Critical Issues in Polarization Encoded Quantum Key Distribution Systems

Nelson J. Muga*†, Álvaro J. Almeida*, Mário F. Ferreira† and Armando N. Pinto*‡
*Instituto de Telecomunicações, Campus Universitário de Santiago 3810-193 Aveiro, Portugal
†Department of Physics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
‡ Department of Electronic, Telecommunications, and Informatics, University of Aveiro,
Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
Emails: muga@av.it.pt, aalmeida@av.it.pt, mfernando@ua.pt, anp@ua.pt.

***Abstract*—An analysis of the most critical issues in quantum key distribution systems with polarization encoded photons is presented. Effects like the fiber birefringence, fiber losses and some technical aspects can difficult the state of polarization control in such kind of systems, leading to an undesired quantum bit-error-rate increment. It is shown that a system with a long fiber, presenting a typical PMD value, only assures a strong correlation between two Stokes vectors for narrow wavelength separations. In terms of time correlation, it is shown that the typical drift times are much longer than delays between reference and data signals. The problematic of the reference pulse leakage to the data detector is also analyzed; a good agreement between experimental and theoretical data is observed.**

***Index Terms*—Optical fibers, polarization, quantum key distribution**

I. Introduction

Quantum key distribution (QKD) assures an unconditional secure exchange of secret keys between two identities (usually known as Alice and Bob) [1]. The implementation of such protocols can be made by encoding the information into the state of polarization of single photons. Changes and instability on the state of polarization (SOP) emerging at the fiber output should be avoided [2]. This reveals important since in this encoding scheme Alice and Bob's polarizers must be aligned during the period of exchanging qubits. In order to avoid errors and make polarization encoding feasible both time division multiplexing (TDM)- and wavelength division (WDM)-based polarization control schemes solutions were proposed in the literature [3], [4], [5].

For long fibers, SOP changes are highly dependent of the physical characteristics of the optical channel, in particular polarization mode dispersion (PMD) [6], and of the environment conditions. In contrast with the high-birefringence fiber, where the SOP evolves periodically [7], these changes have a random behavior in time and frequency domains [2], [8]. However, if the effects of polarization dependent losses (PDL) are negligible, the relation between the SOP at the input and output of the fiber is unitary. This means that the SOP changes suffered along the propagation can be reversed by compensating two non-orthogonal SOPs [3], [9], [10]. In order to assure that, a feedback system looking to two nonorthogonal SOPs can be implemented at the receiver. In conjugation with a proper algorithm, the feedback system uses two nonorthogonal reference signals to actuate on an electronic polarization controller, assuring that all polarizations, including the quantum signal polarization, are reverted. These SOP control systems can be implemented by multiplexing two reference signals with the quantum information into the time or frequency domains (TDM and WDM-based schemes, respectively).

In this paper we perform an analysis of the most important impairments for quantum key distribution with polarization encoding. Although both WDM and TDM SOP compensation schemes were proposed, the are still some physical and technical effects that limit the performance of the QKD systems [11]. We show that a system with a long fiber, presenting a typical PMD value, only assures a strong correlation (autocorrelation function (ACF) $>$90 %) between Stokes vectors for narrow wavelength separations (much smaller than 0.8 nm). This limits the performance of systems with WDM-based SOP compensation schemes. When Stokes vectors are measured at different instants, we show that abrupt environmental changes on the fiber can reduce the degree of correlation. The reference pulse leakage to the data detector is also analyzed.

This paper is organized in five sections. In section II, the birefringence-induced SOP decorrelation in the frequency domain is analyzed. The decorrelation in the time domain is presented in section III. Subsequently, in section IV we analyze the problematic of the minimum time separation between the reference and data pulses on QKD systems with TMD based SOP compensation schemes. The main conclusions are presented in section V.

II. Wavelength Polarization Decorrelation

WDM-based SOP control schemes use different wavelengths for data and reference signals. However, it is well-known that the correlation between the SOP of two signals depends on its wavelength separation [8]: this represents some physical limitations for the SOP control system in terms of wavelength separation between reference anda data signals and propagation distances.

This work was supported in part by Fundação para a Ciência e Tecnologia, under the PhD Grant SFRH/BD/28275/2006, and the "QuantTel-IT/LA" and "QuantPrivTel-PTDC/EEA-TEL/103402/2008" projects.

