Algorithm for Compensation Random Drifts in Polarization Encoding Quantum Communications

Mariana F. Ramos, Andoni C. Santos, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto *Senior Member, IEEE, Member, OSA*

***Abstract*—A quantum bit error rate (QBER) based upper-layer protocol agnostic algorithm for polarization random drift compensation is proposed. The algorithm is based on the mapping of the QBER on the Poincaré sphere. The algorithm reverts the polarization random drift performing two QBER estimations and applying three rotations, at most. The uncertainty on the two QBER estimations defines an area over the sphere surface that lead to the QBER threshold value. In a "worst case" scenario, where a polarization linewidth of 900 nHz was considered, and assuming a 3% QBER threshold, the algorithm provides polarization basis alignment using less than 1.5% of overhead. In this scenario, an average QBER of 0.53% was maintained with a maximum estimated QBER value of 2.1%. In the case of a major external perturbation, that places the QBER well above threshold, the algorithm was also able to force the QBER to a value below the 3% threshold in less than 10 microseconds.**

***Index Terms*—Communications Society, IEEE, IEEEtran, journal, LaTeX, paper, template.**

I. Introduction

QUANTUM communications (QC) have been implemented using polarization encoding [1] [2]. Nevertheless, standard single-mode optical fibers do not preserve the state of polarization (SOP) and therefore an active polarization basis alignment (PBA) scheme is required, which preserves the quantum information [3]. In order to allow the large deployment of polarization encoding QC systems, the PBA scheme must be efficient, simple, upper layer protocol agnostic, and able to operate in a large variety of environment conditions.

In [3], the authors quantitatively analyze an interrupted and a real-time method to implement basis alignment. They assess both methods considering the polarization drift time and tracking speed, showing that interrupted PBA is only feasible in stable environments, like low mechanical-stressed buried fibers [3]. In real-time two different approaches have been presented: wavelength-division multiplexing polarization basis alignment (WDM-PBA) [4] [5] [6] [7], and time-division multiplexing polarization basis alignment (TDM-PBA) [5] [8] [9] [10]. In [6], a protocol agnostic scheme is proposed using WDM-PBA in aerial fibers. In [7] it was reported that polarization drift induces a QBER exceeding 2.5% in less than 7 ms in aerial-fibers, when no automatic compensation scheme is used. In [7], SOP tracking is performed using a hill-climbing algorithm in conjugation with a WDM polarization tracking scheme. In [10], it is shown that the achievable reach can be increased by using TDM-PBA based schemes. TDM-PBA may be implemented using classical [5] [8] or quantum reference signals [9]. In classical based TDM-PBA the co-propagation can produce a strong degradation in the weak quantum signals [5]. In [9], a TDM quantum reference signal is transmitted along with the quantum data signal, also avoiding the need of using classical and quantum receivers. In [11], a protocol dependent real-time scheme, free of reference signals is presented, where the QKD unveiled bits are used to feed the algorithm to compensate random polarization drifts. That method has the advantage of not add additional overhead, but is not protocol agnostic which can limit its usage. In [12], an accurate QBER estimation method is proposed, and a QBER based PBA method is presented. That method is simple, upper-layer protocol agnostic and able to operate under different external conditions [12]. However, it uses a blind algorithm to align the polarization basis, which makes it quite inefficient, namely under large external condition perturbations [6] [7]. In [13], a theoretical polarization drift model, which is able to describe random polarization rotations for installed fibers under different external conditions based on a single parameter is presented. This parameter, named polarization linewidth, mimics how fast the SOP changes with time [13]. In aerial fibers, due to random polarization drifts, transmission windows as short as 1 ms have been reported in polarization encoding quantum communication systems [14].

In this paper, we develop a method to compensate the polarization random drift in optical fibers by mapping the estimated QBER on the Poincaré sphere. We show that polarization random drift can be reversed applying appropriate polarization rotations on the Poincaré sphere, in three iterations at most. This method is able to operate under different external perturbations and it is upper-layer protocol agnostic, does not need auxiliary classical signals, extra spectral bands, nor additional hardware, and provides polarization basis alignment in less than tens of microseconds, which makes it suitable even for aerial fibers applications.

This work is supported by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), and by Regional Operational Program of Lisbon, under the projects QuantumMining reference: POCI-01-0145-FEDER-031826 and DSPMetroNet reference: POCI-01-0145-FEDER-029405, by FCT/MEC through national funds and when applicable co-funded by FEDER-PT2020 partnership agreement under the project UID/EEA/50008/2013 (actions QuantPrivNet, and COHERENTINUOUS), and by the FCT, through the Post-Doc Grant SFRH/BPD/96457/2013.

M. F. Ramos, N. A. Silva, and A. N. Pinto are with the Department of Electronics, Telecommunications and Informatics, University of Aveiro, Portugal, and Instituto de Telecomunicações, Aveiro, Portugal (Emails: marianaferreiraramos@ua.pt, nasilva@av.it.pt, anp@ua.pt).

N. J. Muga is with the Instituto de Telecomunicações, Aveiro, Portugal, and i3N, University of Aveiro, Campus UniversitÃąrio de Santiago, Aveiro, Portugal (Email: muga@av.it.pt).

