Demonstration of a Polarization-encoding Quantum Key Distribution System

Sara T. Mantey[1,2], Mariana F. Ramos[1,2], Nuno A. Silva[1], Armando N. Pinto[1,2], Nelson J. Muga[1]

[1]Instituto de Telecomunicações – Aveiro
Aveiro, Portugal.

[2]Department of Electronics, Telecommunications, and Informatics – University of Aveiro
Aveiro, Portugal.

smantey@ua.pt, marianaferreiraramos@ua.pt, nasilva@ua.pt, anp@ua.pt, muga@ua.pt

Abstract. *In this work, a fully functional polarization-encoding quantum key distribution system (QKD) is demonstrated. At the transmitter side, the polarization states are prepared using an algorithm to determine the voltages to be applied on the electronic polarization controller (EPC), to generate up to four polarization states. At the receiver, a second EPC is used to perform the basis alignment. The symbol synchronization is achieved using a reference optical signal that is wavelength division multiplexed with the quantum signal which carries the polarization-encoded qubit. Frame synchronization is achieved at a protocol level. The presented QKD system works at a repetition rate of 500 Hz, with an average quantum bit error rate of 1.35%.*

1. Introduction

Quantum Key Distribution (QKD) became a topic of high relevance when the scientific community realised the potential of the upcoming quantum computers. Nowadays cryptography mechanisms rely on the complexity of mathematical factorization problems, that would take years to be solved by a generic computer [Sharma 2019]. However, it was shown by [Shor 1999] that a quantum computer is able to solve, for example, the integer factorization problem in a matter of minutes, threatening the security of our information [Cheng 2017].

In order to overcome the threat to cyber security, the research in quantum communications was furthered. Until now, quantum communications, as QKD, have shown to be a promising solution to stand up against quantum computers [Preskill 2018]. QKDs working principle consists in the process of distributing random bit strings, which are known as keys, that are used to encode and decode the information during the communication. For this purpose, the key needs to be distributed between the transmitter, usually known as Alice, and the receiver, usually known as Bob [Gisin 2002]. This key sharing process needs to be done with an authenticated quantum channel, to ensure that no eavesdropper gets access to the key [Gisin 2002]. After the key is shared, communication can be performed through a regular classical channel, which also needs authentication, using the encrypted data.

The first QKD protocol was proposed in 1984 by Bennet and Brassard, called the

BB84 protocol [Bennet 1984], which was based in polarization-encoding. Nowadays there are several other methods to encode quantum bits, by exploiting several degrees of freedom of single photons, leading to polarization-entanglement [Gariano 2018], or time-bin [Vagniluca 2020], or a combination of, for example, polarization and time-bin [Agnesi 2022], among others. Nevertheless, the use of polarization remains a highly appellative approach giving its high versatility (free space and fiber optics) [Gao 2022], achievable reach [Boaron 2018], key-rates [Grünenfelder 2020], and error rates [Agnesi 2020].

In this work, we demonstrate a polarization-encoding QKD system. At the transmitter of this QKD system, two optical signals are prepared. The quantum signal will carry the polarization states, for which a correct and efficient generation mechanism is needed. This State of Polarization (SOP) generation is achieved using an Electronic Polarization Controller (EPC) based on piezoelectric technology [Mantey 2022]. The other optical signal is used for synchronization purposes. The receiver of this QKD system also uses an EPC, here to perform the basis alignment for the SOP measurement. At the receiver, beyond the SOP measurement, a synchronization mechanism is employed. Symbol synchronization is achieved by the detection of the second optical signal prepared at the transmitter, which serves as trigger signal for the Single Photon Detectors (SPDs) and control units [Ramos 2021]. Frame synchronization is achieved at a protocol level. With this QKD system, a repetition rate of 500 Hz is achieved with an average Quantum Bit Error Rate (QBER) of 1.35%, estimated following [Muga 2010]. All these subsystems will be explained in detail in this work.

2. Overview of the QKD System

The QKD system can be divided into three layers, the physical layer, which englobes all the optical components to achieve the key encryption, decryption and transmission, the middleware layer, which comprises all the control units that receive and send signals to the physical layer, and which makes the connection between the physical layer and the third layer – the protocol layer. Fig. 1 is a schematic representation of the arrangement and purpose of each layer, at transmitter and receiver side.