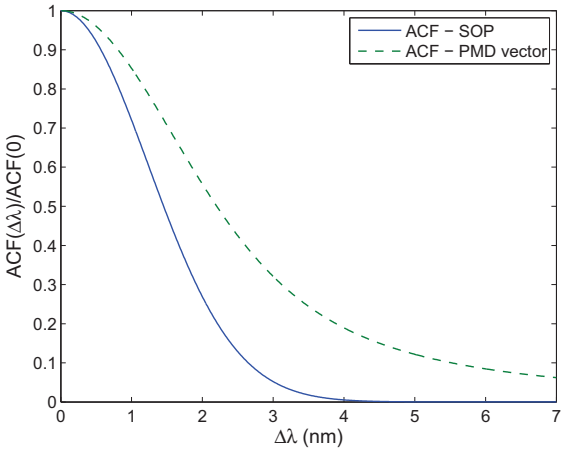

Fig. 1. A comparison between the autocorrelation function (ACF) of the absolute state of polarization $\hat{s}$ (solid line) and PMD vector $\vec{\tau}$ (dashed line). Curves are obtained assuming $D_p = 0.2$ ps/km$^{1/2}$ and $z = 40$ km;

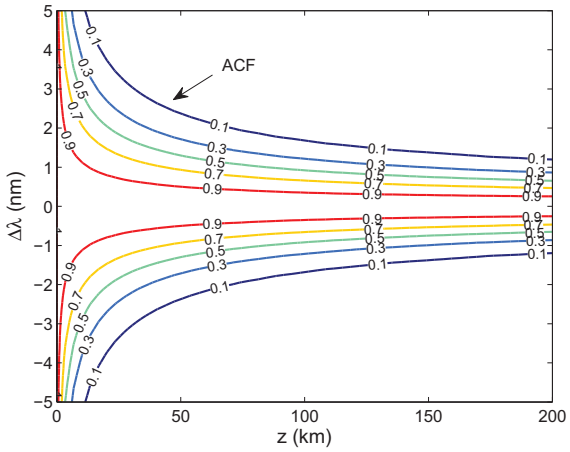

Fig. 2. Frequency ACF map of the Stokes vector $\hat{s}$ as a function of the wavelength separation and the propagation distance, assuming a PMD coefficient equal to $D_p = 0.2$ ps/km$^{1/2}$.

As much closer the reference and data wavelengths are, stronger will be the correlation presented by the respective SOPs. This means that the way to assure a strong polarization correlation is to use a narrow wavelength separation between signals. Nevertheless, if we aim to build an experimental SOP control setup using by preference standard telecom components, the choice of the reference signal wavelengths should take into account the standard wavelength separation values of the dense wavelength division multiplexing (DWDM) systems [12]. On the other hand, the use of very narrow wavelength separations presents some problems in terms of channels isolation, requiring also a good performance in terms of the laser line stability.

The SOP of an optical signal can be represented by the Stokes vector $\hat{s}$. The $\hat{s}$ vector changes with the frequency; such changes are characterized by the PMD vector $\hat{\tau}$. Indeed, the degree of correlation between two PMD vectors (or two Stokes vectors) at different frequencies are described by the respective frequency autocorrelation function (ACF) [8], [13]. The ACF for the PMD vector is given by

$$\langle \hat{\tau}(\omega_1) \cdot \hat{\tau}(\omega_2) \rangle = 3 \frac{1 - \exp\left(\frac{-\langle \Delta\tau^2 \rangle \Delta\omega^2}{3}\right)}{\Delta\omega^2}, \qquad (1)$$

where $\Delta\omega = \omega_2 - \omega_1$ is the frequency separation and $\langle \Delta\tau^2 \rangle$ is the mean square of the differential group delay. The ACF for the Stokes vector at the position z is given by

$$\langle \hat{s}(\omega_1) \cdot \hat{s}(\omega_2) \rangle = \hat{s}(0,\omega_1) \cdot \hat{s}(0,\omega_2) \exp\left(\frac{-\langle \Delta\tau^2 \rangle \Delta\omega^2}{3}\right), \qquad (2)$$

where $\hat{s}(0,\omega_1)$ and $\hat{s}(0,\omega_2)$ are the input SOPs. Equations (1) and (2) can be written as functions of the distance by using the definition of PMD coefficient D_p: $\langle \Delta\tau^2 \rangle = D_p^2 z$. Note that in the limit $\Delta\omega \to 0$ the ACF for the PMD vector takes the value $\langle \Delta\tau^2 \rangle$ and the ACF for the Stokes vector takes the value $\hat{s}(0,\omega_1) \cdot \hat{s}(0,\omega_2)$. The ACFs can be used to calculate the correlation bandwidths using the integral [13]

$$\omega_c = \int_{-\infty}^{+\infty} \frac{ACF(\Delta\omega)}{ACF(0)} d\Delta\omega. \qquad (3)$$

