ISSN 2007-9737

FPGA-Based Emulation of a Synchronous Phase-Coded Quantum Cryptography System

Arturo Arvizu-Mondragón[1], Josué A. López-Leyva[2], Jorge L. Ureña[1], Francisco J. Mendieta-Jiménez[3], and Juan de Dios Sánchez L.[4]

[1] Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), Baja California, Mexico

[2] CETYS Universidad, Ensenada, Baja California, Mexico

[3] Agencia Espacial Mexicana (AEM), Distrito Federal, Mexico

[4] Universidad Autónoma de Baja California (UABC), Ensenada, Baja California, Mexico

arvizu@cicese.mx, josue.lopez@cetys.mx, sluc16@hotmail.com, mendieta.javier@aem.gob.mx, jddios@uabc.edu.mx

Abstract. We present FPGA-based emulation of a synchronous phase-coded quantum cryptography system. Several of the emulated subsystems are used for implementation in a free space demonstrative QPSK scheme for quantum key distribution with continuous variables (CV-QKD) using a base and optical phase synchronization. The CV-QKD systems are commonly implemented using QPSK modulation with switched or simultaneous detection. In this paper we only make use of one base of the QPSK system in order to get a simpler modulation (BPSK) scheme, used for demonstrative purposes. The reported results from the emulation and the experiment in terms of Quantum Bit Error Rate (QBER) and mutual information for different values of the number of photons per bit are in good agreement.

Keywords. FPGA, quantum cryptography, emulation.

1 Introduction

An optical communication system may be classified as classic (with a relatively large number of photons per bit) or quantum (with very low number of photons per integration period), and the communication channel to be used may be an optical fiber and/or free space. A very important application of the quantum communication systems is the quantum key distribution (QKD). This cryptographic key distribution (between two points usually called *Alice* and *Bob*) is commonly carried out using the well-known (and the first one) protocol BB84 through a private unidirectional channel (optical fiber or free space) where there is the possibility that an eavesdropper (usually called *Eve*) may steal information, while the encrypted data are transmitted via a traditional (classic) telecommunications channel (Fig. 1) [1-3].

At first, the protocol BB84 was implemented through the use of four states of polarization for representing the bases (bases will be defined below), two of them in one base (orientation plane of linear horizontal and vertical polarization states) and other base with a given inclination (orientation plane of linear polarization states with a given inclination). However, later, it was demonstrated that systems with continuous complex amplitude modulation with four possible states (like quaternary phase shift keying, QPSK) might be used for QKD systems [4], i.e., a classical optical transmission and reception system with QPSK modulation may be adapted to be used both in quantum communications as well as in quantum cryptography (like QKD systems).

The design and implementation of QKD systems is usually a complex process which may be simplified by emulating its different subsystems [5, 6]. The main objective of our paper is to show the feasibility of emulating a quantum cryptography system with the help of FPGA and to use the obtained results for making a quicker and more reliable implementation of a physical system.

We have emulated the QKD algorithm corresponding to Alice and Bob; in this case, we chose the algorithm with continuous variables (with acronym CV-QKD) [7]. The algorithm consists of four stages; the first one is the transmission of a stream of photons with a QPSK modulation format on the quantum channel from Alice to Bob to get the *raw key*. In addition, Alice keeps a database of the code used for future operations; this action is performed by the quantum subsystem. In the second step, Bob sends to Alice the base chosen for the measurement process through the classical channel (for example, the Internet); in this case the bases refer to the phase and quadrature components used in the modulation process.

