Adaptive low density parity check encoder for a complete free space optics/continuous variable-quantum key distribution system using commercially available off-the-shelf devices for variable throughput network considering dynamical atmospheric turbulence levels

J.A López-Leyva[a,*], A. Arvizu-Mondragon[b], J. Santos-Aguilar[b], R. Ramos-Garcia[c], and A. Talamantes-Álvarez[a]
[a]*Center for Innovation and Design, CETYS University,*
Camino a Microondas Trinidad s/n. Km. 1, Moderna Oeste, 22860 Ensenada, BC. Mexico.
**e-mail: josue.lopez@cetys.mx*
[b]*Department of Applied Physics. CICESE Research Center. Baja California, México,*
Carret. Ens.-Tij. 3918, Zona Playitas, Ensenada, B.C. 22860, México.
[c]*Department of Electrical and Computer Engineering,*
University of Alabama, Tuscaloosa, AL, 35487, USA.

Received 3 April 2018; accepted 24 May 2018

In this paper, an adaptive low density parity check (LDPC). encoder for complete Free Space Optics/Continuous Variable-Quantum Key Distribution (FSO/CV-QKD) system using a Commercially available Off-The-Shelf (COTS) device for emulated dynamical atmospheric turbulence levels is presented. The experimental and emulation results show the maximum and minimal final secret key rates of ≈ 105 Kbps and $\approx$ 10 Kbps, respectively, for minimal and maximal throughput in a commercial network, 30 Mbps and 90 Mbps, respectively. Our proposal presents an adequate performance for weak and moderate atmospheric turbulence levels and a suitable option for improving the use of Quantum Key Distribution (QKD) systems.

Keywords: Adaptive encoder; atmospheric turbulence; COTS device.

PACS: 03.67.Dd; 05.40.Ca; 07.50.Qx

1. Introduction

Currently, Quantum Key Distribution (QKD) systems are an excellent option to provide unconditional security to the information transmitted both in open and closed channels (*e.g.* atmospheric channel and optical fiber, respectively) [1-5]. However, each particular channel imposes different trade-offs that affect the overall performance (essentially, Quantum Bit Error Rate (QBER) and Final Secret Key Rate (FSecKR) parameters), for example, the polarization state variation, nonlinear phenomena, among other aspects are present in the optical fiber networks where QKD systems have been implemented [6,7]. On the other hand, the QKD systems implemented in free space optical links (*i.e.* Free Space Optics, FSO) have higher trade-offs because the atmospheric turbulence may affect the phase, amplitude, power distribution profile and wavefront of the optical signal [8,9]. In fact, there exist many technical options to counteract the effects of the atmospheric turbulence such as those based on the modification of the optical power level, the selective analysis time and data (which do not take advantage of the complete transmission time and data), the high performance encoders, etc. [10-12]. However, in order to implement this kind of solutions it is usually required high end hardware (electronic, mechanical and optical systems) such as Field Programmable Gate Arrays (FPGA's), Central Processing Units (CPU's) and Graphics Processor Units (GPU's), precision gimbals, and high efficient optical antennas, etc., in order to achieve a better performance [13]. As a suitable option to replace these high-end equipment (*i.e.* particularly, digital processing devices), there exist the Commercially available Off-The-Shelf (COTS) devices that are an innovative and accessible choice for the implementation of QKD systems. This way, it is only required to focus in optimizing the algorithm as well as on the use of the resources in order not to degrade the secret key rate, and more importantly, the security level [14]. In general, the practical mutual information (ΔI_{real}) in QKD systems is described by $\Delta I_{\text{real}} = \alpha(\beta I(A:B) - S(A:E))$ bits. Here, $I(A:B)$ represents the mutual information that Alice and Bob share (transmitter and receiver systems, respectively, according to the cryptography context), $S(A:E)$ is the maximum mutual information shared between Alice and Eve (eavesdrop system), and the parameters β and α represent the reconciliation and classical channel efficiencies, respectively. In particular, the value of β describes the performance of the raw key detected considering the efficiencies of Alice, Bob and the quantum channel, while α is the ratio of the amount of bits without errors at the receiver and the amount of bits transmitted based on the kind of encoder used in both sides. Thus, the classical channel efficiency has a limit in order to ensure the secret communication as shown in Eq. (1).

