Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on a turbulent channel using an adaptive LDPC encoder

J.A López-Leyva[a,*], A. Arvizu-Mondragon[b], J. Santos-Aguilar[b], and R. Ramos-Garcia[c]
[a]*Center for Higher and Technical Education (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, Mexico.*
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 4 October 2016; accepted 3 March 2017

In this paper, a dynamical and adaptive LDPC coding scheme is proposed in order to improve the performance of the cryptographic key distillation protocol of an FSO/CV-QKD system considering the atmospheric turbulence levels that may be present in the classic channel. In this scheme, the Generator and Parity-check matrices of the encoder are modified according to the Rytov variance values estimated in the classical channel in order to improve the final secret key rate of the QKD system. The simulation results show that the final secret key was incremented 87.5 Kbps (from 52.5 Kbps to 140 Kbps) using the adaptive code rate; meaning that the information encrypted and transmitted is increased. In addition, the use of the dynamical encoder avoids the drastically reduction of the final secret key rate when the conditions of the classical channel are considered. Our proposal might be implemented based on the use of high-speed FPGA's and DSP's commercially available.

Keywords: Atmospheric turbulence; secret key rate; Rytov variance; mutual information.

PACS: 42.68.Bz; 42.79.Sz; 03.67.Dd

1. Introduction

Telecommunication systems play a very important role in the connectivity of many devices, applications, and services in society; hence, the developments of security schemes for these systems are a high priority. The research community and technologists from around the world continue investing great amounts of time and effort to develop strategies that can improve and guarantee the security of the information carried in the telecommunication systems. Among these strategies, the most important alternative is the Quantum Key Distribution (QKD) system, which according to the foundations of quantum mechanics may provide a "true" unconditional security [1,2]. The implementation of QKD systems has been previously addressed using Discrete Variables (DV), Continuous Variables (CV) and Differential-Phase Reference protocol known as DV-QKD, CV-QKD and DPR-QKD systems, respectively [3-5]. Usually, the QKD systems are based on a generic scheme consisting of an optical private quantum channel (fiber or free space) and a public classical channel; the quantum signal (raw key) is sent through the private channel in a unidirectional manner and, the distillation protocol is performed using the public channel (*e.g.*, Radio Frequency links (RF), copper cables and optical channel with many photons per observation time) in a bidirectional way in order to obtain the final quantum cryptographic key [6,7]. The performance of a QKD system depends not only on the noise in the quantum channel (a crucial parameter), but also on the efficiency of the public channel [8]. This channel is susceptible to bit errors, hence it is convenient to utilize different encoders (according to the characteristics of each particular channel) in order to mitigate the erroneous bits that affect the process and performance of the distillation protocol. On the other hand, the errors in the private channel are characterized a priori and an excess of errors means the lack of information due to a spy system (Eve) [9]. Usually, the simulations and experiments of QKD systems only focus on the quantum channel and do not consider the classical channel performance. However, the public channel performance is also important for the performance of the final secret key rate, particularly when the atmospheric turbulence affects the classical RF and Free Space Optics (FSO) channels used in a QKD system, such is the case of the QKD systems that use satellite-ground station links [10,11]. There exist many kind of coding schemes (*e.g.*, Turbo, Reed-Solomon, Convolutional, etc.) that allow to mitigate individual and burst errors in the classical channel; nevertheless, the important issue with such encoders is that the transmission rate of the final quantum key is reduced drastically because these encoders need more processing time according to the processor unit used (Central Processing Unit or Graphics Processing Unit). However, some optimized methods using Turbo codes for QKD systems have been researched [12,13]. In fact, to the best of our knowledge, currently there are not commercially available QKD systems using the encoders mentioned earlier. Hence, the LDPC (Low- Density Parity-Check Codes) is the encoder most widely used in QKD systems due to its simplicity and processing speed. Nonetheless, the conventional