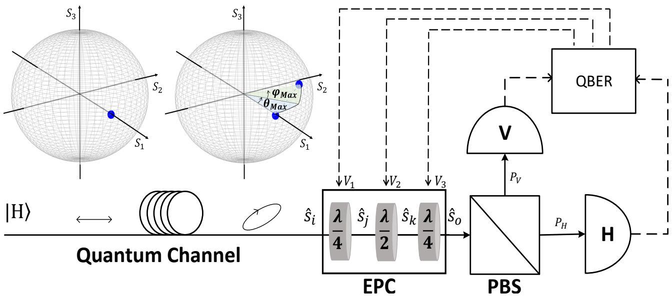
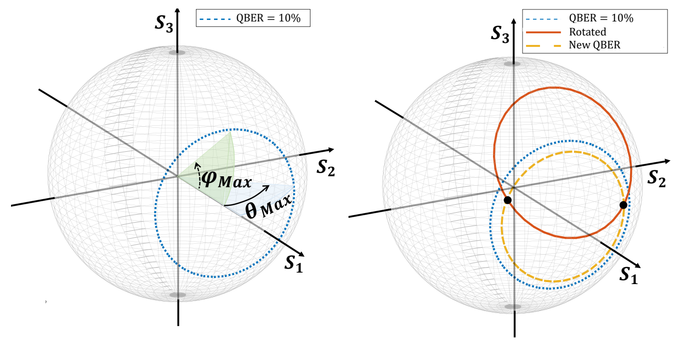


Fig. 1. Horizontal SOP evolution throughout an optical fiber, rotation stage, and detection probabilities at receiver (P_V and P_H). EPC: Electronic Polarization Controller. PBS: Polarization Beam Splitter. V: Single-photon detector in the PBS vertical port. H: Single-photon detector in the PBS horizontal port. V_1, V_2 and V_3: Voltages applied on the EPC to induce a certain rotation. Initially, it is assumed V_1, V_2 and V_3 equal to zero volts, therefore no rotation is induced in the EPC.



(a) (b)

Fig. 2. (a) Circle of a sphere with all possible states on Poincaré sphere that correspond to the QBER = 10%. (b) Circle of a sphere that corresponds to the QBER = 10% rotated considering $\theta_{\max}$ and $\varphi_{\max}$, and circle of a sphere with all possible states on Poincaré sphere that corresponds to the QBER after the previous rotation. The two • represent the two intersection points that correspond to the two possible SOP location.

This paper contains five sections. In section II, the algorithm is detailed. In section III, the QBER estimation impact on polarization compensation algorithm efficiency is discussed. In section IV the algorithm behaviour is assessed. A case study is considered assuming a continuous polarization random drift following [13]. Finally, in section IV the main conclusions of this work are summarized.

II. Algorithm Description

An optical field SOP can be represented in the 3D-Stokes space [13]. We start by showing that it is also possible to map the QBER on the Poincaré sphere. We assume a receiver with two single-photon detectors, see Fig.1. Without any loss of generality, an error at the receiver occurs when a horizontally polarized photon at the quantum communication channel input follows the vertical path of the polarization beam splitter (PBS) at the receiver, inducing a click on the detector V, see Fig.1. Note that any initial polarization state can be reduced to the previous case by a solid rotation of the Poincaré sphere, in the same way that any SOP can be used as a reference for the null QBER.

When a photon reaches the PBS it has the probability P_H to follow the horizontal path [10],

$$P_H = \frac{1}{2}(1 + \cos\theta\cos\varphi), \tag{1}$$

and has the probability P_V to follow the vertical path,

$$P_V = 1 - P_H, \tag{2}$$

where angles $\theta/2$ and $\varphi/2$ correspond to the orientation and ellipticity angles of the arriving photon SOP on Poincaré sphere representation, respectively [15]. Considering a horizontal state at the fiber input, we can write

$$\mathrm{QBER}(\theta,\varphi) = 1 - \frac{1}{2}(1 + \cos\theta\cos\varphi). \tag{3}$$

Therefore, a QBER specifies a set of possible orientation and ellipticity angles. This set of values define a circle of a sphere on the Poincaré sphere, which corresponds to a QBER with reference to a given initial state of polarization. In the present case, apart from an horizontal polarized photon at the input of the quantum communication channel, we are also assuming fully polarized light. Therefore the normalized Stokes parameter s_1 can be written as

$$s_1 = \cos(\theta)\cos(\varphi), \tag{4}$$

where $\theta \in [0, 2\pi]$, $\varphi \in [-\pi/2, \pi/2]$. The QBER can also be written in terms of s_1 as

$$\mathrm{QBER}(s_1) = \frac{1}{2}(1 - s_1). \tag{5}$$

Thus, the circle of a sphere resulting from a QBER value defines a set of possible SOP locations, which are at the same distance from the reference point,

$$d(\mathrm{QBER}) = 2\arcsin(\sqrt{\mathrm{QBER}}). \tag{6}$$

As we can see in Fig.2a, a single value of QBER has more than one possible polarization random drift associated with it, even though a single received SOP leads to a single QBER value. Lets assume that a particular polarization rotation leads to a QBER of 10%, see Fig. 2a. Looking into Fig.2a we can see that the polarization random drift still remains unknown, although it is restrict to rotations that lead the SOP from $(s_1, s_2, s_3)^T = (1, 0, 0)^T$, i.e. a horizontal initial state of polarization, to a point on the circle of the sphere that represents the 10% QBER. A subsequent deterministic rotation in conjunction with a new QBER calculation allows to reduce the number of possible polarization random drifts to only two possibilities, see Fig. 2b. Note that a rotation can be characterized by the two angles, θ and φ,

$$\mathrm{R_T}(\theta,\varphi) = \mathrm{R_1}(\varphi)\mathrm{R_2}(\varphi)\mathrm{R_3}(\theta), \tag{7}$$

where, $\mathrm{R_1}$, $\mathrm{R_2}$, and $\mathrm{R_3}$ are the rotation matrices around the axis S_1, S_2, and S_3, respectively,

$$\mathrm{R_1}(\varphi) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{bmatrix}, \tag{8}$$

$$\mathrm{R_2}(\varphi) = \begin{bmatrix} \cos\varphi & 0 & \sin\varphi \\ 0 & 1 & 0 \\ -\sin\varphi & 0 & \cos\varphi \end{bmatrix}, \tag{9}$$

and

$$\mathrm{R}_{\mathbf{3}}(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{10}$$