$$\alpha \geq \frac{\Delta I_{\text{real}}}{(\beta I(A:B) - S(A:E))} \tag{1}$$

Here, $S(A:E)$ value depends on the kind of attacks that might be used such as side channel attack, photon number splitting attack, Trojan-horse attack, etc., taking into account the kind of quantum and classical channel that are being used. In an ideal case, $\alpha = \beta = 1$, thus achieving the maximum information transmission. Nevertheless, in real scenarios, to achieve maximum efficiency, various novel techniques are used. Examples of these techniques are the Turbo, Reed Solomon and Convolutional encoders that have adequate performance and mitigation with respect to individual and burst errors. However, this type of encoders requires the use of high-speed digital devices to guarantee the process of mitigation of errors according to the specifications of the Raw Key Rate (RKR) and Final Secret Key Rate (FSecKR) [15]. It is pertinent to mention that if you want to use an encoder in the quantum channel, it must be chosen carefully because if it is not, its inclusion can eliminate or reduce the ability to detect the presence of a spy system (Eve). Fortunately, there exist the Low Density Parity Check (LDPC) encoders that are very convenient for cryptographic systems, however it requires high end hardware for their implementation. Besides, other improvements such as low-complexity and optimized algorithms are needed. such as low-complexity and optimized algorithms. In general, the LDPC encoder has a fixed coding gain. However, the encoders with the capacity to modify the coding gain must use state-of-art hardware, becoming a major problem in terms of energy consumption and budget. In a complete free space QKD system (*i.e.* both channels, private and public in free space) as well as on high-performance deep space missions, ultra-high rate satellites links, the atmospheric turbulence may modify the above-mentioned efficiencies (β and α) according to the turbulence level existing on the communications channel. The turbulence level may be described by means of Rytov variance (σ_R^2). Therefore, in this communications channel, the classical and quantum error probability, FSecKR, among other performance parameters depends on the σ_R^2 value. An important characteristic of the atmospheric turbulence is its dynamical behavior (in function of the dynamical weather conditions existing at different heights), so it must be described using probability density functions such as the Gamma-Gamma and log-normal, among others. Thus, the efficiency parameters are also dynamical. However, the majority of QKD systems do not consider a dynamical setting of the efficiency parameters, in fact, the overall performance of the QKD deteriorates in a direct way by the atmospheric turbulence. On the other hand, in the traditional radiofrequency satellite links is used a dynamical configuration regarding transmitted power and encoder gain, but the optical power variation is not a suitable technique for QKD systems. In addition, the Continuous Variable-QKD systems (CV-QKD) have some important advantages respect to hardware and techniques in the transmitter and receiver, mainly, when the modulated weak coherent states and the optical coherent detection are used. In this article, we present a complete FSO/CV-QKD system with an adaptive LDPC encoder implemented in a COTS device (using a 1.2 GHz 64-bit four-core ARMv8 CPU). The LDPC encoder is used for the purpose of mitigating the effect of dynamical atmospheric turbulence on the CV-QKD system. This type of encoder was chosen due to its inherent flexibility in the reconfiguration of its design parameters, in addition to having reduced hardware requirements for its implementation, in contrast to other types of encoders mentioned previously.

