IET Optoelectronics

Special Section: 2019 International Microwave and Optoelectronics Conference

FPGA-assisted state-of-polarisation generation for polarisation-encoded optical communications

ISSN 1751-8768
Received on 5th March 2020
Revised 21st May 2020
Accepted on 10th June 2020
E-First on 21st July 2020
doi: 10.1049/iet-opt.2020.0035
www.ietdl.org

Nelson J. Muga[1,2] ✉, Mariana F. Ramos[1,3], Sara T. Mantey[1,2], Nuno A. Silva[1], Armando N. Pinto[1,3]
[1]*Instituto de Telecomunicações, Universidade de Aveiro, Campus de Santiago, 3810-193 Aveiro, Portugal*
[2]*Department of Physics, University of Aveiro, Campus de Santiago, 3810-193 Aveiro, Portugal*
[3]*Department of Electronics, Telecommunications, and Informatics, University of Aveiro, Campus de Santiago, 3810-193 Aveiro, Portugal*
✉ *E-mail: muga@ua.pt*

Abstract: This study presents a theoretical model for polarisation manipulation using electronic polarisation controllers (EPCs) based on fibre squeezing. A method to calculate the EPC configuration in order to transform between two arbitrary states of polarisation (SOP) is presented. After, a technique to deterministically generate four SOPs for use in polarisation-encoded quantum communication systems is proposed. Moreover, the effectiveness of the proposed technique is experimentally assessed through the generation of two pairs of orthogonal SOPs. The experimental implementation used an field programmable gate array (FPGA) board to electrically control the four waveplates of the EPC, reaching a rate of 500 qubit/s. Results show that this polarisation generation process is intrinsically stable, demonstrating its potential for practical implementations of polarisation-encoding quantum key distribution systems using the BB84 and B92 protocols.

1 Introduction

Communication security is of strategic importance as our sensitive personal financial and health data, as well as commercial and national secrets, are routinely being transmitted through the telecommunication infrastructure. For instance, an optical signal can be easily tapped, once the physical access to the optical fibre is available, thus exposing the data of millions of users and billions of applications to theft or manipulation [1]. Therefore, it is getting more important, in addition to protecting computer systems and personal devices, to also better safeguard our network infrastructure against data leakage and unexpected service outages. In this regard, the unique features of quantum physics enable quantum key distribution (QKD) technology to promise unconditional security [2].

When using single photons to encode the quantum states, different physical properties can be selected for encoding [3, 4]. Usually, QKD systems employ polarisation- or phase-encoding schemes, with the former presenting some practical advantages over the latter, namely in free-space optics applications. This has to do with the difficulty to maintain the state-of-polarisation (SOP) of an optical signal when travelling in an optical fibre due to the existence of an intrinsic residual birefringence. This residual birefringence arises in standard single-mode fibres due to loss of circular symmetry. In practice, such loss of symmetry may result either from a non-circular geometry of the fibre core or from other mechanisms associated with the material anisotropy, likewise asymmetric stresses [5]. In turn, those extrinsic mechanisms make fibre birefringence to change randomly over time, reflecting the environmental conditions, which may request for polarisation rotation compensation schemes [6, 7].

The feasibility of QKD over optical fibres has been investigated and developed, with promising results in terms of reach, key-rates, and practical implementation [8, 9]. In this context, a major effort has been made to develop robust and stable polarisation encoding and decoding unities [10], envisioning its application in QKD systems implementing mainly the BB84 or the B92 protocols [11, 12]. In this context, several polarisation modulation schemes have been proposed to generate fast and stable polarisation states [13, 14]. Active SOP generators and receivers can be implemented using Pockels cells [15], using electro-optical polarisation modulators [16] or squeezing the fibre [17]. Besides that, polarisation modulation schemes can be obtained with optical switches, where an optical signal is split in N arms in order to define N different states of polarisation (SOP) [9, 12]. Alternatively, optoelectronic phase modulators were also employed for SOP generation without the need to split the signal [14, 18]. Nevertheless, in order to improve the stability of the SOP generation and detection stages in the QKD systems, fibre based Sagnac interferometers were proposed using phase modulators [10, 19]. In [20], a polarisation modulation scheme based in an inherently-stable Sagnac interferometer is presented. That scheme is free of polarisation-mode dispersion and calibration process, and it is insensitive to environmental influences. Recently, a self-compensation scheme was proposed based also in a fibre Sagnac loop [21]. Nevertheless, due to the complex experimental implementation of fibre-based Sagnac loops, in [14] authors present a simple configuration to implement a polarisation-encoding and -decoding QKD system using two in-line phase modulators. More recently in [22], authors present a QKD polarisation-based scheme using only a single-phase modulator and a passive detection scheme with two single-photon detectors. Despite the key properties discussed for the dedicated and more customised solutions, it is worth mentioning that the use of electronic polarisation controllers (EPCs) devices can represent a viable solution [17]. In particular, it presents advantages such as the plug and play versatility, low insertion loss and low cost, small size, or wavelength insensitivity.

