Quantum Cryptography in Optical Fibers

Nuno Alexandre Silva

Abstract **–In this work it is discussed recent developments in the field of quantum cryptography in optical fibers. It is presented several quantum protocols for quantum key distribution, and it is also described the implementation of quantum key distribution with single and entangled photon pairs. Is analysed the quantum key distribution with single photons obtained from weak coherent laser pulses, and it is presented a fine alternative based on the stimulated four-wave mixing in optical fibers. This review provides a state of the art on the field of quantum cryptography in optical fibers.**

Keywords **– Optical fiber communication, quantum communications, quantum cryptography, quantum key distribution, single photon source, quantum entanglement, cryptographic protocols.**

I. INTRODUCTION

The increasing dependence of today's society on the telecommunications networks has made security one of the central issues in modern communications systems. The amount of Internet traffic transmitted over optical fibers has seen an enormous surge over the last decade [1]. This increase is likely to continue considering the demand for a greater variety of services and faster download rates [1]. In our increasingly networked world, both the business and government sectors have ever-more demanding secure communications needs [1]. Current communication security protection schemes, encoding protocols, are based on the limited computational power to solve complex problems. Any of that encoding protocol can, in principle, becomes available. Already in 2005 was announced the factorization of the 193-digit number, used in the public-key cryptographic algorithm RSA-640 [2]. That algorithm it became obsolete. The continuous increase of computation power, Moore's law, and the number of networked computers will enable to factorize numbers with more digits and more rapidly [3]. There exists one particular scheme that is not vulnerable to such scenario, the one-time pad protocol, proposed by C. Shannon in 1949. However, that protocol requires that the plaintext is combined with a random key that is as long as the plaintext and used only once, which makes little practical [3]. In this context the quantum cryptography, mainly the quantum key distribution (QKD), emerges as a practical solution to encode and transmit secure information between two places [4].

Quantum information is an area of science that explores the quantum physical properties to code, transmit, store and process information [1]. Nowadays, this area has attracted enormous interest due to the potential applications, such as computation and quantum cryptography [5]. Quantum cryptography is the first technology in the area of quantum information that is in the process of making the transition from purely scientific research to an industrial application. There are currently companies offering commercial quantum cryptography systems, whereas several others also have active research programmers on this information area [4].

Quantum cryptography is a way of generating and sharing a secret key that can be used to encrypt and decrypt messages. Moreover, it allows to detect the presence of any eavesdropper during the process of sharing the secret key between the two users [4]. The first idea of using the laws of quantum mechanics to create a system of encoding messages appears in 1970 by Wiesner [6]. However only in 1984 has been proposed the first protocol for quantum cryptography by Charles H. Bennett and Gilles Brassard [7]. That protocol is known as BB84, and it is the most usual in quantum cryptography systems. The security of this protocol is assured by the impossibility of measure a quantum system without disturbing, the Heisenberg uncertain principle [4]. Typically, in quantum cryptographic systems the information that we want to transmit is encoded in the quantum properties of single photons, such as polarization or phase [4]. Nowadays, in optical fibers, it is possible transmit information encoded in the phase of single photons through distances until 250 km [8], whereas for polarization encoded photons it is possible achieved distances until 50 km [9]. Currently, exist an effort of international of the scientific community in order to establish the first network operating on a global scale of quantum key distribution [10].

A fine alternative to the QKD with single photons in optical fibers is the quantum cryptography with entangled photon pairs. In 1991, Artur Ekert proposed that the QKD was implemented with entangled quantum states [11]. In that configuration the information is encoded in one of the degrees of freedom of the entangled photon pairs, such as the polarization [11]. In optical fibers the entangled photon pairs can be obtained through the spontaneous four wave mixing process (FWM) [12]. In 2004, was tested the first prototype of QKD with entangled photon pairs in a real scenario in Vienna, Austria [13]. Nowadays, in optical fibers it is possible transmit polarization entangled photon pairs over 100 km [14].

This paper reviews recent progress in the field of quantum cryptography in optical fibers. It is presented a comparison between various schemes and protocols of QKD. This paper contains five sections. In section II it is presented the BB84, B92 and the Ekert protocols for polarization encoding schemes. Section III describes the implementation of these quantum protocols in optical fibers with single photons. In section IV it is discussed the implementation of the

Ekert protocol in optical fibers with entangled photon pairs. Section V summarizes the work present in this paper.

II. POLARIZATION ENCODING SCHEME FOR QKD

The first protocol for quantum communications was proposed by Charles H. Bennett and Gilles Brassard, the BB84 [7]. In that protocol two users, typically known as Alice and Bob, wants to create a random key, which should remain completely secret to a third user who eavesdrop on their communication channel. For polarization encoding scheme, the BB84 protocol, Table I, uses four polarization states that constitute two different bases, one rectilinear (+) and another diagonal ($\times$).