The QPSK modulation scheme consists of four symbols which are binary-represented as 00, 01, 11, 10, where the first bit indicates the base used ("0" and "1" logic, corresponding to the in-phase and quadrature components, respectively) and the second bit indicates the phase shift ("0" and "1" logic corresponds to a phase shift of zero and of 90 degrees with reference to the base, respectively). Alice receives this information and determines which were the base coincidences between the two systems, and then communicates to Bob the wrong ones, so that both sides eliminate the non-matching bases, thus obtaining the filtered key, called the *sifted key*. At this point, the length of the sifted key should be approximately half of the raw key, but if not, the communication is canceled and a new raw key is generated due to the possibility of the presence of a spy. There may be errors in the data of the sifted key measured by Bob because of the normal performance of the transmission system or because of a spy system. So, Bob has to determine the QBER (Quantum Bit Error Rate), i.e., the errors in the measured data, and compare them against the theoretical QBER and/or with the QBER used for the calibration of the communication link. If the QBER obtained with the data measured is higher than its theoretical value (taking into account a margin of error), it is acknowledged that there is a spy in the channel and the transmission is aborted and a new key raw must be generated. The third step is to correct errors in the sifted key by means of an error correction algorithm; this stage is called *reconciliation*. In this case, we decided to analyze the parity blocks of different lengths to determine the position of the bits with error and then to proceed to the correction process. Until now, it might be considered that the key obtained after reconciliation is safe; however, there is still a method to improve safety called security amplification, this being the fourth stage where a particular function of the family of Hash functions used in conventional or classical cryptography is chosen. Previously, Alice and Bob must have in their database the Hash functions (usually compression functions) that could be used in a way that when they communicate through the classical channel, they will determine which function must be used to get the final key [8]. However, in this paper we do not take into account the security amplification stage due to the fact that this process is used in order to increase the security level via classical methods.

Usually, a quantum key distribution (QKD) system is implemented using the following subsystems: a) a quantum subsystem of transmission–reception, its function is to generate, transmit, and detect the quantum signal that will represent the final quantum key using a unidirectional private channel, b) a classical subsystem of transmission–reception, it uses a bidirectional public channel in order to perform the algorithm for producing the quantum key, c) a processing subsystem to realize control and data acquisition, as well as to execute such algorithms as phase lock, bit synchronization, several kind of diversity and multiplexing, among others.

There are a number of books and papers which report emulation of diverse physical systems using FPGA's with applications such as industrial systems, radio frequency communication, instrumentation, quantum computing and quantum communications (see, for example, [21]), among others.

In this work we report the emulation of a synchronous QKD system with coded phase

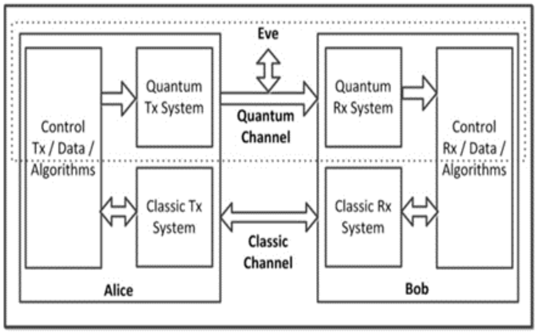


Fig. 1. A typical QKD system

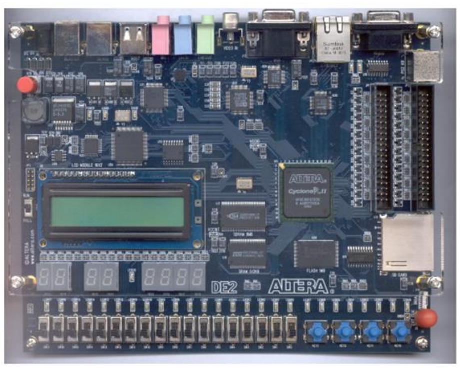


Fig. 2. FPGA Altera DE2 Evaluation Board

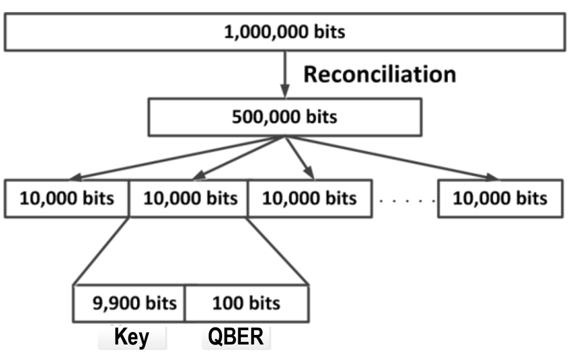


Fig. 3. Process for obtaining the quantum key and the Quantum Bit Error Rate (QBER)

using an FPGA. As mentioned above, the CV-QKD systems are commonly implemented using QPSK modulation with switched or simultaneous detection. If we consider the use of only one base of a QPSK system, it can be reduced to a BPSK modulation scheme which we think is sufficient for demonstration purposes. Based on the emulation, we implemented and characterized a quantum channel using optical BPSK modulation on the transmitter side and coherent detection on the receiver side (using an optoelectronic Costas loop) in free space.

2 Emulation

The emulated system consists of the subsystems for generating the bases and symbols for Alice and only the bases for Bob, as well as the reconciliation operations between them. The emulation is done using VHDL language with the Quartus II software in the FPGA Altera DE2 (see Fig. 2).