LDPC is not suitable for classical channels with variable conditions (*i.e.* the code rate is fixed without considering the channel conditions) such as the atmospheric turbulence [14]. Thus, different techniques to mitigate the effect of the atmospheric turbulence in the classical channel for QKD systems have been proposed, such as the LDPC codes adapted in the Slepian-Wolf coding system [15] and a hybrid RF-FSO system with adaptive modulation and coding (*i.e.* with adaptive powers and rates) in order to maximize the channel capacity [16]. However, in the context of FSO-QKD systems, mainly on the private channel, the power modification may not be an adequate technique, because it reduces the performance of the overall system and increases the risk for information losses due to Eve. Although [13] presented a theoretical model of a QKD system using Turbo coding with better performance that a LDPC coding, the theoretical model does not consider the adaptability for different transmission conditions. On the other hand, there also exist other dynamical techniques based on the selection of the intervals with higher channel transmissivity in order to mitigate the effects of the atmospheric turbulence [17]. However, the main disadvantage is that this system uses only the interval with best performance of the raw key; therefore, the useful raw key rate is reduced. A general scheme of a complete FSO-QKD system using the adaptive code rate in the classical channel in order to mitigate the effect of the atmospheric turbulence over the final secret key rate from weak to moderate turbulence regimes is proposed in this paper. We consider that, our technique is different than other approaches because is based on the constant raw secret key rate allowing higher transmission rate. Also, our work considers the full FSO-QKD systems that permit the enhanced performance using optics link in the classical channel for particular application (*e.g.* FSO-QKD systems for deep space missions without uses RF link in the classical channel). The organization of this paper is as follows: Section 2 describes the mathematical framework necessary to calculate the final secret key rate in a QKD systems, Sec. 3 describes the mathematical framework concerning the effect of the atmospheric turbulence in the QKD systems and, finally, Secs. 4 and 5 show the scheme simulation proposed and the numerical results of the final secret key rate using a LDPC with adaptive code rate for different atmospheric turbulence levels.

2. Mutual information in real QKD systems

In general, the final secret key rate may be defined as the mutual information shared between the Alice (A) and Bob (B) systems in the presence of a spy system called Eve (E) using the expression shown in Eq. (1) (the final secret key rate considering the transmission rate will be considered after) [18]:

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

Here, ΔI_{real} is the real secret key rate of the QKD system after the distillation protocol without considering the kind of variables (CV-QKD and DV-QKD), $I(A:B)$ represents the mutual information that Alice and Bob shared and $S(A:E)$ is the maximum mutual information shared between Alice and Eve. Thus, $I(A:B) - S(A:E)$ represents the ideal secret key rate of any QKD system. However, the distillation protocol performed for generate the quantum key is imperfect (due to multiple variables in the channels and systems used), thus, the shared information between Alice and Bob is decreased by a factor of β. Therefore, the secret key is $\beta I(A:B) - S(A:E)$, where β is the reconciliation efficiency. In order to obtain a better approximation of the final secret key rate, the efficiency of the classical channel (α) must be considered. The channel efficiency may be calculated as the ratio of the amount of bits without errors at the receiver and the amount of bits transmitted. In addition, this efficiency is related to the concept of code rate, *i.e.*, different code rates provide different channel efficiency, where lower code rates produce greater efficiency, and higher code rates produce lower efficiency. In specific way, the code rate (k/n) is a value that relates the original information bits (k) and the redundant bits ($n-k$) necessaries for the detection and correction of the erroneous bits, given that the encoder generates n bits of data. Therefore, an adequate encoder used in the classical channel must produce a value of $\alpha \approx$ (*i.e.* an adequate code rate will improve the channel efficiency), which means that a lot of errors are corrected. Finally, if a spy does not exist in the private channel (an FSO link in this case), it is possible to assume that $S(A:E) = 0$, and therefore $\Delta I_{\text{real}} = \alpha(\beta I(A:B))$. In other words, ΔI_{real} only depends of the efficiencies values (β and α). In a traditional and complete QKD system, the raw key is directly affected by β, while α affects the sifted key. In this study, the parameter α_f was used to indicate that the value of α is a fixed efficiency of the classical channel for a specific encoder with fixed code rate [19]. Thus, considering different technical parameters (*i.e.*, the values of β and α depends of the overall efficiencies of the optical and electronical schemes), the efficiency of classical public communication channel has the mathematical limit shown in Eq. (2) to assure a secure communication link:

$$\alpha \geq \frac{\Delta I_{\text{real}}}{(\beta I(A:B) - S(A:E))} \xrightarrow{FSO} \frac{\Delta I_{\text{real}}}{\beta I(A:B)} \tag{2}$$

Therefore, the parameter $\Delta\beta I(A:B)$ may be calculated considering that the quantum channel of a QKD system can use different protocols or modulation schemes in order to transmit the raw key. For example, [20] shows a QPSK modulation scheme that transmits symbols and bases through the quantum channel based on a BB84 protocol and a Differential Phase Shift Keying (DPSK) protocol in [21]. However, the focus of the present work is related to the classical channel, which in general, it may use a variety of modulation schemes. Since the QPSK modulation scheme is utilized here for the communication through the classical channel, it is possible to represent the mathematical functions for the probability error (in the quantum limit) of the classical ($P_e(\alpha)$) and quantum

($P_e(\beta)$) channels using the Eqs. (3) and (4) without considering the values of α and β (the efficiencies are not considered in many cases).