In the first step, Table I, over a quantum channel, Alice sends to Bob individual photons in states chosen random among the four states, $\rightarrow$, $\uparrow$, $\nearrow$ and $\searrow$ corresponding to linearly polarization states 0°, 90°, +45° and -45°, respectively. In this step Alice can also attribute the binary value 0 for example to $\{\uparrow,\nearrow\}$ and the value 1 to $\{\rightarrow,\searrow\}$ [7], [15]. Next Bob measure the incoming polarized photons in one of the two bases, chosen randomly. After Bob has measured all the photons, he tells Alice which basis he used for measure each incoming photon. Alice tells Bob which bases are correct, and they keep only the data from these correctly measured photons. The last two steps, the public discussion, are performed over a classical communication channel. The outcome binary string is the secret key that Alice and Bob can use to share secret information [7], [15]. The presence of an eavesdropper (Eve) in the communication channel, can also be tested using a subset of the photons on which both Alice and Bob publicly agree reveal the polarization of the photons sent by Alice and the result of Bob measurement. The presence of the eavesdropper is discovery, due to the fact that whenever Eve makes a measurement Eve changes the quantum state of the photon sent by Alice. Therefore, when Bob receives the photon, he obtains an erroneous bit value even when he and Alice use compatible bases. Comparing the photon polarization sent by Alice and the Bob measurement result it is possible discovery the presence of an eavesdropper in the communication channel [7], [15], [4]. The security of the protocol is based in three fundamental principles of the quantum mechanics, the non-cloning theorem, the uncertain principle, and the impossibility of discriminating deterministically between two non-orthogonal quantum states [4].

In 1992, Charles Bennett proposed what is essentially a simplified version of the BB84, the B92 quantum protocol [16]. In [16] Bennett refers that for implement a system of quantum key distribution it is not necessary four quantum states, but only two non-orthogonal states. Indeed the security of the B92 quantum protocol relies on the inability of an eavesdrop to distinguish unambiguously and without perturbation the different states sent by Alice to Bob [16], [4]. In this protocol the binary value 0 can be attributed to the 0° photon polarization state, whereas value 1 can be attributed to the 45° state of polarization, as shown in Fig. 1. As in BB84, Table I, Alice transmit to Bob a string of polarization encoded photons with randomly chosen bits. However, in this protocol Alice chooses dictates which bases she must use. Bob chose randomly one of the two bases for measurement, rectilinear or diagonal. However, if Bob choose a wrong basis, he will not measure anything, a condition which in quantum mechanics is known as erasure [17]. In the public discussion, Bob can simply tell Alice after each bit she sends whether or not he measured is correctly. Although this protocol is simpler to implement than BB84, in practice it is not a good solution due to security problems. Although two non-orthogonal states can not be distinguished unambiguously without perturbation, Eve can unambiguously distinguish them at the cost of some losses present in the quantum channel [4]. This possibility has been demonstrated in practice [18]. This mean that to ensure a high security level in the quantum channel to implement this protocol, both Alice and Bob would have to monitor the attenuation of the quantum channel. However, if Eve were able to replace part of the quantum channel by a more transparent (with less losses) the channel loss monitoring is not enough. In that case, beyond the single photon source in the quantum channel, must be also present in the same channel a bright pulse. In this case Bob can monitor the bright pulses to make sure that Eve does not remove any part of the quantum channel [16], [4].

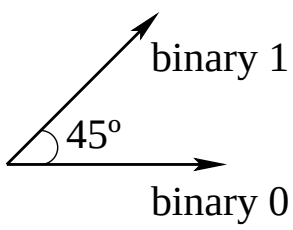

Fig. 1 - Polarization scheme for the B92 quantum protocol.

In 1991 Artur Ekert contributed a new approach to quantum key distribution. Instead using single photons Ekert proposed that QKD be implemented using quantum entangled states [11]. Entanglement is the non-local quantum mechanical correlation that can exist between two quantum systems that have interact at some point [19]. The idea consists in replacing the quantum channel aforementioned, where Alice sends single polarized photons to Bob, by a channel where there is a common source that emits pairs of entangled particles, such as polarized photons in the same state chosen randomly among the four states of the BB84 protocol [4]. That particles are separated and Alice and Bob receive a single photon from each entangled photon pairs. At this point, when both Alice and Bob receives their photons from the source, they measure their particle in one of the two bases, chosen randomly and independently. The source then announces the bases, and Alice and Bob keep the data only when they happen to have made their measurements in the compatible basis. In this possibility, this protocol is equivalent to that of BB84 [4]. The security of the Ekert protocol is based on the Bell's inequality. The Bell's inequality demonstrates that some correlations predicted by quantum mechanics can not be reproduced by any local theory [19].

TABLE I
BASIC BB84 QKD PROTOCOL FROM REF. [7].

Alice's random bits	0	1	1	0	0	0	1
Alice's random	+	+	×	+	×	×	+
Photons sending Alice	↑	→	↘	↑	↗	↗	→
Bob random bases	+	×	×	×	×	+	+
Bob's measurements	↑	↗	↘	↗	↗	→	→
Public discussion							
Bob reports the bases	+	×	×	×	×	+	+
Alice says which are correct	✓		✓		✓		✓
Outcome	0		1		0		1

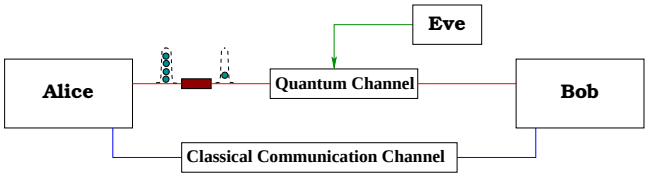

Fig. 2 - QKD with single photons obtained from attenuated laser pulses and transmitted via a quantum channel (optical fiber) from Alice to Bob. Bob measure the polarization of the arriving photons in one of the two bases. Through the classical communication channel (public discussion) they keep only those correctly measured photons, and they are able to establish a key.

