OPEN ACCESS
IOP Publishing
Journal of Optics
J. Opt. **26** (2024) 075704 (10pp)
https://doi.org/10.1088/2040-8986/ad535a

Design and implementation of a polarization-encoding system for quantum key distribution

Sara Mantey[1,2,*], **Nuno Silva**[1], **Armando Pinto**[1,2] **and Nelson Muga**[1]

[1] Instituto de Telecomunicações and University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal
[2] Department of Electronics, Telecommunications and Informatics, University of Aveiro, Campus Universitário de Santiago, 3810-193 Aveiro, Portugal

E-mail: smantey@ua.pt

Received 16 February 2024, revised 15 May 2024
Accepted for publication 3 June 2024
Published 13 June 2024

Abstract

We present the design and implementation of a state-of-polarization (SOP) management technique and two efficient synchronizing methods for quantum key distribution (QKD) systems. This is achieved following a wavelength-division multiplexing approach, where the classical synchronization signal and the quantum states are propagated in the same optical fiber. The employed frame synchronization method is based on the monitoring of the quantum bit error ratio (QBER) of the quantum channel, thus avoiding additional hardware and high computational resources. We evaluate the operation of SOP generation method through the assessment of the individual response of the waveplates that comprise the employed electronic polarization controller. Finally, the performance was assessed by computing the overall QBER and the QBER contributions of each of the four polarization states associated with the different qubits. The measurements, obtained during six hours, show a slight variation of the QBER values associated with the individual contributions, reaching an overall QBER of 0.75%. This demonstrates the capability of the presented methods to operate, stably, with very low QBER values, making its application in practical QKD systems reliable.

Keywords: polarization-encoding, quantum key distribution, synchronization, quantum bit error rate

1. Introduction

Quantum key distribution (QKD) presents a promising solution towards unprecedented high-level security data transfer, being based on the laws of quantum mechanics, which allow to detect an eavesdropper in the case of its presence [1]. The most used degrees of freedom to encode data in QKD systems are the polarization or phase of single photons. Polarization-encoding presents some advantages over phase-encoding as for example in terms of the complexity of the practical implementation, and its potential use for free-space applications [2]. However, when considering the required set of states-of-polarization (SOP), four in the case of the original BB84 protocol [3], its generation needs to be precise but simple. In this context, a start-up calibration mechanism are mandatory to ensure the correct generation of the SOPs and the consequent efficient and secure operation of QKD systems.

Several degrees of freedom of single photons, e.g. phase coding [4], frequency coding [5], polarization [6], time-bin [7], and hybrid time-bin and polarization [8], have already been proposed. Nevertheless, polarization based QKD has shown promising results regarding the reach [9], versatility

* Author to whom any correspondence should be addressed.

[10], key-rates [6], and error-rates [11], showing the importance of the development of polarization-encoding QKD systems and subsystems. Polarization-encoding has also shown to be a very promising solution for free-space QKD, crucial for satellite-based QKD [12], as well as for the implementation of other beyond QKD protocols [13]. One important part of polarization-encoding QKD systems is the SOP generation mechanism itself. This subsystem influences the error-rates and, therefore, the reachable distance and secret key rates [14]. Several state of polarization (SOP) generation methods have been proposed, for example, using balanced Mach–Zehnder interferometers [15, 16], or fiber-based Sagnac loops [17], among others. However, even though the Mach-Zehnder scheme is simple to implement, it is highly unstable because of its sensitivity to environmental perturbations [18]. On the other hand, fiber-based Sagnac interferometers can generate highly stable SOPs, however, they present a complex experimental implementation [18]. Taking this into account, it is important to develop simple SOP generation methods that overcome these issues, for example using electro-optic polarization controllers (PCs) [19]. Similarly to other communication systems, QKD requires reliable and efficient synchronization mechanisms. In this regard, several frame synchronization methods have also been proposed, for example, using intensity modulation [21], using quantum bit error rate (QBER) monitoring [22], or based on correlation monitoring techniques [23]. One considerable drawback of several of these methods, is their requirement of additional hardware, which implies further costs, or the high computational complexity associated to them. It is also worth mentioning that for frame synchronization methods, it is indispensable to have the ability of operating under the utmost severe QKD conditions, namely, that a highly attenuated signal arrives at the receiver. Therefore, efficient methods are needed, that achieve synchronization in a timely manner, even considering the low number of photons that reach the receiver.

In this work, we expand the analysis of our recently proposed SOP generation method [24], towards the implementation of polarization-encoding QKD physical layers. This implementation comprises the automatic polarization calibration at the transmitter, a classical optical signal for the symbol synchronization, and a frame synchronization mechanism deployed at the receiver. With this polarization generation method a simple implementation is achieved overcoming, e.g. the need for highly synchronized pulses at the transmitter as required by balanced Mach–Zehnder interferometers, or the complexity of fiber-based Sagnac loops [18]. The properties of the polarization-encoding method are validated by integrating it in a real-time QKD system, with a newly proposed and implemented QBER-assisted frame synchronization mechanism [25]. This method allows to synchronize the frames in roughly 10^4 clock cycles, nevertheless, the number of clock cycles can be optimized according to the system requirements. Its flexibility regarding the used header presents an advantage when compared with the method proposed in [11]. To further analyse the accuracy of the implemented SOP generation mechanism, the contributions of each generated polarization state to the QBER are estimated. The system achieved an overall QBER of 0.75%,

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

This paper is organized into six sections. In section 2, some formalism and theoretical concepts supporting the understanding of the polarization control methods discussed in this work are described. A comprehensive analysis of the polarization state generation algorithm, followed by a detailed description of the setup used for the experimental validation, including the transmitter, receiver, and synchronization mechanisms, is given In section 3. Section 4 presents the results obtained with the system described in section 3, including, in a first stage, the performance analysis of the state generation algorithm, and, in a second stage, the performance of the entire system by analyzing the overall QBER, as well as the individual contribution of the quantum states used in the implementation of the BB84 protocol. These results are then discussed in section 5. Finally, in section 6, a brief conclusion of the system and its results is presented.