The Alice and Bob subsystems were programmed to take into account the probability of occurrence of the bases as well of the bits according to the BB84 protocol [9, 11]. A pseudorandom number generator (PRNG) based on Flip-Flops was programmed in the FPGA in order to emulate the pseudorandom and uniform probability of occurrence of the bases (as well as of the bits) in the subsystem of Alice which is interconnected with the quantum channel using a digital-to-analog converter (DAC7541AJP) controlled by the FPGA. We make the required changes in the programs so that depending on the bits transmitted by Alice, the FPGA gets the sequence of bits needed to generate the analog voltage desired.

The emulation of Bob is easier because its function is simply to choose one of 2 bases at random to measure the information sent by Alice. In order to randomly select the Bob's bases we programmed another PRNG in a similar fashion as for Alice but with different initial conditions on the Flip-Flops. Next, we evaluate the performance of the QKD system emulated (considering efficiency $\eta = 0.7$) for different optical powers (0.1, 1, and 10 photons per bit). Table 1 shows the QBER on the emulated system (QBERS) as well as their theoretical probability of error (Pe). Fig. 3 shows the block division and the average bit

ISSN 2007-9737

Table 1. Parameters used and results obtained in the emulated system and the experimental set-up for the processes of key distillation and correction for several photon numbers

N_S	Power Fw	P_e	$QBER_S$	$QBER_P$	Blocks	Bits
0.1	4.5	$10^{-0.5}$	$10^{-0.5}$	$10^{-0.7}$	2	245950
1	45	10^{-1}	10^{-1}	$10^{-1.3}$	5	395430
10	450	10^{-5}	10^{-5}	----	25,000	494880

resulting after the process of key distillation as well as the average bit after the error correction process. Since the PRNG implemented in the FPGA is not (obviously) truly random, there was some variation in the choice probability of the bases and the corresponding bit of Alice, Bob, and Eve (1.24%, 1.53%, and 1.1%, respectively), according to the theoretical values of 25%, 50%, and 50%, respectively.

In the context of classical optical communications, the rate of bits in error is simply called Bit Error Rate (BER), while in the context of quantum communications (mainly when a photon counting system is used) there exists an alternative term known as the quantum bit error rate (QBER) of the final quantum key (sifted key). However, the same acronym (QBER) is frequently used in quantum cryptography systems with coherent detection, but strictly speaking such systems do not perform the photon counting process, but obtain the probability of error similar to the photon loss of the photon counting systems. Also, sometimes the term BER is used in QKD systems knowing that it refers to QBER [9, 10].

If one wishes to generate “truly” random data, the use of the so-called true random number generators [12] is required; however, we did not have any of such generators at the moment of our experimental setup implementation.

3 Optical Set-Up

Based on the FPGA emulation system, we implemented a quantum communication system in free space (for convenience we use a self-homodyne configuration operating at 1550 nm) (Fig. 4). The receiver based on a Costas-loop configuration is capable of obtaining the quadrature components of the optical fields in a simultaneous way through the use of the states of polarization (SOP) of the local oscillator LO (circular) and the data signal (linear to 45 degrees), using a quarter wave plate (QWP) and a half wave plate (HWP), respectively. In order to obtain a signal with a low photon number per bit, we use a set of neutral density filters (NDF). Such signal is detected at the same time by a) a coherent detection scheme, b) a single photon detector (SPD), and c) an ultrasensitive optical power meter (with a power sensitivity of $10x10^{-15}$ Watts). The coherent detection is performed by balanced homodyne detectors (BHD) with the bandwidth and gain adjusted according to the different optical power levels received. A BPSK optical modulation is obtained with an electronic pseudorandom binary sequence (driven by the PRNG subsystem implemented on the FPGA) at 350 Kbps. We inject an electronic noise signal to an optical phase modulator in order to add phase fluctuations over the optical carrier of the data. In order to get a phase error signal on the electronic domain (for our optoelectronic Costas loop), we use an electronic multiplier circuit with unitary gain (AD734). This signal is processed by a) a set of electronic filters optimized (TL741CN), b) an inverter and integrator circuits (AD830) for the purpose of modifying the input signal that drives an optical phase modulator with a narrow dynamic range but with a relatively high speed. These electronic devices are shown in Fig. 5, while in Fig. 6.a, b we present two photos of the experimental quantum transmission-reception system.

