QBER Estimation in QKD Systems With Polarization Encoding

Nelson J. Muga, Mário F. S. Ferreira, and Armando N. Pinto, *Senior Member, IEEE*

***Abstract*—A model for quantum BER estimation in polarization encoded quantum key distribution systems is presented. Both TDM and WDM based polarization control schemes are analyzed. It is shown that TDM presents some important advantages when compared with the WDM control scheme. In WDM, the polarization decorrelation between the reference and data signals is an intrinsic and very limitative impairment. This effect has a contribution to quantum BER that increases with the propagation distance, and is highly dependent on the fiber polarization mode dispersion. In the TDM control scheme, the polarization decorrelation is less critical and other issues, like the single photon detector and feedback polarization control system performance tend to dominate. We show that for long distances the fiber losses represent the main contribution to the total quantum BER. Nevertheless, for distances shorter than 70 km and frequencies higher than 5 MHz the after pulse detections provide an important contribution to the total quantum BER.**

***Index Terms*—Optical fiber communication, optical fiber polarization, quantum communication.**

I. Introduction

Quantum key distribution (QKD) uses the laws of quantum mechanics in order to assure an unconditional secure distribution of secret keys between two parties [1]. The first QKD protocol was developed in 1984 by Bennet and Brassard [2] and, height years later, Bennett *et al.* [3] have reported the first QKD experiment using a 32-cm free-space transmission line. Since that pioneer work, several new experiments were presented and nowadays it is possible to share quantum information through telecom fibers for distances of the order of tens kilometers [4], [5]. The implementation of QKD protocols (for instance BB84 [2], or B92 [6]) can be performed encoding quantum bits into the polarization of individual photons [1], [7]. In order to make polarization encoding feasible, both time division multiplexing (TDM) and wavelength division multiplexing (WDM) based polarization control schemes have been proposed in the literature [7]–[12].

The photon state of polarization (SOP) evolution is highly dependent on the environmental conditions and on the physical characteristics of the optical channel (in particular polarization mode dispersion (PMD) [13]). In general, the SOP evolution has a random behavior in time and frequency domains [14], [15]. However, if the effects of polarization dependent losses are negligible, the relation between the SOP at the input and output of the fiber is unitary [16]. This means that the SOP changes can be reversed by compensating two non-orthogonal SOPs [10], [16], [17]. An active full polarization control scheme using two classical signals at different wavelengths is reported in [9] and [12]. The SOP control can also be performed using the same wavelength for both reference and data signals. This has been done alternating between a control and data mode [7], [8], [10], or by time interleaving control pulses with polarization encoded photons [11]. In the last case, the TDM based SOP control scheme assures a continuous transmission of quantum data information with real-time polarization control. A maximum transmission distance of 50 km was reported [11].

In this paper, we present a model for quantum BER (QBER) estimation in polarization encoded QKD systems with TDM and WDM based polarization control schemes. In both cases, we analyze the different contributions to the total QBER, and compare the results of our model with the experimental data presented in the literature. For the WDM scheme implementation, the decorrelation between the reference and data signal reveals to be a fundamental impairment. In the TDM scheme, we analyze the time autocorrelation function (ACF) of the Stokes vector, the cross-talk between reference and data signals, and the after pulse probability detection. The results presented here can be useful to understand the performance of these SOP control schemes and can lead to the optimization of polarization encoded QKD systems.

This paper is organized in four sections. In Section II, a model for the QBER in systems using a WDM based SOP control scheme is developed. The main impairments of the TDM based SOP control scheme and their contributions to the QBER are presented in Section III. The main conclusions are summarized in Section IV.

II. WDM Based SOP Control Scheme

In a WDM based SOP control scheme the three wavelengths, corresponding to two reference signals and the quantum signal, can be combined into the fiber using an optical multiplexer (MUX) and after propagation they can be separated using an optical de-multiplexer (DMUX). However, this scheme presents some problems in terms of polarization decorrelation

Manuscript received July 28, 2010; revised November 30, 2010; accepted December 09, 2010. Date of publication December 17, 2010; date of current version January 31, 2011. This work was supported in part by Fundação para a Ciência e Tecnologia, under the Ph.D. Grant SFRH/BD/28275/2006, and the "QuantTel-IT/LA" and "QuantPrivTel-PTDC/EEA-TEL/103402/2008" projects.

N. J. Muga is with the Department of Physics, University of Aveiro, and Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal (e-mail: muga@av.it.pt).

M. F. S. Ferreira is with the Department of Physics, University of Aveiro, and I3N, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal (e-mail: mfernando@ua.pt).

A. N. Pinto is with the Department of Electronic, Telecommunications, and Informatics, University of Aveiro, and Instituto de Telecomunicações, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal (e-mail: anp@ua.pt).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2010.2099643

between the different wavelengths. In this section we present a theory able to describe the WDM control scheme performance.

A. *Wavelength Polarization Correlation*

Generally, when two signals with different wavelengths are launched into an optical fiber their SOPs evolve differently [14]. The degree of correlation between the SOPs evolution of two signals depends on their wavelength separation. One way to assure a strong SOP correlation is to use a narrow wavelength separation between them [18]. However, the use of very narrow wavelength separations presents problems in terms of channels isolation, requiring also a good performance in terms of the laser line stability. If we aim to build an experimental SOP control setup using standard telecom components, the choice of the signal wavelengths should account for the standard wavelength separation values. In the following we assume a wavelength separation equal to 0.8 nm [19].