2. Experimental and Emulation Set-Up

First, a general description of the adaptive encoder is presented and the experimental emulation configuration used in this work is described below. The adaptive LDPC encoder uses a generator matrix (G) and a binary message (related to the binary sequence presented in a distillation protocol) (u), both parameters used in order to generate a codeword (c) as follows, $c_i = [u_i]_{1xk}[G_i]_{kxn}$, where k and $n(k < n)$ are the binary sequences length of u and c, respectively, and α_i has a relationship with the coding gain (k/n). These parameters (G_i, u_i and c_i) are dynamic and adaptive according to the $\sigma_{R_i}^2$ value calculated in each particular analysis time frame (i) (something that is not done in the "traditional" LDPC encoders). Thus, atmospheric turbulence and noise (n_i) affect to c_i and Bob receives the signal, $r_i = c_i(n_i, \sigma_{R_i}^2)$. Next, Bob system calculates the syndrome, $s_i = [H_i]_{kxn}[r_i]_{nx1}$, in order to allow the detection and error correction, where H_i represents the dynamical parity-check matrix [16]. The $\sigma_{R_i}^2$ value is calculated using the bit error rate measurements in (i) related to error probability in the classical channel, $P_e(\alpha, \alpha_{gg}, \beta_{gg})_C$, for Gamma-Gamma function where α_{gg} and β_{gg} are the effective numbers of large-scale and small-scale, respectively as shown in Eq. (2) using an On-Off Keying modulation scheme (OOK), although a Continuous Wave (CW) optical signal also is suitable.

$$P_e(\alpha, \alpha_{gg}, \beta_{gg})_C = \frac{1}{2\alpha}\exp(-\eta_C E[N_C]) \tag{2}$$

$$P_e(\beta, \alpha_{gg}, \beta_{gg})_S = \frac{1}{2\beta} erfc(\sqrt{\eta_S E[N_S]}\cos\theta_e) \tag{3}$$

Where η_C and η_s are the overall efficiency considering both Alice and Bob systems for classical and quantum channel, respectively, θ_e is the residual error phase considering a phase-locked loop, $E[N_C]$ and $E[N_s]$ represent the average photons numbers per observation time in the classical and quantum channel, respectively. In particular, in our set-up the data transmitted are affected by the emulated atmospheric turbulence. We make use of a Maximum Likelihood Algorithm (MLA) in order to generate data with a specific probability density function according to different levels of turbulence [17]. Equations (2) and (3) mean that both channels are affected by emulated atmospheric turbulence, however, the proposal in this paper does not consider the analysis of the turbulence in quantum states rather than the analysis and compensation for the classical channel (in any case, the effect of turbulence will be present in quantum detection).

The dynamical encoder algorithm and MLA were implemented in the COTS devices shown in Figs. 1 and 2. The figures show the experimental set-up implemented in our laboratory that consists of a laser that generates optical coherent

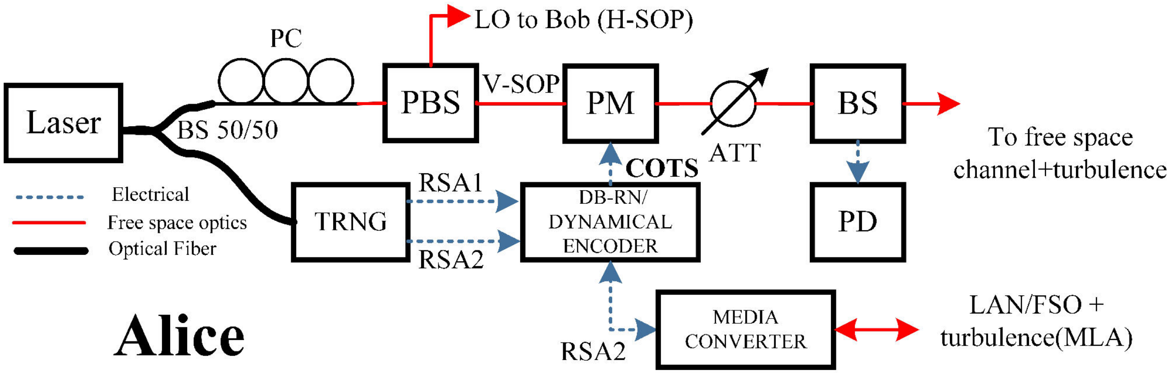

FIGURE 1. Alice experimental set-up.