ISSN 2007-9737

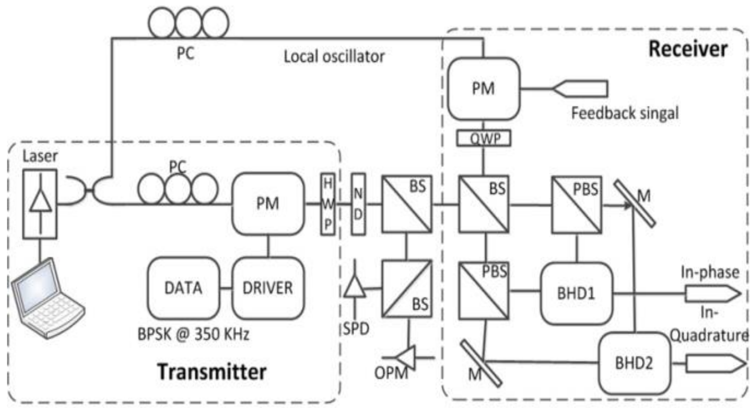


Fig. 4. Experimental set-up; PM: phase modulator, HWP: half wave plate, NDF: neutral density filter, SPD: single photon detector, OPM: optical power meter, BS: beam splitter, QWP: quarter wave plate, PBS: polarizing beam splitter, M: mirror, BHD: balanced homodyne detector, PC: Polarization controller

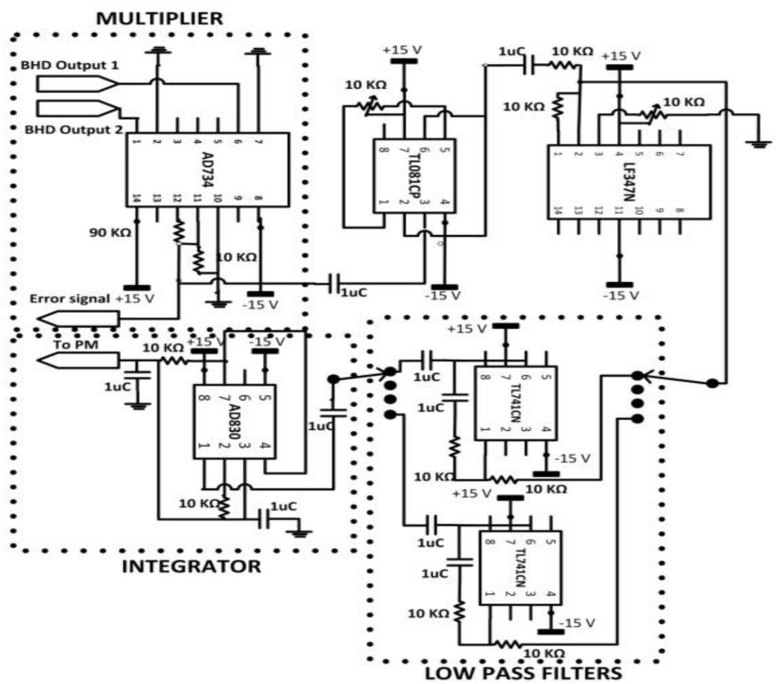
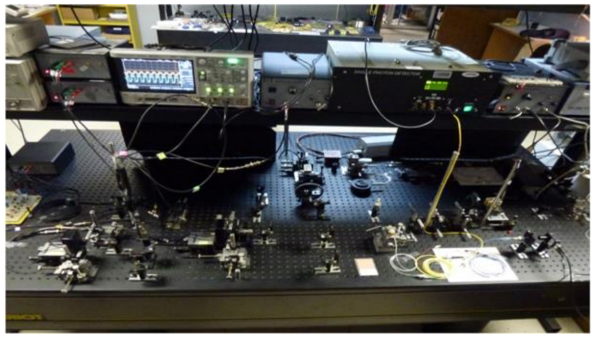
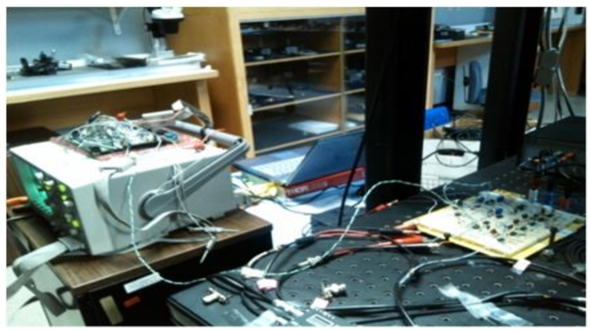


Fig. 5. Electronic stage of the opto- electronic Costas loop

We obtained bit error rate measurements (for each photon number) using the electrical signals of the BHD's and then with these measurements we estimated the SNR using off-line processing.