Once a rotation has been performed, as shown in Fig.2b, another calculation of QBER is done. Lets assume the performed rotation was done using the orientation angle $\theta_{\max}/4$ and ellipticity angle $\varphi_{\max}/4$, where $\theta_{\max}$ and $\varphi_{\max}$ are the maximum angles defined by the circle of the sphere corresponding to the first QBER value calculated, see Fig. 2a. A new value for QBER allows to draw another circle of a sphere on Poincaré sphere, which intercepts the previous rotated circle in two points, which are shown in Fig. 2b with circle marks. Therefore, the initial infinite number of possible polarization random drifts is reduced to only two possibilities, which correspond to the two intersection points. In order to obtain an analytical expression for the two intersection points, we can consider the parametric equations of a 3D circle, see (11). Note that m takes the value 1 for the initial QBER rotated circle, and 2 for the circle of a sphere after the QBER recalculation,

$$\begin{cases} x^{(m)} = x_c^{(m)} + r_m \cos(\phi) x_{m1} + r_m \sin(\phi) x_{m2} \\ y^{(m)} = y_c^{(m)} + r_m \cos(\phi) y_{m1} + r_m \sin(\phi) y_{m2} \\ z^{(m)} = z_c^{(m)} + r_m \cos(\phi) z_{m1} + r_m \sin(\phi) z_{m2} \end{cases}, \tag{11}$$

where ϕ is a real value between 0 and 2π.

In (11), $(x_c^{(m)}, y_c^{(m)}, z_c^{(m)})$ are the center coordinates, and r_m is the radius of each circle m. Note that after measuring the QBER, a circle of sphere is defined. From (3), $(x_c^{(m)}, y_c^{(m)}, z_c^{(m)})$, r_m, and the plane containing the circle defined by the orthogonal vector $\vec{n} = \vec{v}_{m1} \times \vec{v}_{m2}$, where $\vec{v}_{m1} = (x_{m1}, y_{m1}, z_{m1})$ and $\vec{v}_{m2} = (x_{m2}, y_{m2}, z_{m2})$, can be readily obtained.

The two measured QBER values define two circles of a sphere that intersect in two points, which can be obtained from

$$\begin{cases} x^{(1)} = x^{(2)} \\ y^{(1)} = y^{(2)} \\ z^{(1)} = z^{(2)} \end{cases}, \tag{12}$$

and represented in the 3D-Stokes space by,

$$\begin{aligned} s_1^{(n)} &= \cos\theta^{(n)} \cos\varphi^{(n)} \\ s_2^{(n)} &= \sin\theta^{(n)} \cos\varphi^{(n)} \\ s_3^{(n)} &= \sin\varphi^{(n)}, \end{aligned} \tag{13}$$

where $n \in \{1, 2\}$. Subsequently, the algorithm chooses a value of n to perform a new rotation. Lets assume that we pick $n = 1$. After applying a rotation with angles $(\theta^{(1)}, \varphi^{(1)})$, the QBER is recalculated, see (3). If the QBER approaches zero, the polarization random drift has been compensated. Otherwise, the polarization random drift compensation can now be uniquely calculated, and the compensation can be performed applying the rotation matrices,

$$\mathrm{R_T}(\theta^{(2)}, \varphi^{(2)}) \mathrm{R_T}^{-1}(\theta^{(1)}, \varphi^{(1)}). \tag{14}$$

In any of the two scenarios, the algorithm needs only three QBER calculations and three rotations at most to revert the polarization random drift due to birefringence effects along the optical fiber link.

To summarize, the algorithm comprises the following stages:

label=

1) Map the circle corresponding to the QBER calculated on Poincaré sphere according with (3), see Fig.2a.
2) Perform a rotation with a given θ and φ, see Fig.2b.
3) Calculate a new QBER, see Fig.2b. If the QBER decreases bellow a user defined threshold the algorithm stops to actuate in the current mode. Otherwise, it continues as following.
4) Find the two intersection points, see (12) and (13).
5) Choose one out of the two intersection points to perform a new rotation, so that $\mathrm{R_T}(\theta^{(i)}, \varphi^{(i)})\hat{s}^{(n)} = (1, 0, 0)^T$, see (7).
6) Re-calculate the QBER. If the QBER approaches zero, the polarization random drift has been reverted. Otherwise, perform another rotation following (14).
7) The random polarization drift is reverted.

Note that the voltages applied on the EPC, V_1, V_2, V_3, can be written in terms of angles θ and φ. These voltages induce a certain phase shift on the wave-plates, which implies a rotation of the SOP based on a set of rotation angles, χ_1, χ_2, χ_3. These angles can be written in terms of the orientation and ellipticity angles, θ and φ. Looking into Fig. 1, a random SOP $\hat{s}_i$ inputs the EPC facing the first quarter-wave-plate(QWP) that outputs, in turn, the state of polarization $\hat{s}_j$,

$$\hat{s}_j = \mathrm{R}(\chi_1) \mathrm{M}_{\lambda/4} \mathrm{R}(-\chi_1) \hat{s}_i, \tag{15}$$

where $\mathrm{M}_{\lambda/4}$ is the QWP matrix [16] and $\mathrm{R} = \mathrm{R}_{\mathbf{3}}(2\chi_1)$ is the rotation matrix of the wave-plate . The angle χ_1 is given by [16],

$$\chi_1 = \frac{1}{2} \arctan\left(\frac{\sin\theta\cos\varphi}{\cos\theta\sin\varphi}\right). \tag{16}$$