The SOP of a light beam can be represented in the 3-D Stokes space through a Stokes vector. The degree of correlation along propagation between two Stokes vectors at different frequencies, ω_1 and ω_2, can be characterized by the respective ACF. The frequency ACF is defined as the average dot product between two Stokes vectors considering the SOPs of two signals at a given position z inside the fiber [14]

$$\begin{aligned}\mathrm{ACF}(z,\Delta\omega) &= \langle \hat{s}(z,\omega_1)\cdot\hat{s}(z,\omega_2)\rangle \\ &= \exp(-\langle\Delta\tau^2\rangle\Delta\omega^2/3)\end{aligned} \tag{1}$$

where $\Delta\omega = \omega_2 - \omega_1$ is the frequency separation, $\hat{s}(z,\omega_1)$ and $\hat{s}(z,\omega_2)$ are the SOPs at ω_1 and ω_2, respectively, and $\langle\Delta\tau^2\rangle = D_p^2 z$ is the mean square of the differential group delay, in which D_p is the PMD coefficient. If two signals are launched into an optical fiber their ACF assumes the maximum value at the fiber input, and as the signals propagate their ACF tends to zero. This function also tells how large the frequency separation must be in order to make the SOPs uncorrelated after propagation over a distance z. The ACF can be used to calculate the correlation bandwidth by using the integral $\Delta\omega_c = \int_{-\infty}^{+\infty}(\mathrm{ACF}(\Delta\omega)/\mathrm{ACF}(0))d\Delta\omega$ [14]. Using (1) into the previous integral, we obtain a correlation bandwidth $\Delta\omega_c = 2\sqrt{2}/\langle\Delta\tau\rangle$, where $\langle\Delta\tau\rangle = \sqrt{8/3\pi}D_p\sqrt{z}$. Assuming, for instance, a fiber length equal to 40 km and $D_p = 0.2$ ps/km$^{1/2}$, we obtain $\langle\Delta\tau\rangle = 0.5827$ ps and a correlation bandwidth $\Delta\lambda_c = 2\pi c\Delta\omega_c/\omega^2 = 6$ nm. For wavelengths separations larger than 6 nm the ACF presents values lower than 5%, confirming the small degree of correlation. Indeed, for distances longer than 50 km, a degree of correlation higher than 95% only occurs for wavelengths separations smaller than 0.7 nm.

B. *QBER Model*

A general WDM based SOP control scheme for QKD is presented in Fig. 1. We assume that the active control scheme is able to perform an ideal SOP control of the reference signals. Therefore, the polarization control device (PCD) placed at the receiver will be able to completely reverse the SOP rotation suffered by the two reference signals at wavelengths λ_1 and λ_2 (see Fig. 1, where only one reference signal is represented for convenience). In order to explain the model, we consider that the reference signal at λ_1 has a vertical linear polarization. If all signals are ideally correlated, then the quantum signal SOP evolution is also completely compensated. Nevertheless, the reference and quantum signals are launched at different wavelengths and therefore their SOPs present a degree of correlation lower than 100%. Therefore, the full control of the reference signal SOP cannot assure an absolute control of the quantum signal SOP.

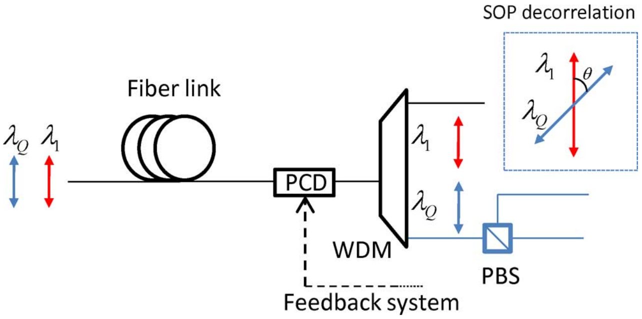

Fig. 1. Schematic diagram of a WDM control scheme for QKD systems with polarization encoding. The quantum and reference signals are represented by λ_Q and λ_1, respectively (only one reference signal is represented).

The ACF of the SOP, given by (1), can be used to estimate the angle between the two vectors and therefore the QBER contribution due to the decrease of the polarization correlation. Using the definition of the inner product, and since the Stokes vectors are unit vectors, the ACF can be written as

$$\mathrm{ACF}(z,\Delta\omega) = \langle\hat{s}(z,\omega_1)\cdot\hat{s}(z,\omega_Q)\rangle = \langle\cos\phi\rangle \tag{2}$$

where ϕ represents the angle between the two SOP vectors in the 3-D Stokes space [20]. As we are assuming that reference signal SOP, $\hat{s}(\lambda_1)$, is completely compensated, then it is well defined whereas (2) defines an ensemble of the most probable quantum signal SOPs, $\hat{s}(\lambda_Q)$. The Stokes vectors verifying (2) define on the Poincaré sphere a circumference centered on the axis defined by the Stokes vector of the reference signal (which in this case is given by $\hat{s}(\lambda_1) = [-1,0,0]^T$, where T means transpose). The most probable Stokes vectors of the quantum signal have the same value of the first Stokes parameter $s_1(\lambda_Q)$; this means that in the 2-D space theirs polarization ellipsis have the same projection on the horizontal and vertical axis. Photons with a general polarization can be described by [21]

$$|\psi_g\rangle = \sin\theta \mathrm{e}^{i\psi_x}|x\rangle + \cos\theta \mathrm{e}^{i\psi_y}|y\rangle \tag{3}$$