2. Formalisms for polarization control

Polarization control can be achieved with several methods, but the main idea behind all of them is to induce a phase difference between the two transverse components of a polarized light beam. This phase difference can be achieved, for example, with crystals that delay one of the components of the light more than the other component by a certain amount. This delay is due to different refractive indexes for the two transverse components. The amount of delay between the transverse components depends on the thickness of the crystal [26]. These crystals can be rotated, in order to change the orientation of the fast and slow axis [27]. This way, many polarization control devices are based on mechanically rotating waveplates to induce controlled polarization variations [28]. However, these methods are usually slow, and are very susceptible to environmental perturbations. There are more recent

methods, as for example, using thin-film lithium niobate [29], or using spherical phase-induced multicore waveguides [30], which represent fast and stable methods.

The polarization transformations caused by the methods mentioned above, that is, transformations caused by phase retarders, can be mathematically described by the following Jones matrix [31]:

$$U(\theta,\delta)=\begin{bmatrix} e^{i\delta}\cos^2(\theta)+\sin^2(\theta) & \left(e^{i\delta}-1\right)\sin(\theta)\cos(\theta) \\ \left(e^{i\delta}-1\right)\sin(\theta)\cos(\theta) & e^{i\delta}\sin^2(\theta)+\cos^2(\theta) \end{bmatrix}, \tag{2}$$

where θ is the orientation of fast axis angle of the retarder, and δ stands for the phase retardation. Polarization transformations can also be represented in the Stokes space by a 4×4 matrix. In the particular case when the transformations are unitary, i.e. when the total intensity of light, corresponding to the first Stokes parameter, is constant, the Muller matrix can be represented by a 3×3 matrix. This way, the linear retarder can be described, in the Stokes space, by the Muller matrix presented in (1) [31].

The product of this matrix with a given SOP results in a 3×1 Stokes vector, which was rotated around a vector that points to the equator of the Poincaré sphere. The direction of this vector is defined by the angle θ, and the degree of rotation is defined by δ. By using the Stokes parameters as coordinates of the Poincaré sphere, the polarization states and transformations can easily be visualized in a 3D space.

Electronic polarization controllers (EPC) are a practical way to induce polarization changes in an optical beam by means of a set of electrical voltages. In this work, and without loss of generality, we consider a piezoelectric EPC (model: General Photonics—Polarite III), which consists of a concatenation of four linear retarders. The first and third retarders have a fast axis oriented at 45 degrees in relation to the second and fourth retarders, and an adjustable phase retardation that enables a rotation of the SOP from 0 to 2π in the direction defined by the fast axis orientation, see figure 1. By replacing the fast axis value, θ in (1), by 0 degrees, the Muller matrix of the first and third retarders of such EPC can be written as [31]:

$$R(0^\circ,\delta)=\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\delta & -\sin\delta \\ 0 & \sin\delta & \cos\delta \end{bmatrix}. \tag{3}$$

Similarly, by replacing the fast axis angle, θ, in (1), by 45 degrees, the Muller matrix of the second and fourth retarders can be written as [31]:

$$R(45^\circ,\delta)=\begin{bmatrix} \cos\delta & 0 & \sin\delta \\ 0 & 1 & 0 \\ -\sin\delta & 0 & \cos\delta \end{bmatrix}. \tag{4}$$

The phase retardation of the waveplates of this EPC is adjustable, and can be controlled by applying a certain voltage to the waveplates. The relation between the phase retardation, δ, and the applied voltage, V, can be represented by the following equation:

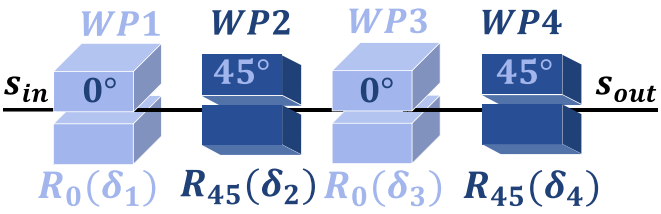

Figure 1. Schematic representation of the piezoelectric EPC, that comprises the concatenation of four retarders, such that the second and fourth are oriented at 45 degrees in relation to the first and third retarders.

$$V=\frac{\delta V_\pi}{\pi}, \tag{5}$$

where V_π is the half-wave voltage, i.e. the voltage needed to induce a change of 180 degrees between the phase of the orthogonal components of the polarized light.

Using the concatenation of retarders mentioned above, it is possible to obtain any polarization state, with an arbitrary input polarization, see figure 2. Figure 2 shows a numerical simulation of the SOPs obtained at the output of the EPC, represented in figure 1, when the phase retardation (voltage), results from a set of random values uniformly distributed between 0 and $\delta_{\max}=\frac{\pi}{10}$, $\frac{\pi}{5}$, π, or 2π. The input polarization, s_{in}, was set to $s=\frac{1}{\sqrt{3}}[1,1,1]^T$, representing an elliptical SOP. One observes that the smaller the phase retardation interval is, the smaller the covered area of SOPs that one can achieve at the output. With a retardation of, for example, $2V_\pi$, all polarization states can be obtained. This EPC's property, is taken into account in the polarization state generation algorithm in order to generate the SOPs required by the quantum protocol in the QKD system.