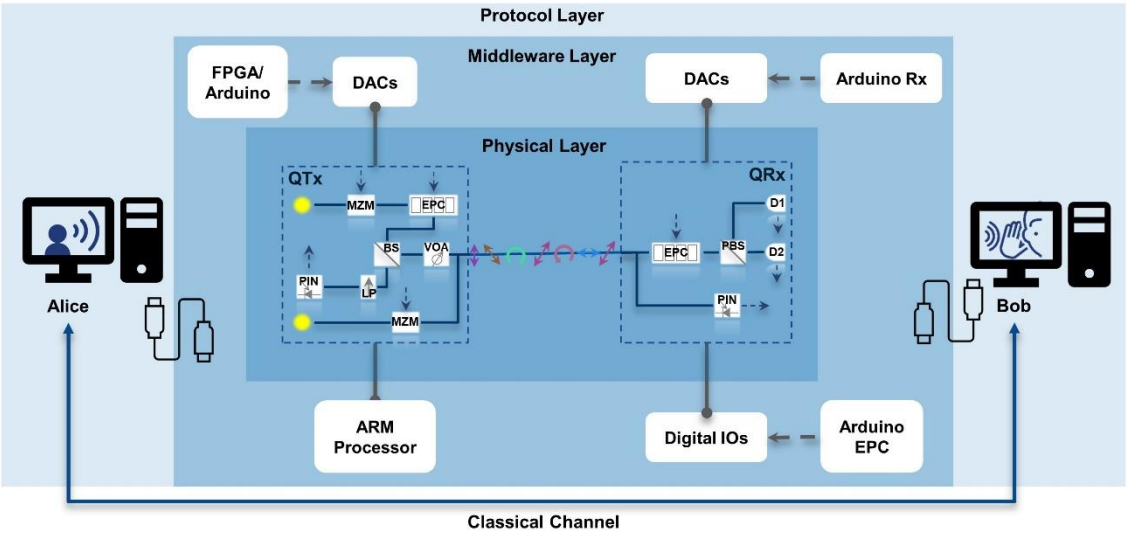

Figure 1. Schematic overview of the polarization-encoding QKD system

At protocol layer, at the transmitter side, Alice has two random binary sources, which determine the data, i.e., the qubit, and basis to encode it, resulting in one of four possible polarization states, that should be sent to the receiver. For each pulse sent through the quantum channel one state is sent and recorded. At the protocol layer of the receiver, Bob has one random binary source which determines in which basis the polarization of the arriving photon should be measured. Here, the protocol layer also processes the measurements of the SPDs and, is responsible for the frame synchronization.

3. Transmitter of the QKD System

At the transmitter, two optical signals are prepared, as mentioned above. The reference signal is emitted by an External Cavity Laser (ECL) source with a wavelength of 1510.00 nm, to be modulated in amplitude by a Mach-Zehnder Modulator (MZM). The MZM imposes a frequency of 500 Hz, and a pulse width of 100 ns to the reference signal. The digital signal for the MZM is sent from the transmitters FPGA board, see Fig 2.

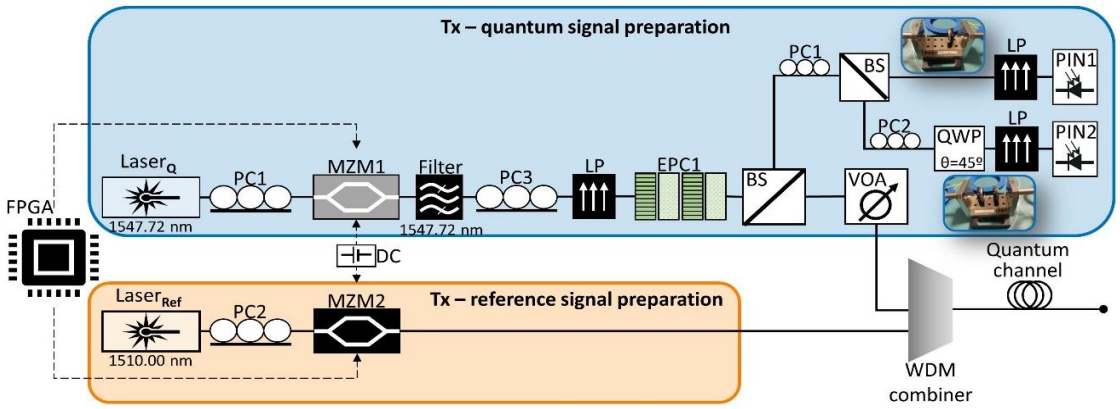

Figure 2. Schematic representation of the experimental setup present at the transmitter of the QKD system.

The quantum signal is emitted by an ECL with a wavelength of 1547.72 nm, then, it is also modulated by a MZM to have a frequency of 500 Hz, however, with a pulse width of 1 ns. After the modulation in amplitude, the quantum signal is filtered to eliminate out-of-band noise, then a Linear Polarizer (LP) is used to ensure that the polarization at the entrance of the EPC (General Photonics - Polarite III) is maintained stable. After the LP, the piezoelectric EPC generates the SOPs to encode the data. The voltages needed to apply on the EPC for each of the four possible SOPs (horizontal, vertical, right circular, and left circular) is determined using a SOP monitoring setup, which is located after one of the two outputs of a 50/50 Beam Splitter (BS).