III. QKD WITH SINGLE PHOTONS

Experimental quantum key distribution was demonstrated for the first time in October 1989, over a distance of 32 cm free air optical path [15], [20]. Since then, tremendous progress has been done. Nowadays it is possible implement a quantum channel over a distance of 250 km in optical fiber, using phase encoding scheme [8]. Information can be encoded in the quantum states of photons in several ways. Encoding in the polarization is a natural solution. In the first experimental solution Bennett and co-workers made use of this choice [15], [20]. However, in single-mode fibers the random polarization inside the fiber, polarization effects, is a common source of problems in all optical communication schemes [21], [22]. All fiber-based implementations of QKD have to face this problem, even the phase-based systems, since interference visibility depends on the polarization states [4]. Compared with phase-encoding, polarization encoding needs no precise active modulation to overcome the instability and error rate caused by the phase shift in fibers [9]. It can be easily implemented in a "one way" fiber system with the decoy-state QKD protocol to enhance its security in the lossy transmission channels [9]. Nevertheless, the polarization encoded QKD suffers from random fluctuation of polarization in a long-distance fiber. It is necessary to have a robust and efficient control on the polarization of the signal photons in the fiber. To implement polarization-encoded QKD systems it is need compensate passively or actively the random fluctuation of polarization in the fiber [9], [23], [24].

A typical quantum communication system with the B92 protocol using the polarization of the photons is shown in Fig. 3 [23]. Alice's system consists of one laser, that emit short classical photons that are polarized at 0° or 45° degrees, controlled by the electrical polarizer R_A [23]. The pulses are then attenuated and sent along the quantum channel, optical fiber. It is essential that the pulses remain polarized for Bob to be able to extract the information encoded by Alice. However, as aforementioned the random rotation of the state of polarization inside the fiber may depolarize the photons [23]. To avoid this, Alice and Bob implement two classical control channels LD_1 and LD_3, and uses the electrical polarizers R_1 and R_3 to compensate the random rotations of the polarization inside the fiber [23]. With this system they monitor the polarization fluctuations in the fiber, and can invert the transformation induced by the optical fiber. The arriving single photons at the Bob side are analyzed in the polarizer R_B, which randomly chose one of the two polarization bases, diagonal or rectilinear [23]. With this scheme they, Alice and Bob, are able to establish a secret key using polarization encoded photons.

Optical quantum cryptography is based on the use of single-photons. Unfortunately, single-photons sources are difficult to realize experimentally [4]. Single-photon sources as quantum dots [25] or excitation of nitrogen vacancy centers in diamond [26] carry another problem that is the photon coupling into the fiber. Nowadays, practical implementations of QKD systems uses faint laser pulses, as source of single-photons [4], see Fig 2. This photon source can easily be realize using only standard semiconductor lasers and calibrated attenuators. This configuration allow obtain coherent states with an ultra low mean photon number μ [4]. This source of photons obey a Poisson statistics, and the probability of obtain n photons is

$$P(n,\mu) = \frac{\mu}{n!}e^{-\mu}\,, \tag{1}$$

and the probability that a non-empty pulse contains more than one photon is

$$P(n>1) = \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}}\,. \tag{2}$$

The attenuator can made $P(n>1)$ very small. However, when μ is small most of the pulses are empty, does not contain any photon. Most of the experiments relied on $\mu = 0.1$, meaning that 5% of the non-empty pulses contain more than one photon [4]. However, the optimal value of μ depends on the optimal losses in the quantum channel, and on assumptions about eavesdrop's technology [27].

The photon loss in the quantum channel, optical fiber,

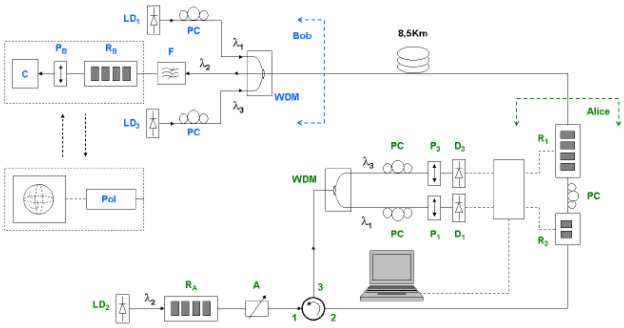

Fig. 3 - Typical system for quantum cryptography using polarization coding in optical fiber (From Ref. [23]). Experimental set-up: PC: Manual polarization controllers, R: Electrically driven polarization controllers, P: Polarizers, F: Filter, D: Classical photodetectors, C: Single photon counting module, LD: Laser diodes, A: Attenuator, Pol: Polarimeter.

limits also the distance over which the quantum cryptographic system can be applied. For this reason, the best performance in optical fibers is achieved using photons with wavelength of 1550 nm [21]. In this spectral window the standard optical fibers are relatively transparent, with only a loss of $\alpha \approx 0.2$ dB/km.

The success of a quantum cryptographic system essentially depends on the capability of detecting single photons. In principle the detection of single photons can be achieved using many techniques [4]. Nowadays the best choice is avalanche photodiodes (APD's). APDs are usually operated in the so-called Geiger mode. In this mode, the applied voltage exceeds the breakdown voltage, leading an absorbed photon to trigger an electron avalanche consisting of thousands of carriers. In the 1550 nm spectral window the APD's are made from InGaAs/InP [4]. In this spectral region, this kind of APD's present a quantum efficiency of approximately 10% and a dark count rate of 10^{-5}, for a operating temperature of 220 K [28].