It is important to clarify that, a code rate variation affects in a direct way to the coding gain (related to $\sqrt{\eta N_c}$) and finally, also to the channel efficiency. However, in this paper the linear effect of the channel efficiency is taken into consideration caused by the variation of the code rate when coherent detection is used in the receiver stage. This kind of detection was selected due to its inherent spectral filtering and the coherent amplification that may be obtained on the received signal. Therefore, in this case, the error functions must consider the channel efficiency value as shown in Eqs. (3) and (4) where N_c and N_q represent the photons number of the classical and quantum channel respectively, θ_e is the phase error signal using coherent detection and the phase synchronization schemes, and η is the overall efficiency of the overall system.

$$P_e(\alpha) = erfc(\sqrt{\eta N_c}\cos\theta_e)/2\alpha \tag{3}$$

$$P_e(\beta) = erfc(\sqrt{\eta N_q}\cos\theta_e)/2\beta \tag{4}$$

An important assumption is that the error phase signal is minimized for the phase synchronization scheme in different time windows. For such reason, the performance done in this works takes into consideration the efficiency α and that the value of β is fixed; nevertheless, the improvement in the performance of both channels is possible. As mentioned above, in the case of the absence of the Eve system, the following expression is valid: $S(A:E) = 0 \Leftrightarrow N_{AE} = 0 \Leftrightarrow N_q = N_{AB}$. However, if an Eve system performs a Photon Number Splitting (PNS) attack, the expression will be $S(A:E) \neq 0 \Leftrightarrow N_{AE} \neq 0 \Leftrightarrow N_q = N_{AB} - N_{AE}$, where N_{AE} is the amount of photons (stolen photons) received in Eve from Alice [22]. Thus, the Eq. (4) can be modified according to $S(A:E)$. Finally, the parameter $I(A:B,\beta)$ can be expressed as [3,18]:

$$I(A:B,\beta) = 1 + \chi\log_2\chi + (1-\chi)\log_2(1-\chi)\text{bits}, \tag{5}$$

where $\chi = P_e(\beta)$. Finally, considering the efficiency of the classical channel, the result of ΔI_{real} may be described in a more detailed way using (5) as $\Delta I_{\text{real}}(\alpha,\beta) = \alpha I(A:B,\beta)$.

3. Atmospheric turbulence in FSO-QKD systems

In the FSO links used in communications, the atmospheric channel may be extremely aggressive with the performance of the complete system. Therefore, considering the performance parameters of the FSO-QKD systems, the adequate analysis and detailed design of the FSO links is essential. In order to reach the best performance, it is required the use of probabilistic models to describe the effect of the atmospheric turbulence in the free space links, in our case, for the QKD application. A common parameter used for characterizing the atmospheric conditions is the Rytov variance (σ_R^2), which describes the variability of the optical intensity (*i.e.* irradiance fluctuations) under different weather conditions or regimes; for a regime of weak turbulence $\sigma_R^2 \ll 1$, $\sigma_R^2 \approx 1$ for moderate turbulence and $\sigma_R^2 > 1$ for strong turbulence. The Rytov variance is defined in Eq. (8) [23]:

$$\sigma_R^2 = 1.23c_n^2 k^{7/6} L^{11/6}, \tag{6}$$

where L is the distance of the communications link, C_n^2 is the refractive index structure parameter and $k = 2\pi/\lambda$ is the optical wave number for a specific wavelength λ. Although there exist different probability functions for the analysis of optical turbulence in FSO systems, it is well known that the Gamma-Gamma function allows a good characterization of the channel (due to the fact that it considers the effects of both the small and large scale particles) [23]. Therefore, the Gamma-Gamma function was chosen for the analysis of FSO-QKD system. At the same time, an analysis of the optical channel using the Rayleigh distribution was included because previous works have made use of it to describe the effects of the optical turbulence from the weak to moderate turbulence regimes; also, this function is useful for modeling the pointing losses in FSO systems [24,25]. In addition, the results obtained in this way are straightforward and easier to interpret in comparison with the more general results obtained with the Gamma-Gamma function. Hence, in this case, the Rayleigh distribution function that describes the variation of the optical intensity may be written as shown in Eq. (9).