This paper expands our previous work [23], where we proposed and demonstrated a technique for the polarisation encoding process in QKD systems employing fibre-squeezing-based EPCs. Using this technique, we experimentally demonstrate a field programmable gate array (FPGA)-assisted generation of four SOPs at a frequency of 500 Hz. Results show that this technique is suitable for polarisation-coding stages in BB84 and B92 QKD protocols. The approach consists of using the three first waveplates (WPs) of an EPC in order to rotate the input SOP to a defined position. This allows the fourth WP to generate the four different SOP when loaded with four different voltages, delivering four retardation angles, corresponding to four different SOPs. By integrating the EPC driving input voltages into the FPGA board we can centralise the quantum codifying system along with other optical signal modulation sub-systems, thus reducing the complexity of the transmitter side.

© The Institution of Engineering and Technology 2020

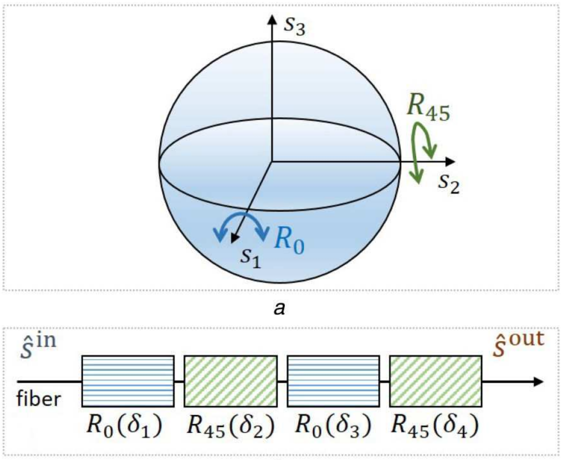

Fig. 1 *Evolution of the SOP in EPCs comprised by the concatenation of fixed-angle WPs*
(a) Schematic diagram of SOP rotations in the Poincaré sphere induced by a linear retarder, assuming two particular orientations for the fast axis of each device: $\theta = 0°$ and $\theta = 45°$, ***(b)*** Concatenation of four WPs that can be used to control the SOP, whose principal axes have a relative angle orientation of $\theta = 45°$ between each other

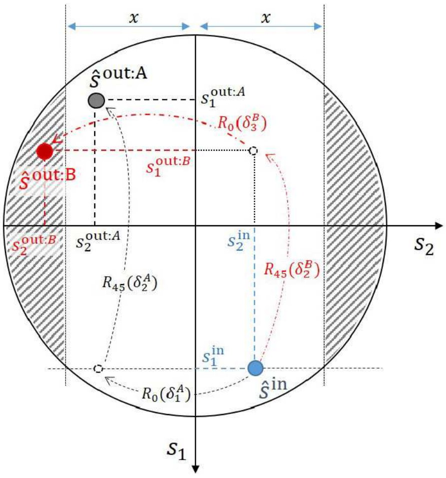

Fig. 2 *Schematic diagram of input and output representation in the Stokes space's $s_1 s_2$ plane. Two output notice that the distance x corresponds to the right hand side of (4)*

2 Theoretical EPC's WP model

This section presents a mathematical description of the EPC's WP and a model to easily compute the EPC configuration, i.e. the input voltages, in order to transform between an arbitrary input SOP into an arbitrary output SOP (see (1)) .

2.1 Mathematical description of a linear retarder

In general, the Mueller matrix for a linear retarder with fast axis orientated with an angle θ and retardation δ can be mathematically represented by (1). Depending on the employed technology, the WPs may have a fixed retardation angle and a tunable fast axis, e.g. the fibre coil (Mickey mouse ears) approach [24], or a fixed fast angle orientation and tunable retardation phase, likewise the all-fibre squeezing approach [25]. In this work, we will address the latter one, where fibre squeezers are driven by an applied voltage signal. Squeezing the optical fibre produces a linear birefringence in the fibre, and thus alters the state of polarisation of a light signal passing through it. Two particular cases occur when the fast axis is fixed and oriented at angles $\theta = 0°$ and $\theta = 45°$, with the WPs rotating the SOPs in the Poincaré sphere around the axes s_1 and s_2, respectively (see Fig. 1*a*). Hereafter, these two particular cases will be represented by the matrices $\boldsymbol{R}_0(\delta) = \boldsymbol{R}(\theta = 0°, \delta)$ and $\boldsymbol{R}_{45}(\delta) = \boldsymbol{R}(\theta = 45°, \delta)$.

2.2 Model to transform between two SOPs

Fig. 1*b* shows a schematic diagram of a generic EPC, comprised by the concatenation of four WPs. In the case under analysis, and without loss of generality, we assume that the fast axes of the first and third WPs are oriented at 0°, whereas the fast axis of the second and fourth WPs is aligned at 45°. The SOPs at the input and output of the EPC can be represented in the Stokes space by the vectors

$$\hat{\boldsymbol{s}}^{\text{in}} = \begin{bmatrix} s_1^{\text{in}} \\ s_2^{\text{in}} \\ s_3^{\text{in}} \end{bmatrix} \tag{2}$$

and

$$\hat{\boldsymbol{s}}^{\text{out}} = \begin{bmatrix} s_1^{\text{out}} \\ s_2^{\text{out}} \\ s_3^{\text{out}} \end{bmatrix}, \tag{3}$$

respectively, and s_i^{in} and s_i^{out} are the *i*th component of the input and output Stokes vector, respectively. The input SOP is sequentially transformed by the different WPs that are mathematically represented by the matrices $\boldsymbol{R}_0(\delta_1)$, $\boldsymbol{R}_{45}(\delta_2)$, $\boldsymbol{R}_0(\delta_3)$, and $\boldsymbol{R}_{45}(\delta_4)$, with $\boldsymbol{R}_i(\delta_i)$ representing the *i*th WP.