Due to the difficulty of obtain pulses of single photons, the authors in [29], [30] analyze the possibility of generating single photons inside optical fibers through stimulated four-wave mixing (FWM) process. In this configuration the single photon source is an optical power, see Fig 4. FWM is a nonlinear process described by the third order nonlinear response function of the fiber, $R^{(3)}_{ijkl}$ [21]. This nonlinear process occurs when two (or more) frequencies (known as pump and signal fields) are launched into an optical fiber, giving rise to a new frequency, known as idler wave. In quantum mechanical terms, FWM occurs when two photons from the pump field are annihilated and two new photons are created, one at the idler frequency and another in the signal field [21]. The number of photons that are created in the idler wave is dependent of the pump and signal power and their wavelength separation, $\lambda_p - \lambda_s$. Efficient generation of the idler wave also requires that the phase matching condition $\Delta\beta$ is achieved. The average number of the photons that are created through stimulated FWM inside the fiber in the idler wave is given by [29], [30]

$$\langle n \rangle = P_i \frac{\lambda_i T_g}{hc} 10^{-\alpha_d/10}\,, \tag{3}$$

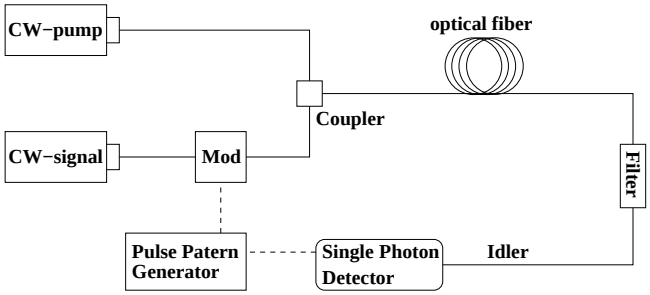

Fig. 4 - Single photon source based on stimulated FWM inside an optical fiber (From Ref. [29]).

where P_i represents the idler power at the exit of the fiber, T_g is the time during which the gate of the single detector photon is open, h is the Planck constant, c is the speed of light in vacuum and α_d is the attenuation, in decibels, from the fiber output to the single photon detector, see Fig. 4. The idler power at the end of the photon source (optical fiber) is given by [29]

$$P_i = (\gamma L_{eff} P_p)^2 P_s e^{-\alpha L} \left| \frac{\sinh(\kappa L)}{(\kappa L)} \right|^2 , \tag{4}$$

where γ is the nonlinear parameter of the fiber, α is the fiber losses, L is the length of the photon source, P_p and P_s are the pump and signal powers, respectively. In (4)

$$L_{eff} = \frac{1 - e^{-\alpha L}}{\alpha}\,, \tag{5a}$$

$$\kappa = \sqrt{\frac{\Delta\beta}{2}\left(\frac{\Delta\beta}{2} + 2\gamma P_p \frac{L_{eff}}{L}\right)}\,. \tag{5b}$$

A schematic of the experimental setup is show in Fig. 4. In the experimental setup, Fig. 4, a pump, λ_p from a DFB laser source operating in a continuous mode is coupled to another optical signal, λ_s from a tunable laser source, that is modulated externally to produce optical pulses with a width at half maximum of approximately 1.6 ns and repetition rate of 610.3 kHz. The two optical fields are launched into a dispersion-shifted fiber (DSF), with incident powers P_p and P_s for pump and signal fields, respectively. The DSF has a dispersion slope at zero-dispersion wavelength $dD_c/d\lambda = 0.069$ ps/nm^2-km, length $L = 8865$ m, zero-dispersion wavelength $\lambda_0 = 1547.34$ nm, attenuation $\alpha_{dB/km} = 0.2$ dB/km and nonlinear coefficient $\gamma = 2.36$ W^{-1}km^{-1}. At the fiber output, a filter blocks the pump and signal waves. The idler wave, $\lambda_i = \lambda_p\lambda_p/(2\lambda_s - \lambda_p)$, passes through the filter and reaches a single-photon detector [29]. The single-photon detector is based on an APD, operating in the so-called Geiger mode, being $T_g = 2.5$ ns the time during which the gate of the detector is open. The detector quantum efficiency is $\eta_{det} = 10\%$ and the dark count probability per gate is $Pr_{dc} = 5 \times 10^{-5}$. The Noise Equivalent Power of the detector is NEQ $\approx 2.56 \times 10^{-16}$ W/$\sqrt{\text{Hz}}$, and the probability of having a count when a single-photon reaches the detector compared with the probability of having a count due to the dark counts is $Pr_{eff} = 5\times10^{-4}$ [28].