(a)



(b)

Fig. 6. Experimental quantum transmission-reception system

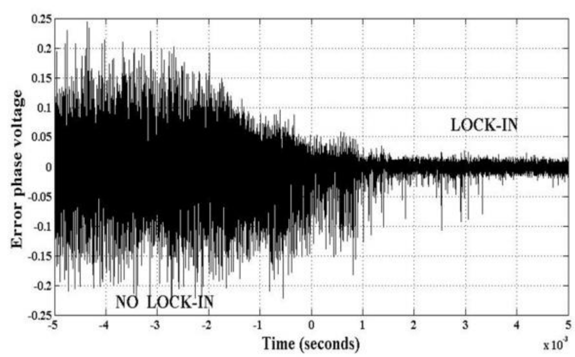


Fig. 7. Phase error signal at the output of the multiplier circuit for 5 photons per bit

We implemented a set of first-order active low-pass electronic filters which were optimized with respect to the amplitude and phase noises of the optical signals from 0.25 to 5 photons per bit.

These different filters naturally lead to different natural frequencies of our loop for each case (from 167 Hz to 1.2 kHz) as well as different values for the gain of the sinusoidal optical phase detector (from 7.6×10^{-3} to 59×10^{-3} V/rad). In order to perform the optimization process, we must take into account the gains of the diverse electrical circuits that are part of the equivalent Voltage Controlled Oscillator (VCO). Fig. 7 shows the phase error signal at the output of the multiplier

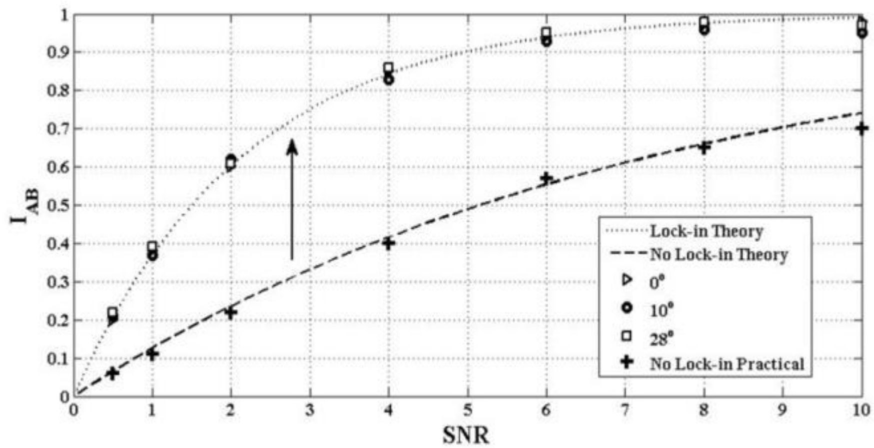


Fig. 8. Theoretical and experimental performances of mutual information (I_{AB}) for different phase errors and SNR values in the phase-locked condition

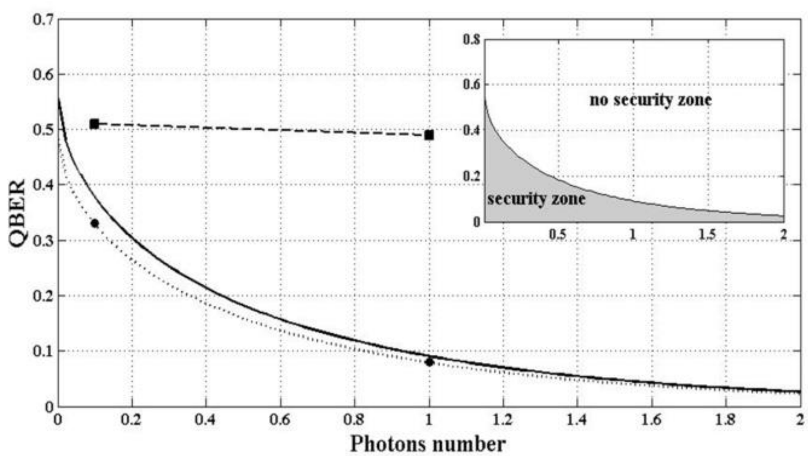


Fig. 9 Experimental results of the security level using both emulation and quantum system