Using the ACFs defined in (1) and (2) into (3), the correlation bandwidths $\omega_c = 4\sqrt{2}/\langle \Delta\tau \rangle$ and $\omega_c = 2\sqrt{2}/\langle \Delta\tau \rangle$ are obtained for the PMD vector and Stokes vector, respectively. This result shows that the correlation bandwidth of the Stokes vector is half of the PMD vector, which means that the use of PSP bandwidth [14] in order to asses the Stokes vector correlation could be inadequate. The two ACFs, given by (1) and (2) are graphically represented in Fig. 1, assuming a fiber length equal to 40 km and $D_p = 0.2$ ps/km$^{1/2}$. A higher correlation decrease is observed for the Stokes vector, which is in good agreement with the two values obtained for the correlation bandwidth. For these particular fiber parameters we have $\langle \Delta\tau \rangle = 1.1654$ ps, and therefore $\lambda_c = 2\pi c \omega_c / \omega^2$ is equal to 6 nm and 3 nm for the PMD vector and the Stokes vector, respectively. It can be observed that for these values both ACF present values lower than 10% confirming the small degree of correlation. On the other hand, for a wavelength separation equal to 0.8 nm the Stokes vector has a correlation of 81% whereas the PMD vector as a correlation of 90%. The ACF map represented in Fig. 2 shows how the correlation between two Stokes vectors evolves with the wavelength separation and the propagation distance, assuming a particular PMD value ($D_p = 0.2$ ps/km$^{1/2}$). Results show that the correlation decreases quickly with the propagation distance and the wavelength separation. For distances longer than 20 km the high degree of correlation events only occurs for narrow wavelength separations (much smaller than 0.8 nm). Figure 3 shows the ACF of the SOP as a function of the distance assuming a wavelength separation equal to 0.8 nm, for different values of D_P. Results show that for this wavelength separation the correlation decreases quickly, namely for the cases of higher PMD values; even for a fiber

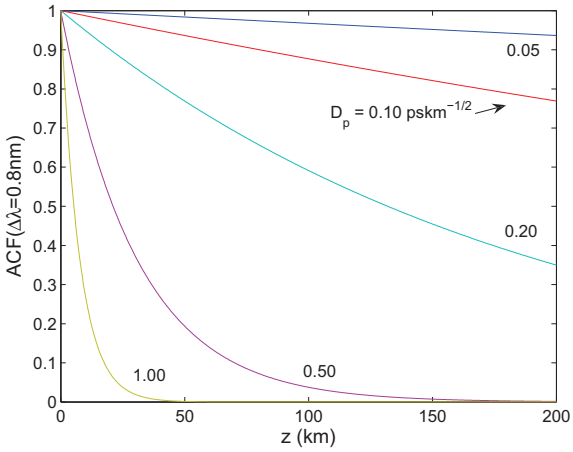

Fig. 3. Frequency ACF of the Stokes vector as a function of the distance assuming a wavelength separation equal to 0.8 nm, for different D_P values.

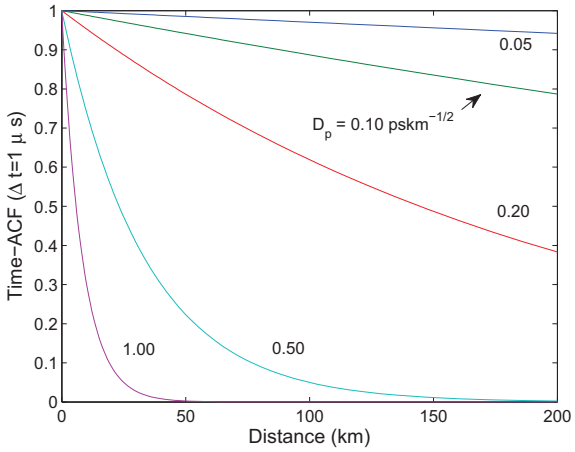

Fig. 4. Time-ACF as a function of the distance for different values of the PMD coefficient.

with $D_p = 0.1$ ps/km$^{1/2}$ the maximum distance for which the polarization of two signals separated by 0.8 nm will be highly correlated (ACF≥90%) is 80 km. Table I shows the distances for which the ACF≥90%.