TABLE II
AVERAGE NUMBER OF IDLER PHOTONS PER PULSE VERSUS SPECTRAL SPACING BETWEEN PUMP AND SIGNAL FIELDS

$\lambda_p - \lambda_s$ nm	$\langle n \rangle$	$\lambda_p - \lambda_s$ nm	$\langle n \rangle$
1.251	3.034	5.626	0.821
1.65	3.016	6.022	0.559
2.049	2.959	6.418	0.320
2.447	2.894	6.814	0.164
2.845	2.673	7.210	0.064
3.243	2.525	7.606	0.025
3.640	2.308	8.001	0.051
4.038	2.071	8.397	0.102
4.435	1.778	8.792	0.107
4.832	1.401	9.186	0.115

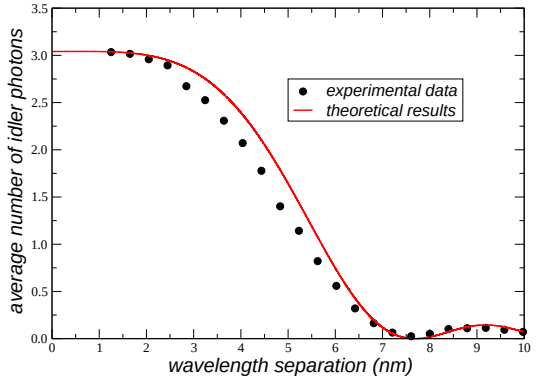

Fig. 5 - Average number of idler photons generated by FWM as a function of wavelength separation between pump and signal fields (From Ref. [30]). The circles represents the measured optical power, the line represents the theoretical model given by (3) and (4).

In the experiment performed the estimation of $\langle n \rangle$ using a measurement period of 20 s. The average number of idler photons that reaches to the single-photon detector is given by [31], [32]

$$\langle n \rangle = \frac{1}{\eta_{det}} \ln \left(\frac{Pr_{dc} - 1}{Pr_{av} - 1} \right) , \qquad (6)$$

where Pr_{av} is the probability of avalanche per gate.

In Table II is presented the average number of idler photons generated through stimulated FWM process as a function of the spectral spacing between pump and signal fields. From the results present in Table II, we can see that FWM in optical fibers can produces single-photons that can be used for QKD systems. It can also be seen that the average of idler photons can be increased or diminished by simple adjusting of the signal detuning.

In Fig. 5 it is plotted the average number of idler photons as a function of the wavelength separation between pump and signal fields

From Fig. 5 we can see that for $\lambda_p - \lambda_s < 2.8$ nm the theoretical model given by (3) and (4) describes correctly the

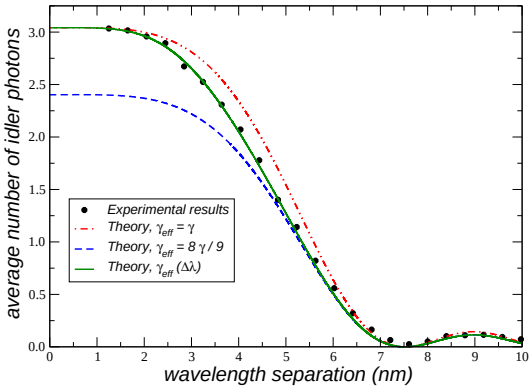

Fig. 6 - Average number of idler photons generated by FWM as a function of wavelength separation between pump and signal fields for three different values of γ_{eff}.

experimental results. However, for 2.8 nm $< \lambda_p - \lambda_s <$ 5 nm the theoretical models and the experimental data does not coincide [29]. That difference between the theoretical model and experimental data can be understood in terms of polarization effects that occurs during the generation of the idler photons inside the optical fiber. It is known that the efficiency of the FWM process is dependent of the relative polarization of pump and signal fields [21]. In the results presented in Fig. 5, we can see that with the increase of the wavelength separation between pump and signal, the average number of idler photons measured experimentally is smaller than the theoretical predictions. In the theoretical model, equation (4), it was assumed that all fields remain co-polarized along the propagation in the fiber [29]. However, when the wavelength separation between pump and signal is increased the fields go from an almost co-polarized situation to a decorrelated state of polarization. The loss of efficiency in the FWM process due to the polarization decorrelation can be seen as a reduction of the value of the nonlinear parameter γ. This can be described through a new parameter called effective nonlinear parameter γ_{eff}, which is dependent of the wavelength separation between pump and signal fields [29].

In Fig. 6 it is plotted the average number of idler photons as a function of the wavelength separation between pump and signal fields for three different values of γ_{eff} [29].

The results show that the effective nonlinear parameter is approximately equals to γ for $\lambda_1 - \lambda_2 < 2.8$ nm [29]. However, with the increasing separation between pump and signal fields, the value of γ_{eff} rapidly decreases to $8\gamma/9$, and remains constant for $\lambda_1 - \lambda_2 > 5$ nm. This value for the effective nonlinear parameter is in agreement with theoretical predictions for polarization dependent processes in a strong mode coupling. In order to describe analytically the γ_{eff} variation with the wavelength separation between pump and signal, we fit the result present in Fig. 5 with an hyperbolic secant function given by [29]

$$\gamma_{eff}(\Delta\lambda) = \frac{8\gamma}{9} + \frac{\gamma}{9} \mathrm{sech} \left(\frac{(\Delta\lambda)^{A_0}}{T_0} \right) , \qquad (7)$$

where A_0 and T_0 are the fitting parameters, and $\Delta\lambda = \lambda_p - \lambda_s$ [29]. The results presented in Fig. 6 show that the hyperbolic secant describes correctly the variation of the

$\gamma_{eff}(\Delta\lambda)$ parameter with wavelength separation between pump and signal fields in the transition region 2.8 nm $< \lambda_1 - \lambda_2 <$ 5 nm [29].