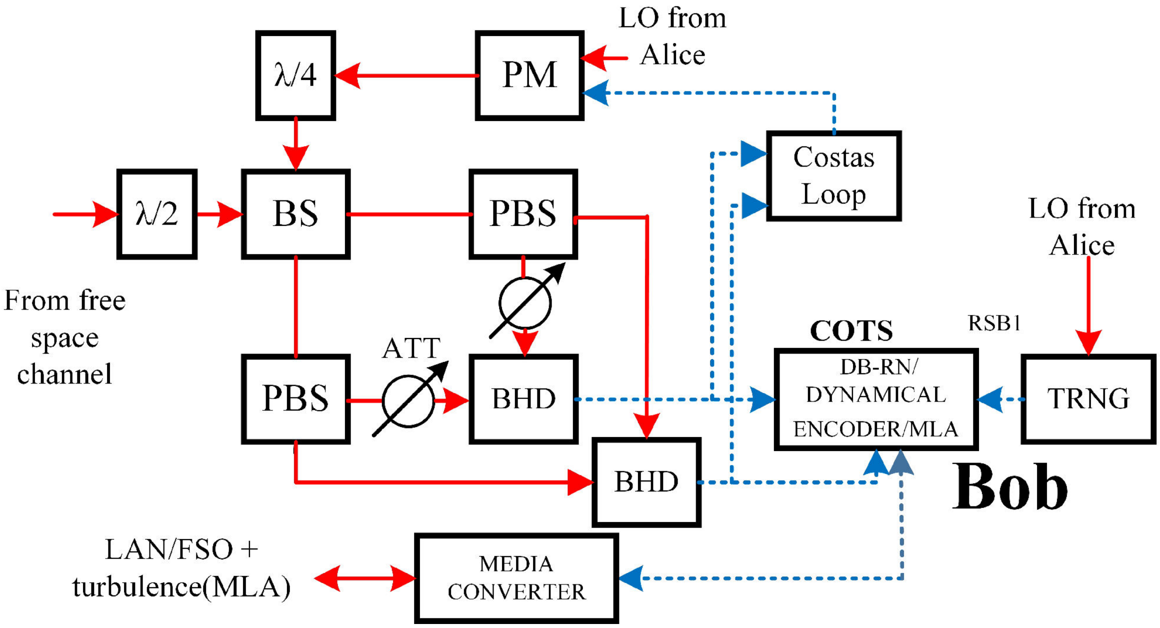

FIGURE 2. Bob experimental set-up.

states at 1550.1 nm with diffused phase, which are consequently, it is divided into two paths (upper and lower). The upper path consists of a Polarization Control (PC) and a Polarized Beam Splitter (PBS) in order to fix a Vertical State of Polarization (V-SOP) in the input optical signal in the Phase Modulator (PM) in order to reduce the residual amplitude modulation. In addition, a PBS generates a Local Oscillator (LO) signal with H-SOP. In the lower path, the optical signal is used by a True Random Number Generator (TRNG) based on the detection of the vacuum quantum state by an auto-homodyne scheme to generate two random binary sequences, Random Sequence # 1 and # 2 in Alice, (RSA1 and RSA2, respectively), then, both random sequences are recorded in a database by the COTS device. The TRNG is capable of generating random sequences up to 10 Mbps, that meets particular tests in order to determine the randomness level, some results are a bias probability of 0.0002 and an autocorrelation factor of 0.0001 [18]. Random sequences are stored on a Data Base of Random Number (DB-RN) implemented in COTS devices in order to increase the final secret key rate and improve the mutual information between Alice and Bob. In addition, the COTS devices perform the LDPC adaptive algorithm. The PM uses the electrical signal from the COTS device as a driver signal for a Binary Phase Shift Keying (BPSK) modulation scheme. A Half Wave Plate ($\lambda/2$) (in Bob) modifies the SOP of the output optical signal (of Alice) in the PM and an attenuator (ATT) generates Weak Coherent States (WCS). Finally, Alice uses a Beam Splitter (BS) and a low noise photodetector (PD) in order to monitor the optical power (*i.e.* to measure the photons number) before the transmission of the optical signal to the free space channel with emulated dynamical atmospheric turbulence; reaching 11.25×10^{-15} W at 350 KHz, which is equivalent to $E[N_s] = 0.25$ photons per pulse. In general, the overall efficiency is $\eta_s = 0.7$. The above mentioned is regarding the quantum channel, on the other hand, with respect to the classical channel, the COTS device is connected to a Local Area Network using a customized media converter ($\eta_C = 0.91$) with adaptation to a free space optical bidirectional channel at 100 Mbps with emulated turbulence to send the RSA2 to Bob in order to perform the quantum cryptography protocol; in our case, a simplified cryptography protocol based on BPSK modulation and a Random Sequence # 1 in Bob (RSB1) signal signal are used [14]. In the Bob side (Fig. 2), the optical signal transmitted by Alice is received and detected by Bob. The optical phase of the Local Oscillator (with optical power of 5×10^{-3} W) is modified in a dynamical way using an opto - electronical Costas loop and a Quarter Wave Plate ($\lambda/4$) modifies the SOP in order to detect both quadrature components of the WCS in a simultaneous way. In particular, the Costas loop has the following technical characteristics: integrator gain of 0.3 V/V, gain of the equivalent oscillator of 20.655×10^{-3} rad/(V-sec), natural frequency (f_n) of 360.97×10^3 Hz for the loop filter (low-pass active filter) and a phase detector gain of 5.8×10^{-6} V/rad, the parameters mentioned were optimized for low photons number using the Eq. (4):

