Reference Clock Signal Distribution for Quantum Key Distribution

Mariana F. Ramos[12], Nuno A. Silva[1], Nelson J. Muga[1], Armando N. Pinto[12]

[1]Instituto de Telecomunicações, Aveiro, Portugal.

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

marianaferreiraramos@ua.pt

Abstract. *Quantum key distribution (QKD) requires high synchronization accuracy, specially in systems that use gated detectors at the receiver station. In this work, we present a reference clock distribution method to support long-term QKD. An average quantum bit error rate (QBER) of* 1.8% *was measured, which is suitable for different QKD implementations. This method is suitable for long-distance and long-term QKD implementations and does not require additional transmitted qubits for synchronization.*

1. Introduction

Nowadays, with the development of internet of things, our sensitive individual financial and health data is commonly transmitted through internet channels, requiring high-level security [Diamanti et al. 2016]. Quantum key distribution (QKD) provides unconditional secure communications, since the security relies on physics laws instead of on computational complexity [Bennett et al. 1992]. Practical QKD allows the key sharing between two distant parties, known as Alice and Bob (transmitter and receiver, respectively). To achieve this, symbol temporal synchronization is of high importance, specially in gated-detectors based QKD receiver systems [Patel et al. 2012].

An intuitive approach to solve symbol synchronization in QKD is the use of paired-fibers to transmitted reference and quantum data signals through different channels. However, temperature can induce delays between paired fibers, which may result in degradation of synchronization accuracy [Tanaka et al. 2008]. Time-division multiplexing (TDM) schemes, where the synchronization pulses are lagged transmitted from quantum pulses, overcome this issue. However, TDM schemes bring other problems, such as bit rate limitation, since these techniques require sufficiently long-time intervals between quantum and reference signals [Tanaka et al. 2008]. Recently, different QKD clock recovery algorithms avoiding the use of additional classical reference signals have been proposed. In [Pljonkin and Rumyantsev 2016], it is proposed a synchronization algorithm where the time frame is divided in smaller time windows, with a synchronization time consuming of 788.6 ms and a probability of synchronization failing of 0.01%. In [Rumyantsev and Rudinskiy 2017], the authors proposed an algorithm that does not include the time frame division providing higher speed synchronization time of 3.216 ms with an error probability of 0.0043%. However, the last can only be applied on QKD systems where the stations are not far more than tens of km from one another, while the former can be applied in QKD systems with hundreds of km. On the other hand,

a different approach to synchronization is the use of wavelength division multiplexing (WDM) architectures allocating the quantum data signal and the reference clock signal in different wavelengths [Muga et al. 2011]. This technique allows the transmission of the reference signal superimposed by modulation onto the optical pulse to be received by direct detection in a far different station [Tang et al. 2011]. Furthermore, there is a one to one correspondence since every reference pulse is transmitted with every quantum pulse to denote the time the single-photon detector opens the gate for a particular quantum pulse [Tang et al. 2011]. Nevertheless, practical WDM synchronization implementation requires additional precautions, such as the power to be used to avoid nonlinear cross-talk between signals, as well as distortions on reference clock signal due to not achieve extremely high extinction ratio for the reference pulses neither precise compensation of distorted wave-forms cause by chromatic dispersion.

In this work, we propose an algorithm for reference clock signal recovering at receiver together with the use of a WDM scheme for reference clock signal distribution. The developed technique uses the optical reference clock signal by direct detection and applies a post-processing algorithm to recover the clock signal eliminating additional errors induced throughout the optical fiber channel. This algorithm does not require additional qubits for synchronization, it is suitable for long-distance practical QKD systems, and for long-term operation.

This paper is divided in five sections. In section 2, the physical experimental system is described. In section 3, we describe the operation mode of the symbol synchronization method implemented in the physical-layer. In section 4, the experimental validation of the method is presented. Finally, in section 5, the main conclusions of this work are summarized.

2. System description

In this section, we present the experimental discrete-variable (DV)-QKD system based on single-photon polarization encoded scheme. The scheme of the experimental setup is presented in Figure 1, and it allows the implementation of any upper-layer quantum cryptography protocol. On Alice's side a optical signal at $\lambda_Q = 1547.72$ nm from a laser source is modulated on a Mach-Zehnder to obtain a coherent state with 1 ns pulse width at 500 Hz repetition rate. The 1 ns pulse is generated from a 393.216 MHz internal