Assuming an arbitrary input SOP, $\hat{\boldsymbol{s}}^{\text{in}}$, and a target output SOP, $\hat{\boldsymbol{s}}^{\text{out}}$, we should be able to compute a set of retardation angles, δ_1, δ_2, δ_3, δ_4 capable of transforming between two arbitrary SOPs. The first step of the proposed method consists in testing the following condition:

$$\left| s_2^{\text{out}} \right| \le \sqrt{1 - \left(s_1^{\text{in}}\right)^2} \tag{4}$$

When condition ((4)) is verified, it means that the output SOP, $\hat{\boldsymbol{s}}^{\text{out}}$, lies in the inner area of the $s_1 - s_2$ plane (see Fig. 2); otherwise, it lies into one of the two dashed areas.

2.2.1 Scenario A:

For the first scenario (hereafter called as scenario A), and according to the WP's SOP rotation principles discussed in the previous subsection, WP1 imposes a retardation phase δ_1 to rotate the polarisation from $\hat{\boldsymbol{s}}^{\text{in}}$ to $\hat{\boldsymbol{s}}^{\text{WP1}}$ (see Fig. 2), assuring that

$$s_2^{\text{WP1}} = s_2^{\text{out}}. \tag{5}$$

Using some trigonometric operations, we can write the retardation angle of WP1 as a function of the input and the target output SOPs

$$\delta_1^A = \angle\left\{ \begin{bmatrix} s_2^{\text{in}} \\ s_3^{\text{in}} \end{bmatrix}, \begin{bmatrix} s_2^{\text{out}} \\ \sqrt{x^2 - \left(s_2^{\text{out}}\right)^2} \end{bmatrix} \right\} \tag{6}$$

where $x = \sqrt{1 - \left(s_1^{\text{in}}\right)^2}$, and $\angle\{\boldsymbol{A}, \boldsymbol{B}\}$ denotes the angle between the vectors $\boldsymbol{A}$ and $\boldsymbol{B}$.

$$R(\theta, \delta) = \begin{bmatrix} \cos(2\theta)^2 + \cos(\delta)\sin(2\theta)^2 & -\cos(2\theta)\sin(2\theta)(\cos(\delta) - 1) & -\sin(2\theta)\sin(\delta) \\ -\cos(2\theta)\sin(2\theta)(\cos(\delta) - 1) & \cos(\delta)\cos(2\theta)^2 + \sin(2\theta)^2 & \cos(2\theta)\sin(\delta) \\ \sin(2\theta)\sin(\delta) & -\cos(2\theta)\sin(\delta) & \cos(\delta) \end{bmatrix} \tag{1}$$

© The Institution of Engineering and Technology 2020

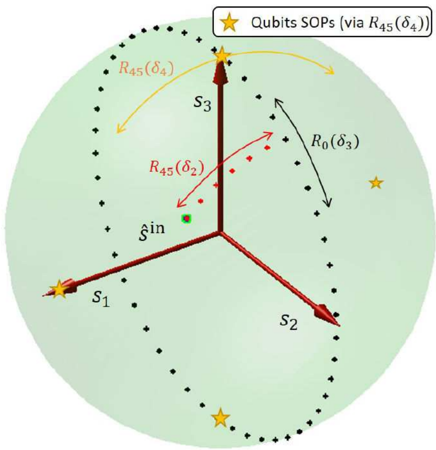

Fig. 3 *Schematic representation of the SOP evolution in the Poincaré sphere. In this case, the three first WPs are responsible to rotate the input SOP in order to allow the fourth WP to codify four qubits in the H-V and RC-LC bases*

After passing through the first WP, WP2 imposes a phase δ_2 to rotate the SOP $\hat{s}^{\text{WP1}}$ to a polarisation $\hat{s}^{\text{WP2}} = \boldsymbol{R}_2(\delta_2)\hat{s}^{WP1}$ assuring that, $s_1^{\text{WP2}} = s_1^{\text{out}}$. Regarding the WP2, the retardation angle can be written as

$$\delta_2^A = \angle\left\{\begin{bmatrix} s_1^{\text{in}} \\ \sqrt{x^2 - (s_2^{\text{out}})^2} \end{bmatrix}, \begin{bmatrix} s_1^{\text{out}} \\ s_3^{\text{out}} \end{bmatrix}\right\} \quad (7)$$

After the two previous rotations, the first and second Stokes parameters of the $\hat{s}^{\text{WP2}}$ equal to the ones of the desired output SOP. As rotations are performed over the surface of the Poincaré sphere, the third component of the Stokes vector is automatically matched, thus making

$$\hat{s}^{\text{WP2}} = \boldsymbol{R}_{45}(\delta_2^A)\boldsymbol{R}_0(\delta_1^A)\hat{s}^{\text{in}} \equiv \hat{s}^{\text{out}}, \quad (8)$$

with δ_1 and δ_2 given by (6) and (7), respectively.