$$f_n = \sqrt{\frac{2\Delta v N_s}{3\pi T_p}}, \tag{4}$$

where Δv is the linewidth of the laser, T_p is the observation time (bit duration) and N_s is the photons number in the quantum channel. Therefore, the phase error variance, σ_e^2, (considering the performance of θ_e) is described as follows:

$$\sigma_e^2 = \frac{\Delta v}{\sqrt{2} f_n} + \frac{3\pi T_p f_n}{2\sqrt{2} N_S} \tag{5}$$

Therefore, the performance of the Costas loop based on the θ_e value and Eqs. (4) and (5) modify the overall performance of QKD systems considering the Eq. (2) and (3). In addition, in order to eliminate the direct voltage component in the output electrical signal, a Balanced Homodyne Detector (BHD) was used for each quadrature component and different attenuators modify and calibrate the optical power variation of different optical paths based on the transmission matrix of each discrete optical component (*i.e.*, transmission and reflection efficiencies, $> 90\%$ and $> 99.5\%$, respectively). A local COTS device in Bob set-up uses the quadrature components information to determine the turbulence level present in the atmospheric channel for each interval analysis based on the MLA; the parameters encoder (G_i, u_i and c_i) are modified in a dynamical way according to the calculated turbulence level. Because the dynamical atmospheric turbulence affects the quantum performance, Alice and Bob negotiate the functional encoder parameters of each side based on the Rytov variance in a particular analysis time ($\sigma_{R_i}^2$) using the classical channel. Therefore, the classical channel is used for the cryptography distillation protocol and the encoder parameters negotiation.

3. Results

Figure 3 shows the performance of the FSecKR using the DB-RN and the adaptive LDPC encoder considering a controlled fixed throughput (bits per second in a Local Area Network) in the classical channel based on a throughput controller software and raw key rate of 350 Kbps. In particular, the optical signals transmitted through private and public channel are affected by emulated dynamical turbulence. When the adaptive LPDC encoder is not used (*i.e.* constant coding gain, k/n_f), the FSecKR value monotonically decreases in the range $0.1 \leq \sigma_R^2 \leq 2$, then, it is maintained (≈ 30 Kbps) without significant variations for $\sigma_R^2 > 2$. On the other hand, when the adaptive LDPC encoder is used (*i.e.* dynamical coding gain, k/n_d), the FSecKR value is maintained with slight variations in the range $0.1 \leq \sigma_R^2 \leq 1$, *i.e.* it is possible to consider the constant value (≈ 105 Kbps) of the FSecKR. However, when the $\sigma_R^2 > 1$, the FSecKR decreases up to a value lower than the FSecKR without using the adaptive encoder.