$$f(N_C,\sigma_R^2) = \frac{N_C}{\sigma_R^2}\exp\left(-\frac{N_C}{2\sigma_R^2}\right) \tag{7}$$

In particular, the Rayleigh function is dependent of the optical intensity ($N_c hv/Tm^2$), where besides the Planck constant (h), the frequency (v), observation time (T), and the area of the photo receiver (m^2) remain also constant. Thus, Eq. (9) has a most appropriate representation in the QKD context. The function $f(N_C,\sigma_R^2)$ describes the variation of the optical intensity of the classical signal received in a FSO-QKD system in a time window analysis. It is possible to relate it to the error probability of the overall system considering the effect of the channel efficiency and the atmospheric turbulence as shown in Eq. (10):

$$P_e(\alpha,\sigma_R^2)_c, p_e(\alpha,\alpha_{gg},\beta_{gg})_c = \frac{1}{2\alpha}erfc \times (\sqrt{\eta E[N_c]}\cos\theta_e) \tag{8}$$

where $E[N_C]$ is the expected value of the photons number using (9) in the time window used for the analysis; on the other hand, when the Gamma-Gamma function is used, Eq. (10) is modified so that $E[N_C]$ is calculated based on the Gamma-Gamma function, where α_{gg} and β_{gg} are the effective numbers of large-scale and small-scale, respectively [23-25].

4. Simulation scheme

The simulation scheme shown in Fig. 1 was implemented to evaluate the proposed method. In this simulation, the Alice system has a quantum subsystem (unidirectional) and a classic transmitter / receiver subsystem (bidirectional). In the private channel segment, the parameters $(\beta I(A:B), S(A:E))$ mentioned previously are calculated. The setup also has a dynamical and adaptive encoder able to modify the code rate considering the turbulence levels in the classical channel. Thus, the final secret key rate is also dynamical according to the value of σ_R^2.

Figure 2 shows the dynamical iterative process for estimate parameters in the classical channel. In particular, the iterative procedure in the Bob system is as follows: First, the communication in the classical channel uses an initial code rate $((k/n)_{t_1})$ at time t_1; next, Bob calculates the classical channel efficiency using the Bit Error Rate (BER) measurement (the BER has a relationship with the theoretical value of error probability, $P_e(\alpha, \sigma_R^2)_C$ and $P_e(\alpha, \alpha_{gg}, \beta_{gg})_C$). Once that Bob determinates the channel efficiency using the error probability calculated using the BER measurement, Bob informs to Alice using the same code rate $(k/n)_{t_2}$ the future modification of the code rate $(k/n)_{t_2}$ to be used in the next communication according to the atmospheric turbulence detected. The atmospheric turbulence characterization depends on the environmental conditions which may vary with time, but usually the atmospheric conditions has a relatively slow modification rate compared to the data signal processing speed currently available. Based on this fact, the value of the turbulence is assumed to be constant in the temporal processing interval $(t_2 - t_1)$, hence that the code rate is able to minimize the effect of the turbulence in the communication link.

As mentioned previously, both quantum and classical channels are FSO links; therefore, an important assumption is that the atmospheric turbulence level is considered the same (or very similar) in both channels in a time window analysis. In fact, both channels do not transmit at the same time, *i.e.*, the raw key is transmitted in a non-continuous way in order to calculate a new quantum final key for each time window analysis. In addition, althoug turbulence in the quantum channel exists, the simulation does not take into consideration the modified characteristics of the raw key (*i.e.* the variation of the encoder in the quantum channel is not considered) in order to maintain the capability of detecting the excess of noise in the quantum channel due to future implementation of Eve.

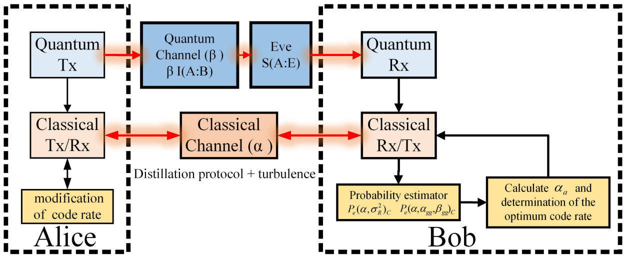
Quantum Tx
Quantum Channel (β)
β I(A:B)
Eve
S(A:E)
Quantum Rx
Classical Tx/Rx
Classical Channel (α)
Classical Rx/Tx
Distillation protocol + turbulence
modification of code rate
Probability estimator
$P_e(\alpha,\sigma_R^2)_C$ $P_e(\alpha,\alpha_{gg},\beta_{gg})_C$
Calculate α_a and determination of the optimum code rate
Alice
Bob

FIGURA 1. Block diagram of the simulation-experimental setup of the QKD system proposed with dynamical encoder for different atmospheric turbulence levels.