The second wave-plate is a half-wave-plate (HWP), and transforms the linear SOP $\hat{s}_j$ into another linear SOP [16], which in practice means a rotation by θ around S_3 when $\varphi = 0$,

$$\hat{s}_k = \mathrm{R}(\chi_2) \mathrm{M}_{\lambda/2} \mathrm{R}(-\chi_2) \hat{s}_j, \tag{17}$$

where, $\mathrm{M}_{\lambda/2}$ is the HWP matrix, and $\hat{s}_j = (s_{1j}, s_{2j}, 0)^T$ defined by (10) in [16]. In this way,

$$\chi_2 = \frac{1}{4} \arctan\left(\frac{s_{2j}}{s_{1j}}\right), \tag{18}$$

where, s_{1j}, s_{2j} are defined by (19) and (20), respectively.

$$\begin{aligned} s_{1j} &= s_{1i}\cos^2(2\chi_1) + s_{2i}\cos(2\chi_1)\sin(2\chi_1) \\ &\quad + s_{3i}\sin(2\chi_1), \end{aligned} \tag{19}$$

$$\begin{aligned} s_{2j} &= s_{1i}\cos 2\chi_1 \sin(2\chi_1) + s_{2i}\sin^2(2\chi_1) \\ &\quad - s_{3i}\cos(2\chi_1), \end{aligned} \tag{20}$$

In addition, $s_{1i} = \sin\theta\cos\phi$ and $s_{2i} = \cos\theta\sin\varphi$, see (13). Finally, the EPC output SOP is defined as,

$$\hat{s}_o = \mathrm{R}(\chi_3) \mathrm{M}_{\lambda/4} \mathrm{R}(-\chi_3) \hat{s}_k, \tag{21}$$

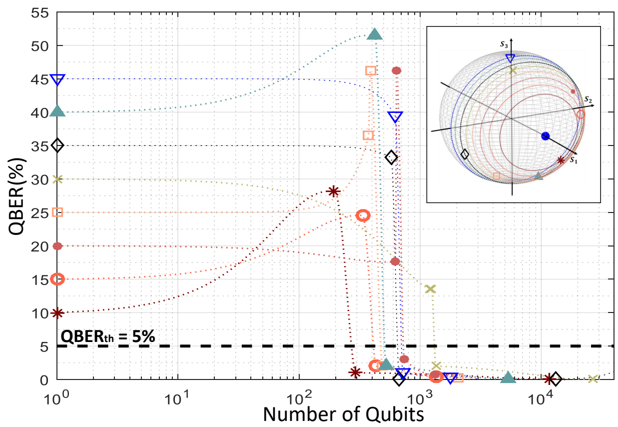


Fig. 3. QBER evolution during random polarization random drift compensation algorithm running. Markers represent QBER measurements. The SOP locations are represented on the inset sphere on the right.

where,

$$\chi_3 = \frac{1}{2}\arctan\left(\frac{s_{2k}}{s_{1k}}\right). \tag{22}$$

Fig. 3 shows numerical results for different initial QBER values between 10% and 45%. Note that in a practical scenario QBER is estimated taken into account a certain number of received qubits, N_r using

$$\widehat{\text{QBER}} = \frac{e_r}{N_r}, \tag{23}$$

where e_r is the number of errors in N_r qubits [12]. This estimation is performed with a certain confidence interval which depends on the number of qubits that we use to perform it. In this section, we are assuming that N_r is large enough to provide an accurate estimation of the QBER. In the next section, we are going to consider the impact of N_r during the algorithm's running. We also assume a threshold $\text{QBER}_{\text{th}} = 5\%$. Above the threshold, the quantum communication system cannot operate. The goal of the presented algorithm is to force the QBER to be below the threshold. Fig. 3 shows eight different cases corresponding to different initial conditions, where it is shown that regardless the respective initial QBER, the final QBER is always below the threshold. The inset in Fig. 3 shows the location of the different SOPs on Poincaré sphere, where each one is on the circle of a sphere corresponding to the QBER measured. In Fig. 3 every case starts from an initial QBER estimation, i.e the first marker. The algorithm starts from this initial QBER estimation and performs the first rotation. The second marker is the QBER estimation after the first rotation. Here, the algorithm chooses one of the two intersection points, see (12). After that, we wait for a 5 errors event, or for 100 qubits received to estimate the new QBER. Note that more than 5 errors implies an estimated QBER larger than the threshold, in this case where a 5% threshold was assumed. When it wrongly chooses the intersection point, the next marker is a QBER above the QBER_{th}. On the other hand, when it rightly chooses the intersection point, the next marker is a QBER below threshold, and the following. A final marker with a high accuracy on QBER estimation is also included in the figure, to show the proper operation of the algorithm. In Fig.3, we have shown that the algorithm compensates any polarization random drift leading the initial QBER to a value below the threshold after two or three rotations, at most.

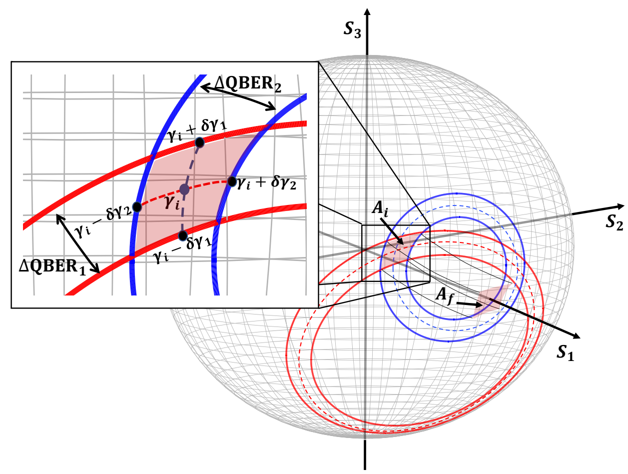


Fig. 4. Representation of the area defined by the uncertainties of the first and second QBER estimations on the Poincaré sphere surface, A_i. This area is preserved after the final rotation, i.e. $A_i = A_f$.