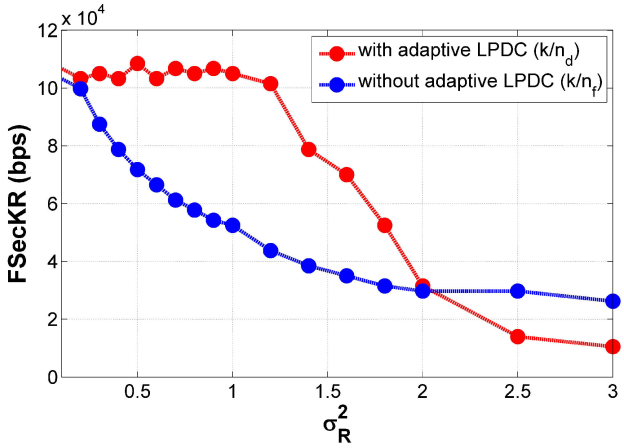

FIGURE 3. Experimental results of the FSecKR for different atmospheric turbulence levels with an average throughput of 90 Mbps.

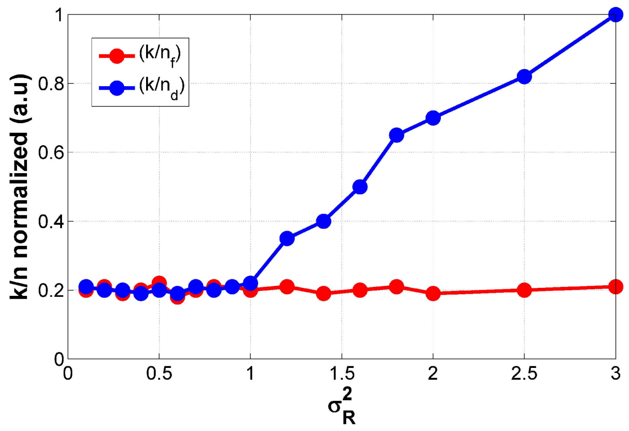

FIGURE 4. Normalized ratio of k/n using/not using the adaptive LDPC encoder, k/n_d and k/n_f, respectively.

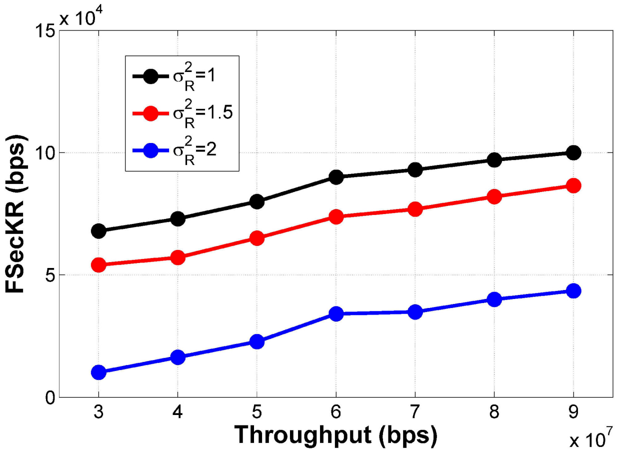

FIGURE 5. Experimental results of the FSecKR for different atmospheric turbulence levels and average throughput using the adaptive LDPC encoder.

Figure 4 shows the normalized value for k/n_d and k/n_f. In particular, k/n_f remained constant in the complete range of atmospheric turbulence. However, k/n_d increased significantly for Rytov variance values greater than $\sigma_R^2 = 1$. This last statement means that the adaptive LDPC encoder needs to add more redundant bits in order to mitigate the bit errors induced by the atmospheric turbulence. Therefore, the COTS device requires more processing time to perform the encoder algorithm affecting the FSecKR value.