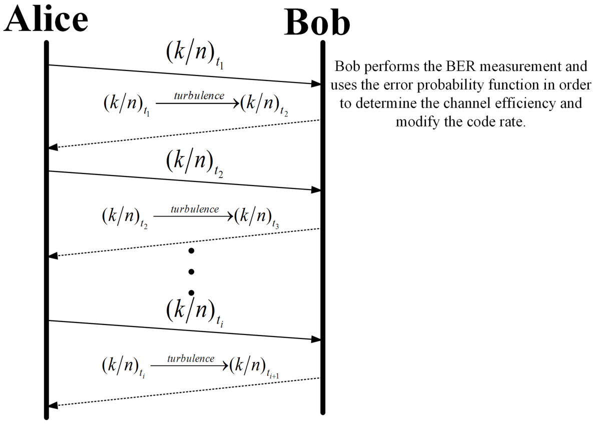
Alice
Bob
$(k/n)_{t_1}$
$(k/n)_{t_1} \xrightarrow{turbulence} (k/n)_{t_2}$
Bob performs the BER measurement and uses the error probability function in order to determine the channel efficiency and modify the code rate.
$(k/n)_{t_2}$
$(k/n)_{t_2} \xrightarrow{turbulence} (k/n)_{t_3}$
$(k/n)_{t_i}$
$(k/n)_{t_i} \xrightarrow{turbulence} (k/n)_{t_{i+1}}$

FIGURA 2. Dynamical process of negotiation of the code rate considering the turbulence in the classical channel

Considering the classical theory of LDPC coding, the LDPC design parameters were modified in this work with respect to the turbulence regimes (Rytov variances); therefore, different generator matrices (G) are established. Thus, the codeword (c) transmitted through the classical channel using the binary message (u) is given in Eq. (11) where the index (i) represents the analysis iteration in the time $(t_{i+1} - t_i)$.

$$c_i = [u_i]_{1xk}[G_i]_{kxn} \tag{9}$$

Next, the codeword transmitted is affected by the channel noise (n_i) and turbulence (σ_R^2), and this manner, the decoder uses the received signal $(r_i = c(n_i, \sigma_R^2))$ in order to determine the syndrome (s) considering the corresponding Parity-check matrix (H_i) as described in Eq. (12) (note that $G_i H_i^T = 0$) .

$$s_i = [H_i]_{kxn}[r_i]_{nx1} \tag{10}$$

The value of s_i allows the detection and correction of the errors in the communication link. An important parameter is n, that define the dimension of G_i and H_i and depends of the turbulence in the classical channel. At same time, the error probability is calculated in order to modify the parameters $(k/n)_i$, G_i and H_i to be used in the next analysis (for more details of LPDC coding consult [19]). Figure 3 shows the detailed block diagram of the LPDC encoder proposed where Bob determines the efficiency of the classical channel using the bit error rate measurement (the figure shows the error probability in order to maintain the style of the equations used). Given the fixed amount of information bits (u), Bob modifies the code rate according to the turbulence regime calculated.

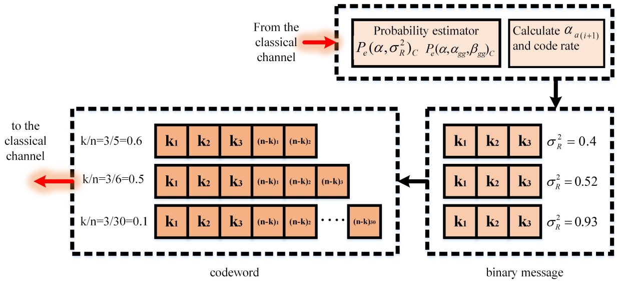
From the classical channel
Probability estimator
$P_e(\alpha,\sigma_R^2)_C$ $P_e(\alpha,\alpha_{gg},\beta_{gg})_C$
Calculate $\alpha_{a(i+1)}$ and code rate
to the classical channel
k/n=3/5=0.6
k/n=3/6=0.5
k/n=3/30=0.1
k1 k2 k3 (n-k)1 (n-k)2 (n-k)3 (n-k)30
$\sigma_R^2 = 0.4$
$\sigma_R^2 = 0.52$
$\sigma_R^2 = 0.93$
codeword
binary message

FIGURA 3. Block diagram of the LDPC coding with adaptive code rate considering the value of the Rytov variance.