where $|x\rangle$ and $|y\rangle$ represent the states of the photons that exit through the horizontal and vertical ports, respectively, θ is related with polarization ellipsis projection, and ψ_x and ψ_y are the phases of the horizontal and vertical components, respectively. Such photons have the probability

$$p_h = |\langle x|\psi_g\rangle|^2 = 1 - \cos^2\theta \tag{4}$$

to follow through the horizontal polarization beam splitter (PBS) port, and the probability

$$p_v = |\langle y|\psi_g\rangle|^2 = \cos^2\theta \tag{5}$$

to follow through the vertical PBS port. Note that these probabilities are only dependent on θ, which means that all quantum signal SOPs verifying (2) have indeed the same probability to follow to the wrong port of the polarizer. In order to use the information given by the ACF into the calculation of p_h and p_v we should find a relationship between $\langle \cos\phi \rangle$ and the term $\cos^2\theta$ appearing in (4) and (5). Knowing that angles in the 2-D Jones and in the 3-D Stokes spaces are related by a factor of two, i.e., $\theta = \phi/2$, we have

$$\langle \cos^2\theta \rangle = 1/2\,(1 + \langle \cos\phi \rangle). \tag{6}$$

Using (1) and (2) into (6), we obtain

$$\langle \cos^2\theta \rangle = 1/2 + 1/2\,\exp(-\langle \Delta\tau^2 \rangle \Delta\omega^2/3). \tag{7}$$

For strongly correlated SOPs we have $\langle \cos^2\theta \rangle = 1$, whereas when the SOPs are completely uncorrelated $\langle \cos^2\theta \rangle = 1/2$. Therefore, the probability of a photon to follow through the wrong PBS port can be written as

$$p_{\mathrm{fACF}} = 1/2 - 1/2\,\exp(-\langle \Delta\tau^2 \rangle \Delta\omega^2/3). \tag{8}$$

The QBER is defined as the ratio between the wrong detections and total detections. In terms of rates, we have [1]

$$\mathrm{QBER} = R_{\mathrm{error}}/(R_{\mathrm{shift}} + R_{\mathrm{error}}) \tag{9}$$

where R_{error} represents the rate of error and R_{shift} is the rate of the shifted key. Due to the incompatible choice of bases $R_{\mathrm{shift}} = 1/2 R_{\mathrm{raw}}$, where R_{raw} is the rate corresponding to the raw key. The raw key rate can be written as [1]

$$R_{\mathrm{raw}} = f_{\mathrm{rep}} \langle n \rangle t_{\mathrm{link}} \eta_{\mathrm{det}} \tag{10}$$

where f_{rep} is the pulse rate, $\langle n \rangle$ is the mean number of photons per pulse, η_{det} is the detector efficiency, and $t_{\mathrm{link}} = 10^{-\alpha z/10}$ is the transmission efficiency (α and z are the fiber losses and length, respectively). The total error rate can be written as

$$R_{\mathrm{error}} = R_{\mathrm{fACF}} + R_{dc} \tag{11}$$

where R_{fACF} represents the error rate contribution due to the frequency decorrelation between reference and data SOPs, and R_{dc} represents the contribution due to dark counts. The contribution due to the decorrelation is given by

$$R_{\mathrm{fACF}} = R_{\mathrm{shift}} p_{\mathrm{fACF}} \tag{12}$$

where p_{fACF} is the probability of a photon to be detected in the wrong detector, given by (8). The R_{dc} contribution is given by [1]

$$R_{dc} = 1/4\, f_{\mathrm{rep}} P_{dc} n_{\mathrm{det}} \tag{13}$$

where n_{det} is the number of detectors, P_{dc} is the dark count probability, and the 1/4 factor is related with the choice of incompatible bases, which contributes with one half, and with the chance of occurring in the correct detector, which contributes with another one half. Using the last four equations into (9), we obtain

$$\begin{aligned}\mathrm{QBER} &= \mathrm{QBER}_{\mathrm{fACF}} + \mathrm{QBER}_{dc}\\ &= \frac{1 - \exp(-\langle \Delta\tau^2 \rangle \Delta\omega^2/3)}{3 - \exp(-\langle \Delta\tau^2 \rangle \Delta\omega^2/3) + P_{dc}/(\langle n \rangle t_{\mathrm{link}})}\\ &\quad + \frac{P_{dc}}{\langle n \rangle t_{\mathrm{link}}[3 - \exp(-\langle \Delta\tau^2 \rangle \Delta\omega^2/3)] + P_{dc}}. \end{aligned} \tag{14}$$

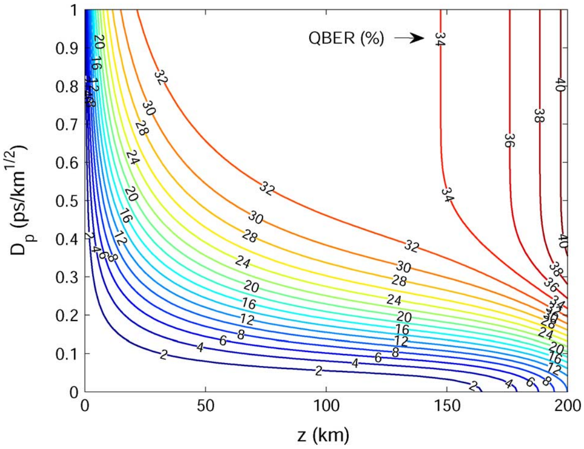

Fig. 2. QBER estimation map for WDM based SOP control scheme as function of the distance and PMD coefficient, D_p, assuming a wavelength separation equal to 0.8 nm.