Although the polarization effects are very important to describe correctly the single photon source, there is another optical nonlinear effect that was not taken into account in the theoretical model given by (4), the stimulated Raman scattering (SRS). This nonlinear effect becomes quite important as the optical pump, λ_p, reaches the fiber zero-dispersion wavelength λ_0. SRS is third order nonlinear effect that occurs inside an optical fiber. The SRS process in optical fibers is an inelastic scattering process in which energy is transfered between the optical fields and the dielectric nonlinear medium [21]. In this nonlinear process the optical frequencies from the pumps transfer their energy to lower frequencies (Stokes amplification) and to higher frequencies (anti-Stokes amplification), through molecular vibrations [21]. In [33] the authors analyse the influence of SRS on the stimulated FWM process. In that paper, the authors found that the evolution of the optical power of idler wave with the wavelength separation between the pump and signal field is given by [33]

$$\frac{P_i(z)}{P_s(0)} = (\gamma P_p z)^2 \left|\varrho(\Omega_{ip})\right|^2 \left|\frac{\sinh(g(\Omega_{ip})z)}{g(\Omega_{ip})z}\right|^2 . \quad (8)$$

whit

$$g^2(\Omega_{ip}) = (\gamma\varrho(\Omega_{ip})P_p)^2 - (\kappa(\Omega_{ip})/2)^2 , \quad (9a)$$

$$\kappa(\Omega_{ip}) = \Delta\beta + 2\gamma P_p(\zeta(\Omega_{ip}) - 1) , \quad (9b)$$

$$\varrho(\Omega_{ip}) = 1 - f_R + f_R\tilde{R}_a(\Omega_{ip}) + f_R\tilde{R}_b(\Omega_{ip}) , \quad (9c)$$

$$\zeta(\Omega_{ip}) = 2 - f_R + f_R\tilde{R}_a(\Omega_{ip}) + f_R\tilde{R}_b(\Omega_{ip}) \quad (9d)$$

where $\tilde{R}_a$ and $\tilde{R}_b$ are the delayed Raman response of the fiber and f_R represents the fractional contribution of the delayed Raman response to the nonlinear refractive index of the nonlinear dielectric medium [33]. In Fig. 7 and Fig. 8 it is presented the variation of the optical power of the idler wave with the wavelength separation between pump and signal fields.

Results presented in Fig. 7 show that the SRS can increase the optical power of the idler wave when compared with the situation $f_R = 0$, absence of the delayed Raman response. However, when $\lambda_p \neq \lambda_0$, Fig. 8, the difference between the two cases is very slight, due to the fact that in this situation, $\lambda_p \neq \lambda_0$, the most significantly contribution for the efficiency of the FWM arise from the phase matching condition $\Delta\beta$ [33].

The results presented in Fig. 6, Fig. 7 and in Fig. 8 show that a correctly description of the single photon source based on the stimulated FWM process must take into account the polarization effects that occurs in the fiber, as well the delayed Raman response of the nonlinear medium.

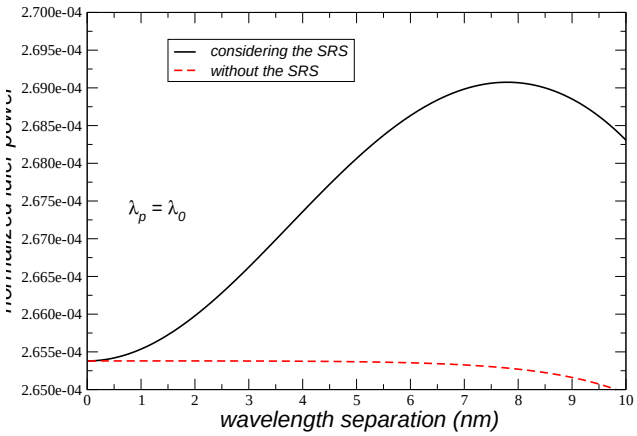

Fig. 7 - Theoretical predictions for the optical power evolution of the idler wave, given by (8) as a function of the wavelength separation between pump and signal for $\lambda_p = \lambda_0$.

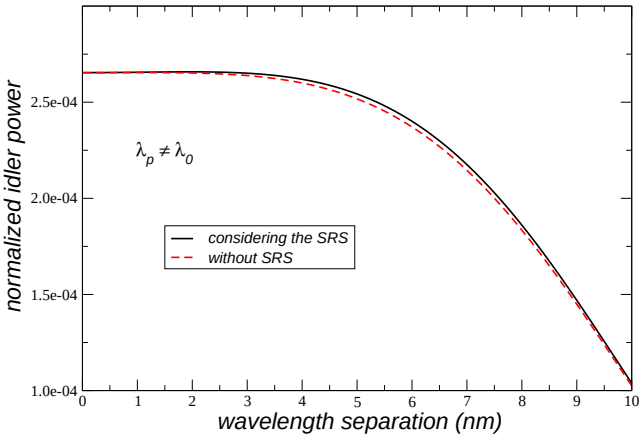

Fig. 8 - Theoretical predictions for the optical power evolution of the idler wave, given by (8) as a function of the wavelength separation between pump and signal for $\lambda_p \neq \lambda_0$.

IV. QKD WITH ENTANGLED PHOTONS PAIRS

In 1991 Ekert proposed that the QKD be implemented using quantum entangled states [11]. One advantage of using photon pairs for QKD is the fact that one can remove empty pulses [4]. Today is well established that photon pairs can be obtained in many sorts of entanglement, as polarization, time and momentum [19]. The essence of the protocol proposed by Ekert is as follows: Alice and Bob can obtain from a source entangled pairs single photons, see Fig. 9. Measuring them one basis, Alice and Bob obtain a string of perfectly (anti)correlated bits, i.e., the key. The key does not exist until the detection process [19]. To verify whether it is secure, they check Bell inequalities on a selected portion of the pairs. If Eve knew the values that Alice and Bob obtained in their measurement, this would mean that the values existed before the measurement, hence Bell's inequalities would not be violated [19], [4].