III. Impact of QBER Estimation accuracy

In order to assess the impact of the QBER estimation accuracy in the algorithm performance, we are going to use a new coordinate γ, such that

$$\cos(\gamma) = \cos\theta\cos\varphi, \tag{24}$$

where γ is the angle between the axis S_1, and the vector defined by the SOP. In this way, the QBER in (3) can be written in terms of γ as

$$\text{QBER}(\gamma) = \frac{1}{2}(1-\cos\gamma). \tag{25}$$

The number of qubits required for each algorithm iteration is the sum of the qubits used for each QBER estimation, occurring in stages (i), (iii) and (vi), see section II. The last QBER estimation, at stage (vi), does not lead to any rotation, and therefore does not require high accuracy. In this way, we can assume that

$$n_1, n_2 \gg n_3, \tag{26}$$

where n_1, n_2 and n_3 are the number of qubits used in QBER estimations at (i), (iii), and (vi), respectively. Therefore, the total number of qubits required to compensate the polarization random drift can be written as, see (15) from [12],

$$\begin{aligned} n_b &\simeq n_1(\Delta\text{QBER}_1, \text{QBER}_1, \alpha) \\ &+ n_2(\Delta\text{QBER}_2, \text{QBER}_2, \alpha), \end{aligned} \tag{27}$$

where ΔQBER_1 and ΔQBER_2 are the uncertainty associated with the QBER_1 and QBER_2 estimations at stage (i) and (iii) of the algorithm, respectively, and $1-\alpha$ is the confidence interval. Note that the QBER estimation uncertainty, at stages (i) and (iii), can be written as

$$\Delta\text{QBER}_i = \text{QBER}(\gamma_i + \delta\gamma_i) - \text{QBER}(\gamma_i - \delta\gamma_i), \tag{28}$$

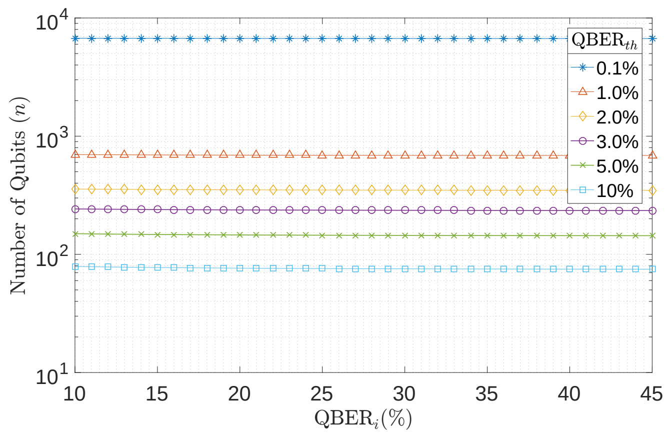
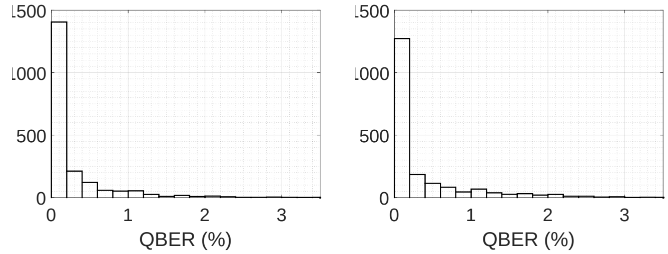


Fig. 5. Number of qubits, n, required for each QBER estimation, at stages (i) and (iii) of the algorithm, aiming to reach a final QBER below the threshold. A confidence interval of $1-\alpha = 99\%$ was used, and n was calculated for different $\mathrm{QBER_{th}}$ considering an initial QBER from 10% to 45%.



(a) Initial QBER of 10%

(b) Initial QBER of 40%

Fig. 6. Histogram of the final QBER for two different values for the initial QBER. A $\mathrm{QBER_{th}}$ of 3% was defined as well as a confidence level of 99% for each QBER estimation, at stages (i) and (iii) of the algorithm.

where $\delta\gamma_i$ is the maximum deviation on γ_i, see Fig. 4. At stage (iv) of the algorithm, i.e. after two QBER estimations, an area can be defined due to the QBER estimation uncertainties, see inset on Fig. 4.

From (25) and (28), the uncertainty $\Delta\mathrm{QBER}_i$ at stages (i) and (iii) can be related to the corresponding γ_i, as well as to $\delta\gamma_i$, using

$$\Delta\mathrm{QBER}_i \approx \delta\gamma_i \sin\gamma_i. \tag{29}$$

The induced rotation into the SOP associated with the QBER estimations, at stage (v), is going to place the uncertainty area, A_i, around the target SOP, preserving its shape, A_f, as shown in Fig. 4. Note that the final QBER, QBER_f, is null at $\gamma_f = 0$, therefore from (25) we obtain

$$\Delta\mathrm{QBER}_f = \mathrm{QBER}(\delta\gamma_f) \approx \frac{\delta\gamma_f^2}{4}. \tag{30}$$

The final QBER estimation uncertainty depends on the first and second QBER estimations, and as a consequence, the $\Delta\mathrm{QBER}_f$, see (30), depends on the $\delta\gamma_1$ and $\delta\gamma_2$. Note that the uncertainties $\Delta\mathrm{QBER}_1$ and $\Delta\mathrm{QBER}_2$ define an area that remains constant after the final rotation, see Fig. 4. In the worst case scenario, $\delta\gamma_f$ will be the sum of both uncertainties $\delta\gamma_1$ and $\delta\gamma_2$,

$$\delta\gamma_f \leq \delta\gamma_1 + \delta\gamma_2. \tag{31}$$

For a given confidence interval $1-\alpha$, the algorithm satisfies

$$P(\mathrm{QBER}_f \geq \Delta\mathrm{QBER}_f) \leq 2\alpha. \tag{32}$$

Following this discussion, we can calculate the number of qubits required for QBER estimation at stages (i) and (iii) of the algorithm, so that the polarization control random drift algoritm assures a QBER_f below a certain QBER threshold, $\mathrm{QBER_{th}}$, with a certain probability. Note that in a small rotation regime in stage (ii), we can also assume that $\delta\gamma_1 \approx \delta\gamma_2 \approx \delta\gamma$, and $\gamma_1 \approx \gamma_2 \approx \gamma$, which implies $\Delta\mathrm{QBER}_1 \approx \Delta\mathrm{QBER}_2$. Therefore $n_1 \approx n_2 \approx n$, and so that the total number of required qubits will be $n_b = 2n$.

