Optimization of Polarization Control Schemes for QKD systems

Nelson J. Muga[a,b], Álvaro J. Almeida[a], Mário F. Ferreira[a], and Armando N. Pinto[a,c]

[a]Instituto de Telecomunicações, Campus de Santiago, 3810 Aveiro, Portugal;
[a]Departement of Physics, University of Aveiro, Campus de Santiago, 3810 Aveiro, Portugal;
[b]Departement of Electronics, Telecommunications and Informatics, University of Aveiro, Campus de Santiago, 3810 Aveiro, Portugal

ABSTRACT

In this work we develop an analysis of polarization control schemes suitable for quantum key distribution systems. Both time division multiplexing and wavelength division multiplexing based schemes are considered. A model for the optimization of the temporal separation between reference pulses and polarization encoded photons is presented. The model accounts for the reference pulse shape, the single photon detector gate width, and the respective temporal separation between them. The theoretical results are validated through experimental measurements. These results can be used to optimize the performance of polarization control schemes and therefore to optimize the polarization encoded quantum key distribution systems.

Keywords: Light polarization control, quantum key distribution systems, quantum bit error rate

1. INTRODUCTION

Quantum key distribution (QKD) systems use the natural laws of quantum mechanics, assuring in this way an unconditional secure distribution of secret keys.[1] The polarization encoding of single photons arises as a natural and promising approach for practical quantum key distribution systems. Nevertheless, in order to make this kind of encoding feasible, random polarization drifts should be compensated. These polarization changes cannot be reversed using traditional polarization controllers.[2] Indeed, active and efficient polarization control schemes, using feedback algorithms, are required. The state of polarization (SOP) control system can be implemented by multiplexing two non-orthogonal reference signals with the quantum information into the time or frequency domains.

Active full polarization control schemes using two classical signals at different wavelengths were reported by Xavier *et. al.*[3,4] The SOP control can also be performed using the same wavelength for both reference and data signals, and in such case the system should be able to alternate between data communication and the reference signals. Indeed, a method and device for readjusting the polarization drift in the QKD systems was already patented.[5] These setups can be implemented using classical signals,[5] where a switch alternates between the transmission of polarization encoded signals and the SOP control system, or using pulses with a low mean number of photons per pulse.[6,7] Chen *et. al.*[8] have presented an incremental real-time polarization control scheme where the reference and signal pulses are time delayed. These systems assure a continuous transmission of quantum data information with real-time polarization control. A maximum transmission distance of 50 km is reported. Muga *et. al.* have presented a model for quantum bit error rate (QBER) estimation in polarization encoded quantum key distribution systems, where both time division multiplexed (TDM) and wavelength division multiplexed (WDM) based polarization control schemes are analyzed.

In this paper, we develop an analysis of both TDM and WDM based polarization control schemes. A model for the optimization of the temporal separation between reference pulses and polarization encoded photons is

Further author information: (Send correspondence to N.J.M.)
N.J.M.: E-mail: muga@av.it.pt, Telephone: +351 234377900
A.J.A.: E-mail: aalmeida@av.it.pt, Telephone: +351 234377900
M.F.F.: E-mail: mfernando@ua.pt, Telephone: +351 234377900
A.N.P.: E-mail: anp@ua.pt, Telephone: +351 234377900

International Conference on Applications of Optics and Photonics, edited by Manuel F. M. Costa,
Proc. of SPIE Vol. 8001, 80013N · © 2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.892221

presented. The problematic related with the leakage of reference photons to the data single photon detector gate is also analyzed. Our model accounts for the reference pulse shape, the single photon detector gate width, and the respective temporal separation between them. The theoretical results are validated through experimental measurements using a commercial single photon detector module (SPDM) id201 from IdQuantique. Results presented here can be used to optimize the performance of the polarization control schemes and therefore to optimize the polarization encoded quantum key distribution systems.

This work is organized as follows. In Section II, we present the theoretical expressions describing the QBER of both TDM and WDM based polarization control schemes. Experimental results of photon-counts in a quantum data detector due to the reference pulse leakage are analyzed in section III. The main conclusions of this work are presented in section IV.