Finally, Fig. 5 shows the FSecKR results for different throughput (from 30Mbps to 90 Mbps, which means a realistic classical network for multiple user and/or diverse network applications where the QKD system is implemented) and variable atmospheric turbulence levels considering a dynamic coding gain, k/n_d. In particular, when $\sigma_R^2 = 1$, the FSecKR value is ≈ 105 Kbps and ≈ 60 Kbps, maximum (MFSecKR) and minimum (mFSecKR) rates respectively. According to the increase of the atmospheric turbulence levels, the MFSecKR and mFSecKR decreases. Therefore, for $\sigma_R^2 = 2$, MFSecKR is ≈ 45 Kbps and mFSecKR is ≈ 10 Kbps. The reduction of MFSecKR and mFSecKR parameters for different atmospheric turbulence levels is due to the extra added bits in order to mitigate the errors caused by the turbulence.

4. Conclusions

In this paper, we have shown an adaptive LDPC encoder implemented in COTS devices in order to improve the overall performance of a complete FSO/CV-QKD system considering dynamical emulated atmospheric levels in the classical channel. The experimental results showed that, the dynamical coding gain allows to maintain the FSecKR in ≈ 105 Kbps for a throughput 90 Mbps considering weak to moderate atmospheric turbulence levels ($0.1 \leq \sigma_R^2 \leq 1$). This means an adequate final secret key rate for many applications, such as, providing high speed quantum security in a local network or telecommunications systems with similar throughput. In addition, the experimental results showed that the adaptive encoder implemented in a COTS device is not suitable for strong atmospheric turbulence levels. Even though the COTS device has many advantages, it is necessary to increase the digital processing speed in order for the adaptive encoder proposed to be suitable for strong turbulence levels. In addition, the algorithm performed by the COTS device requires to add more redundant bits, for example, the relation between k/n_d and k/n_f is 26.98 dB for $\sigma_R^2 = 3$. Therefore, there exists an important trade-off between the coding gain, processing speed and atmospheric turbulence levels for the FSecKR to remain constant. Finally, the proposed systems achieved a mFSecKR ≈ 10 Kbps and MFSecKR ≈ 105 Kbps for $0.1 \leq \sigma_R^2 \leq 2$ and for 30 Mbps and 90 Mbps, minimum and maximum throughput, which means an innovative proposal for a CV-QKD system that uses both classical and quantum channels in free space.

1. L. Sheng-Kai, *et al.*, *Nature Photonics* **11** (2017) 509-513.
2. L. Bacsardi, *et al.*, in 24th *European Signal Processing Conference*, (2016).
3. V. Scarani, *et al.*, *Rev. Mod. Phys* **81** (2009) 1301-1350.
4. F. Grosshans, *et al.*, *Phys. Rev. Lett*. **88** 057902 (2002).
5. D. Bacco, *et al.*, *Scientific Reports* **6** (2016) 1-7.
6. L. O. Mailloux, *et al.*, *IEEE Security & Privacy* **13** (2015) 30-40.
7. L.O. Mailloux, *et al., Access* **3** (2015) 110-130.
8. L. Moli-Sanchez, *et al., J, on Selec. Areas in Comm*. **27** (2009) 1582-1590.
9. A. Jaiswal, *et al., J. of Opt. Comm. & Netw*. **9** (2017) 149-160
10. X. Sun, *et al., Photonics Jour* **8** (2016) 1-14.
11. P. Wang, *et al.*, in *Wireless Communications and Networking Conference*, (2015).
12. G. Vallone, *et al.*, *Phys. Rev. A* **91** (2015) 042320.
13. K. Cui, *et al.*, *Trans. on Inf, Foren. & Sec* **8** (2013) 184-190.
14. J.A. Lopez-Leyva, *et al.*, *Opt. Applic*. **47** (2017) 411-419.
15. S. Yoon and J. Heo, in *International Conference on Convergence*, (2013).
16. J.A López-Leyva, *et al.*, *Rev. Mex. de Fis*. **63** (2017) 268-274.
17. D. Bykhosky, *J. of Light Tech.*, **34** (2016) 2106-2110.
18. J.A. Lopez-Leyva, *et al.*, *DYNA* **83** (2016) 93-98.