Experimentally, entangled state quantum cryptography has been first demonstrated in 1999, using polarized entangled photons [34]-[36]. Nowadays, it is possible transmit polarization entangled photon pairs over distances until 100 km [14]. In optical fibers the entangled photon pairs

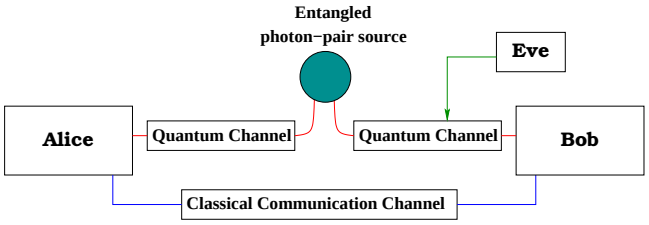

Fig. 9 - QKD with entangled photon pairs obtained from an Einstein-Podolsky-Rosen (EPR) source pulses and transmitted via two quantum channels. Alice and Bob measure the polarization of the arriving photons in one of the two bases. Through the classical communication channel (public discussion) they keep only those correctly measured photons, and they are able to establish a key.

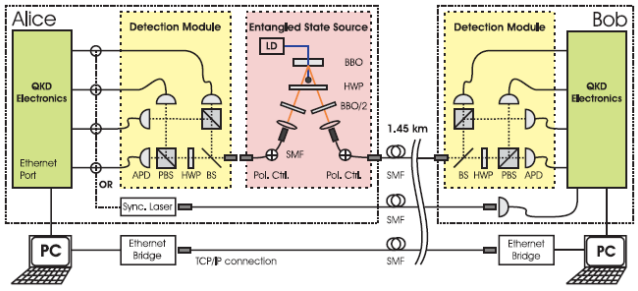

Fig. 10 - Experimental setup used to implement a QKD system with polarization entangled photon-pairs (From Ref. [13]).

can be obtained by parametric processes, such as spontaneous FWM [12], [37]. This nonlinear process create an entangled photon pair, in which each photon as frequency ω_s and ω_i, such that $2\omega_p = \omega_s + \omega_i$. That means that the interaction between two photons of the pump field at ω_p and the fiber create an entangled photon pair. This nonlinear process has been recently studied theoretical and experimental, and the obtained results are very promising [38], [37]. This king of entangled photon source have the advantage of generating the photons already inside the fiber, and in that way avoid the coupling loss.

In this trial field, in 2004 A. Poppe and co-workers presented a quantum cryptographic system that operate in a real-world application scenario [13]. They in that experiment were able to perform a transfer between a bank and the Vienna City Hall, over a distance of 1.45 km of optical fiber [13]. Instead use an optical fiber as source of the polarization entangled photons, they use a nonlinear BBO crystal, due to the fact that the BBO crystal is a more efficient nonlinear medium to create entangled photon pairs. In Fig. 10 it is presented the experimental setup used by A. Poppe and co-workers [13].

In Fig. 10 we can see that an entangled photon source sends one photon to Alice and another to Bob, over an optical fiber [13]. The polarization measurement is done in two non-orthogonal bases, 0° and 45° [13]. The beam splitter (BS) sends randomly the photons to one of the two polarization beam splitters (PBS), at Alice and Bod sides [13]. One of the PBS is defined for measurement in the 0° basis, and the other in the 45° basis. The compensation of polarization rotation in the fibers was done using fiber polarization controllers [13]. Once a photon is detected at one of Alice's four avalanche photodiodes an optical trigger pulse is created (Sync. Laser) and sent over a standard telecommunication fiber to Bob to establish a common time basis [13]. At both sides, the trigger pulses and the detection events from the APDs are fed into a dedicated quantum key generation device for further processing [13].

This pioneer experiment show that it is possible implement a system of QKD in optical fibers with polarization entangled photons. However, must the work related with this trial field remain only in terms of laboratory experiment, due to the high experimental complexity of this configuration for QKD in optical fibers.

V. CONCLUSIONS

In summary, it was presented a selection of recent results of QKD with single and entangled photon pairs, and three different quantum protocols, the BB84, B92 and the Ekert were discussed. In the configuration with single photons it was presented two different sources. A first approach uses photons obtained from a weak coherent laser pulses. A second approach is based on the stimulated FWM process in optical fibers. A theoretical analyse of that source was briefly described, and some experimental results was presented. Results show that the FWM in optical fibers can produces single photons. Moreover, the number of photons produced by FWM can be increased or diminished by simple adjusting the wavelength separation between the pump and signal fields. Results also show that to obtain a correctly description of the FWM in optical fibers it is needed taken into account the polarization effects during the generation of the idler photons and the delayed Raman response. In the configuration with entangled photon pairs it was presented the first real world application scenario. In both configurations, results show that possibility of implement QKD in the current telecommunication systems, mainly the configuration with single photons. The configuration with entangled photons remains nowadays only in terms of laboratory experiments. So far there is no commercial device for QKD based on the quantum Ekert protocol.

REFERENCES

[1] Alexander V. Sergienko, *Quantum Communications and Cryptography*, Crc Press, Florida,USA, 2006.