2. QUANTUM BER THEORY

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

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{error}}{R_{shift} + R_{error}} \approx \frac{R_{error}}{R_{shift}}, \tag{1}$$

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

2.1 WDM-based SOP control schemes

As refereed in the introduction, WDM-based SOP control schemes use two reference pulses with different wavelength. The correlation between the SOP of two signals depends on its wavelength separation. As much closer the wavelengths are, as stronger the correlation presented by the SOP. The degree of correlation between two Stokes vectors, at different frequencies, can be characterized by the respective frequency autocorrelation function ACF. This correlation function can be used to calculate the QBER expression for this kind of SOP control schemes[9]

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

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

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

2.2 TDM-based SOP control schemes

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

QBER can be written as[9]

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

where T_{rep} is the inverse of the pulse rate (f_{rep}), Δt is the temporal separation between the reference and data pulses, t_0 represents the drift time of the index difference between the fast and slow fiber axes, Θ and g are parameters related with the feedback SOP control,[9] η_{det} is the quantum detector efficiency, P_{af} is the afterpulse probability, $\langle n_g\rangle = A\langle n_r\rangle$ is the mean number of reference photons per pulse leaked to the data detector gate, with $\langle n_r\rangle$ being the mean number of reference photons per pulse, and the parameter A the fraction of photons that are leakage to the wrong detector.

The $QBER_{leak}$ contribution is directly related with the time separation between reference and data pulses. Indeed, the time position of the different signals propagated into the fiber can impose some limits on the maximum rate of the quantum channel. In the next section we analyze the optimization of the time separations between reference and data pulses.

3. EXPERIMENTAL RESULTS

Here we analyze experimentally the leakage of photons from the reference pulse to the data detector gate ($QBER_{leak}$), and its contribution to the total QBER. In TDM-based SOP control schemes, reference and quantum signals are time multiplexed, and generally both signals are present in the quantum data and reference arms. Therefore, in order to select the correct pulse, quantum data and reference detectors have the respective gates delayed by Δt, which equals the time separation between quantum and reference pulses.

The probability of photons traveling in the reference pulse be detected at the quantum data detector due to leakage, P_{leak}, will be dependent on the reference pulse shape, data gate width, and temporal separation between the reference and quantum data signals, Δt. Such probability can be written as

$$P_{leak} = \eta_{det} t_{link} \langle n_g\rangle. \tag{4}$$

Considering an ideal (square) quantum data gate with a width equal to T_g, and that the center of the quantum data gate and the center of the reference pulse are separated by Δt (see inset of Fig. 1), the fraction of photons that are leakage to the wrong detector, i.e., A is given by

$$A = \int_{\Delta t - T_g/2}^{\Delta t + T_g/2} |f(t)|^2\, dt, \tag{5}$$

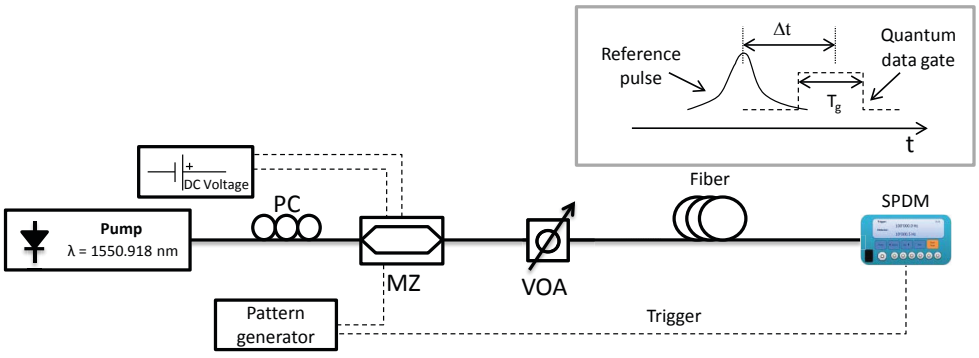

Figure 1. Experimental setup used to measure the leakage of reference photons to the gate of the data detector: PC - polarization controller, MZ - Mach-Zehnder modulator, VOA - variable optical attenuator, and SPDM - single photon detector module. A reference pulse and the data detector gate are schematically represented in the inset.