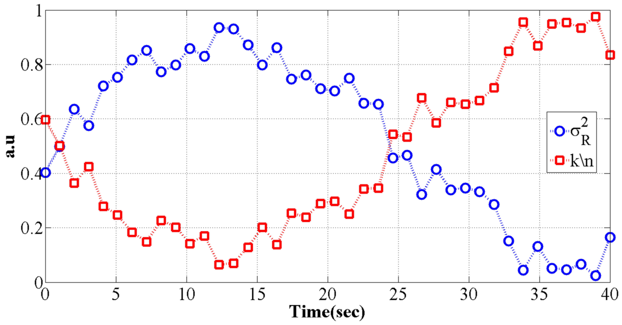

FIGURA 4. Numerical results of the code rate using different values of Rytov variance in order to obtain a $\alpha = 0.55$; The computation time required for the calculation of the code rate is 1 second (a.u.: arbitrary units).

5. Numerical results and analysis

In the simulation, a bit stream of 10×10^6 bit/sec (without encoding) was used for the transmission in the classical channel. In order to clarify this issue, the transmission rate is not possible to ensure in the simulation considering the hypothetical classical channel due to the different variations of processing time of the computer used; therefore, the stream length per second is used as assumption for the proof of concept of the scheme proposed. The bit error rate is measured in order to determine the value of the σ_R^2 using the Eq. (10) after the bit stream has been affected by the turbulence simulated. Thus, the values of α_i were calculated considering different σ_R^2 in order to modify the value of (k/n) and inherently the channel efficiency (α_{i+1}). Figure 4 shows the calculated numerical values of the code rate for the Bob system considering the variation of σ_R^2 calculated according to the Gamma-Gamma function in order to maintain a $\alpha = 0.55$. The calculation of the code rates was chosen each 1 second in a complete time analysis of 40 seconds, however the analysis time can be decreased or increased. In this way, for greater values of σ_R^2 the bit error rate measured $(P_e(\alpha, \sigma_R^2)_C$ and $P_e(\alpha, \alpha_{gg}, \beta_{gg})_C)$ are significantly increased. Therefore, the code rate (k/n) is reduced because the Alice system has to add more redundant bits in order to maintain a constant channel efficiency.

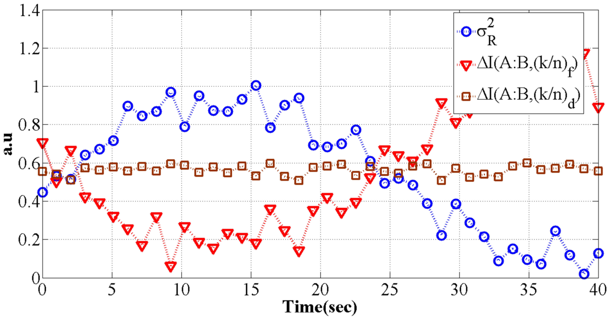

FIGURA 5. Performance of the mutual information considering different values of Rytov variance according to the Gamma-Gamma function using a fixed and variable code rates (a.u.: arbitrary units).

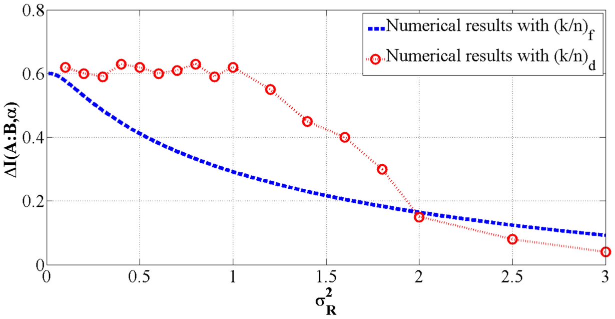

FIGURA 6. Numerical results for the mutual information using adaptive coding for different turbulence regimes.

Figure 5 shows the mutual information results using a fixed code rate $(k/d)_f$ ($i.e.$, a G_i and H_i fixed).In this scenario, higher values of will result in a decreased in the mutual information; otherwise, when using a dynamical code rate $(k/d)_d$ ($i.e.$, dynamical G_i and H_i), the mutual information is maintained constant. Based on the Fig. 5, it is possible to observe that for small values of with $(k/d)_f$, the mutual information is increased, while the mutual information is still constant when $(k/d)_d$ is used. The reason of this performance is that the proposed system was designed in order to maintain a specific mutual information value between the Alice and Bob systems, regardless of the channel conditions. However, it is possible to modify the mathematical model of the encoder in order to improve the performance.