Fig. 2 shows a map of the total QBER, given by (14), as a function of the distance, z, and of the PMD coefficient, D_p, assuming a wavelength separation equal to 0.8 nm. Our model shows that errors are strongly dependent on D_p. For high D_p values ($\geq$0.5 ps/km$^{1/2}$), the QBER grows quickly, reaching values higher than 30% for relatively short distances (~60 km). Between 60 km and 150 km, the QBER is almost constant, nevertheless, for distances longer than 150 km it starts to increase. In this regime, the transmission efficiency is strongly reduced by fiber losses, making the QBER_{dc} dominant. For PMD coefficients smaller than 0.1 ps/km$^{1/2}$, the QBER presents low values for short distances, however for long distances the transmission efficiency decreases and the QBER_{dc} contribution induces also an exponential increment on the total QBER. When the QBER_{dc} contribution is small, the PMD coefficient plays an important role if we aim to increase the length of the quantum channel. Assuming for instance a fiber length equal to 8.4 km and a $D_p = 0.2$ ps/km$^{1/2}$ (values corresponding to the experimental conditions reported in [9]), the QBER given by (14) takes the value 2.1%, whereas assuming a fiber length equal to 16 km and a $D_p = 0.076$ ps/km$^{1/2}$ (values corresponding to the experimental conditions reported in [12]) the QBER takes the value 0.6%. Note that the use of a fiber with the $D_p = 0.2$ ps/km$^{1/2}$ for a distance equal to 16 km will double (from 2.1% to ~4%) the QBER value obtained for 8.4 km. This is in agreement with the experimental results reported in [9] and [12]. Indeed, ours results show that the loss of correlation between reference and data signals due to the increment of distance cannot be compensated with an improved WDM based SOP control system. From de above discussion, we can conclude that the use of fibers with low PMD values is mandatory if we aim to design a system with a low QBER, based on a WDM SOP control scheme.

III. TDM Based SOP Control Scheme

In this section, we present a model for the estimation of the QBER, taking in account the main impairments of TDM based SOP control scheme. A general control scheme for QKD based on TDM is illustrated in Fig. 3. Reference and data signals are time multiplexed and separated by Δt. A correct synchronization of detector gates assures that data and reference pulses are

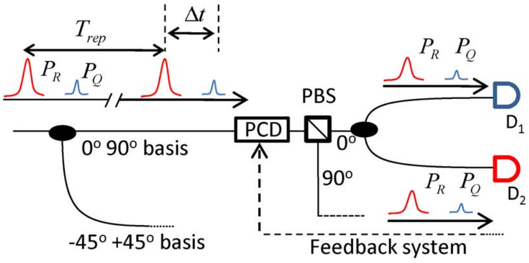

Fig. 3. Schematic diagram of a TDM control scheme for QKD systems with polarization encoding. Reference and quantum signals are time multiplexed: after passing through the PBS, the signals are split and both signals are present in the data (D_1) and reference (D_2) arms.

detected at D_1 and D_2, respectively. The feedback system uses the count records of D_2 to actuate on the PCD in order to align the input photons with vertical polarization with the vertical port of the PBS.

A. Time Polarization Correlation

Generally, when two pulses with the same wavelength are launched into an optical fiber at different time instants their SOPs evolve differently [14]. The correlation between the two SOPs depends on its time separation. The time ACF is defined as the average dot product between two Stokes vectors, representing the polarization of the same wave, at a position z inside the fiber, separated by a time interval δt [14]

$$\langle \hat{s}(z,t_1)\cdot\hat{s}(z,t_2)\rangle = \exp(-|\delta t|/t_d) \tag{15}$$

where $\delta t = t_2 - t_1$, and t_d is the typical drift time for the SOP vector. It depends on the PMD coefficient as $t_d = t_0/(3\omega^2 D_p^2 z)$, where t_0 represents the drift time of the index difference between the fast and slow fiber axes [14]. The ACF assumes the maximum value at the fiber input, and as the signal propagates the ACF tends to zero. This function tells how large a time separation between two pulses must be in order to make their SOPs uncorrelated after propagation over a distance z. Therefore, for a particular value of t_0, the changes on the absolute SOP will be faster for longer fibers and higher PMD coefficients. Since the data pulses arrive first at the PBS (see Fig. 3), the time delay at this point between the last reference pulse and the next data pulse will be $\delta t = T_{\mathrm{rep}} - \Delta t$, where $T_{\mathrm{rep}} = 1/f_{\mathrm{rep}}$. Therefore, after passing through the PCD reference photons will follow the correct port of the PBS. On the other hand, data photons will present a nonzero probability to follow through the wrong port dependent on the time ACF. The reference and data Stokes vectors will present an angle ϕ between them, verifying $\langle\cos\phi\rangle = \exp(-|\delta t|/t_d)$. Using this expression in conjugation with (6) into (4) we obtain the probability of a photon follow through the wrong port due to time decorrelation

$$p_{t\mathrm{ACF}} = 1/2 - 1/2\,\exp\left(-3\omega^2 D_p^2 z|\delta t|/2t_0\right). \tag{16}$$

Fig. 4 shows the error contribution given by (16) as a function of the distance, for different values of D_p. For higher PMD coefficients we have a stronger penalty in terms of QBER. The results also show that, within the plotted distance range, systems with low PMD present a QBER that grows linearly with the distance.