3. Polarization generation method integration

3.1. The polarization state generation algorithm

The SOP generation algorithm consists of two branches with different polarization dependent components, in order to assess the input SOP from power measurements. The setup used to support this method is shown with detail in figure 3. This setup is divided into two main branches, the linear branch, associated to the linear polarization basis, which is used to determine the voltages for the linear states (horizontal and vertical), and the circular branch, associated with the circular polarization basis, which is used to determine the voltages to generate the circular states (right-circular and left-circular). The linear branch comprises a LP (Linear Polarizer) before a PIN photodiode (PIN), while the second also has a quarter waveplate (QWP) at a 45° angle placed before a LP in order to rotate circular states to linear states. The function of these two branches is to enable the detection of linear or circular states at the entrance of the branches. The manual PCs, PC1

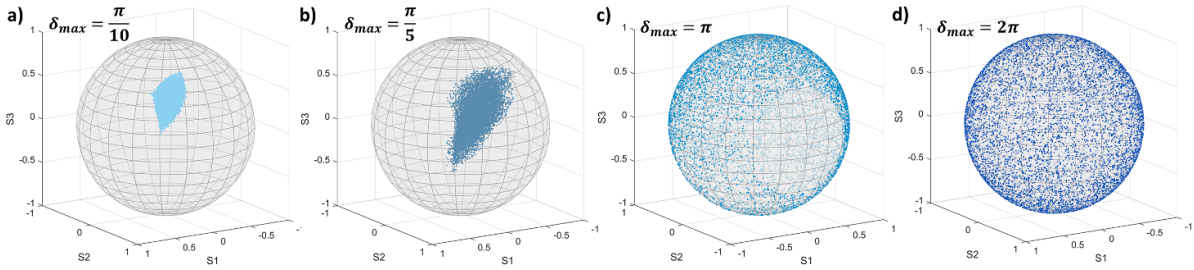

Figure 2. Simulation of the resulting output SOPs, s_{out}, when considering an $s_{in} = \frac{1}{\sqrt{3}}[1,1,1]^T$, and with a retardation angle randomly obtained from an uniform distribution between 0 and: (a) $\frac{\pi}{10}$, (b) $\frac{\pi}{5}$, (c) π, and (d) 2π.

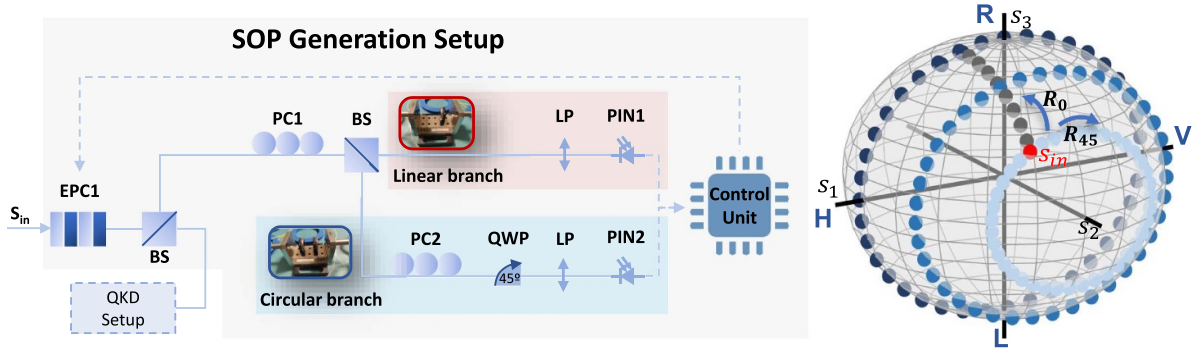

Figure 3. Schematic representation of the SOP generation setup. The inset shows the rotations of the SOP around the Poincaré sphere in order to determine the voltages to generate the four polarization states (horizontal, vertical, right-circular, and left-circular).

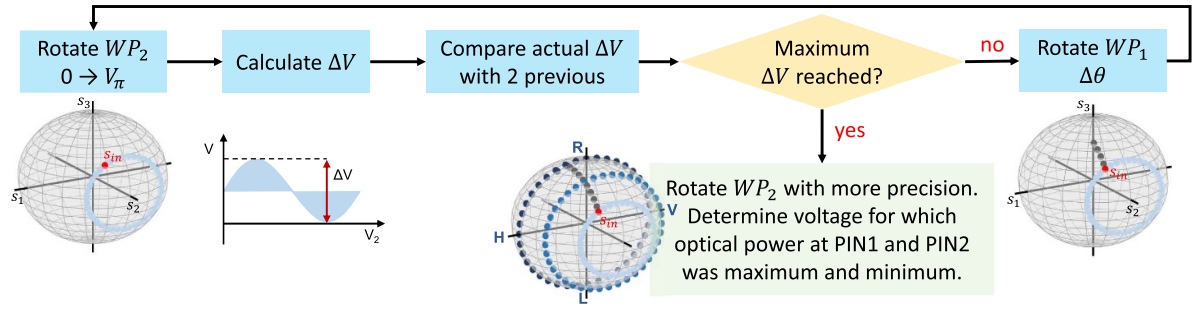

Figure 4. Fluxogram of the algorithm used by the proposed SOP generation method to determine the voltages needed to generate the H, V, R and L polarization states.

and PC2, are used to ensure that the SOP at the entrance of the two branches is equal. This is achieved by adjusting the waveplates of PC1 until the optical power reaching PIN1 is maximized, and after, adjusting the waveplates of PC2, without the QWP inserted, until the optical power reaching PIN2 is also maximized.

The first step of the algorithm is to rotate the SOP until it is located on the maximum perimeter circle of the Poincaré sphere, as shown by the dark blue line in figure 3. This maximum perimeter circle is strategically chosen, given that from here, using only one waveplate, it is possible to generate all four SOP [24].

To determine the maximum perimeter circle, the optical power that reaches PIN1 is monitored while the voltages on the waveplates of the EPC are changed. First the SOP is rotated around the S_2 axis using the second or fourth waveplate, see figure 4. The optical power at PIN1 should vary according to a sinus-shaped curve while the mentioned rotation is performed. The amplitude of the sinus-shaped curve, referred to as ΔV, which depends on the position of the SOP, is calculated and registered. After, using the first or third waveplate, one step around the S_1 axis is made. Then, again a complete turn around the S_2 axis is performed and the ΔV is calculated and registered. This process goes on until the maximum ΔV is found, which corresponds to the amplitude of the optical power registered by PIN1 when a rotation around the maximum perimeter circle is performed. After the maximum circle is found we can perform another rotation around that axis with a smaller step, increasing the precision. While doing this rotation, not only the optical power reaching PIN1 should be monitored but also the one reaching PIN2. The voltage applied on the EPC for which the optical power at PIN1 is maximum and minimum corresponds to the voltage that needs to be applied to generate the horizontal and vertical SOPs, respectively. In the