Fig. 5 shows the number of qubits used to perform each QBER estimation, n, calculated given a certain $\mathrm{QBER_{th}}$, using (30) and (31) to calculate $\delta\gamma$, and using (25) to obtain γ in order to obtain the initial QBER uncertainty. Using the initial QBER uncertainty, the initial QBER, and for a given confidence level using (27), we can obtain the total number of required qubits, n_b, and subsequently n, the number of qubits to estimate QBER in stage (i) and (iii). Fig. 5 shows that the number of qubits required, n, is almost independent of the initial QBER, QBER_i. On the contrary, the final QBER threshold has a high impact on the number of qubits required. As one can see in Fig. 5 the number of qubits is inversely proportional to the QBER threshold, i.e for smaller $\mathrm{QBER_{th}}$ a larger number of qubits is required. Table I summarizes the number of qubits required for each QBER estimation, at stages (i) and (iii), for a given QBER threshold.

TABLE I
NUMBER OF QUBITS REQUIRED FOR ESTIMATION OF QBER IN TERMS OF UNCERTAINTY $\mathrm{QBER_{TH}}$ FOR A CONFIDENCE LEVEL OF 99%.

$\mathrm{QBER_{th}}$	$n(\mathrm{QBER_{th}})$
0.1 %	6743
1.0 %	699
2.0 %	357
3.0 %	243
5.0 %	150
10.0 %	79

In order to assess the algorithm, we perform a simulation for a QBER threshold of 3%, considering two initial values for QBER, 10% and 40%. The SOP at the receiver input is randomly chosen between all possible SOP on the circle of a sphere corresponding with the desirable initial QBER. Following Table I, and considering the 3% threshold, we use 243 qubits to estimate each QBER, at stages (i) and (iii) of the algorithm. We run 1000 simulations for each initial QBER, and the results are shown in Fig. 6. Moreover, the reached QBER estimation was performed with a high accuracy, 3500 qubits were used. Note that this estimation is not part of the algorithm, and it was only performed here to assess the algorithm performance. The obtained results shows that for an initial QBER of 10% and 40%, the reached QBER is above the $\mathrm{QBER_{th}}$ only in 1.3% and 1.8% of the cases, respectively, which is in good agreement with (32), considering a confidence level of 99%, i.e. $\alpha = 1\%$.

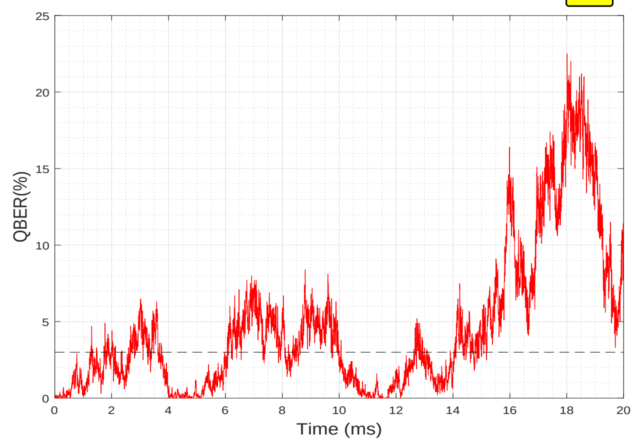
IV. Case Study

We applied the proposed algorithm to a realistic quantum optical communication system using polarization encoding. We assumed that the system operates at 100 Mqubit/s, which is a reasonable value considering current single photon detectors technology [17]. We also assumed that the number of photons in the control qubits was adjusted to make the non-click probability and the double-click probability negligible. Our goal was to maintain the QBER threshold and protocol overhead bellow 3%. These values should allow current quantum communication protocols to operate smoothly [18][19].

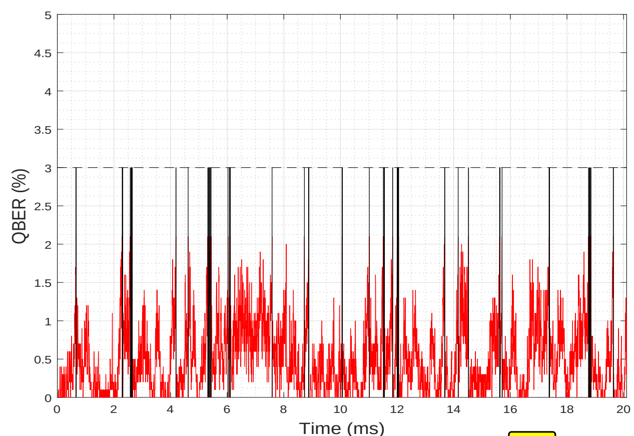
Under heavy external conditions, for instance in aerial optical fiber installations, polarization can remain stable in a window as short as 1 ms [14]. To consider this "worst case" scenario, we modeled the polarization drift following [13], with a polarization linewidth of 900 mHz. In Fig. 7a, we plotted the QBER evolution without any polarization control scheme, and as it is shown, after basis alignment the QBER only remains below the QBER threshold in time windows with a duration around 1 ms.