The SOP monitoring setup consists of two branches, one responsible for determining the voltages for the linear SOPs, and one responsible for determining the voltages for the circular SOPs. The manual Polarization Controllers (PC) are there to ensure that the polarization at the entrance of both branches is the same. The linear branch consists of a LP and a P-I-N photodiode (PIN), whereas the circular branch consists of a Quarter Waveplate (QWP), which rotates the circular states to a linear state, then a LP, and a second PIN. The working principle of the above explained setup consists of two main parts: the finding of the maximum perimeter circle on the Poincaré sphere, and the determination of the voltages for each SOP. The operation principle of both branches of this SOP generation algorithm is to maximize and minimize the optical power at the

entrance of the PIN by changing the voltage on the EPCs waveplates, following an algorithm detailed in [Mantey 2022].

As mentioned above, one output of the referred BS is used by the SOP generation algorithm. The other output is connected to a Variable Optical Attenuator (VOA) to attenuate the signal to a quantum level (about 0.1 photons per pulse). After, the quantum signal and the reference signal are combined by a WDM and sent through the optical channel.

4. Receiver of the QKD System

At the receiver, the reference signal and the quantum signal are splitted by a WDM. The reference signal is detected by a PIN. The trigger signal outputted by the PIN is used by the SPDs, that operate in the gated mode, and by the control units to perform symbol synchronization, see Fig. 3.

The quantum signal, after being separated from the reference signal, is filtered again, and passes on to another EPC. This EPC aligns the detection setup with one of two measuring basis, linear or circular, according to the random binary number generated at the protocol layer. The output of the EPC is connected to a Polarization Beam Splitter (PBS). Each output of the PBS is connected to one SPD, this in order to distinguish between horizontal and vertical polarization. The voltages to apply on the EPC for each of the two basis are, for now, previously determined.

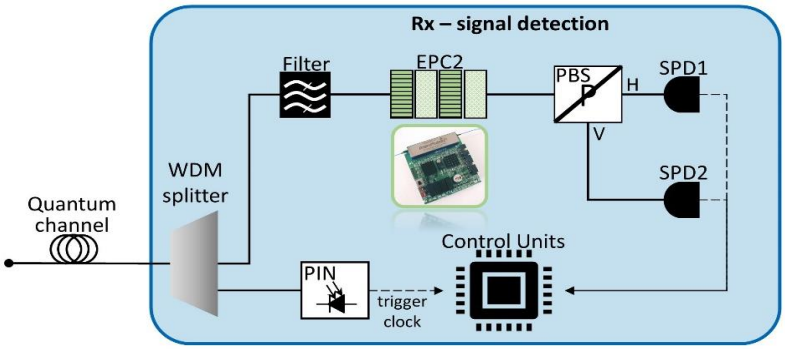

Figure 3. Schematic representation of the experimental setup present at the receiver of the QKD system.

The measurements of the SPDs are processed by the protocol layer in order to determine which state was sent. The measured state, and the base in which the measurement was performed is registered.

At the beginning of each data transmission, a frame synchronization must be performed. In this QKD system, the synchronization mechanism is based on a QBER monitoring approach. In this regard, at the beginning of data transmission, the transmitter sends a set of synchronization frames that are known to the receiver. The receiver compares the received bits with the ones of the pre-agreed frames and shifts the received ones until the highest number of matches is obtained. After a certain number of frames (high enough to ensure that frame positioning is achieved) is sent by the transmitter, another set of frames is sent but with the zeros and ones inverted. This way, jumping from the highest number of matches to the highest number of mismatches. The number of inverted frames is also a pre-agreed quantity, after which the receiver knows that data transmission has started.

5. Results of the Demonstrated QKD System

Using random SOPs being emitted by the transmitter, and random basis for the measurement at the receiver, the afore explained system was able to obtain QBERs of the order of 2%, using a repetition rate of 500 Hz, see Fig. 4. This result was computed by comparing the registered measurements and used basis at the receiver, with the data and basis registered by the transmitter.

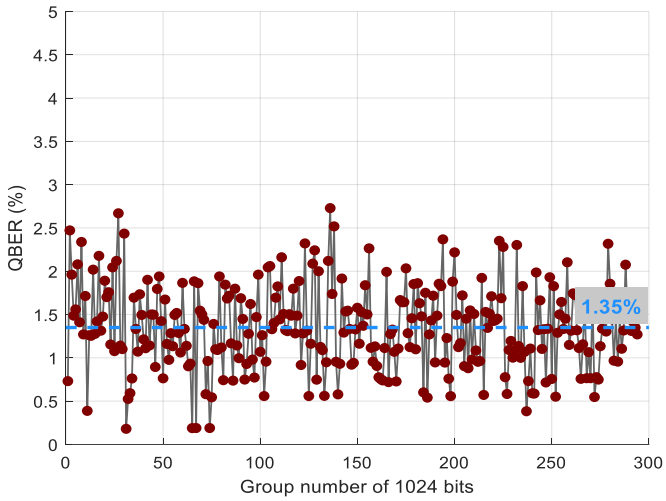

Figure 4. QBER results obtained with the presented QKD system.