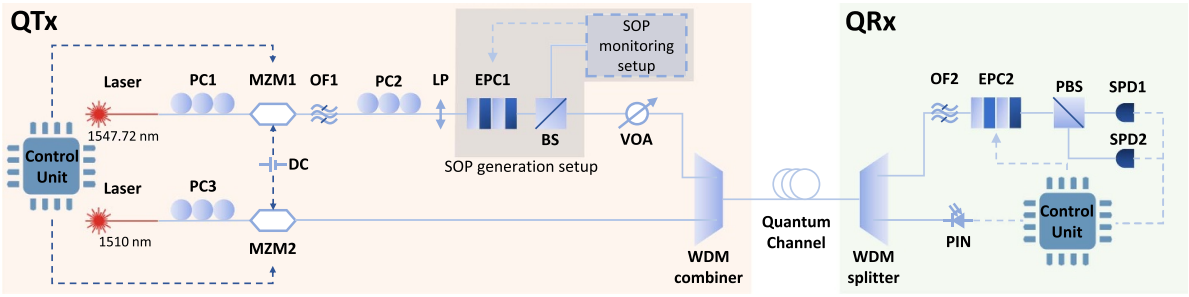

Figure 5. Schematic representation of the polarization-encoding QKD system. PC1, 2, and 3 - polarization controller; MZM1, and 2 - Mach–Zehnder modulator; OF1, and 2 - optical filter; LP—linear polarizer; EPC1, and 2 - electronic polarization controller (model: General Photonics—Polarite III); BS—beam splitter; VOA—variable optical attenuator; WDM—wavelength-division multiplexer; PBS—polarization beam splitter; SPD1, and 2 - single photon detector (model: ID Quantique—id210); PIN—P-I-N photodiode.

same way, the voltage applied on the EPC for which the optical power at PIN2 is maximum and minimum corresponds to the voltage that needs to be applied to generate the right-circular and left-circular SOPs, respectively. With this SOP generation algorithm, the four polarization states can be originated disregarding the SOP at the entrance of the EPC. Considering that this algorithm is designed to be implemented at the transmitter of polarization-encoded QKD systems, it only needs to determine the set of voltages for each state once, so the impact on the systems performance can be considered limited. Nevertheless, if the algorithm had to be applied during the secret key generation, the secret key rate would be affected as the transmission would have to be paused. The use of electronically driven waveplates allows us to exploit advantages such as, e.g. the plug and play versatility, low insertion loss, small size, and wavelength insensitivity, presenting some advantages over other more complex and potentiality unstable implementations, e.g. the ones employing interferometers [18].

3.2. Algorithm Integration into the QKD system

The practical QKD system used consists of a transmitter, where the state preparation takes place, the quantum channel, which in this case consists of an optical fiber, and a receiver, where the basis alignment and selection takes place. At the receiver, the quality of transmission is estimated and the assessment if an eavesdropper was present or not by computing the QBER is performed.

To validate the proposed algorithms and techniques (SOP generation, and synchronization), we used a polarization-encoded QKD setup schematically represented in figure 5. At the transmitter, two signals are generated, a classical reference signal for synchronization purposes and a quantum signal for the polarization state carrying, see figure 5. The SOPs, for the quantum state carrying, are generated using an algorithm, this way enabling an automatized state preparation at the transmitter. At the receiver, the polarization of the carrier signal is measured, and the reference signal is used as a trigger for the single photon detectors (SPD) (model: ID Quantuique ID210 with 25% detection efficiency and $\sim 10^{-5}\text{ns}^{-1}$ dark count rate) to achieve symbol synchronization.

3.2.1. Transmitter. As mentioned above, the transmitter prepares two signals, see figure 5. These two signals need to be prepared with enough spectral distance in order to prevent cross-talk. Therefore, the reference signal, is prepared with a wavelength of 1510.00 nm, and the quantum signal with a wavelength of 1547.72 nm. After, the reference signal is modulated by the Mach-Zehnder Modulator 2 (MZM), which imposes a pulse width of 200 ns and a frequency of 500 Hz. The quantum signal is modulated by the MZM1 to have a frequency of 500 Hz, however, with a pulse width of 1 ns. It is worth mentioning that this low repetition rate of 500 Hz is a limitation imposed by the maximum operation frequency of the EPC used in this setup. After the modulation, the quantum signal passes through an OF (Optical Filter) to eliminate intensity noise. A fixed LP is placed to ensure that the polarization at the entrance of the EPC is well defined. The voltages to be applied on the piezoelectric EPC for each of the four SOPs are determined using the SOP alignment setup, placed at one of the outputs of the beam splitter (BS). The other output of the BS is connected to a variable optical attenuator (VOA) which attenuates the carrier signal to a quantum level before it is combined with the reference signal by WDM technology and passed on to the quantum channel.

The EPC being used comprises four waveplates, the first and the third waveplates have a fixed fast-axis angle which is oriented 45° in relation to the fast-axis angle of the second and fourth waveplates. This way, using the first and third waveplates the SOP will be rotated around the S_1 axis of the Poincaré sphere. Using the second and fourth waveplate rotates the SOP around the S_2 axis. The retardation of all four waveplates is adjustable. Notice that this algorithm can be adjusted to be implemented with other polarization encoding architectures employing electro-optic devices with faster response times, e.g. lithium niobate-based modulators as used in [32, 33] to achieve higher repetition rates.

3.2.2. Receiver. After passing through the quantum channel, the quantum and reference signals are separated by a WDM splitter and follow different paths, see figure 5. The reference signal is detected by a PIN, which outputs a electric

trigger signal. Such signal is used to time the detection events at the SPDs operating in the gated mode, and to synchronize the control unit responsible for the base alignment. The quantum signal, in its turn, is filtered and passed on to the receiver's EPC. This EPC is identical to the one used at the transmitter, and is used to select the basis (linear or circular) in which the received quantum states are measured. After the EPC, a polarization beam splitter (PBS) is used to distinguish between orthogonal polarization states.