[2] Eric W. Weisstein, "Rsa-640 factored", url:mathworld.wolfram.com/news/2005-11-08/rsa-640.

[3] P. Lambropoulos and D. Petrosyan, *Fundamentals of Quantum Optics and Quantum Information*, Springer, New York, USA, first edition, 2006.

[4] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar 2002.

[5] Charles H. Bennett and David P. DiVincenzo, "Quantum information and computation", *Nature*, vol. 404, pp. 247–255, 2000.

[6] Stephen Wiesner, "Conjugate coding", *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[7] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: public key distribution and coin tossing", in *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984.

[8] D Stucki, N Walenta, F Vannel, R T Thew, N Gisin, H Zbinden, S Gray, C R Towery, and S Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres", *New Journal of Physics*, vol. 11, no. 7, pp. 075003, 2009.

[9] J Chen, G Wu, L Xu, X Gu, E Wu, and H Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing", *New Journal of Physics*, vol. 11, no. 6, pp. 065004, 2009.

[10] SeCoQC, "Development of a global network for secure communication based on quantum cryptography", url:www.secoqc.net.

[11] Artur K. Ekert, "Quantum cryptography based on bell's theorem", *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug 1991.

[12] M. Fiorentino, P.L. Voss, J.E. Sharping, and P. Kumar, "All-fiber photon-pair source for quantum communications", *Photonics Technology Letters, IEEE*, vol. 14, no. 7, pp. 983–985, Jul 2002.

[13] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons", *Opt. Express*, vol. 12, no. 16, pp. 3865–3871, 2004.

[14] Hannes Hübel, Michael R. Vanner, Thomas Lederer, Bibiane Blauensteiner, Thomas Lorünser, Andreas Poppe, and Anton Zeilinger, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber", *Opt. Express*, vol. 15, no. 12, pp. 7853–7862, 2007.

[15] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental quantum cryptography", *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992.

[16] Charles H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[17] Samuel J. Lomonaco, "A quick glance at quantum cryptography", *Cryptologia*, vol. 23, no. 1, pp. 1–41, 1999.

[18] Roger B. M. Clarke, Anthony Chefles, Stephen M. Barnett, and Erling Riis, "Experimental demonstration of optimal unambiguous state discrimination", *Phys. Rev. A*, vol. 63, no. 4, pp. 040305, Mar 2001.

[19] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki, "Quantum entanglement", *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, 2009.

[20] C. H. Bennett and G. Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working", *SIGACT News*, vol. 20, no. 4, pp. 78–80, 1989.

[21] Govind P. Agrawal, *Nonlinear Fiber Optics*, Academic Press, San Diego, third edition, 2001.

[22] J. P. Gordon and H. Kogelnik, "PMD fundamentals: Polarization mode dispersion in optical fibers", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 97, no. 9, pp. 4541–4550, 2000.

[23] G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding", *Opt. Express*, vol. 16, no. 3, pp. 1867–1873, 2008.

[24] G B Xavier, N Walenta, G Vilela de Faria, G P TemporÃ£o, N Gisin, H Zbinden, and J P von der Weid, "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation", *New Journal of Physics*, vol. 11, no. 4, pp. 045015, 2009.

[25] D C Unitt, A J Bennett, P Atkinson, K Cooper, P See, D Gevaux, M B Ward, R M Stevenson, D A Ritchie, and A J Shields, "Quantum dots as single-photon sources for quantum information processing", *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 7, no. 7, pp. S129, 2005.

[26] David D. Awschalom, Ryan Epstein, and Ronald Hanson, "The diamond age of spintronics", *Scientific American*, vol. 297, pp. 84–91, 2007.

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

[28] id Quantique, "id 200 single-photon detector module", url:www.idquantique.com/products/files/id200-operating.pdf.

[29] Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, "Effective nonlinear parameter measurement using fwm in optical fibers in a low power regime", *To be published on: Quantum Electronics, IEEE Journal of*, 2009.

[30] Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, "Single-Photon Generation", in *ConfTele - 7th Conference on Telecommunications*, Portugal, May 2009.

[31] Alexei Trifonov, Darius Subacius, Audrius Berzanskis, and Anton Zavriyev, "Single photon counting at telecom wavelength and quantum key distribution", *Journal of Modern Optics*, vol. 51, no. 9-10, pp. 1399–1415, 2004.

[32] Mingguo Liu, Chong Hu, Xiaogang Bai, Xiangyi Guo, Joe C. Campbell, Zhong Pan, and M. M. Tashima, "High-performance InGaAs/InP single-photon avalanche photodiode", vol. 13, pp. 887–894, 2007.

[33] N.A. Silva, N.J. Muga, and A.N. Pinto, "Influence of the stimulated Raman scattering on the four-wave mixing process in birefringent fibers", *Lightwave Technology, Journal of*, vol. 27, no. 22, pp. 4979–4988, 2009.

[34] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states", *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4737–4740, May 2000.

[35] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: Eavesdropping on the ekert protocol", *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4733–4736, May 2000.

[36] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, "Quantum cryptography with entangled photons", *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4729–4732, May 2000.

[37] Hiroki Takesue and Kyo Inoue, "Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop", *Physical Review A*, vol. 70, pp. 031802, 2004.

[38] Q. Lin, F. Yaman, and Govind P. Agrawal, "Photon-pair generation in optical fibers through four-wave mixing: Role of raman scattering and pump polarization", *Physical Review A*, vol. 75, pp. 023803, 2007.