circuit (AD734) for 5 photons per bit. It may be seen that, as expected, when the feedback loop is not active (no lock-in condition), the amplitude of the phase error is greater than in the case when the loop is switched on (lock-in condition) enabling the operation of the driver circuit of the PM. The theoretical value of error phase variance is 0.02º, while the real value is 0.018º for 5 photons. When the experiment was in the phase-locked condition, we obtained simultaneous measurements of the quadrature components (at a rate of $4x10^9$ samples per second, acquiring about 100000 samples, corresponding to 3500 data in order to be processed off-line); obviously, this measurement process is degraded when the system is not in the phase-locked condition.

As mentioned above, Table 1 shows the measured QBER (after off-line post-processing) in the free space experiment ($QBER_P$). In the case of 10 photons per bit, there are no experimental results for the BER with post-processing, because the experiment in free space does not consider such a case due to limitations in the capability of the single photon detector (optical power saturation). Then we measured the mutual information (I_{AB}) between Alice and Bob for different photon numbers (i.e., different SNR's) and different phase errors as shown in Fig. 8 according to [13]. It may be observed that when the locking system is switched on, the mutual information is increased; moreover, it is found that the Costas loop design has been appropriate because the system is able to correct phase fluctuations.

Furthermore, by setting a threshold that defines the security zone (considered as 10% above the reference value of QBER) of both the QKD system emulated on the FPGA [14-16] and the quantum communication free space system, two measurements were obtained that show (see Fig. 9) that when the link is active, the measurements fall in the security area without Eve. Other measurements fall in the no-security zone when the emulated subsystem of Eve is present. Our experimental results present an adequate performance that is in good agreement with the theory and they are comparable with the results obtained using other similar systems such as the one reported in [17] with the important difference that the authors of the mentioned paper make use of a sequential measurement of the in-phase and quadrature components instead of making real-time measurements (as is our case).

From our point of view, the main advantage of our experiment is that it allows an increase of the transmission rate due to the simultaneous measurement (in real time) of the quadrature components, in contrast to the sequential measurement in [17], but on the other hand, in [17] the transmission rate is half of our experimental transmission rate because of the phase switching of the local oscillator. However, our experiment presents more quantum noise due to the unused ports of the optical set-up. In addition, the experimental set-up implemented and reported in our paper had a minimum error probability of $10^{-0.7}$ with a transmission rate of 350 KHz. These measurements are similar to the results reported in [18, 19], with a minimum error probability of 10^{-6} and a transmission rate of 2 KHz. The differences between our system and the one reported in [18, 19] are due to the trade-off between the transmission rate and the security level (a parameter related to the probability of error) in the QKD systems [20]. This means that the transmission rate and the security level is inversely proportional; for this reason, our scheme presents a less error probability ($10^{-0.7}$) in comparison with [18, 19]; however, it has a higher transmission rate (350 KHz).

4 Conclusions

In this paper we have presented FPGA-based emulation of a synchronous phase-coded quantum cryptography system. We implemented an experimental quantum transmission-reception system (quantum channel) and performed QBER measurements. When we compared the results obtained by the FPGA we showed that they are in good agreement. Also, we performed measurements on both the QKD system emulated on the FPGA and the free space quantum communication system to determine if the link is in the security zone for a given photon number. The free space quantum communication system can be used for QKD with continuous variables and different quantum states. Also, it was found that the optical synchronization structure has a good performance according to the BER and the mutual information for different phase errors. For us, the use of the QKD system emulated on the FPGA has been very useful for the design of our experimental set-up; it also helped us to determine their optimum operating conditions. As mentioned above, the real QKD system design can be complex, but in our case the design is facilitated by the use of the FPGA-based emulator. It is worth mentioning that we have used a low-cost general-purpose FPGA for the emulation of our QKD system taking into account that the key rate is usually of the order of hundreds of Hz to tens of kHz. However, if we want to integrate the FPGA as a building block of the QKD system operating in real time, it is convenient to use FPGA's with greater performance speed and better power consumption.