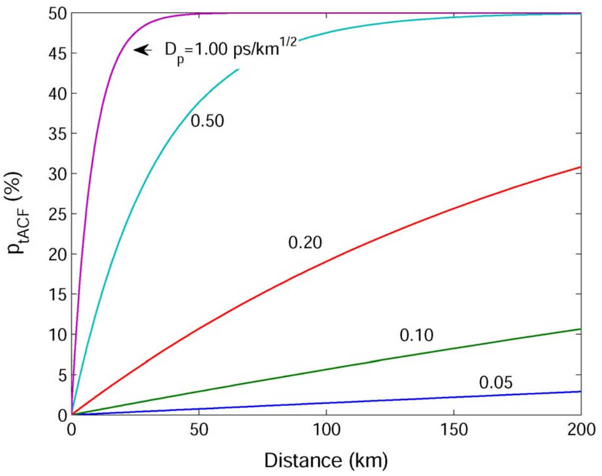

Fig. 4. QBER in a system with a TDM based SOP control scheme due to the SOP decorrelation as a function of the distance, assuming different values of D_p and a time delay equal to 1 μs.

B. Feedback SOP Control Model

In contrast with the WDM control scheme, where a large number of photons can be used in the feedback system, the TDM control scheme uses a low number of photons, making its performance pulse rate dependent [11]. We account for this aspect by modeling the angle between the obtained and the target SOPs in the Stokes space as

$$\theta = \Theta(1 - \exp(-gT_{\mathrm{rep}})) \tag{17}$$

where Θ is the angle without the feedback SOP control, and $1/g$ is the characteristic time decay of the obtained SOP to Θ. For high values of pulse rates the SOP at the PCD output will be close to the target value, i.e., $\theta \to 0$, whereas for low rates the SOP will present a random value in the Poincaré sphere, i.e., $\theta \to \Theta$ [22]. Using (17) into (4) we obtain the following expression for the errors due to the imperfect operation of the feedback SOP control

$$p_{\mathrm{SOP}} = 1 - \cos^2[1/2\,\Theta(1 - \exp(-gT_{\mathrm{rep}}))]. \tag{18}$$

The error probability given by (18), and illustrated in Fig. 5, shows that, independently of the g value, the QBER contribution due to the feedback SOP control can be minimized if a high pulse rate is used.

C. Cross-Talk Between Reference and Data Signals

In this scheme, reference and quantum signals are time multiplexed, and both signals are present in the data and reference arms (see Fig. 3). Therefore, in order to select the correct pulse, detectors D_1 and D_2 have the respective gates delayed by Δt, i.e., the time separation between quantum and reference pulses. The probability of photons traveling in the reference pulse being detected at D_1 due to the cross-talk, P_{leak}, will be dependent on the reference pulse shape, data gate width, and temporal separation, Δt, between the reference and data signals. We can write

$$P_{\mathrm{leak}} = \eta_{\mathrm{det}} t_{\mathrm{link}}\langle n_g\rangle \tag{19}$$

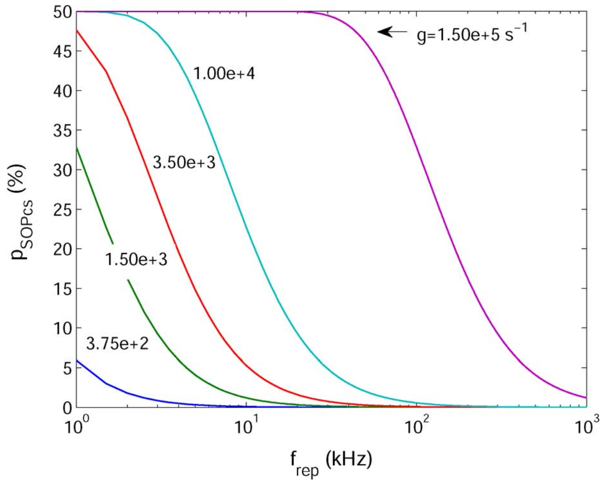

Fig. 5. Feedback SOP control QBER contribution, for different values of the characteristic parameter g.

where $\langle n_g \rangle = A\langle n_r \rangle$ is the mean number of reference photons per pulse leakage 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. Considering a data gate width equal to T_g, and that the center of the data gate and the center of the reference pulse are separated by Δt, the coefficient A is given by

$$A = \int_{\Delta t - T_g/2}^{\Delta t + T_g/2} |f(t)|^2 dt \tag{20}$$

where $\int_{t_1}^{t_2} |f(t)|^2 dt$ represents the probability of a photon be detected in the interval $t_1 - t_2$, and $f(t)$ is related with the pulse shape. Note that $f(t)$ should be a normalized function, i.e., if $t_1 \rightarrow -\infty$ and $t_2 \rightarrow +\infty$ then $\langle n_g \rangle \rightarrow \langle n_r \rangle$. Assuming a Gaussian pulse shape $f(t) = 1/(T_p\sqrt{\pi})^{1/2} \exp(-t^2/(2T_p^2))$, then A is given by

$$A = \frac{1}{2}\left[\text{erf}\left(-\frac{(2\Delta t - T_g)}{2T_p}\right) + \text{erf}\left(\frac{(2\Delta t + T_g)}{2T_p}\right)\right] \tag{21}$$

where T_p is the half-width at $1/e$-intensity of $f(t)$, which is related with the pulse full width at half maximum (FWHM) by $T_{\text{FWHM}} = 2\sqrt{\ln 2}T_p$. In order to account for the pulse broadening due to chromatic dispersion, we should replace T_p in (21) by

$$T_p(z) = T_p[1 + (z/L_D)^2]^{1/2} \tag{22}$$

where $L_D = T_p^2/|\beta_2|$ is the dispersion length [13].