The polarization control system comprises two operation modes: a monitoring mode and an actuation mode. In the monitoring mode the QBER is continuously estimated using a user defined sliding window. We assumed a 1 ms sliding window for the QBER estimation. The user also defines a QBER_{min}, smaller than the QBER threshold. As long as the estimated QBER remains below this QBER_{min}, the algorithm runs only in the monitoring mode. We assumed a 2% value for the QBER_{min}. Considering the QBER_{th} of 3% and the uncertainty values associated with the QBER estimation presented in table I, we used 1 control bit in each 300 qubits for QBER monitoring, which allows to estimate the QBER in the 1 ms sliding window with 333 qubits. Note that the number of single photons in the control qubits was adjusted to make the non-click probability negligible. When the QBER rises above the QBER_{min}, the algorithm enters in the actuation mode. In this mode, the algorithm follows the steps presented in section III. In the actuation mode, all transmitted qubits are used for polarization control. After the algorithm actuation, the QBER estimation window is reset.

In order to assess the algorithm's performance, we measured the algorithm's overhead, actuation frequency, average QBER, and maximum QBER. The algorithm's overhead is defined as the ratio between the sum of qubits used for polarization monitoring and control, and all transmitted qubits. The algorithm's actuation frequency is defined as the number of times that the algorithm actuates per unit of time. The average and maximum QBER are calculated considering the data qubits. To demonstrate the algorithm execution on the defined scenario, we performed several simulations during 20 ms time windows. To emulate a major external perturbation, we induced a random polarization rotation at 10 ms which imposed a QBER of 25%, i.e. a value well above the QBER_{th}. In Fig. 7b, we present the results of a single simulation run, all the other results are similar.



(a)



(b)

Fig. 7. (a) - QBER monitoring during a 20 ms time window without polarization random drift control scheme. (b) - QBER monitoring during 20 ms time window with actuation of the proposed algorithm for polarization random drift compensation.

Fig. 7a shows the impact on QBER of random polarization drift with time, according with the defined polarization linewidth with no polarization control scheme. Fig. 7b shows the evolution of QBER according with the same polarization linewidth, but using the proposed polarization random drift control algorithm. As it is shown, whenever the QBER rises above the QBER_{min}, 2.0%, the algorithm actuates. Note that even at 10 ms, where a major external perturbation was induced, the algorithm actuates as soon as the estimated QBER rises above 2.0%, being able to reestablish the qubits data transmission in less than 10 microseconds, assuming a negligible actuation time for the EPC. The actuation times are represented by vertical lines in the plot. The width of the lines correspond to the algorithm actuation time. In average, the algorithm actuates 1.9 times per millisecond, imposing an overhead of 1.23%. The average QBER during data qubits transmission is 0.52%, and a maximum QBER of 2.1% was obtained.

V. Case study II

In this section, other error sources are considered. We will first analyze the power losses throughout the optical fiber chan-

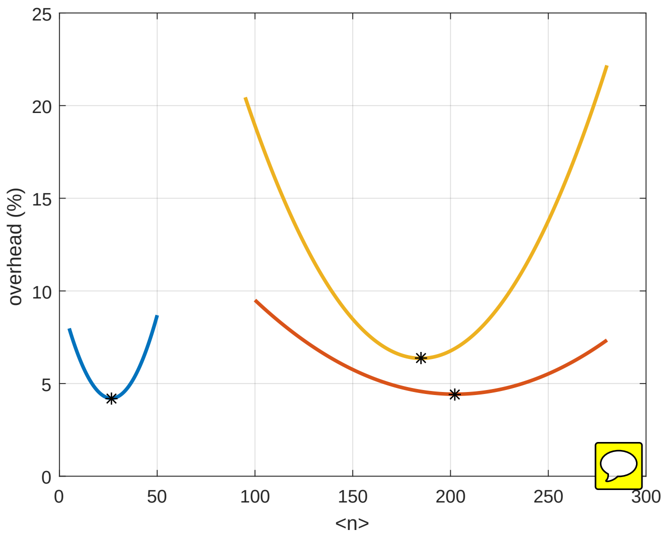


Fig. 8. Overhead measured for different average number of photons per control pulse. Four different scenarios were simulated considering 80 km and 40 km for fiber length. For each fiber length the overhead were measured considering the EPC actuation time and considering it negligible. The EPC actuation time induces an overhead less than 2% and an optimum number of 5 photons per control pulse was found.

nel. We assumed a typical value for attenuation of 0.2 dB/km, which is the loss through a silica optical fiber for 1550 nm [20]. Since we are working on a quantum regime, the effect of attenuation will highly impact the no-click probability. Furthermore, the no-click event is also caused by the detection efficiency of single-photon detectors. In order to overcome the issues related with no-click events, and reduce its impact on algorithm's performance, the number of photons in control pulses is optimized. By increasing the number of photons in each control pulse, where the photons are not perfectly aligned due polarization random drift, can lead to double-click events. These events are also caused by dark-counts, which depend in part on single-photon detectors efficiency. Both, no-click and double-click events will impact the overhead consumed by the algorithm, since the qubits measured in that situation are discard and not taken into account for QBER estimation. Now, the need to established a balanced number of photons in control pulses has arisen, and they should be defined to be convenient for the best trade-off between both no-click and double-click events. In this way, we perform the same simulation considering different numbers of photons per control, with a transmission rate of 100 Mqubits/s, an average number of photons per data pulse of 0.1 at the transmitter output, since it assures a pulse intensity that prevents beam splitting attacks [21]. Two optical fiber channel with a lengths were defined to perform these simulations, 80 km and 40 km. Fig. 8 shows the results for both optical fiber lengths. The number of photons per control pulse presented in Fig. 8 refer to the number of photons at the transmitter output, which in both cases correspond to approximately 5 photons per pulse at the receiver's input.