Glossary of acronyms

BHD: balanced homodyne detector
BS: beam splitter
BPSK: binary phase shift keying
BER: bit error rate
CV-QKD: quantum key distribution with continuous variables
FPGA: field programmable gate array
HDL: hardware description language
HWP: half wave plate
LO: local oscillator
PBS: polarizing beam splitter
PC: polarization controller.
Pe: probability of error
PRNG: pseudorandom number generator
QBER: quantum bit error rate
QKD: quantum key distribution
QWP: quarter wave plate
QPSK: quadrature phase shift keying
Rx: receiver
SNR: signal to noise ratio
SOP: states of polarization
SPD: single photon detector
Tx: transmitter
VCO: voltage-controlled oscillator
VHDL: VHSIC + HDL
VHSIC: very high speed integrated circuit

Acknowledgments

This work was supported by CONACYT Basic Science Grant.

References

1. **Gao, F., Qin, S.J., Guo, F.Z., & Wen, Q.Y. (2011).** Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols. *IEEE Journal of Quantum Electronics*, Vol. 47, No. 5, pp. 630–635.
2. **Yan, Z., Meyer-Scott, E., Bourgoin, J.P., Higgins, B.L., Gigov, N., MacDonald, A., Hübel, H., & Jennewein, T. (2013).** Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links, *Journal of ligthwave technology*, Vol. 31, No. 9, pp. 1399–1408. DOI: 10.1109/JLT.2013.2249040
3. **Huang, J., Yin, Z., Chen, W., Wang, S., Li, H., Guo, G., & Han, Z. (2013).** A survey on device-independent quantum communications. *China Communications*, Vol.10, No. 2, pp. 1–10. DOI:10.1109/CC.2013.6472853
4. **Agnolini, S. & Gallion, P. (2004).** Implementation of BB84 protocol by QPSK modulation using Mach-Zehnder modulator. *IEEE ICIT '04 International Conference on Industrial Technology*. Vol. 1, pp. 250–253. DOI: 10.1109/ICIT.2004.1490292
5. **Liao, S., Liu, S., Wang, J., Liu, W., Peng, C., & An, Q. (2012).** Time interval analyzer with FPGA-based TDC for free space quantum key distribution: Principle and validation with prototype setup. *Real Time Conference (RT), 18th IEEE-NPSS*, 1-6.
6. **Zhang, H.F., Wang, J., Cui, K., Luo, C.L., Lin, S.Z., Zhou, L., Liang, H., Chen, T.Y., Chen, K., & Pan, J.W. (2012).** A Real-Time QKD System Based on FPGA. *Journal of ligthwave technology*, Vol. 30, No. 20, pp. 3226–3234. DOI:10.1109/JLT.2012.2217394
7. **Oesterling, L., Hayford, D., & Friend, G. (2012).** Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. *IEEE Conference on Technologies for Homeland Security (HST),* pp. 156–161.
8. **Trappe, W. & Washington, L.C. (2002).** *Introduction to Cryptography with Coding Theory*. Pearson Prentice Hall. pp. 25–50.
9. **Bennett, C. & Brassard, G. (1984).** Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.
10. **Silva, M.B.C, Xu, Q., Agnolini, S., Gallion, P., & Mendieta, F.J. (2006).** Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol, *International Conference on Application of Photonic Technology.*
11. **Jouguet, P., & Kunz-Jacques, S. (2014).** High Performance error correction for quantum key distribution using polar codes. *Quantum information and computation*, Vol. 14, No. 3, pp. 329–338.
12. **Lopez Leyva, J.A. (2014).** Dual Quantum Random Number Generator using a FPGA for QKD-CV systems: Preliminary results. *International Journal of Emerging Research in Management & Technology,* Vol. 3, No. 6, pp. 6–8.