2.2.2 Scenario B: In the second case (hereafter called as scenario B), the first WP does not need to actuate, i.e. we can set $\delta_1^B = 0$ and move to the second WP. As we are going to show later, this avoids to actuate in more than two WPs to transform between two arbitrary SOPs. By moving to the second WP, one imposes a retardation phase δ_2^B in order to rotate the SOP from $\hat{s}^{\text{in}}$ to $\hat{s}^{\text{WP2}}$ (see Fig. 2), assuring that $s_1^{\text{WP2}} = s_1^{\text{out}}$. Similarly to scenario A, the angle of WP2 can be written as

$$\delta_2^B = \angle\left\{\begin{bmatrix} s_1^{\text{in}} \\ s_3^{\text{in}} \end{bmatrix}, \begin{bmatrix} s_1^{\text{out}} \\ \sqrt{(s_1^{\text{in}})^2 + (s_3^{\text{in}})^2 - (s_1^{\text{out}})^2} \end{bmatrix}\right\} \quad (9)$$

For this scenario B, the WP3 must actuate in order to move $\hat{s}^{\text{WP2}}$ to $\hat{s}^{\text{WP3}}$, thus assuring $s_2^{\text{WP3}} = s_2^{\text{out}}$. In this way, the retardation angle of WP3 can be written as

$$\delta_3^B = \angle\left\{\begin{bmatrix} s_2^{\text{in}} \\ \sqrt{(s_1^{\text{in}})^2 + (s_3^{\text{in}})^2 - (s_1^{\text{out}})^2} \end{bmatrix}, \begin{bmatrix} s_2^{\text{out}} \\ s_3^{\text{out}} \end{bmatrix}\right\} \quad (10)$$

After the two previous rotations, the first and second Stokes parameters of the $\hat{s}^{\text{WP3}}$ are equal to the desired output SOPs. As rotations are performed over the surface of the Poincaré sphere, the third component of the two Stokes vectors is automatically matched, thus making

$$\hat{s}^{\text{WP3}} = \boldsymbol{R}_0(\delta_3^B)\boldsymbol{R}_{45}(\delta_2^B)\hat{s}^{\text{in}} \equiv \hat{s}^{\text{out}}, \quad (11)$$

with δ_2^B and δ_3^B given by (9) and (10), respectively.

The results presented above show that in order to guarantee the transformation between two arbitrary SOPs, the minimum EPC's configuration is comprised of three WPs.

3 Using the EPC in polarisation-encoded QKD

Commercial EPCs based in fibre squeezing can be assembled with four or more WPs. The concatenation of several WPs integrated into the same device permits large flexibility at the same time that improves the reliability of its simultaneous usage. This, in conjugation with the outputs of the model derived in the previous section, allows concluding that this kind of EPCs can be straightforwardly employed for quantum bit (qubit) coding in polarisation-encoded QKD protocols, namely the two-state protocol B92 and the four-state protocol BB84 [11].

Two approaches can be considered for the generation of different SOPs with EPCs based in fibre squeezing, as follows.

3.1 Look-up-table approach

A first approach consists of using the four WPs to generate the desired SOPs in a look-up-table mode, i.e. a set of four voltages are associated with the different target SOPs. Notice that this approach is assuming that the SOP at the input of the first WP is known and fixed. A disadvantage of this operation mode is that we need to update the voltages of all the four WPs for each coded qubit, which can be limited by the specification of the EPCs in terms of the maximum bandwidth of the high-voltage amplifiers.

3.2 Geometric approach

A more efficient approach consists in using the three first WPs to rotate the input SOP to a defined position, allowing the fourth WP to generate the four different SOPs when loaded with a set of four different voltages, delivering four retardation angles, corresponding to four different SOPs (see Fig. 3). Here, the main advantage is the possibility to change between the four SOPs by changing the voltage of a single WP. Notice that this operation maximises the operation bandwidth of the system as WPs are driven by high-voltage amplifiers.

4 Polarisation encoding experimental setup

Fig. 4 shows the experimental diagram of the quantum communication system implemented in our laboratory to generate and transmit photonic qubits. It uses the polarisation degree of freedom of single photons to encode information. In a QKD system, the transmitter is usually called Alice, whereas the receiver is known as Bob. Alice and Bob use a quantum channel (an optical fibre) to transmit the single-photons. Moreover, Alice also sends to Bob a classical optical signal to frame synchronisation purposes, and to Bob implement synchronised post-processing algorithms to extract the quantum keys. Fig. 5 shows a lab picture with key components of the experimental setup schematically represented in Fig. 4.