Each QBER shown in Fig. 4, was estimated with 1024 bits. It is worth noticing that given the nature of a QKD system, where the signal is highly attenuated, and due to the typically low efficiency of the SPDs (about 10 to 15%), only very few photons arrive at the receiver. This way, for the results shown in Fig. 4, the emitted bits for which no photon was detected at the receiver were removed. For a total of about 300000 bits received, an overall average QBER of 1.35% was obtained.

6. Conclusions

In this work, a fully functional polarization-encoding QKD system was presented, where each sub-system was explained in detail. At the transmitter side, an algorithm is used to determine the voltages to apply on the EPC for each of the four possible states. At the receiver side, a second EPC is used for basis alignment. Here the voltages for each basis are pre-computed. The synchronization mechanism of this system englobes a symbol synchronization, which is performed using a reference optical signal that is combined with the quantum signal using WDM technology. The frame synchronization is achieved at the protocol layer, using a QBER monitoring mechanism. With this system, a repetition rate of 500 Hz is achieved, and an average QBER of 1.35% was obtained.

7. Acknowledgements

This work is supported by Fundação para a Ciência e a Tecnologia (FCT) through national funds, by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Programme (COMPETE 2020), under the project QuantumPrime reference: PTDC/EEI-TEL/8017/2020, and by FCT/MCTES through national funds and when applicable co-funded EU funds under the

projects UIDB/50008/2020 and UIDP/50008/2020 (actions QuRUNNER, QUESTS, and DigCORE).

8. References

Sharma, A., Kumar, A. (2019) “A Survey on Quantum Key Distribution”, 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), IEEE, vol. 1, pp. 1-4.

Shor, P. (1999) “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, SIAM Review, vol. 41, no. 2, pp. 303-332.

Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017) “Securing the Internet of Things in a quantum world”, IEEE Communications Magazine, vol. 55, no. 2, pp. 116-120.

Preskill, J. (2018) “Quantum Computing in the NISQ era and beyond”, In: Quantum, vol. 2, pp. 79.

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002) “Quantum Cryptography”, In: Reviews of Modern Physics, vol. 74, no. 1, pp. 145.

Bennet, C., Brassard, G. (1984) “Quantum Cryptography: Public Key Distribution and Coin Tossing”, International Conference on Computer Systems and Signal Processing, vol. 1, pp 175-179.

Gariano, J., & Djordjevic, I. (2018), “Polarization entanglement QKD with covert classical communications”, In 2018 IEEE Photonics Conference (IPC), IEEE, pp. 1-2.

Vagniluca, I., et al. (2020) “Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution”, Physical Review Applied, vol. 14, no. 1.

Agnesi, C., et al. (2022) “Time-bin Quantum Key Distribution exploiting the iPOGNAC polarization modulator and Qubit4Sync temporal synchronization”, in Optical Fiber Communication Conference (OFC) 2022, Optica Publishing Group.

Gao, T., et al. (2022) “A Quantum Key Distribution Testbed using a Plug&play Telecom-wavelength Single-photon Source”, Applied Physics Reviews, vol. 9, no. 1.

Boaron, A., et al. (2018) “Secure Quantum Key Distribution over 421 km of Optical Fiber”, Physical Review Letters, vol. 121, no. 19.

Grünenfelder, F., et al. (2020) “Performance and security of 5 GHz repetition rate polarization-based quantum key distribution”, Applied Physics Letters, vol. 117, no. 14.

Agnesi, C., et al. (2020) “Simple QKD with qubit-based synchronization and a self-compensating polarization encoder”, Optica, vol. 7, no. 4, pp. 284-290.

Ramos, M., N. Silva, N. Muga, A. Pinto, (2021) “Reference Clock Signal Distribution for Quantum Key Distribution”, Anais do I Workshop de Comunicação e Computação Quântica, Uberlândia, SBC, pp.31-36.

Mantey, S., Ramos, M., Silva, N., Pinto, A., Muga, N., (2022) "Demonstration of an Algorithm for Quantum State Generation in Polarization-Encoding QKD Systems”, 2022 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1-3.

Muga, N. J., Ferreira, M. F., & Pinto, A. N. (2010) “QBER estimation in QKD systems with polarization encoding”, Journal of Lightwave Technology, 29(3), 355-361.