TABLE I
MAXIMUM DISTANCES FOR WHICH THE ACF≥90%

D_p (ps/km$^{1/2}$)	0.05	0.1	0.2	0.5	1.0
L (km)	321	80	20	3.2	0.8

Results present here show that the performance of WDM-based SOP control schemes are affected by fiber birefringence. Due to random birefringence the SOP decorrelation decreases with the distance and wavelengths separations.

III. Time Polarization Decorrelation

Analogously to the wavelength domain, the correlation between two SOPs depends on the time separation measurement. This is particulary relevant for the TDM-based SOP control schemes, where the data and reference signals are delayed, and therefore detected at different instants. If we analyze the SOP at certain wavelength at two distinct time instants, t_1 and t_2, as much close the time instants are as stronger the correlation presented by the SOPs will be. The correlation of two absolute SOP vectors measured at times t_1 and t_2 is given by [8]

$$\langle \hat{s}(t_1) \cdot \hat{s}(t_2) \rangle = \exp\left(-\frac{|\delta t|}{t_d}\right), \tag{4}$$

where $\delta t = t_2 - t_1$, and t_d is the typical drift time for the SOP vector. This is an individual parameter that has to be measured for each fiber. In [8], it is shown that t_d depends on the PMD as $t_d = t_0/(3\omega^2 D_p^2 z)$, where t_0 is a measure of the drift time of the index difference in the birefringent element used to model the fiber. Therefore, for a particular value of t_0, the changes on the absolute SOP will be as faster as longer the fiber and as higher the PMD coefficient.

In TDM-based SOP control systems data pulses arrive first at the receiver [4], and therefore the time delay at this point between the last reference pulse and the next data pulse will be $\delta t = T_{rep} - \Delta t$, where $T_{rep} = 1/f_{rep}$, and Δt is the delay between reference and data pulses. Fig. 4 shows the evolution of the time ACF with distance, assuming for instance f_{rep} =1 MHz and $\Delta t = 50$ ns. The different curves correspond to different values of PMD, for a time separation between two pulses of $\Delta t = 1$ μs and a drift time of the index difference of $t_0 = 18.5$ s. Results show a quick decrease of the ACF with the distance, in particular for PMD values higher than 0.2 ps/km$^{1/2}$. Since characteristic drift times are parameters that depend on the fiber environment, the performance of TDM based SOP control systems can be strongly affect by time decorrelation events.

IV. Cross-talk Between Signals

TDM-based SOP control schemes can also lead with the leakage of photons from the reference to data pulses. In this scheme, reference and quantum signals are time multiplexed, and both signals are present in the data and reference detection stages (see for instance [4]). Therefore, in order to select the correct pulse, the two detectors have the respective gates delayed by Δt.

The probability of photons traveling in the reference pulse being detected at the data detector due to the cross-talk, P_{leak}, will be dependent on the reference pulse shape, data gate width, and temporal separation Δt. We can write

$$P_{leak} = \eta_{det} t_{link} \langle n_g \rangle, \tag{5}$$

where η_{det} is the detector efficiency, $t_{link} = 10^{-\alpha z/10}$ is the transmission efficiency, in which α and z are fiber losses and length, respectively, $\langle n_g \rangle = A\langle n_r \rangle$ 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. We will assume that detectors have an ideal gate, i.e., a square gate with width equal to T_g, and that the center of the data gate and the center of the

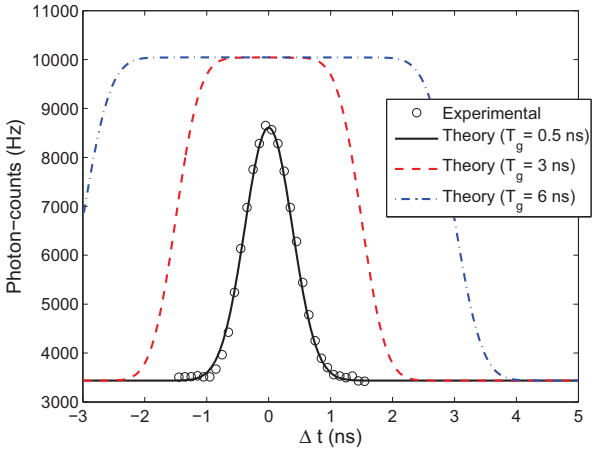

Fig. 5. Photon-counts in the data detector due to the reference pulse leakage, considering a Gaussian pulse with full width at half maximum equal to 0.83 ns, assuming a gate width equal to 0.5 ns (solid line), 3 ns (dashed line), and 6 ns (dashdot line). Experimental results are represented as circles (only for gate width equal to 0.5 ns).