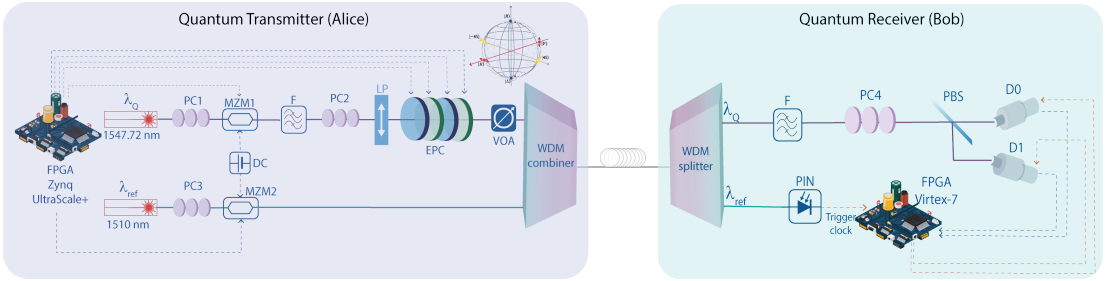


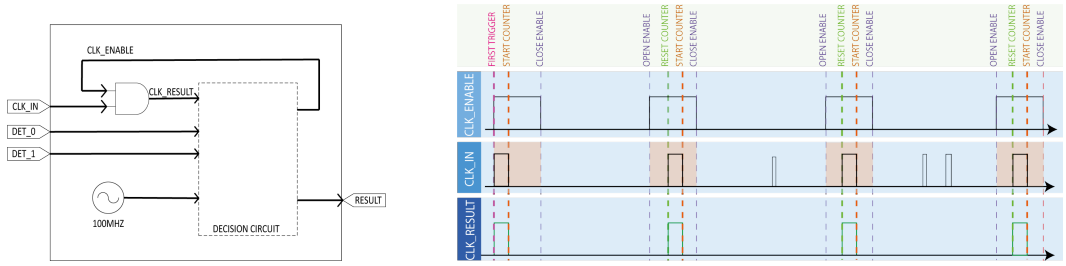
Figure 1. Schematic diagram of the implemented QKD system based on single-photon polarization encoding with a WDM scheme for reference clock signal distribution.

FPGA clock signal. The polarization modulation of single-photons is obtained after the data signal passes through an electronic polarization controller (EPC). After, the EPC the signal is attenuated by a variable optical optical attenuator (VOA) up to a quantum level, where the average number of photons per pulse is 0.1. After the VOA the photons are sent to a wavelength multiplexer combiner. Still at Alice's side, another optical signal at $\lambda_{\text{ref}} = 1510$ nm from a tunable laser source is modulated through a Mach-Zehnder in order to obtain a square classical signal used for clock synchronization. This square 100 ns width signal is generated from a 393.216 MHz internal FPGA clock signal modulated with 500 Hz repetition rate. After this second Mach-Zehnder modulator the reference optical signal is also sent to the wavelength multiplexer combiner. Moreover, PC1, PC2 and PC3 are used to align the polarization of the signals to the principal axis of the opto-electronic devices the signal is entering on, see Figure 1. After the wavelength multiplexer combiner, both signals are driven by the same optical fiber that works as quantum communication channel. All electrical signals needed to modulate as the quantum data signal as the reference signal are generated on the FPGA, and connected to the physical setup through digital-to-analog converter (DAC) SMA board. The DACs are synchronized between each other using an internal phase-locked loop with a 245.76 MHz reference clock.

At the receiving side, both the quantum signal and the reference signal are separated by a wavelength multiplexer splitter. Bob measures the qubit states using two avalanche photo-diodes id210 from IdQuantique working in gated mode (D0 and D1). The detectors operate with a time gate width of $\tau_g = 2.5$ ns. The detector D0 in Figure 1 has an efficiency of $\eta_0 = 20$ %, and a dark count probability of $P_{dc}^0 = 5.59 \times 10^{-6}$ %. For the same gate width as the last, the detector D1 has an efficiency of $\eta_1 = 25$ %, and a dark count probability of $P_{dc}^1 = 6.51 \times 10^{-6}$ %. Since the signal period is much higher than the recovering time of the avalanche photo-diode material, the chosen dead-time is not relevant for the current study. After being separated from the reference signal, the quantum data signal passes through an optical filter F to eliminate side wavelengths that can compromise the qubits information. PC4 is used to manually align the polarization state of the photons at fiber output with one of two orthogonal axis of the polarization beam splitter maximizing the counts on the correspondent detector. Each detector D0 and D1 is associated with one of the two orthogonal states of polarization, for instance $|H\rangle$ and $|V\rangle$. Regarding the reference signal, it goes into a photo-detector where the optical signal is converted in an electrical signal, which in turn is connected to a SMA digital input of FPGA. This SMA digital input is sampled at 100 MHz. After processing the reference signal, the FPGA provides the trigger signal to the single-photon detectors, which sets the opening gate time instant, which is synchronized with the qubits arrival time. The post-processing method related with the symbol synchronization will be detailed in next section. The measurements are also received from the FPGA, which is responsible for a first processing task related with the decision process, and for sending the results to the upper-layer.