In our experimental setup, the different SOPs are obtained using the EPC to change the polarisation of the quantum states. Each WP of the EPC is individually controlled by an electrical analogue signal generated from the FPGA board. We have used the Zynq UltraScale + RFSoC ZCU111 Evaluation Kit, from Xilinx. This board provides a set of digital-to-analogue converter (DAC) interfaces able to generate voltages with 1 V peak-to-peak (around 2.2 V), which allows completing a full rotation on the Poincaré sphere of the signal polarisation. In our experimental implementation each SOP results from a set of four voltage values (one for each WP), as discussed in the previous section. At the FPGA board, the electrical signals are generated at higher frequencies since the sampling frequency of the DACs in the board is of the order of GHz. However, as the available EPC is only able to switch between different SOPs at a maximum frequency of 500 Hz (which is bounded by the bandwidth of the high-power RF amplifiers), we down-sampled the board DACs clock in order to obtain the aimed qubits repetition rate.

© The Institution of Engineering and Technology 2020

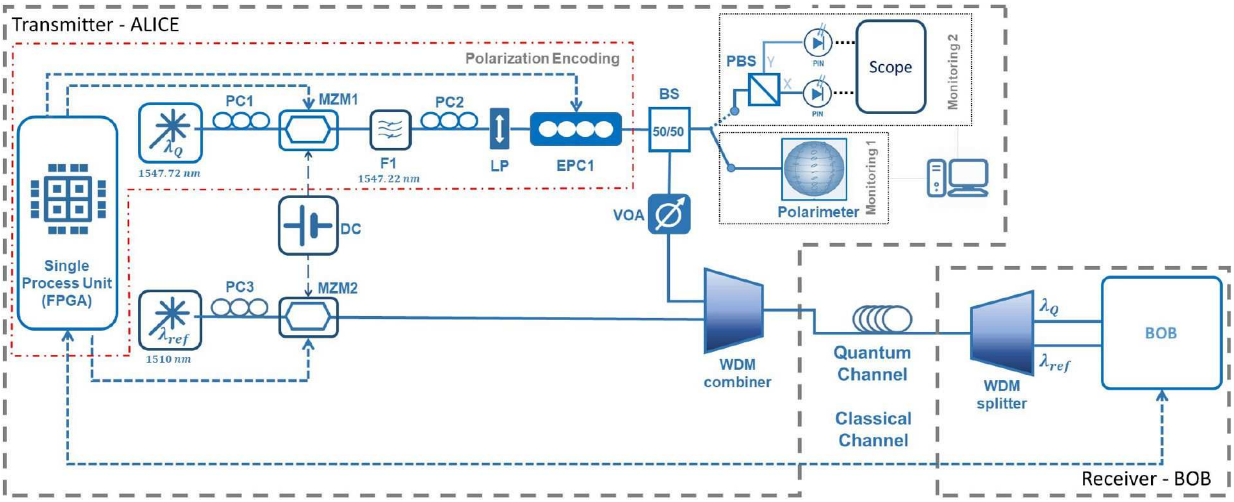

Fig. 4 *Schematic diagram of the polarisation-encoding QKD system. The experimental setup of transmitter-side, Alice, is shown with more detail, whereas, for simplicity, the receiver side is represented as a single unit receiving the quantum and reference signals, as well as the classical channel. Highlighted blocks at the transmitter side show the devices used to validate the SOP generation technique as well as to obtain the experimental SOP monitoring data reported in the following section. The monitoring process is done by either a Polarimeter, able to measure the three Stokes parameters when using low frequencies, and a polarisation beam splitter (PBS) followed by two PINs to measure the projections on the X and Y axes for higher frequencies. BS – beam splitter, MZM – Mach-Zehnder modulator, EPC – electronic polarisation controller, PC – manual polarisation controller, WDM – wavelength-division multiplexing, VOA – variable optical attenuator*

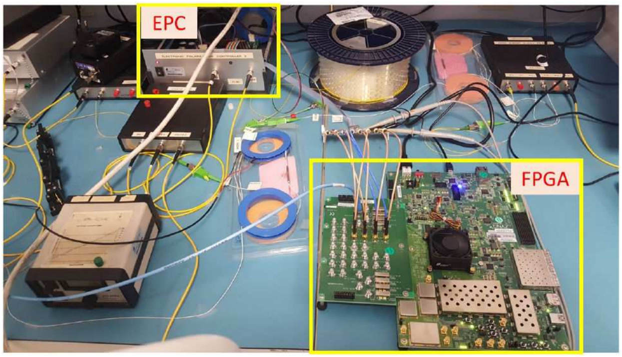

Fig. 5 *Picture of the experimental setup, schematically represented in Fig. 4, showing the key components EPC and FPGA board used in the polarisation encoding subsystem*

In QKD systems based in single photons, the Bob detection system typically operates in the Geiger mode. This means that the qubits generated by Alice have a finite time duration. To achieve that, Alice uses an amplitude modulator [we used a Mach-Zehnder modulator (MZM)]. Therefore, the FPGA board also generates the RF signals to control the external modulation of the optical signals. As shown in Fig. 4, the optical pulses of the quantum signal are generated through MZM1. Moreover, the classical signal used to synchronise Alice and Bob systems is also a pulsed optical signal with the same repetition rate as the quantum signal and is generated by a second MZM2. These two optical signals are generated at different wavelengths (1547.72 and 1510 nm) to avoid signal cross-talk, and are combined in the same optical fibre via a wavelength division multiplexer (WDM) combiner at the end of the Alice transmitter. In detail, the quantum signal is modulated at the MZM1 using an RF signal from the FPGA board with a 1 ns width. On the other hand, the classical signal used for Alice and Bob's side synchronisation is modulated with a 50% return-to-zero RF signal, also from the FPGA board.