We now add the actuation time of EPC to our system. Due technological limitations, the EPC does not induce an instantaneous rotation, and it demands a certain time interval to stabilize the output SOP. In this way, the EPC actuation time should be considered in the system assessment. An EPC actuation time of 20μs was assumed [6], which corresponds to increase the overhead by 2000 qubits in each performed rotation for a transmission rate of 100 MQubits/s. Fig. 8 also shows the overhead resulted from adding the EPC actuation time for both cases, an optical fiber length of 40 km and 80 km. Two simulations were performed for a total acquisition time of 20 ms, one taken into account the EPC actuation time and other assuming a negligible EPC actuation time. Figure 8 shows that the EPC actuation time interval adds an overhead lower than 2%.

VI. Conclusion

We presented an algorithm to automatically compensate the polarization random drift in polarization-encoding based quantum transmission systems. This algorithm is based on QBER estimation and on its representation on the Poincaré sphere. From the estimated QBER, a circle on the Poincaré sphere is defined leading to a set of possible polarization states. By performing a deterministic rotation, the algorithm reduces this set of polarization states to only two possible SOP. From this two possible states of polarization the algorithm is able to compensate the polarization random drift in a very short time.

It was shown that the polarization random drift control algorithm is always able to force the QBER to a value bellow a user-defined threshold in three iterations, at most. In addition, the uncertainty in the final QBER was related with an area calculated in the Poincaré sphere surface based on two QBER estimation uncertainties. From this area, we obtain the number of qubits required in the QBER estimations to guarantee a final QBER bellow the threshold.

Moreover, the proposed algorithm was applied on a first case study, where a polarization linewidth of 900 nHz was assumed, which limits the transmission window to around 1 ms, and other error sources were assumed negligible. The algorithm was capable of maintain the QBER bellow the 3% threshold using only 1.3% of overhead, with an average QBER of 0.52%, and a maximum QBER of 2.1%. Furthermore, the algorithm was also applied to a case study taken into account other system source errors, such as attenuation, single-photon detectors efficiency and technological hardware limitations like the EPC actuation time. An optimum average number of photons per control pulse of 5 was found, although the overhead increased compared with the previous case study. Still, the algorithm was able to keep the data transmission QBER bellow the 3% defined threshold.

References

[1] K. Takemoto, Y. Nambu, T. Miyazawa, Y. Sakuma, T. Yamamoto, S. Yorozu, and Y. Arakawa, "Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors," *Scientific reports*, vol. 5, p. 14383, 2015.

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.

[3] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Polarization variations in installed fibers and their influence on quantum key distribution systems," *Optics express*, vol. 25, no. 22, pp. 27 923–27 936, 2017.

[4] G. Xavier, G. V. de Faria, G. Temporão, and J. Von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," *Optics express*, vol. 16, no. 3, pp. 1867–1873, 2008.

[5] G. Xavier, N. Walenta, G. V. De Faria, G. Temporão, N. Gisin, H. Zbinden, and J. 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, p. 045015, 2009.

[6] D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen *et al.*, "Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback," *Optics Express*, vol. 26, no. 18, pp. 22 793–22 800, 2018.

[7] T. Pengyi, L. Guochun, G. Song, Y. Gang, D. Yunqi, X. Yao, L. Dongdong, Z. Yinghua, W. Bing, Z. Ziyan, G. Dequan, L. Jianhong, and W. Jian, "Fast polarization feedback algorithm for quantum key distribution with aerial fiber for power grid," *Acta Optica Sinica*, vol. 38, no. 1, p. 0106005, 2018.

[8] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, "Active polarization stabilization in optical fibers suitable for quantum key distribution," *Optics express*, vol. 15, no. 26, pp. 17 928–17 936, 2007.

[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, p. 065004, 2009.

[10] N. J. Muga, M. F. Ferreira, and A. N. Pinto, "QBER estimation in QKD systems with polarization encoding," *Journal of Lightwave Technology*, vol. 29, no. 3, pp. 355–361, 2011.

[11] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, S. Wang, Z.-Q. Yin, G.-C. Guo, Z.-F. Han *et al.*, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," *Optics letters*, vol. 42, no. 6, pp. 1023–1026, 2017.

[12] Á. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. André, and A. N. Pinto, "Continuous control of random polarization rotations for quantum communications," *Journal of Lightwave Technology*, vol. 34, no. 16, pp. 3914–3922, 2016.

[13] C. B. Czegledi, M. Karlsson, E. Agrell, and P. Johannisson, "Polarization drift channel model for coherent fibre-optic systems," *Scientific reports*, vol. 6, p. 21217, 2016.

[14] R. Liu, H. Yu, J. Zan, S. Gao, L. Wang, M. Xu, J. Tao, J. Liu, Q. Chen, and Y. Zhao, "Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design," *Optical Fiber Technology*, vol. 48, pp. 28–33, 2019.

[15] D. H. Goldstein, *Polarized Light, revised and expanded*. CRC press, 2003.

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

[17] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in ingaas/inp single-photon detector systems for quantum communication," *Light: Science & Applications*, vol. 4, no. 5, p. e286, 2015.

[18] L. Bouchoucha, S. Berrah, and M. Sellami, "Influence of experimental parameters inherent to optical fibers on quantum key distribution, the protocol bb84," *Semiconductor Physics, Quantum Electronics & Optoelectronics*, vol. 21, no. 1, pp. 73–79, 2018.

[19] M. Lopes and N. Sarwade, "On the performance of quantum cryptographic protocols sarg04 and kmb09," in *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*. IEEE, 2015, pp. 1–6.

[20] G. Agrawal, *Nonlinear Fiber Optics*, 5th ed. Academic Press, 10 2012.

[21] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

Mariana F. Ramos Biography text here.