Before the key transmission starts, for the basis alignment, the set of voltages to align the receiver with the rectilinear and circular basis are found by changing the voltages on the receivers EPC until the QBER is minimized. For the rectilinear basis this is achieved while continuously sending the horizontal polarization state. After the voltages that minimize the QBER for this state are determined, a circular state is continuously sent, and again, the voltages that minimize the QBER are determined. The voltage values for the two basis are registered to be used for the basis selection. Given that the system is being tested in a back-to-back configuration no polarization compensation mechanism was implemented at the receiver.

The measurements of the SPDs as well as the selected bases are processed by an upper layer responsible for the protocol implementation. For the correct operation of the QKD system described above, a rigorous synchronization is needed. In the following subsections we present the symbol and frame synchronization methods implemented to set up the QKD system.

3.3. Synchronization systems

The explored QKD system comprises two different synchronization mechanisms. The first one, symbol synchronization, enables the system to correctly time the incoming optically transmitted symbols. Once this is achieved, it is needed to correlate the received bits with the correct bits transmitted, which consists of the frame synchronization. This method allows to register the transmitted and received bits in the right positions, enabling further protocols execution, including the correct QBER estimation.

3.3.1. Symbol synchronization. As mentioned above, the symbol synchronization is supported by an optical signal with a 200 ns pulse width, which is transmitted with the quantum signal in the same optical fiber. To correctly detect and process this signal, a decision block was implemented, more details can be found in [20]. One of the four input signals of the decision block is the 100 MHz internal clock of the receivers field programmable gate array (FPGA) which is used to set the sampling rate of the other input signals to 10 ns. The trigger signal, *clock_result*, is obtained from an AND operation between two signals: *clock_enable* and *clock_in*. The *clock_enable* starts on a high level, this way, when the *clock_in* signal is triggered, the *clock_result* switches to a high level until the *clock_in* falling edge is detected, from here a counter starts to increment at a 10 ns rate, as defined by the internal clock of the FPGA. The *clock_enable* signal switches to a low level when the incremented value is equal to a pre-defined value, chosen by the user. The *clock_enable* signal switches again to a high level when the counter reaches another pre-defined value. The counter resets when a rising edge of *clock_in* is detected, and the process explained above is restarted.

The other two input signals mentioned are the counts coming from the SPDs. The decision circuit reads these signals only during the period in which the *clock_enable* signal is on a high level. If one of the two signals coming from the SPDs is on a high level then the output of the decision circuit will be equal to the bit received (0 or 1), which depends on which detector sent the high level. If both signals coming from the SPDs are detected as high levels, the output will be a 2, meaning that a double click was detected. On the other hand, if no high level is detected, the output will be a 3, meaning that a no-click occurred.

3.3.2. Frame synchronization. After the symbol synchronization, a frame synchronization method must also be implemented [25]. The frame synchronization must establish a way to match the start of data transmission of the transmitter with the start of data reception at the receiver. The method we implemented consists of, at the beginning of transmission, sending a header, that is a pre-shared bit sequence (frame) so that the receiver can compare the received bit string with the expected one, and shift the received bits until a reasonable number of matches is achieved. For this implementation, the transmitter side sends 15 frames, each one consisting of a 40 bit sequence where each bit was repeated ten times, giving a total of 400 bits per frame. After the 15 frames are sent, the transmitter starts to send 11 inverted frames (where the 0's were changed to 1's, and the 1's to 0's), see figure 6(a). The number of inverted frames is also a pre-agreed number, therefore, the importance of the inverted frames is to enable the receiver to detect the transition between the normal and inverted frames. From the moment on the frame inversion was detected, the receiver starts to count the number of inverted frames received, knowing that after the pre-agreed number data transmission starts.

At the beginning, the receiver compares the pre-shared bit sequence with the received sequence, comparing a large number of bits at a time. When the number of coincidences between the pre-shared and received sequences is above a certain threshold the frame is considered to be positioned, see figures 6(b)–(d). Hereafter, the receiver starts to compare the sequences frame by frame, in order to correctly detect the frame inversion. After detecting frame inversion the number of bits being compared at a time can be increased again, given that the number of inverted frames is known, see figure 6(e). It is worth noticing that the high number of bits per frame is due to the high optical attenuation, intrinsic to the nature of QKD systems. With this synchronization mechanism a total of 10 400 bits is used, which at a repetition rate of 500 Hz

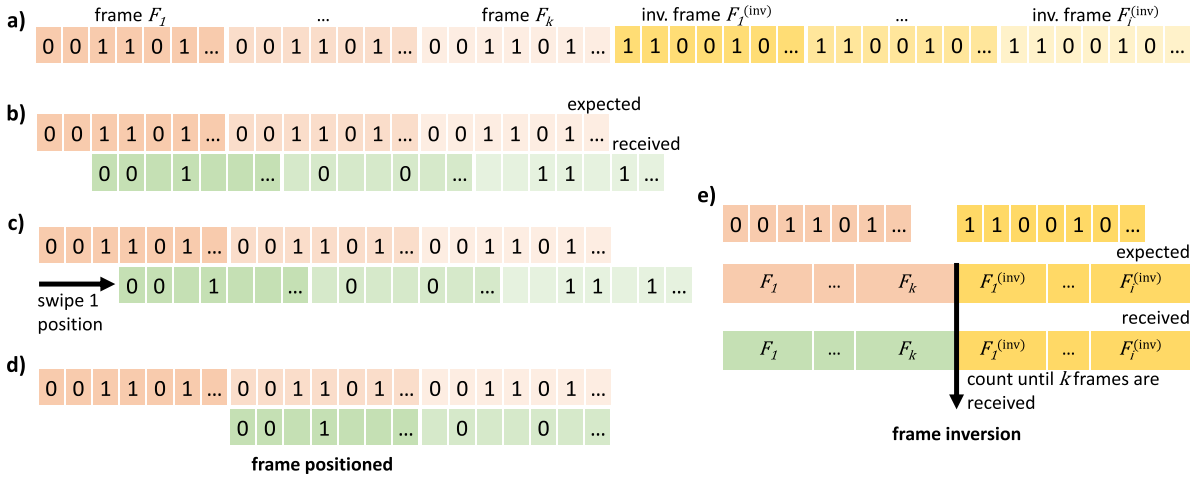

Figure 6. Schematic explanation of the frame synchronization method: (a) structure of the frames, F_k, sent by the transmitter, in this case with $k = 1,\ldots,N$, and $N = 15$ normal frames, and $F_i^{(inv)}$, inverted frames, with $i = 1,\ldots,M$, with $M = 11$; (b) comparison bit by bit of the expected frame and the received frame at the QRx, while not positioned; (c) swiping received frames until the frame positioning is achieved; (d) frame positioning was achieved; (e) comparison frame by frame until the detection of the frame inversion in order to know when data transmission starts.