reference pulse are separated by Δt. Then, A is given by

$$A = \int_{\Delta t - T_g/2}^{\Delta t + T_g/2} |f(t)|^2 \, dt, \tag{6}$$

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 $t_1 \to -\infty$ and $t_2 \to +\infty$ then $\langle n_g \rangle \to \langle n_r \rangle$. 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

$$A = \frac{1}{2}\left[\text{erf}\left(-\frac{(2\Delta t - T_g)}{2T_p}\right) + \text{erf}\left(\frac{(2\Delta t + T_g)}{2T_p}\right)\right], \tag{7}$$

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 $T_{FWHM} = 2\sqrt{\ln 2}T_p$. 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

$$N = f_{rep} P_{click} = f_{rep}(P_{leak} + P_{dc} - P_{leak}P_{dc}), \tag{8}$$

where P_{click} is the click probability, P_{dc} is the dark count probability, and P_{leak} is given by (5). Figure 5 represents the photon-counts given by (5) as a function of Δt, considering different gate widths, in a back-to-back scenario ($z = 0$). Results show that for small time delays the photon-counts on the data detector coming from the reference pulse start to increase. Considering the particular gate width $T_g = 6$ ns we observe that this occurs for $\Delta t \approx 3.5$ ns. Figure 5 also shows the experimental data obtained with an InGaAs/InP avalanche photodiode from IDQuantique (id201), operating in a gated Geiger mode [15]. The detector has a dark count probability $P_{dc} = 5\times10^{-6}$, and a quantum detection efficiency $\eta_{det} = 10$ %. We used pulses with $T_{FWHM} = 0.83$ ns (and shape close to Gaussian), mean number of photons $\langle n_r \rangle = 0.18$, and a repetition rate $f_{rep} = 550.540 \times 10^3$ Hz, and a id201 gate width equal to 2.5 ns. Note that although we have selected a gate width equal to 2.5 ns, this gate width results in an effective gate of typically 0.5 ns [16]. This means that our model is in good agreement the experiential data. This model can therefore be used in order to estimate the minimum separation between reference and data pulses that assures a isolation between the two kind of signals.

V. Conclusion

We have analyzed the effects of the fiber birefringence in quantum key distribution systems with polarization encoded photons. Decorrelation between Stokes vectors, both in time and frequency domains, can influence and limit the performance of both TDM- and WDM-based SOP control schemes. We have also presented a model for the minimum separation between reference and data signals in TDM-based SOP control schemes. A good agreement between theory and experimental data was observed.

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

[3] A. Poppe, "Method and device for readjusting a polarization drift," *United States Patent, no. US2008/0310856 A1*, Dec 18 2008.

[4] 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.

[5] 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.

[6] P. K. A. Wai and C. R. Menyuk, "Polarization mode dispersion, decorrelation, and diffusion in optical fibers with randomly varying birefringence," *J. Lightwave Technol.*, vol. 14, no. 2, pp. 148–157, 1996.

[7] N. J. Muga, N. A. Silva, M. Ferreira, and A. N. Pinto, "Evolution of the degree of co-polarization in high-birefringence fibers," *Optics Communications*, vol. 283, no. 10, pp. 2125 – 2132, 2010.

[8] 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.

[9] 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.

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

[11] N. J. Muga, M. Ferreira, and A. N. Pinto, "QBER Estimation in QKD Systems with Polarization Encoding," *submitted to IEE/OSA J. Lightwave Technol.*, 2010.

[12] ITU-T G. 694.1, "Spectral grids for WDM applications: DWDM wavelength grid," 2002.

[13] M. Karlsson and J. Brentel, "Autocorrelation function of the polarization-mode dispersion vector," *Optics Letters*, vol. 24, no. 14, pp. 939–941, 1999.

[14] C. D. Poole and R. E. Wagner, "Phenomenological approach to polarization dispersion in longe-single mode fibres," *Electron. Letters*, vol. 22, pp. 1029–1031, 1986.

[15] 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." *Journal of Modern Optics*, vol. 51, no. 9, pp. 1381–1398, 2006.

[16] IDQuantique, *id201 dtasheet*, www.idquantique.com, 2010.