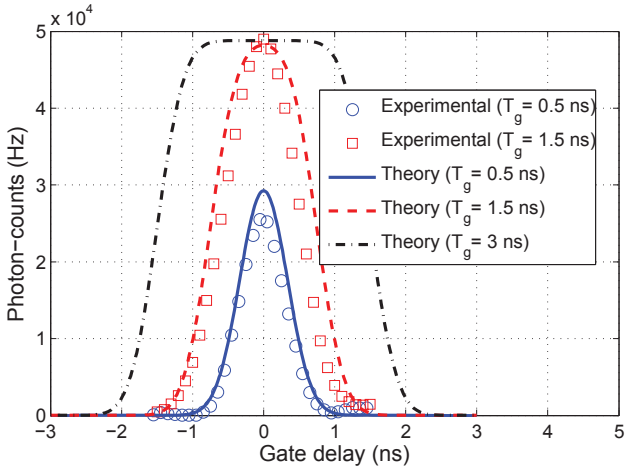

Figure 2. Experimental and theoretical photon-counts in a data detector due to the reference pulse leakage, considering a pulse with rate of 1.22 MHz, and a full width at half maximum equal to 0.7 ns. Tree gate widths equal to 0.5 ns (blue solid line), 3 ns (red dashed line), and 3 ns (black dashdot line) are theoretically considered. Experimental results are represented as blue circles (T_g =0.5 ns) and red squares (T_g =1.5 ns).

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

$$A = \frac{1}{2}\left[\mathrm{erf}\left(-\frac{(2\Delta t - T_g)}{2T_p}\right) + \mathrm{erf}\left(\frac{(2\Delta t + T_g)}{2T_p}\right)\right], \tag{6}$$

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 $T_{FWHM} = 2\sqrt{\ln 2}T_p$. In order to account for the pulse broadening due to chromatic dispersion, we should replace T_p in (6) by

$$T_p(z) = T_p\left[1 + (z/L_D)^2\right]^{1/2}, \tag{7}$$

where $L_D = T_p^2/|\beta_2|$ is the dispersion length.[10]

Assuming, for instance, that quantum 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, and P_{leak} is given by (4).

In order to analyze the separation between reference pulses and polarization encoded photons we have used the experimental setup schematically represented in Fig. 1. Reference pulses were obtained through a CW laser, centered at 1550.918 nm, whose light was pulsed using a Mach-Zehnder modulator (MZ). At the MZ output a variable optical attenuator (VOA) reduces the mean number of photons per pulse to a value lower than 1. An accurately trigged SPDM, operating in a gated Geiger mode,[11] is used to measure the photon counts.

The photon-counts given by (8) are represented in Fig. 2 as a function of time separation between the center of the reference pulse and the center of the gate, 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 $T_g = 3$ ns we observe that this occurs for $\Delta t \approx 2$ ns. We also observe that for large gate widths the maximum photon-counts saturates. This occurs when the gate completely overlaps the pulse. Figure 2 also shows the experimental data obtained with the SPDM from IDQuantique (id201). The detector has a dark count probability $P_{dc} = 2.55 \times 10^{-5}$, and a quantum detection efficiency $\eta_{det} = 10$ %. We used pulses with $T_{FWHM} = 0.7$ ns (and shape close to Gaussian), mean number

of photons $\langle n_r \rangle = 0.4$, and a repetition rate $f_{rep} = 1.22 \times 10^6$ Hz. We have performed the measurements using id201 gate widths equal to 2.5 ns and 5 ns. Note that although we have selected gate widths equal to 2.5 ns and 5 ns, these gate widths correspond to effective[12] gates widths of typically 0.5 ns and 1.5 ns, respectively. Broader gates will be incompatible with maximum id201 gate delay. Results presented in Fig. 2 show that the model presented in Section II is in good agreement with 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. Results show that pulses separations larger than 5 ns assure a very low number of counts.

4. CONCLUSION

We have analyzed the QBER for both TDM and WDM based polarization control schemes. A model for the optimization of the temporal separation between reference pulses and polarization encoded photons was presented. The problematic related with the leakage of reference photons to the data detector gate was also analyzed. Theoretical results were validated through experimental measurements using a SPDM from IdQuantique. Results presented here can be used to optimize the performance of the polarization control schemes and therefore to optimize the polarization encoded quantum key distribution systems.

ACKNOWLEDGMENTS

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

REFERENCES

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

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

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

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

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

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

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

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

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

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

[11] Ribordy, G., Gisin, N., Guinnard, O., Stuck, D., Wegmuller, M., and Zbinden, H., "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: Current performance.," *Journal of Modern Optics* **51**(9), 1381–1398 (2006).

[12] IDQuantique, *id201 datasheet*. www.idquantique.com (2010).