corresponds to a synchronization time of less than 30 seconds. It is important to notice that the frame length can be optimized. The optimum value will be dependent on the channel efficiency of the QKD system. Additionally, given that during the synchronization period no secret key is being generated, the average number of photons can also be adjusted. In the conditions tested, the frame synchronization method here presented requires roughly 10^4 clock cycles and does not need a specific sequence to work. Its adaptability and efficiency present an advantage over the frame synchronization method presented in [11], where a specific synchronization string is required.

4. Performance assessment

4.1. Polarization state generation

In this section, we perform a deep analysis of the transmitter performance in terms of polarization generation accuracy. First, we measured the voltages received at PIN1 while the SOP alignment algorithm was searching for the maximum perimeter circle. These voltages were plotted as a function of the voltage applied on the first and fourth waveplate (WP) of the EPC as a three-dimensional representation. Each curve corresponds to one constant voltage applied on the first waveplate as a function of a varying voltage applied to the fourth waveplate, see figure 7(a). Figure 7(b) shows the increasing ΔV as a function of the voltage applied on the first waveplate.

As expected, given that the input SOP projection on the S_2 axis was positive, the response to a increasing voltage on the first waveplate increased the amplitude of the sinusoidal curve caused by the variation of the fourth waveplate. The algorithm stops when the maximum perimeter circle is found. This is determined by the ΔV values such that, when the following conditions are full-filled, the maximum is considered found:

$$\begin{aligned} &\Delta V(k) < \Delta V(k-1) \quad \text{and} \quad \Delta V(k-2) < \Delta V(k-1) \\ &\qquad\qquad \text{or,} \\ &\Delta V(k-1) = \Delta V(k) \quad \text{and} \quad \Delta V(k-2) < \Delta V(k-1) \end{aligned} \tag{6}$$

where k is the index of the ΔV that was determined.

After the voltage applied on the first waveplate, that corresponds to the maximum circle, was found, the swipe of voltage values applied on the fourth waveplate is performed with a smaller step, in order to obtain the voltage values for each state with more precision. As mentioned above, during this swipe, both, the optical power reaching PIN1 and PIN2 are monitored. A fitting of a sinusoidal function is performed around the maxima and minima of both curves, see figure 7(c). This fitting is made in order to obtain a more accurate estimation of the best voltages for each state, even in the presence of some received optical power oscillations. From the fittings performed to the curves of figure 7(c), the voltage values for the four SOPs are determined. Results in figure 7(c) also show that the EPC presents a slight irregularity noticeable when comparing the lower aperture of the linear and circular curves. The aperture of the circular curve is slightly wider than the aperture of the linear curve. This irregularity might cause small deviations from the optimal SOP.

4.2. Transmission

To assess the performance of the physical layer the QBER is a metric given that it evaluates the errors occurred during transmission. To obtain the QBER estimations when four states of polarization are sent, the basis alignment and selection must be performed at the receiver. Figures 8(a) and (b) show the QBER results for a pseudo-random sequence sent. The basis used to encode and decode the sequence, at the transmitter and receiver, respectively, were also pseudo-random following the BB84 protocol. The QBER was calculated as:

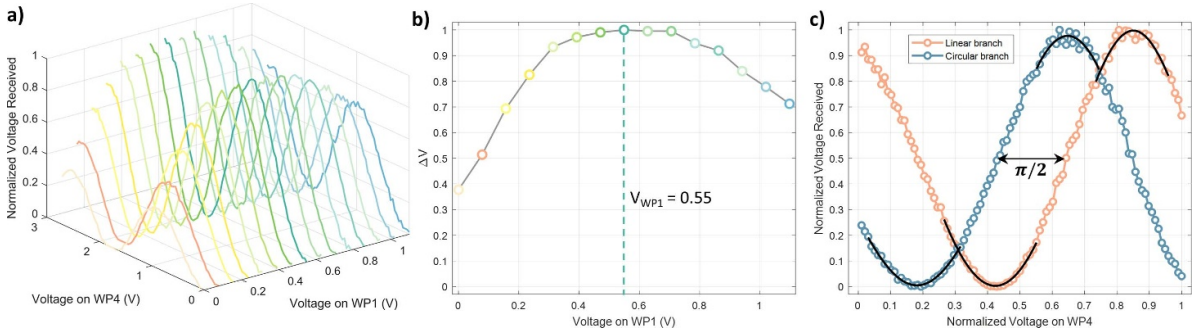

Figure 7. (a) Evolution of the normalized voltage detected by the PIN1 as a function of the voltage applied on WP4, and WP1. (b) Evolution of the normalized amplitudes in (a), ΔV, as a function of the voltage applied on the WP1. The green-dashed line represents the voltage corresponding to the maximum perimeter circle shown in figure 7. The color of each curve, in (a), matches with the same color as the points in (b), allowing a correspondence between the curve with the respective ΔV; (c) optical power as a function of the voltage applied on the fourth waveplate, received by PIN1, which corresponds to the linear branch, and by PIN2, which corresponds to the circular branch. The black lines represents the fit performed in order to obtain the voltage to apply on WP4 for each state with more precision.