3. Symbol synchronization

In this section we detail the method implemented for symbol synchronization in the experimental physical quantum communication system described in previous section. Figure 2. (a) shows the VHDL diagram of the code implemented on the FPGA at receiving side. After being converted to the electrical domain, the reference clock signal,



(a) (b)

Figure 2. (a)- VHDL diagram implemented at receiver side reference clock signal post-processing and measuring decision circuit implementation. (b)- Method for reference clock signal post-processing. CLK_ENABLE is the signal used as measurement opening window. CLK_IN is the clock received from Alice with errors during the period interval. CLK_RESULT is the clock signal result from the AND operation between the previous two signals.

CLK_IN in Figure 2. (a), is a TTL 100 ns width square signal. Since the reference signal enters through a digital port, a digital high level is set when the voltage level of CLK_IN rises above a certain threshold defined by port characteristics, and it is set as digital low level when the same signal has a voltage bellow another threshold. Nevertheless, this architecture induces errors in the decision output resulting in a wrong detection of the clock rising edge. A simple algorithm to overcome this problem was developed in VHDL.

The decision circuit block has four input and two output signals. The first input signal is a FPGA 100 MHz internal clock, which defines for each one of the other three inputs a sampling rate of 10 ns. Figure 2. (b) summarizes the algorithm operation result. The CLK_ENABLE signal starts on an high level. As soon as the CLK_IN is triggered the signal CLK_RESULT changes to an high level, and when a CLK_IN falling edge is detected a counter starts incrementing at a rate defined by the 100 MHz clock. The CLK_ENABLE changes to a low level when the counter is equal to a clock enable width value defined by the user. After this first step the counter increments until being equal to other integer value defined by the user to change the CLK_ENABLE signal again to an high level. When the CLK_IN rising edge is detected the counter is reset and the process runs again as previously described. Even if a CLK_IN rising edge is not detected at the instant it is supposed to be triggered, the circuit forces a CLK_RESULT as supposed, working similarly to a regular PLL circuit. The other two signal inputs, DET_0 and DET_1, corresponds to the counts output signals from each single-photon detectors. These are digital signals already, therefore not causing problems in signals reading from FPGA. The decision circuit looks into these two inputs only during the CLK_ENABLE high level. If during this interval one the two signals assumes the high value, the decision circuit outputs a RESULT equal to the bit associated with each detector, 0 or 1. Otherwise, the RESULT signal assumes the value 3 if none of the two signals assume the high level, and the value 2 if both signals assume the high level during this interval.

4. Experimental validation

In this section we present the experimental validation of the developed method. The DV quantum key distribution physical system presented in Figure 1 was experimentally implemented in the lab. The clock reference signal and the quantum data signal

are electrical generated by the FPGA and superimposed by modulation onto the optical pulses from two laser sources at different wavelengths as described in section 2. The figure of merit used to assess the system performance is the quantum bit error rate (QBER), and the method for its calculation was implemented based on the work presented in [Almeida et al. 2016] in the upper-software layer after receives the data from the FPGA carried by signal RESULT, see Figure 2. (a).

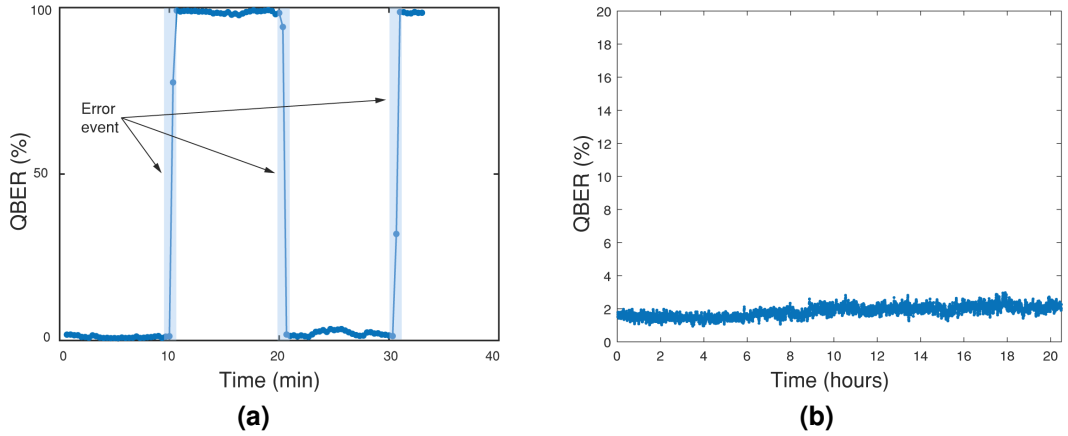


Figure 3. (a)-QBER measured for an alternated sequence bits without implementation of the proposed synchronization method. (b) - QBER measured for a pseudo-random sequence with the implementation of the proposed synchronization method.