Assuming, for instance, that data pulse is removed, then the total number of counts on the quantum data detector due to reference pulse leakage is given by

$$N = f_{\text{rep}}P_{\text{click}} = f_{\text{rep}}(P_{\text{leak}} + P_{dc} - P_{\text{leak}}P_{dc}), \tag{23}$$

where P_{click} is the click probability, and P_{leak} is given by (19). Fig. 6 represents the photon-counts in the data detector as a function of Δt. We have used $T_g = 2$ ns, $T_{\text{FWHM}} = 1$ ns, $\langle n \rangle = 0.1$, $\alpha = 0.2$ dB/km, $z = 50$ km, $f_{\text{rep}} = 1$ MHz, $\eta_{\text{det}} = 10\%$, and the number of dark counts $P_{dc} = 2 \times 10^{-5}$. In Fig. 6 it is shown that for time delays smaller than 3 ns the photon-counts on the data detector coming from the reference pulse start to increase, which is in good agreement with the experimental results reported in [11]. In that work, the data and the two reference pulses were separated by large delays, 50 ns and 90 ns, assuring that no reference pulses reached the data detector [11].

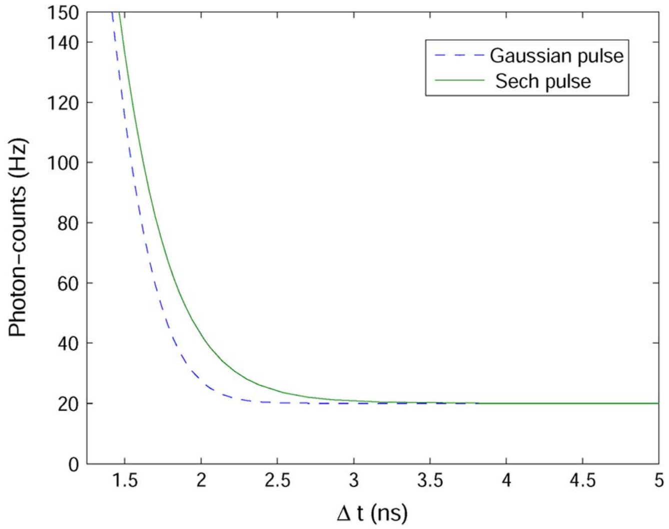

Fig. 6. Photon-counts in the data detector due to the reference pulse leakage, considering Gaussian (dashed line) and Sech (solid line) pulses with full width at half maximum equal to 1 ns.

D. After Pulse Probability

High power reference pulses can induce after pulse detections. The after pulse probability results from the trapping of charge carriers during an avalanche or due to photons impinging outside the gate [23]. We will assume that this probability depends on the arrival time before the gate as

$$P_{af}(T_{af}) = g_{af}/T_{af} \tag{24}$$

where g_{af} is a characteristic constant of the detector, and T_{af} is the difference between the time arrival of the reference pulse and the next data gate opening $T_{af} = T_{\text{rep}} - \Delta t$. Using the experimental data presented in [23] we have found the following value for the characteristic constant of the detector $g_{af} = 2.79 \times 10^{-12}$ s.

E. Total QBER due TDM Based SOP Control

According to the analysis presented above, the total error rate can be written as

$$R_{\text{error}} = R_{t\text{ACF}} + R_{\text{SOP}} + R_{\text{leak}} + R_{af} + R_{dc} \tag{25}$$

where $R_{t\text{ACF}}$ represents the contribution due to the time decorrelation between reference and data SOPs, given by $R_{t\text{ACF}} = R_{\text{shift}}p_{t\text{ACF}}$, in which $p_{t\text{ACF}}$ is given by (16). R_{SOP} represents the contribution due to the feedback SOP control system, and can be written as $R_{\text{SOP}} = R_{\text{shift}}p_{\text{SOP}}$, where p_{SOP} is given by (18). The contribution due to the leakage of photons from the reference pulse to the data one, is given by $R_{\text{leak}} = (1/4)\, f_{\text{rep}}P_{\text{leak}}$. The 1/4 factor in the above equation is related with the transmitter and the receptor choice of incompatible bases [1], which contributes with one half, and with the probability of the leak photon to coincide with a correct data qubit, which contributes with another half. The contribution due to the after pulse probability related with the photons impinging outside the gate, is given by $R_{af} = (1/2) f_{\rm rep} t_{\rm link} \langle n_r \rangle P_{af}$, where P_{af} is given by (24). R_{dc} represents the contribution due to dark counts, given by (13).

Using the previous results into (9), we obtain the following expression for the total QBER

$$\begin{aligned} \mathrm{QBER} &= \mathrm{QBER}_{t\mathrm{ACF}} + \mathrm{QBER}_{\mathrm{SOP}} + \mathrm{QBER}_{\mathrm{leak}} \\ &\quad + \mathrm{QBER}_{af} + \mathrm{QBER}_{dc} \\ &\quad = 1/4 - 1/4 \exp\left(-3\omega^2 D_p^2 z |T_{\rm rep} - \Delta t|/(2t_0)\right) \\ &\quad + 1 - \cos^2(1/2\,\Theta(1 - \exp(-gT_{\rm rep}))) \\ &\quad + \frac{1}{2}\frac{\langle n_r\rangle A}{\langle n\rangle} + \frac{\langle n_r\rangle P_{af}}{\langle n\rangle \eta_{\rm det}} + \frac{1}{2}\frac{P_{dc} n_{\rm det}}{\langle n\rangle t_{\rm link}\eta_{\rm det}}. \end{aligned} \quad (26)$$

Some contributions to the QBER in (26) depend on the propagation distance. In the case of QBER_{dc}, it occurs because the detector dark-counts are constant whereas $R_{\rm shift}$ decreases with $t_{\rm link}$. The contribution due to the pulse leakage, $\mathrm{QBER}_{\rm leak}$, is dependent on the propagation distance, since for narrow pulses chromatic dispersion can induce pulse broadening. With that, and since 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 $\mathrm{QBER}_{t\mathrm{ACF}}$ will increase with the distance.