$$QBER = \frac{N_{\text{error}}}{N_{\text{all}}}, \tag{7}$$

where N_{error} is the number of errors that occurred when the right basis was used for the measurement, and N_{all} stands for the total number of bits that were measured with the right basis selected. Figure 8 b) shows the contribution of each polarization state to the overall QBER. For this estimation, only the errors that occurred when a specific state was sent, and measured in the right basis, were considered. This number was divided by the total number of those states sent, measured in the right basis. Thus, this QBER is obtained by computing:

$$QBER_S = \frac{N_{\text{error},S}}{N_{\text{all},S}}, \tag{8}$$

where $N_{\text{error},S}$ is the number of errors that occurred when the polarization state $S = H, V, R,$ or L was sent, where $H, V, R,$ and L correspond to the horizontal, vertical, right circular, and left circular polarization states, respectively. This contribution only includes the measurements that were performed with the right basis selected. The variable $N_{\text{all},S}$, corresponds to the total number of states S that were sent and measured in the right basis. Each point of figure 8(a) was estimated with 2000 bits, that is, with $N_{\text{all}} = 2000$, while each point of figure 8(b) was estimated with $N_{\text{all}} = 8000$ bits, to have approximately 2000 bits measured in the right basis of each polarization state. The results were obtained during roughly six hours, and an overall average QBER of 0.75% was achieved, see figure 8(a). The system demonstrated its stability, as evidenced by the constant QBER throughout the six-hour experiment, without the need for additional calibration.

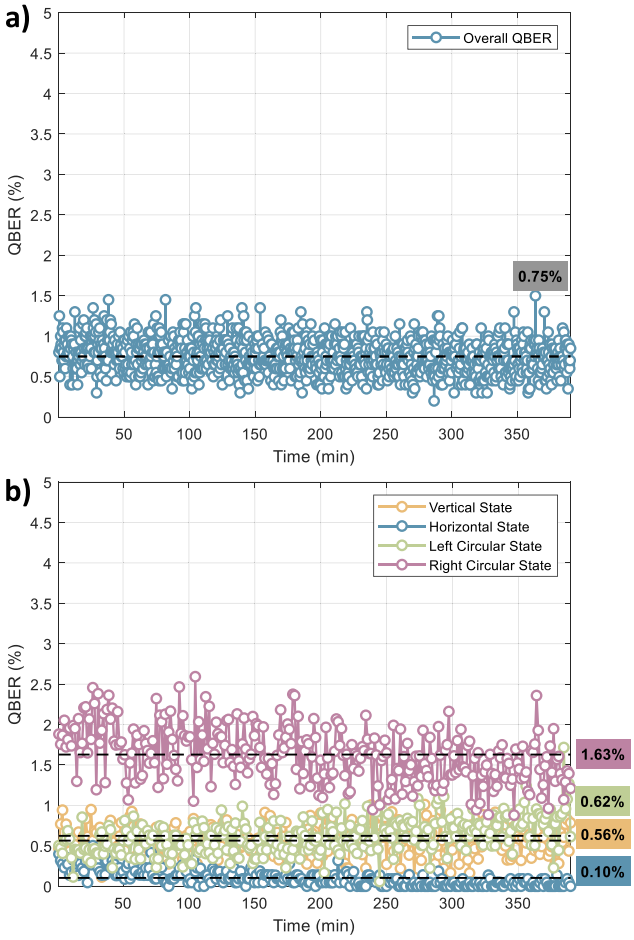

Figure 8. (a) QBER estimation as a function of time, for a total acquisition time of roughly six hours. An overall average QBER of 0.75% was obtained. (b) Analysis of the QBER contribution of each of the four polarization states used. Considering separately, the horizontal, vertical, left-circular, and right-circular states, the QBER was 0.56%, 0.10%, 0.62%, and 1.63%, respectively.

5. Discussion

Regarding the performance of the SOP generation, results in figure 7 show that the algorithm correctly detects the maximum circle of the Poincaré sphere, and that the sinus-shaped curves are correctly obtained. This enables a correct choice for the set of voltages to apply on each waveplate for each of the four polarization states. Although these results show that the method is effective, the individual analysis of the QBER showed slight asymmetries in terms of the relative contribution from each of the states generated. Indeed, results show that

the highest contribution to the overall QBER was given by the right-circular polarization state, with an average value of 1.63%. The other three states show a similar QBER among each other, being 0.10%, 0.56%, and 0.62%, for the vertical, horizontal, and left-circular polarization states, respectively. To test if the higher contribution occurs because of a slight misalignment during state preparation, or during the basis alignment at the receiver, the results were retaken with different alignments at the receiver. Although not represented here, the results confirmed the tendency of one state to have a slightly higher contribution than the average of the other three. Therefore, one may conclude that the misalignment occurs during the state preparation. Note that one effect that needs to be considered when employing piezoelectric EPCs is its intrinsic hysteresis [34], which potentially affects the accuracy of the generated states of polarization and therefore contributes to the intrinsic QBER associated with the polarization misalignment. In fact, the QBER values reported include this contribution, which are therefore compatible with the implementation of a secure QKD protocol. It is worth noticing that imperfect state preparation can present a security impairment that, when taken into account, may significantly reduce the distance up to which secret key generation is possible [35]. However, such security implications can be overcome by calibrating and monitoring the detection efficiency of the SPDs [36]. Moreover, associated to imperfect state preparation, can be removed during the key reconciliation (error correction) process, as QBER values up to 3% can be considered a reasonably low amount of leakage [6].

Regarding the EPC used, it is important to mention that this EPC has intrinsic advantages such as plug and play versatility, low insertion loss, small size, and wavelength insensitivity, which smoothed the way for the first validation of the polarization state generation algorithm proposed in this work [19]. However, the above-mentioned hysteresis and its low modulation bandwidth make this kind of EPC not suitable for practical QKD implementations, as it will be unable to provide competitive final secret key rates. In any case, the method here proposed can be adapted to be implemented in lithium niobate-based polarization modulators, which present much faster response times, allowing to reach realistic key generation rates [32, 33]. For long transmission distances, errors associated to the polarization drift can arise, impacting the performance of the system. However, this polarization drift can be mitigated by implementing efficient polarization compensation methods such as proposed in [37]. Additionally, it is worth mentioning that the sub-systems here presented are fully compatible with decoy-state protocols, which are mandatory to make these systems secure and to improve the secret key rates [38, 39]. This way, the suitability of the SOP generation method for practical QKD systems is shown.

