Demonstration of an Algorithm for Quantum State Generation in Polarization-Encoding QKD Systems

S. T. Mantey[1,3], **M. F. Ramos**[1,3], **N. A. Silva**[1], **A. N. Pinto**[1,3], **N. J. Muga**[1,2]

[1] *Instituto de Telecomunicações, University of 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*

smantey@ua.pt

Abstract: We experimentally demonstrate a polarization-state generation algorithm using off-the-shelf components. The method was implemented using a laboratory QKD testbed running for 21 hours with an average QBER of 1.8%. © 2022 The Author(s)

1. Introduction

The security of information has been an increasing concern, giving the huge amount of information transmitted over the Internet [1]. Nowadays, most cryptography protocols use public keys. However, one flaw of those systems is the uprising of quantum computers which compromises the robustness of public key systems when facing the computational power of those computers. A solution for data security relies in the use of symmetric key protocols which are assumed to be secure even in the presence of a quantum computer [2]. With the use of quantum cryptography, key exchange for symmetric key protocols is theoretically secure [3].

The first quantum protocol was proposed in 1984, the BB84 protocol [4], which uses the polarization of single photons to encode the data. Since then, polarization-encoding systems were studied and have shown promising results for fiber-based and free space Quantum Key Distribution (QKD) [5]. Several methods have been proposed aiming a fast and stable State of Polarization (SOP) generation using, e.g., Mach-Zehnder interferometers [6], phase-modulators [7], Sagnac interferometers [5], amongst others. These polarization-encoding mechanisms have shown to achieve low Quantum Bit Error Rates (QBER), high key transmission rates, stability and reach. However, there are some drawbacks as, e.g., the complex implementation of Sagnac interferometers, or the sensitivity to environmental disturbances of Mach-Zehnder interferometers.

Here we present and validate an algorithm for SOP generation, by exploring the advantages of electronically-driven waveplates, e.g., the plug and play versatility, low insertion loss, small size, and wavelength insensitivity [8]. The proposed method overcomes the previously mentioned complex implementations, and instabilities caused by disturbances that lead to SOP misalignments. The algorithm and corresponding setup were tested using a laboratory QKD system as testbed. Four SOPs were generated, therefore demonstrating its compatibility with the BB84 and B92 QKD protocols.

2. Proposed SOP Generation Method

To enable the developed algorithm to generate the SOPs, a setup as shown in Fig. 1 (b) is needed. A polarization modulator, capable of performing controlled rotations of the SOP is a key element. In this work, we use an EPC that comprises four piezoelectric waveplates, with an adjustable retardation angle and a fixed fast axis angle. The second and fourth waveplates have a fast axis that makes an angle of 45 degrees in relation to the first and third waveplate. By applying a given voltage to each waveplate the retardation angle is adjusted. This way, the EPC enables a SOP movement around the S_1 and S_2 axis of the Poincaré sphere, allowing to transform an arbitrary input SOP into any wished output SOP.

By monitoring the optical output of the linear branch, the projection of the SOP on the S_1 axis is measured. In a first approach, the second waveplate of the EPC is triggered to, step-by-step, rotate the SOP around the S_2 axis. In each step the optical power received by P-I-N Photodiode 1 (PIN1) is measured and registered. Note that a step-by-step increasing voltage applied on the second waveplate, typically implies that the voltage received by the PIN follows a sine function with a defined period. After a complete turn was performed the optical power difference, ΔV is calculated, see Fig. 1 (a). After, one step is performed around the S_1 axis, by triggering the first waveplate. Again, a rotation around the S_2 axis is performed and the next ΔV is calculated. This procedure is

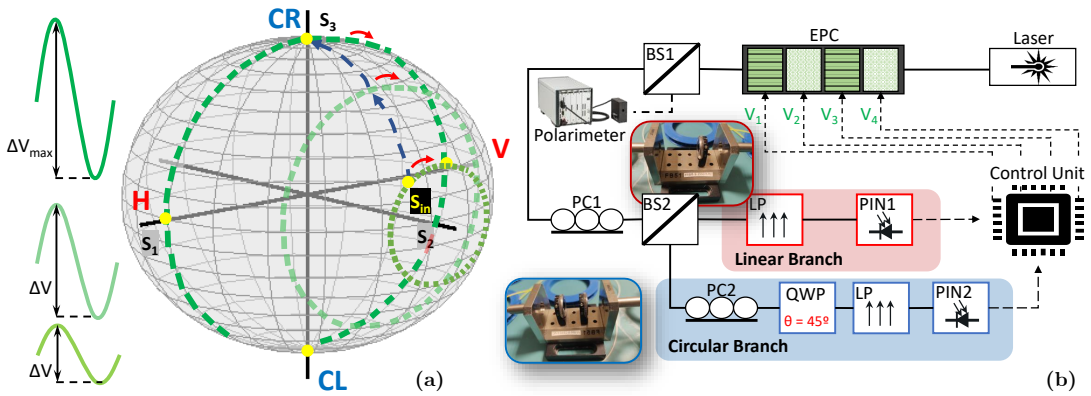

Fig. 1: (a) Schematic representation of the working principle of the SOP generation algorithm: SOP rotations performed to determine the set of voltages needed to generate each of the four SOPs, horizontal, vertical, right circular, and left circular. (b) Setup used for the voltage determination.