Concerning the frequency, we observe that only $\mathrm{QBER}_{\rm leak}$ and QBER_{dc} are frequency independent. Both $\mathrm{QBER}_{\rm SOP}$ and $\mathrm{QBER}_{t\mathrm{ACF}}$ contributions decrease with the frequency; in the first case, because as more photons are received at the SOP controller system, smaller will be the deviations from the target SOP at the PCD output; in the second case, because as higher the frequency is, smaller will be the separation between the reference and data pulses, which means a stronger correlation between their SOPs. On the other hand, the QBER_{af} contribution increases with frequency since T_{af} decreases with the increment of $f_{\rm rep}$.

Fig. 7 shows a map of the total QBER, given by (26), as a function of pulse rate, $f_{\rm rep}$, and propagation distance, z. The following parameters values were used in order to plot the map: $\beta_2 = -20$ ps^2/km, $\langle n_r \rangle = 4$, $\langle n \rangle = 0.1, \alpha = 0.22$ dB/km, $T_{\rm FWHM} = 1$ ns, Δt $= 100$ ns, $D_p = 0.2$ ps/km$^{1/2}$, $T_g = 2$ ns, $\eta_{\rm det} = 10\%, g_{af} = 2.77 \times 10^{-12}$ s, $t_0 = 8.5 \times 10^7$ s, $P_{dc} = 1 \times 10^{-6}$, $\Theta = \pi/2$ rad, and $g = 0.5 \times 10^2$ s^{-1}. Our model shows that for distances smaller than 70 km the QBER increases with the frequency. In this regime, the QBER system is dominated by the after pulse contribution QBER_{af}. This process limits the maximum frequency rate for small distances, where fiber losses are not the main impairment. The fiber losses become dominant for distances longer than 100 km. In such case, the QBER increases exponentially and reaches values higher than 7% for distances longer than 140 km. For low frequencies (<1 kHz) the QBER can present high values if the SOP control system is characterized by a high value of the parameter g (see Fig. 5).

The QKD experiment over 50 km of fiber with a TDM control scheme presented in [11] reports a QBER of 5.3%. The authors identify two main contributions to the total QBER: a contribution of 3.3% resulting from the dark noise detections, and 2% from the SOP control imperfections. They claim that the effectiveness of the SOP control can be improved if higher pulse rates are used, which is in agreement with the results presented here. Nevertheless, we show that for high pulse rates the after pulse detections can become an important impairment, and therefore a good balance between QBER_{dc}, $\mathrm{QBER}_{\rm SOP}$ and QBER_{af} contributions is needed.

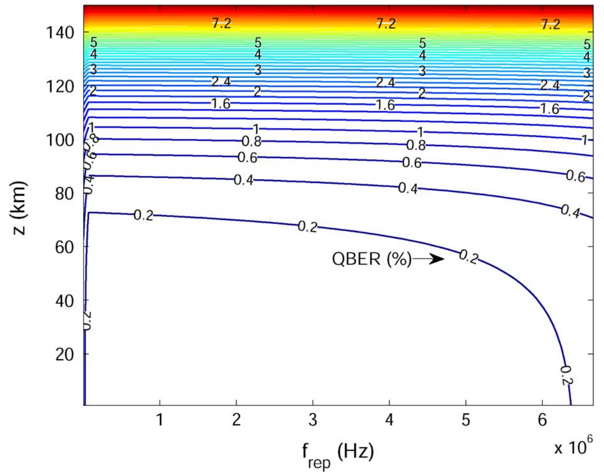

Fig. 7. QBER estimation map for TDM based SOP control scheme as a function of the distance z and pulse rate $f_{\rm rep}$. The parameters used to plot the map are given in Section III-E.

The influence of the SOP compensation system on the quantum channel should be avoided or, at least, minimized. This is an important aspect to evaluate the global performance of a SOP control system [1]. When co-propagating into the fiber, reference and data signals should be uncorrelated, otherwise any eavesdropping of the reference pulses will affect the security of the communication.

IV. Conclusion

We have derived novel analytical expressions to estimate the QBER in QKD systems based on polarization encoding with SOP control schemes. Such expressions, given by (14) and (26), are in agreement with experimental results reported in the literature. We have shown 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 control scheme, we have identified some limitative technical aspects, likewise the single photon detector 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. For distances shorter than 70 km and frequencies higher than 5 MHz the after pulse probability reveals an important contribution to the QBER.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, pp. 3–28, 1992.

[4] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, "100 km differential phase shift QKD experiment with low jitter upconversion detectors," *Opt. Exp.*, vol. 14, no. 26, pp. 13 073–13 082, 2006.

[5] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," *Nature Photon.*, vol. 1, no. 6, pp. 343–348, 2007.