The proposed technique for deterministic SOP generation was tested with a four-channel EPC from General Photonics (PolaRITE III). In order to assess the generation of different SOPs, we have implemented two monitoring systems. Then, the monitoring process was done by a polarimeter from Thorlabs (PAX5710VIS-T), able to measure the three Stokes parameters when using low frequencies, and a customised optical photonic system. Such customised optical photonic system comprises a polarisation beam splitter (PBS) followed by two photodetectors (PINs) to measure the projections on the two orthogonal axes. This allows us to indirectly verify the effectiveness of higher frequencies of SOP modulation. Then, accordingly to the method described in Section 3, the input light passes through the first three WPs, loaded with three constant voltages, and its polarisation is modulated at the fourth WP. Due to the low bandwidth of the polarimeter, we have firstly generated a set of results at lower frequencies (of the order of tens of Hz). After that, we have increased the frequency up to the maximum bandwidth of the EPC (of the order of hundreds of Hz).

5 Experimental results

Fig. 6 shows the Stokes parameters obtained with the experimental setup described above. The optical signal was collected in the polarimeter with a sampling rate of 200 samples/s, carrying a polarisation modulation frequency of ∼10 Hz. We repeat the sequence of SOPs $|H\rangle$, $|V\rangle$, $|+45\rangle$, and $|-45\rangle$ in order to emulate the two non-orthogonal basis suitable for polarisation encoding. Fig. 6*a* shows the evolution of the three Stokes parameters as a function of time. Notice that the parameter s_3 takes the value zero for all the selected SOPs. However, for this particular Stokes parameter, results show a relatively high noise level when compared with the two other Stokes parameters. When the signal symbols are represented in the Poincaré sphere (see Fig. 6*b*), one observes that the four SOP are accurately generated close to the equator. Moreover, this representation identifies the states $|V\rangle$ and $|+45\rangle$ are the SOPs that are more affected by the noise level observed in Fig. 6*a* for the parameter s_3. This is related to the relaxation time of the squeezing process of the EPC when the RF signal from the FPGA board is turned off. As mentioned above, the usage of the polarimeter is limited to low frequencies. For higher frequencies, we have developed a customised optical analyser in order to check the SOP changes.

The experimental results obtained with the customised optical analyser, comprising a PBS and two PINs, are represented in Fig. 7. In this set of results, we have increased the coding rate of up to 500 qubit/s, with a sampling rate of 5 kHz (i.e. 10 samples per symbol). It is worth noticing that this coding rate is limited by the bandwidth of the high-voltage amplifiers of the EPC. The PIN output voltages represented in the two plots (Figs. 7*a* and *b*) are proportional to the projections of the optical signal in the two orthogonal axes of the PBS (Port X and Port Y). Since the system was configured to generate a repeated sequence of four SOP, $|H\rangle$, $|V\rangle$, $|+45\rangle$, and $|-45\rangle$, four different output voltages are observed at each port. Moreover, we also observe that the two curves are

© The Institution of Engineering and Technology 2020

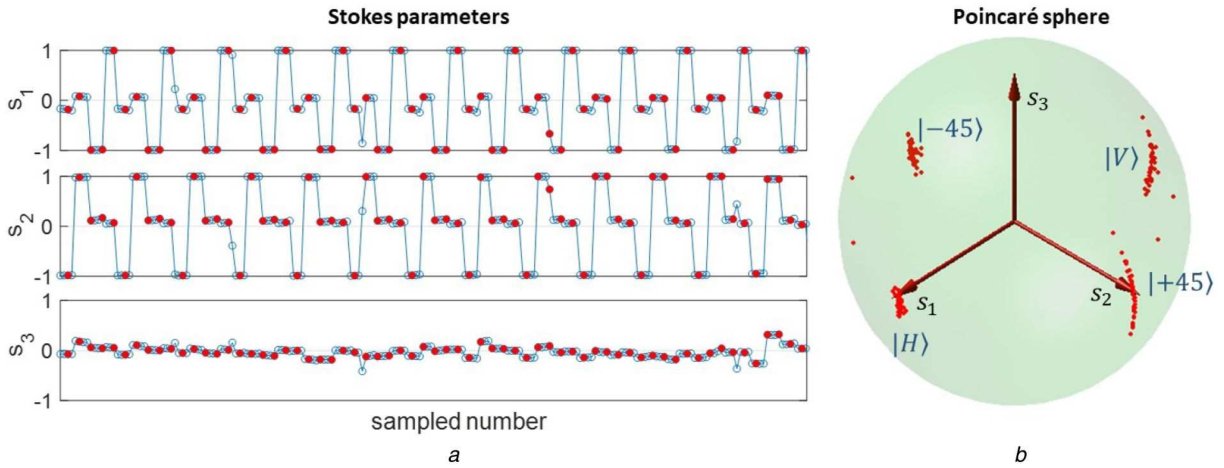

Fig. 6 *Stokes parameters of the different SOPs generated with the proposed technique*
(a) Time evolution of the three signal Stokes parameters, s_1, s_2, and s_3 (small-blue circles) measured by the polarimeter, ***(b)*** Poincaré sphere representation of the SOPs, corresponding to the signal samples represented in (a) as red dots. The states $|H\rangle$, $|V\rangle$, $|+45\rangle$, and $|-45\rangle$ represent the four SOPs of the two non-orthogonal bases used for QKD system implemented in the laboratory