performed until the maximum ΔV is found. The finding of the maximum ΔV means that the SOP is now located on the S_1OS_3 plane. From here, we repeat the turn around the S_1OS_3 plane, monitoring the output of PIN1 and PIN2. The voltage applied on the waveplate for which the optical power of the linear branch is maximum and minimum corresponds to the voltage to generate the horizontal and vertical SOP, respectively. At the circular branch, the quarter waveplate will shift the circular SOPs to the equator of the Poincaré sphere. Therefore, analogously to the procedure for the linear SOPs, the voltage for which the optical output of the circular branch is maximum and minimum corresponds to the right and left circular SOP, respectively. This way, by using only two waveplates we were able to generate the four SOPs.

The setup needed for the SOP generation is represented in Fig. 1 (b). An External Cavity Laser (ECL) laser emits a signal with a wavelength of 1547.72 nm. After, a Beam Splitter (BS) divides the signal. One part goes to the SOP generation setup, and the other can be guided to the QKD system or to a polarimeter (as shown in the figure) for monitoring. The manual Polarization Controlers (PC), PC1 and PC2, have to be adjusted after the S_1OS_3 plane is found. This, in order to ensure that the polarization at the entrance of the Linear Polarizer (LP) of the linear branch is equal to the polarization at the entrance of the Quarter Waveplate (QWP) of the circular branch. This alignment is performed without the QWP inserted.

3. Experimental Validation using a QKD Testbed

The experimental validation of the proposed SOP generation method was performed using a laboratory QKD testbed. At the transmitter (Tx), two laser beams are prepared, one is the signal with the quantum state and the other serves as a reference signal, see Fig. 2. The reference signal correlates the transmitters emission events with the receivers detection events. The reference signal and quantum signal are modulated by Mach-Zehnder Modulators (MZM) to have a frequency of 500 Hz and a pulse width of 100 ns, and 1 ns, respectively. PC1 and PC2 are adjusted to optimize the optical output of the MZMs. After MZM1, the quantum signal is filtered, and PC3 is placed to adjust the polarization in order to optimize the output of the LP. The LP placed before EPC1 ensures that the input polarization of EPC1 is fixed. After, a BS guides the signal to a Variable Optical Attenuator (VOA), and to the SOP generation system that determines the voltages to send to EPC1. The VOA attenuates the signal to a quantum level before it is combined with the reference signal by a Wavelength-Division Multiplexer (WDM) and sent through the quantum channel to the receiver (Rx).

At the receiver, the signal is splitted by a WDM. The reference signal is detected by a PIN to send a trigger

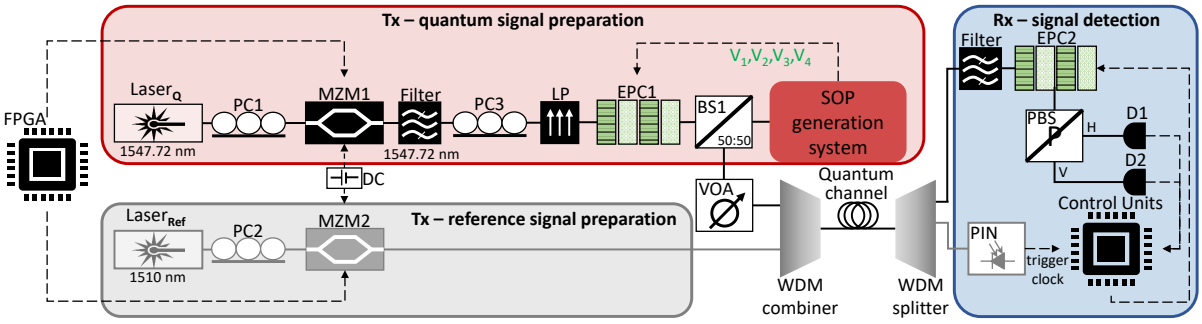

Fig. 2: Schematic representation of the QKD testbed used to assess the performance of the proposed method.