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

[7] P. Cheng-Zhi, Z. Jun, Y. Dong, G. Wei-Bo, M. Huai-Xin, H. Yin, H.-P. Zeng, Y. Tao, W. Xiang-Bin, and P. Jian-Wei, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010505, Jan. 2007.

[8] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, "Active polarization stabilization in optical fibers suitable for quantum key distribution," *Opt. Exp.*, vol. 15, no. 26, pp. 17928–17936, 2007.

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

[10] A. Poppe, "Method and Device for Readjusting a Polarization Drift," U.S. Patent US2008/0310856 A1, Dec. 18, 2008.

[11] 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 J. Phys.*, vol. 11, no. 6, pp. 17 928–17 936, 2009.

[12] G. B. Xavier, N. Walenta, G. V. de Faria, G. P. Temporão, 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 J. Phys.*, vol. 11, no. 4, 2009.

[13] G. P. Agrawal, *Nonlinear Fiber Optics*, 3rd ed. San Diego, CA: Academic, 2001, EUA.

[14] M. Karlsson, J. Brentel, and P. Andrekson, "Long-term measurement of PMD and polarization drift in installed fibers," *J. Lightw. Technol.*, vol. 18, no. 7, pp. 941–951, Jul. 2000.

[15] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Practical aspects of quantum cryptographic key distribution," *J. Cryptol.*, vol. 13, no. 2, pp. 207–220, Dec. 2000.

[16] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, "Unambiguous quantum measurement of nonorthogonal states," *Phys. Rev. A*, vol. 54, no. 5, pp. 3783–3789, Nov. 1996.

[17] M. Martinelli, P. Martelli, and S. M. Pietralunga, "Polarization stabilization in optical communications systems," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 4172–4183, 2006.

[18] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *IEEE J. Quantum Electron.*, vol. 46, no. 3, pp. 285–291, 2010.

[19] "ITU-T G. 694.1," Spectral Grids for WDM Applications: DWDM Wavelength Grid 2002.

[20] J. N. Damask, *Polarization Optics in Telecomunications*. New York: Springer, 2005, EUA.

[21] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics*, 2nd ed. New York: Wiley-VCH, 2003.

[22] N. J. Muga, A. N. Pinto, M. Ferreira, and J. R. F. da Rocha, "Uniform polarization scattering with fiber-coil based polarization controllers," *J. Lightw. Technol.*, vol. 24, no. 11, pp. 3932–3943, Nov. 2006.

[23] G. Ribordy, N. Gisin, O. Guinnard, D. Stuck, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: Current performance.," *J. Mod. Opt.*, vol. 51, no. 9, pp. 1381–1398, 2006.

Nelson J. Muga was born in Mogadouro, Portugal, in 1980. He graduated in physics from the University of Porto, Portugal, in 2002, and received the M.S. degree in applied physics at the University of Aveiro, Portugal, in 2006. He is currently pursuing the Ph.D. degree at the University of Aveiro, Portugal.

In 2004, he joined the Institute of Telecommunications, Aveiro, where he has been working as a researcher in the Optics Communications Group. His current main interests of research are nonlinear and polarization effects in optical fibers. He has published more than 20 scientific papers in international journals and conferences.

Mário F. S. Ferreira was born in Ovar, Portugal. He graduated in physics from the University of Porto, Portugal, in 1984 and the Ph.D. degree in physics from the University of Aveiro, Portugal, in 1992.

He became an Assistant Lecturer first at the Mathematics Department and then at the Physics Department of the University of Aveiro, Portugal. He is now a Professor at the same Physics Department. Between 1990 and 1991 he was at the University of Essex, U.K., performing experimental work on external cavity semiconductor lasers and nonlinear optical fiber amplifiers. At present, he leads a research group dedicated to the modeling and characterization of multi-section semiconductor lasers for coherent systems, quantum well lasers, optical fiber amplifiers and lasers, soliton propagation, polarization and nonlinear effects in optical fibers. He has written more than 200 scientific journal and conference publications, as well as a book with the title: "*Optics and Photonics*" (in Portuguese).

Dr. Ferreira is a member of the Optical Society of America (OSA), SPIE—The International Society for Optical Engineering, The New York Academy of Sciences (NYAS), the American Association for the Advancement of Science (AAAS), the European Optical Society (EOS), the European Physical Society (EPS) and the Portuguese Physical Society. He served in the technical committees of various international conferences. He is presently an Associate Editor of *Optical Fiber Technology—Materials, Devices, and Systems* and a member of the Advisory Board of *Fiber and Integrated Optics*, *Nonlinear Optics, Quantum Optics*, *Research Letters in Optics*, and *International Journal of Optics*. He was the Guest Editor of a Special Issue of *Fiber and Integrated Optics*, published in 2005, dedicated exclusively to the fiber and integrated optics activity carried out in Portugal.

Armando N. Pinto (M'99–SM'07) graduated in electronic and telecommunications engineering in 1994, and received the Ph.D. degree in electrical engineering in 1999, both from the University of Aveiro.

In 2000, he became an Assistant Professor at the Department of Electronic, Telecommunications and Informatics of the University of Aveiro, and a Researcher at the Instituto de Telecomunicações. During the academic year of 2006–2007 he was a Visiting Professor at the Institute of Optics, University of Rochester. At the present, he leads a research group at the Instituto de Telecomunicações focus on high-speed optical communication systems and networks. He has published more than 100 scientific papers in international journals and conferences. He served in the technical committee of various scientific international conferences. He is presently member of the Editorial Board of *The International Journal of Optics*.

Dr. Pinto is a member of the Optical Society of America (OSA).