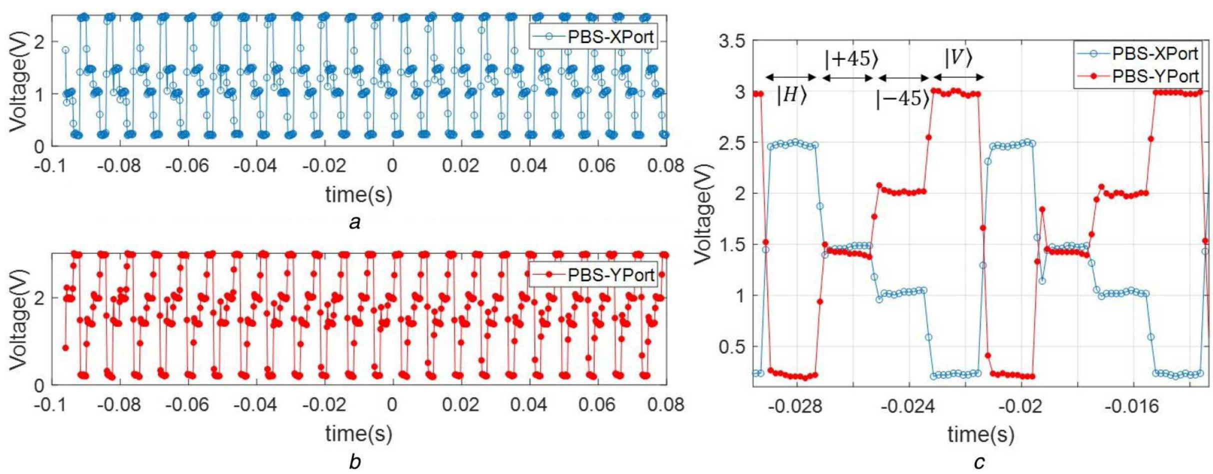

Fig. 7 *Output voltages at the two ports of the PBS. The signal is modulated at 500 qubit/s*
(a), (b) Voltage as a function of time for the *X* and *Y* ports of the PBS, respectively, ***(c)*** Zoom-in of the output voltages of the two ports, showing the sequence of the four different SOPs. Since the two ports correspond to the projection of the two orthogonal polarisations, the obtained results are roughly complementary to each other

roughly complementary. To explain the non-exact complementarity between curves, it should be pointed out that the SOPs reaching the input of the PBS (see Fig. 4) are not the same that the ones that reach the input of the polarimeter. This occurs because these optical paths are different. If the SOPs reaching the input of the PBS are equal to the ones at the input of the polarimeter, then only three voltage levels will be observed at the PINs outputs as the states $|+45\rangle$ and $|-45\rangle$ have the same projection. The two other voltage levels will be associated with the SOPs $|H\rangle$ and $|V\rangle$.

6 Conclusions

A new method to calculate the WP's EPC configuration able to transform between two arbitrary SOPs was presented. This analysis can be used when considering the configuration of the polarisation encoding system, namely in terms of the minimum number of WPs required to transform between two SOPs.

Additionally, a technique to deterministically generate four polarisation states in polarisation-encoded quantum communication systems was also proposed. This approach consists of the employment of the three first WPs to rotate the input SOP to a defined position, allowing the fourth WP to generate the four different SOPs when loaded with four different voltages, delivering four retardation angles, corresponding to four different SOPs.

The effectiveness of the proposed approach was experimentally assessed through the generation of two pairs of orthogonal polarisations. In order to control the voltages of the individual WPs, we used the FPGA ZCU111 Evaluation Kit board. Results confirmed a polarisation encoding process intrinsically stable, which evidences the potential for its use in practical applications of four-state quantum protocols. Depending on the bandwidth of the EPC, systems could operate at speeds higher than tens of kHz. Moreover, by integrating the EPC driving input voltages into the FPGA board, we were able to centralise the quantum codifying system along with other optical signal modulation sub-systems, thus demonstrating its potential to reduce the complexity of the transmitter side.

7 Acknowledgments

This work was supported in part 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) of the Portugal 2020 framework, under the PhD Grant SFRH/BD/145670/2019, and projects DSPMetroNet (POCI-01-0145-FEDER-029405), QuantumMining (POCI-01-0145-FEDER-031826), UIDB/50008/2020 and UIDP/50008/2020.