6. Conclusions

We have presented a fully functional polarization-encoding QKD system, explaining in detail the respective SOP generation algorithm and synchronization mechanisms. After analyzing the integration of the subsystems into the QKD system, the performance of the SOP generation algorithm was assessed by estimating the QBER. For a deeper understanding of this error ratio, the contribution of the individual polarization states was investigated. After a six hour transmission of quantum states, an overall average QBER of 0.75% was achieved. This low value of QBER is compatible with a further implementation of error correction and privacy amplification algorithms, towards the generation of the final secret key. These results indicate that the sub-systems here described represent an efficient solution for the physical layer implementation of polarization-encoded QKD systems.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

This work was supported in part by Fundação para a Ciência e a Tecnologia (FCT), through national funds and when applicable co-funded EU funds, Under the Project UIDB/50008/2020, UIDP/50008/2020, by QuantaGenomics Project, funded within the QuantERA II Programme that has received funding from the European Union's Horizon 2020 research and innovation programme Under Grant Agreement No 101017733, and with co-funding organisations, The Foundation for Science and Technology—FCT (QuantERA/0001/2021), and by European Commission (EC), within the DIGITAL-2021-QCI-01 Programme, through the Project PTQCI (GA 101091730). Sara Mantey acknowledges the FCT PhD Grant 2021.06085.BD.

ORCID iD

Sara Mantey https://orcid.org/0009-0003-1968-1360

References

[1] Gisin N Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[2] Boyd R W Rodenburg B, Mirhosseini M and Barnett S M 2011 *Opt. Express* **19** 18310–7
[3] Bennett C H and Brassard G 1984 *Proc. Int. Conf. on Computer Systems and Signal Processing (ICCSSP) (India)* pp 175–9
[4] Liang W Y *et al* 2014 *Sci. Rep.* **4** 1–6
[5] Sun P C Mazurenko Y and Fainman Y 1995 *Opt. Lett.* **20** 1062–4
[6] Grünenfelder F Boaron A, Rusca D, Martin A and Zbinden H 2020 *Appl. Phys. Lett.* **117** 144003
[7] Bouchard F England D, Bustard P J, Heshami K and Sussman B 2022 *PRX Quantum* **3** 010332
[8] Agnesi C *et al* 2022 *Proc. Optical Fiber Communication Conf. (OFC) (San Diego)*
[9] Liao S-K *et al* 2017 *Nature* **549** 43–47
[10] Liu Y *et al* 2010 *Opt. Express* **18** 8587–94
[11] Calderaro L Stanco A, Agnesi C, Avesani M, Dequal D, Villoresi P and Vallone G 2020 *Phys. Rev. Appl.* **13** 054041

[12] Lu C, Cao Y, Peng C-Z and Pan J-W 2022 *Rev. Mod. Phys.* **94** 035001
[13] Almeida A J, Stojanovic A D, Paunković N, Loura R, Muga N J, Silva N A, Mateus P, André P S and Pinto A N 2016 *J. Opt.* **18** 015202
[14] Muga N Ferreira M F S and Pinto A N 2011 *J. Light. Technol.* **29** 355–61
[15] Sax R *et al* 2023 *Photon. Res.* **11** 1007–14
[16] Li W *et al* 2023 *Nat. Photon.* **17** 416–21
[17] Luo W *et al* 2022 *IEEE Photon. J.* **14** 1–6
[18] Li Y Li Y-H, Xie H-B, Li Z-P, Jiang X, Cai W-Q, Ren J-G, Yin J, Liao S-K and Peng C-Z 2019 *Opt. Lett.* **44** 5262–5
[19] Muga N Ramos M F, Mantey S T, Silva N A and Pinto A N 2020 *IET Optoelectron.* **14** 350–5
[20] Ramos M F *et al* 2021 *Proc. Anais do I Workshop de Comunicação e Computação QuâNtica (Online)*
[21] Lucio-Martinez I Chan P, Mo X, Hosier S and Tittel W 2009 *New J. Phys.* **11** 095001
[22] Tajima A Tanaka A, Maeda W, Takahashi S and Tomita A 2007 *IEEE J. Sel. Top. Quantum Electron.* **13** 1031–8
[23] Wang P Huang P, Chen R and Zeng G 2021 *Opt. Express* **29** 25048–63
[24] Mantey S T *et al* 2022 *Proc. Optical Fiber Communication (OFC) Conf* (San Diego)
[25] Mantey S T *et al* 2022 *Proc. IEEE Global Communications Conf.* (GlobeCom)
[26] Born M and Wolf E *et al* 1999 *Interference and Diffraction of Light* 7th edn (Cambridge University Press)
[27] Lites B W 1987 *Appl. Opt.* **26** 3838–45
[28] Smith A M 1980 *Appl. Opt.* **19** 2606–11
[29] Lin Z *et al* 2022 *Light Sci. Appl.* **11** 93
[30] Sun B *et al* 2022 *Light Sci. Appl.***11** 214
[31] Goldstein D H 2003 *Polarized Light* (CRC Press)
[32] Garcia J D and Amaral G C 2016 *IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)* pp 1–5
[33] Agnesi C Avesani M, Stanco A, Villoresi P and Vallone G 2019 *Opt. Lett.* **44** 2398–401
[34] Ru C and Sun L 2006 *Ultrasonics* **44** e731–5
[35] Reutov A *et al* 2023 *Entropy* **25** 1556
[36] Sun S and Xu F 2021 *New J. Phys.* **23** 023011
[37] Ding Y-Y, Chen W, Chen H, Wang C, li Y-P, Wang S, Yin Z-Q, Guo G-C and Han Z-F 2017 *Opt. Lett.* **42** 1023–6
[38] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[39] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504