, N. J., and Pinto, A. N., "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).

[16] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," *Reviews of Modern Physics* **74**, 145–195 (Mar. 2002).

[17] Xavier, G. B., Walenta, N., Vilela de Faria, G., 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 Journal of Physics* **11**, 045015 (Apr. 2009).

[18] 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 Journal of Physics* **11**, 065004 (June 2009).

[19] Tomita, A. and Chiao, R. Y., "Observation of Berry's topological phase by use of an optical fiber," *Physical Review Letters* **57**, 937–940 (Aug. 1986).

[20] Muga, N. J., Nolasco Pinto, A., Ferreira, M. F. S., and Ferreira da Rocha, J. R., "Uniform Polarization Scattering With Fiber-Coil-Based Polarization Controllers," *Journal of Lightwave Technology* **24**, 3932–3943 (Nov. 2006).

[21] 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).

[22] Silva, N. A., Almeida, Á. J., and Pinto, A. N., "Interference in a Quantum Channel Due to Classical Four-Wave Mixing in Optical Fibers," *IEEE Journal of Quantum Electronics* **48**, 472–479 (Apr. 2012).

[23] Almeida, Á. J., 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* **285**, 2956–2960 (June 2012).

[24] `http://www.idquantique.com`;`http://qlabsusa.com`;`http://aureatechnology.net`.

[25] Assche, G. V., [*Quantum cryptography and secret-key distillation*], Cambridge University Press (2006).

[26] Levitin, L. B., [*Quantum Communication and Measurement*], Plenum, New York (1995).

[27] `http://www.generalphotonics.com`;`http://www.eospace.com`;`http://phoenixphotonics.com`.

[28] `http://www.generalphotonics.com/pdf/PCD-M02.pdf`.

[29] Yao, S., [*Polarization in fiber systems: squeezing out more bandwidth, in The Photonics Handbook (Laurin Publishing, Pittsfield, MA, 2004)*] (2004).

[30] `http://www.eospace.com/polarization_controller.htm`.