Figure 3. (a) shows the QBER measured without signal error correction algorithm for more than half of an hour. In this case, an alternated sequence of bits "01" prepared with the two orthogonal states $|H\rangle$ and $|V\rangle$ from the same basis was transmitted. As one can see in the figure, at the beginning both stations Alice and Bob were temporally synchronized, although this synchronization is lost after only 10 minutes. This error can occurs due two phenomenons: lost of reference pulse, or detection of a pulse rising edge outside at a wrong instant, see signal CLK_IN in Figure 2. In this way, the QBER swaps to a value close to 100% since the sequence changes to opposite values. In Figure 3. (b) we present the experimental measured QBER of the same system but we implemented and tested the developed algorithm considering the previous scenario and the error events disappear. Moreover, we went a little further and tested the developed algorithm on a more complex situation considering a pseudo-random sequence longer than the previous alternated sequence. Figure 3. (b) shows the QBER measured using the proposed algorithm for clock signal recover for tens of hours considering a 7 qubits pseudo-random sequence to be transmitted. An average QBER $= 1.8\%$, with a minimum $\text{QBER}_{\text{min}} = 0.94\%$ and a maximum $\text{QBER}_{\text{max}} = 3\%$ was measured during the data acquisition.

5. Conclusion

We have presented a method for reference clock signal distribution. The method relies on the combination of a WDM scheme to carry the reference clock together with the quantum data signal through the same optical fiber, with a post-processing algorithm to eliminate errors in the reference signal detection process. The method was implemented in a DV-QKD system based on polarization-encoded single-photons. We prepare qubits

at a transmission rate of 500 Hz using two orthogonal states of polarization, $|H\rangle$ and $|V\rangle$, in a single basis. The qubit detection was performed using the single-photon detectors operating on gating mode, using the reference clock signal as the trigger for the gate. We have demonstrated the effectiveness of the method measuring the QBER for several hours. An average QBER $= 1.8\%$ with a minimum $\text{QBER}_{\text{min}} = 0.9\%$ and a maximum $\text{QBER}_{\text{max}} = 3.0\%$ achieved, which makes it suitable for broad QKD implementation.

Acknowledgements

This work is supported by the FEDER, through the COMPETE 2020 [Project Q.DOT (POCI-01-0247-FEDER-039728)], project DSPMetroNet (POCI-01-0145-FEDER-029405), by UIDB/50008/2020-UIDP/50008/2020 (actions DigCORE and Qu-Runner), and by Regional Operational Program of Lisbon, project QuantumMining (POCI-01-0145-FEDER-031826). The work of Mariana F. Ramos was supported by the FCT through Fundo Social Europeu and by Programa Operacional Regional do Centro under Ph.D. Grant SFRH/BD/145670/2019.

References

Almeida, Á. J., Muga, N. J., Silva, N. A., Prata, J. M., André, P. S., and Pinto, A. N. (2016). Continuous control of random polarization rotations for quantum communications. *Journal of Lightwave Technology*, 34(16):3914–3922.

Bennett, C. H., Brassard, G., and Ekert, A. K. (1992). Quantum cryptography. *Scientific American*, 267(4):50–57.

Diamanti, E., Lo, H.-K., Qi, B., and Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1):1–12.

Muga, N. J., Ferreira, M., and Pinto, A. N. (2011). Qber estimation in qkd systems with polarization encoding. *Journal of Lightwave Technology*, 29(3):355–361.

Patel, K., Dynes, J., Choi, I., Sharpe, A., Dixon, A., Yuan, Z., Penty, R., and Shields, A. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2(4):041010.

Pljonkin, A. and Rumyantsev, K. (2016). Single-photon synchronization mode of quantum key distribution system. In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, pages 531–534. IEEE.

Rumyantsev, K. and Rudinskiy, E. (2017). Time synchronization method in quantum key distribution system with automatic compensation of polarization distortions. In *2017 2nd International Conference on Multimedia and Image Processing (ICMIP)*, pages 346–349. IEEE.

Tanaka, A., Fujiwara, M., Nam, S. W., Nambu, Y., Takahashi, S., Maeda, W., Yoshino, K.-i., Miki, S., Baek, B., Wang, Z., et al. (2008). Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Optics express*, 16(15):11354–11360.

Tang, F., Gao, S., Wang, X., and Zhu, B. (2011). A novel synchronization scheme for free-space quantum key distribution system. In *Asia Communications and Photonics Conference and Exhibition*, page 83093C. Optical Society of America.