Figure 6 shows the numerical values for the mutual information considering a fixed and adaptive coding gain. In particular, the performance of the mutual information using the adaptive coding gain is constant from weak to moderate turbulence regimes; however, the mutual information decreased drastically in the strong turbulence regime. The latter can be explained due to the fact that for strong turbulence regime the coding scheme proposed has to add too much redundant bits in order to detect and correct the errors causing a final secret key rate reduction.

Finally, Fig. 7 shows the mutual information and channel efficiency performance when the code rate is modified with respect to the error probability $P_e(\alpha, \alpha_{gg}, \beta_{gg})_C$ with

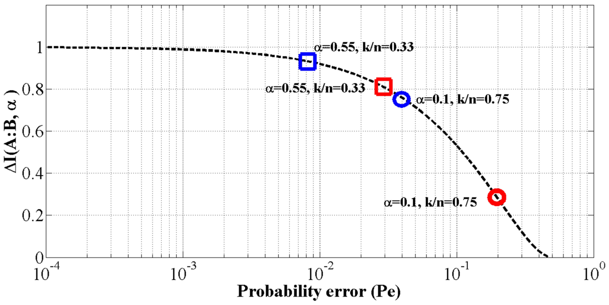

FIGURA 7. Mutual information between Alice and Bob with Rytov variance of 0.53 according to the Gamma-Gamma function. Circle: α without using the adaptive coding. Square: α using the adaptive coding.

$\sigma_R^2 = 0.53$ in order to describe a specific atmospheric turbulence level. Therefore, the final numerical results showed that using a code rate of 0.75 ($k/n = 0.75$), the channel efficiency is 0.1 ($\alpha = 0.1$) and the mutual information is $\Delta I(A : B, \alpha) \approx 0.3$. Nevertheless, when the code rate is modified ($k/n = 0.33$), the channel efficiency and mutual information show an increase of 0.55 ($\alpha = 0.55$) and $\Delta I(A : B, \alpha) \approx 0.8$, respectively. In addition, the length of the bit stream using the dynamical encoder is increased to 13.3×10^6 and 30×10^6 bits according to the code rate modified, respectively.

The results shown in the Figs. 6 and 7 contributed to determine the final secret key rate in a QKD system considering the raw and sifted key rates (bit/sec) without using the privacy amplification in the protocol. In particular, the final secret key rate is defined as $R_{\text{secret}} = R_{\text{sift}}\ \Delta I(A : B, \alpha)$; thus, using a raw key rate of 350 Kbps that our work team reported in [26], the calculated ideal sifted key rate (R_{sift}) was 175 Kbps without considering turbulence in the quantum and classical channels. Consequently, the proposed scheme in this paper improves the performance of R_{secret} modifying the code rate considering the atmospheric turbulence. In particular, the final secret key rate was 52.5 Kbps without using the adaptive code rate, while that using of the adaptive code rate allowes reach up to 140 Kbps in our simulation analysis.

6. Conclusions

A dynamical and adaptive coding scheme is reported for improve the performance of the cryptographic key distillation protocol considering the atmospheric turbulence levels (it were modeled by Gamma-Gamma and Rayleigh functions) that may be present in the classic channel. Specifically, the main objective of this work was to enhance the performance of FSO/CV-QKD systems using a technique that does not require the change of the devices already installed; such technique is based in the knowledge of the dynamic parameters of the overall system, in this case, the classical channel and the modification of the code rate used. Besides, the technique proposed is suitable also for general FSO quantum communications systems due to that dynamical atmospheric turbulence levels are present also. However, on these terms, the modification of the performance theoretical expressions considering the particular technical specifications of such communication system (*i.e.*, the Eve system does not exist and obviously, the distillation protocol is not required) will be necessary. In general, the proposed method showed to be feasible based on the numerical results by incrementing the final secret key rate by 87.5 Kbps (from 52.5 Kbps to 140 Kbps) when the code rate is modified with respect to the atmospheric turbulence. This means that the transmission of a longer final quantum key and higher secret key rate are possible (*i.e.*, double length/rate or more). While it is true that the parameter $\Delta I_{\text{real}}(\alpha, \beta) = \alpha I(A : B, \beta)$ is an adequate general approximation for the final secret key rate, more information regarding the raw key rate and the classical subsystems that will perform the distillation protocol is needed. Thus, the mathematical framework and results obtained in this work shows the potential to optimize the design of FSO/CV-QKD systems. In addition, the variation of the atmospheric turbulence is slow in general, hence, the processing time require for the parameters do not appear to be critical aspect for future physical implementations. In order to be able to mitigate the effects of the optical turbulence over the communications link, it is required that the physical implementation of our adaptive encoder works on real time, *i.e.*, the total processing time must be faster than the cutoff frequency of the optical turbulence. With the high-speed FPGAs and DSPs commercially available, this requirement could be easily met. Finally, the technique proposed requires a complete quantum security analysis considering different attacks against QKD systems for a practical security performance, but due to the particular conditions of the FSO/CV-QKD systems, many considerations are necessary as mentioned previously, *e.g.*, some kinds of attacks are nearly impossible to implement in the quantum channel (*i.e.* in the FSO link) and additional losses and noises should be considered [27,28]. In fact, some parameters that are related in an inherently way with the losses were used in (1)-(4). On the other hand, a man-in-the-middle attack has to be prevented using authenticated classical systems [29]. However, these attack conditions are not the essence of the paper.