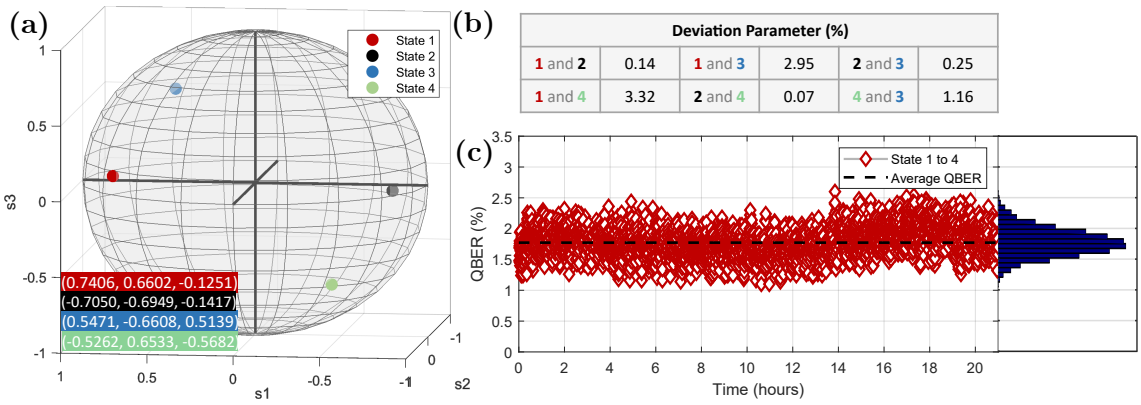

Fig. 3: (a) Generated SOPs represented on the Poincaré sphere and the respective Stokes parameters. (b) Deviation parameter results of the generated SOPs. (c) QBER estimation in function of time, for a total acquisition time of 21 hours, and the respective histogram. An overall average QBER of 1.8% was obtained.

clock to the control units and detectors. The quantum signal, on the other hand, is filtered and guided to EPC2 so that the basis alignment can be performed. EPC2 is fed with two sets of voltages according to the state that is being sent. During the calibration stage, the set of voltages to align the receiver with the linear and circular basis was determined by minimizing the QBER when the transmitter was sending only the horizontal, and then only the right circular SOP, respectively. This alignment serves not only to perform the basis selection but also to compensate for the polarization drift that occurs at the quantum channel. After EPC2, the quantum signal is sent to a Polarization Beam Splitter (PBS). The horizontally polarized output is guided to the Single Photon Detector 1 (D1), while the vertically polarized output is guided to D2. These detectors report their measurements to the control units so that the QBER estimation can be performed.

Two types of measurements were performed to assess the accuracy and general performance of the proposed SOP generation algorithm: measurements of the Stokes parameters and QBER estimations in a polarization-encoding QKD testbed. Using a polarimeter (Thorlabs TXP5004), as shown in Fig. 1 (b), the Stokes parameters of each state were measured, and the Scalar Product (SP) was computed in order to assess the orthogonality between them. The expected SP between two stokes vectors representing two orthogonal states is -1, and between two states that make a 45 degree angle is 0. The SP obtained was subtracted by the expected SP and multiplied by 100 - deviation parameter. This way, the deviation parameter will range from 0 to 100 according to the accuracy of the SOP generation, where zero represents the most accurate and 100 the less accurate. The Stokes parameters obtained for the four states are represented on the Poincaré sphere, see Fig. 3 (a). The results of the deviation parameter are shown in Fig. 3 (b).

The QBER estimation was performed during 21 hours. A pseudo-random, eight bit, data key was sent in loop. The basis used to encode the data key was also a pseudo-random, eight bit sequence in loop. An overall average QBER of 1.8% was obtained, see Fig. 3 (c).

4. Conclusions

A SOP generation algorithm for polarization-encoding QKD systems was demonstrated using off-the-shelf components. The SOP generation accuracy was tested by measuring the Stokes parameters and by estimating the QBER. Results show that the generated SOPs present a low deviation from the theoretical values. The average QBER after 21 hours was 1.8%, with only one calibration at the beginning of the measurements.

This work is supported by FEDER, through COMPETE2020 of the Portugal2020 framework [Project Q.DOT with Nr. 039728 (POCI-01-0247-FEDER-039728)], and by FCT/MCTES through national funds and when applicable co-funded EU funds under the projects QuantumMining (POCI-01-0145-FEDER-031826) UIDB/50008/2020-UIDP/50008/2020 (actions QuRUNNER, QUESTS, and DigCORE). S. T. Mantey and M. F. Ramos work was supported by FCT through FSE and by Programa Operacional Regional do Centro under Ph.D. Grant 2021.06085.BD, and SFRH/BD/145670/2019, respectively.

References

1. C. Cheng, *et al.*, “Securing the Internet of Things in a Quantum World”, IEEE Commun. Mag, 55(2), 116-120 (2017).
2. H. Zbinden, *et al.*, “Quantum Cryptography”, Appl. Phys. B: Lasers and Optics, 67(6), 743–748 (1998).
3. N. Gisin, *et al.*, “Quantum Cryptography”, Rev. Mod. Phys., 74(1), 145 (2002).
4. C. Bennett, *et al.*, “Quantum Cryptography: Public key distribution and coin tossing”, International Conference on Computers, Systems and Signal Processing, 175-179 (1984).
5. Y. Li, *et al.*, “High-speed robust polarization modulation for quantum key distribution”, Opt. Lett, 44(21), 5262-5265 (2019).
6. F. Grünenfelder, *et al.*, “Simple and high-speed polarization-based QKD”, Appl. Phys. Lett., 112(5), 051108 (2018).
7. A. Duplinskiy, *et al.*, ”Low loss QKD optical scheme for fast polarization encoding,” Opt. Express, 25(23), 28886-28897 (2017).
8. N. Muga, *et al.*, “FPGA-assisted state-of-polarisation generation for Polarization-Encoded Optical Communications”, IET Optoelectron., 14(6), 350-355 (2020).