8 References

[1] Pinto, A.N., Silva, N.A., Almeida, A., *et al.*: 'Using quantum technologies to improve fiber optic communication systems', *IEEE Commun. Mag.*, 2013, **8**, (51), pp. 42–48

[2] Tittel, W.: 'Quantum key distribution breaking limits', *Nat. Photonics*, 2020, **13**, pp. 310–311

© The Institution of Engineering and Technology 2020

[3] Kurtsiefer, C., Zarda, P., Halder, M., *et al.*: 'Quantum cryptography: A step towards global key distribution', *Nature*, 2002, **419**, pp. 450–450

[4] Silva, N.A., Pinto, A.N.: 'Comprehensive characterization of a heralded single photon source based on four-wave mixing in optical fibers', *Opt. Commun.*, 2014, **327**, pp. 31–38

[5] Ferreira, M., Pinto, A., André, P., *et al.*: 'Polarization mode dispersion in high-speed optical communication systems', *Fiber Integr. Opt.*, 2005, **24**, pp. 261–285

[6] Almeida, A., Muga, N.J., Silva, N.A., *et al.*: 'Continuous control of random polarization rotations for quantum communications', *IEEE/OSA J. Lightwave Technol.*, 2016, **34**, (16), pp. 3914–3922

[7] Ramos, M.F., Silva, N.A., Muga, N.J., *et al.*: 'Reversal operator to compensate polarization random drifts in quantum communications', *Opt. Express*, 2020, **28**, (4), pp. 5035–5035

[8] Muga, N.J., Ferreira, M.F.S., Pinto, A.N.: 'QBER estimation in QKD systems with polarization encoding', *IEEE/OSA J. Lightwave Technol.*, 2011, **29**, (3), pp. 355–361

[9] Ko, H., Choi, B.S., Choe, J.S., *et al.*: 'High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers', *Photonics Res.*, 2018, **6**, (3), pp. 214–219

[10] Wang, J., Qin, X., Jiang, Y., *et al.*: 'Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units', *Opt. Express*, 2016, **24**, (8), pp. 8302–8309

[11] Gisin, N., Ribordy, G., Tittel, W., *et al.*: 'Quantum cryptography', *Rev. Mod. Phys.*, 2002, **74**, (1), pp. 145–195

[12] Almeida, A., Stojanovic, A., Paunkovic, N., *et al.*: 'Implementation of a two-state quantum bit commitment protocol in optical fibers', *J. Opt.*, 2016, **18**, (1), pp. 015202–015202

[13] Jofre, M., Gardelein, A., Anzolin, G., *et al.*: '100 MHz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm', *J. Lightwave Technol.*, 2010, **28**, (17), pp. 2572–2578

[14] Duplinskiy, A., Ustimchik, V., Kanapin, A., *et al.*: 'Low loss qkd optical scheme for fast polarization encoding', *Opt. Express*, 2017, **25**, (23), pp. 28886–28897

[15] Kim, Y.S., Jeong, Y.C., Kim, Y.H.: 'Implementation of polarization-coded freespace BB84 quantum key distribution', *Laser Phys.*, 2008, **18**, (6), pp. 810–814

[16] Xavier, G.B., de Faria, G.V., ao, G.P.T., *et al.*: 'Full polarization control for fiber optical quantum communication systems using polarization encoding', *Opt. Express*, 2008, **16**, (3), pp. 1867–1873

[17] Almeida, Á.J., Muga, N.J., Silva, N.A., *et al.* 'Enabling quantum communications through accurate photons polarization control', In: Costa, M.F.P.C.M., ed., 8th iberoamerican optics meeting and 11th latin American meeting on optics, lasers, and applications. (SPIE, 2013

[18] Lucio.Martinez, I., Chan, P., Mo, X., *et al.*: 'Proof-of-concept of real-world quantum key distribution with quantum frames', *New J. Phys.*, 2009, **11**, (9), p. 095001

[19] Liu, X., Liao, C., Mi, J., *et al.*: 'Intrinsically stable phase-modulated polarization encoding system for quantum key distribution', *Phys. Lett. A*, 2008, **373**, (1), pp. 54–57

[20] Li, Y., Li, Y.H., Xie, H.B., *et al.*: 'High-speed robust polarization modulation for quantum key distribution', *Opt. Lett.*, 2019, **44**, (21), pp. 5262–5265

[21] Agnesi, C., Avesani, M., Stanco, A., *et al.*: 'All-fiber self-compensating polarization encoder for quantum key distribution', *Opt. Lett.*, 2019, **44**, (10), p. 2398

[22] Grünenfelder, F., Boaron, A., Rusca, D., *et al.*: 'Simple and high-speed polarization-based QKD', *Appl. Phys. Lett.*, 2018, **112**, (5), p. 051108

[23] Muga, N.J., Ramos, M.F., Mantey, S.T., *et al.*: 'Deterministic state-of-polarization generation for polarization-encoded optical communications'. In: Microwave and Optoelectronics Conf. (IMOC) SBMO/IEEE MTT-S Int. IMOC, Aveiro, Portugal, 2019

[24] Muga, N.J., Pinto, A.N., Ferreira, M., *et al.*: 'Uniform polarization scattering with fiber-coil based polarization controllers', *IEEE/OSA J. Lightwave Technol.*, 2006, **24**, (11), pp. 3932–3943

[25] Walker, N.G., Walker, G.R.: 'Endless polarization control using four fibre squeezers', *Electron. Lett.*, 1987, **23**, (6), pp. 290–292

© The Institution of Engineering and Technology 2020