ISSN 2007-9737

13. **Desurvire, E. (2009).** *Classical and quantum information theory.* Cambridge, UK, Cambridge University Press.
14. **Al-Khateeb, W., Al-Khateeb, K., Ahmad, N.E., & Salleh, S.N.M. (2013).** Practical Considerations on Quantum Key Distribution (QKD). *International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* pp. 278–283 *DOI:10.1109/ACSAT.2013.62*
15. **Capraro, I. & Occhipinti, T. (2007).** Implementation of a Real Time High Level Protocol Software for Quantum Key Distribution. *IEEE International Conference on Signal Processing and Communications ICSPC*, pp. 704–707. DOI:10.1109/ICSPC.2007.4728416
16. **Niemiec, M. & Pach, A.R. (2013).** Management of security in quantum cryptography. *IEEE Communications Magazine*, Vol. 51, No. 8, pp. 36–41. DOI:10.1109/MCOM.2013.6576336
17. **Xu, Q., Mondragon, A.A., Gallion, P., & Mendieta, F.J. (2009).** Homodyne In-Phase and Quadrature Detection of Weak Coherent States With Carrier Phase Tracking. *IEEE Journal of Selected Topics in Quantum Electronics, Vol.* 15, No. 6, pp. 581–1590. DOI:10.1109/JSTQE.2009.2023803
18. **Li, J., Chen, J., Zeng, H., & Li, H. (2013).** Design of Quantum Secure Communication System Based on FPGA. *Progress in Electromagnetics Research Symposium (PIERS) Proceedings*, Taipei, pp. 342–346.
19. **Shen, Q., Liao, S., Wang, J., Liu, W., Peng, C., & An, Q. (2013).** An FPGA-Based TDC for Free Space Quantum Key Distribution, *IEEE Transactions on Nuclear Science*, Vol. 60, No. 5, pp. 3570–3577. DOI:10.1109/TNS.2013.2280169
20. **Ma, L., Mink, A., & Tang, X. (2009).** High Speed Quantum Key Distribution Over Optical Fiber Network System. *Journal of Research of the National Institute of Standards and Technology,* Vol. 144, No. 3, pp. 149–177.
21. **Khalid, A.U., Zilic, Z., & Radecka, K. (2004).** FPGA Emulation of Quantum Circuits. *Proceedings of the IEEE Intl. Conf. on Computer Design*, San Jose California, USA, pp. 310–315.

Arturo Arvizu Mondragón received his B.Sc. and M.Sc. degrees in Electronics from the National Autonomous University of Mexico (UNAM) in 1985 and 1990, respectively, and the Ph.D. degree in Telecommunications from the CICESE Research Center, Ensenada, BC, Mexico, in 2000. In 1987 he joined the Institute of Electrical Research, Cuernavaca, Morelos, Mexico, working in projects related to the optical and optoelectronics communication systems with application in power generation systems, and laboratories for testing, measurement, and characterization of electrical systems. In 1992 he joined the CICESE Research Center where he currently works in the fields of quantum communications, optical fiber, and optical wireless communications with coherent detection. In 2000 and 2001 he did a post-doctoral research at the Telecommunications Department on the École nationale supérieure des télécommunications, Paris, France.

Josue A. López Leyva obtained his B.Sc. degree with specialty in Telecommunications from the Superior Technology Institute of Cajeme (ITESCA) in Sonora, Mexico. From 2006 to 2008 he worked in the Networking and Telephony Project. He obtained his Ph.D. in Quantum Communication Using Satellites and Quantum Cryptography at CICESE Research Center in Baja California, Mexico. His current research interests include free space optical communications, coherent optical communications, optical networks, statistical signal processing, and quantum cryptography systems.

Jorge Luis Ureña Castro obtained his B.Sc. in Electronic Engineering with specialty in Telecommunications from the Autonomous University of Baja California (AUBC), and his M.Sc. in Electronics and Telecommunications from the CICESE Research Center, Ensenada, B.C., Mexico, in 2011.

Francisco J. Mendieta-Jiménez obtained his B.Sc. degree from the National University of Mexico, the M.Sc. and Ph.D. degrees from the National Superior School of Telecommunications (ENST, Telecom ParisTech), France, in Optoelectronics and Telecommunications, respectively. At the Institute for Electrical Research (IIE), Mexico, he was involved in development projects on applications of optical fibers to electrical power systems. During his stay at the Utah State University, USA, he participated in a project on instrumentation for space experiments. At CICESE, Mexico, he founded the Optical Communications Group, where he has lead several research projects on telecommunications and sensing. During a sabbatical leave at Telecom Paris-Tech, France, he did research on quantum communications and cryptography. He has published journal papers and conference papers in the field of optical communications and sensing. Currently he is the Director of the Mexican Space Agency (AEM).

Juan de Dios Sánchez L. is Professor of the Engineering Faculty at the Autonomous University of Baja California (UABC), Ensenada. He received the B.Sc. in Electrical Engineering from the Technologic Institute of Madero City in 1989, and the M.Sc. and Ph.D. degrees in Telecommunications Engineering from CICESE Research Center (México) in 1999 and 2009, respectively. His current research interests include free space optical communications, coherent optical communications, optical networks, and statistical signal processing.

Article received on 30/08/2013, accepted on 19/08/2014.
Corresponding author is Arturo Arvizu Mondragón.