1. C.H. Bennett and G. Brassard, in *Proceeding of IEEE International Conference on Computer, Systems Signal Processing,* (1984).
2. V. Scarani, *et al.*, *Rev. Mod. Phys.* **81** (2009) 1301-1350.
3. F. Grosshans, and P. Grangier, *Phys. Rev. Lett.* **88** (2002) 057902.

4. D. Bacco, *et al.*, *Sci. Reports* **6** (2016) 36756.
5. F. Xu, *et al.*, *Nature Photonics*, **9** (2015) 772-773.
6. P.D. Townsend, *Electron. Lett.* **30** (1994) 809-811.
7. S. Aleksic *et al.*, in *Proceedings of 16th International Conference on Transparent Optical Networks*, (2014).
8. T.F. da Silva *et al.*, *J. of Lightwave Technology* **32** (2014) 2332-2339.
9. A. Ferenczi, P. Grangier, and F. Grosshans, in *Proceedings of European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*, (2007).
10. M. Pfennigbauer *et al.*, in *Proceedings of the CNES - intersatellite link Workshop* (2003).
11. P.J. Edward *et al.*, in *Proceedings International Quantum Electronics Conference* (2000).
12. Y.B. Zhao *et al.*, *IEEE Trans. on Inf. Theory* **54** (2006) 2803-2807.
13. N. Benletaief, H. Rezig and A. Bouallegue, *J. of Quantum Inf. Sc.* **4** (2014) 117-128.
14. S. Niuniu *et al.*, in *Proceedings of International Conference on Software Engineering and Service Science*, (2013).
15. P. Treeviriyanupab *et al.*, in *Proceeding of 14th International Symposium on Communications and Information Technologies*, (2014).
16. I.B. Djordjevic and G.T. Djordjevic, *Opt. Exp.* **17** (2009) 18250-18262.
17. G. Vallone *et al.*, *Phys. Rev. A* **91** (2015) 042320.
18. P. Jouguet and S. Kunz-Jacques, *J. Quant. Inf. & Comp.* **14** (2014) 329-338.
19. T. Richardson and R. Urbanke, *Modern Coding Theory* (Cambridge University Press, 2007)
20. Q. Xu *et al.*, *J. of Light. Techn.* **27** (2009) 3202-3211.
21. H. Takesue *et al.*, *New J. of Phys.* **7** (2005).
22. J.A. Lopez *et al.*, *Microwave. and Opt. Tech. Lett.* **57** (2015) 1349-1352.
23. M. Niu *et al.*, *J. of Opt. Commun. and Netw.* **3** (2011) 860-869.
24. M.I. Petkovic *et al.*, in *Proceedings of Telecommunications Forum TELFOR* (2015).
25. W. Gappmair, S. Hranilovic and E. Leitgeb, *IEEE Commun. Lett.* **15** (2011) 875-877.
26. A. Arvizu *et al.*, *Comput. y Sist.* **19** (2015) 185-195.
27. A. Alyssa, I. Djordjevic and M. Neifeld, in *Frontiers in Optics* (2015).
28. E. Diamanti, H.-Kwong Lo, B. Qi and Z. Yuan, *npj Quantum Information*, **2** (2016) 1-12.
29. N. Hosseinidehaj and R. Malaney, in *IEEE International Conference on Communications* (2015).