Atmospheric Turbulence-Controlled Cryptosystems

Ivan B. Djordjevic, *Fellow, IEEE*

University of Arizona, Department of Electrical and Computer Engineering, 1230 E. Speedway Blvd., Tucson, AZ 85721, USA

Manuscript received September 2, 2020. This paper was supported in part by the NSF.

Abstract: To overcome the limitations of QKD, post-quantum cryptography, and computational security-based cryptography protocols in this paper, an atmospheric turbulence-controlled cryptosystem is proposed. The proposed encryption scheme employs the traditional scheme to utilize the atmospheric turbulence as the common source of randomness only in the initialization stage to determine the common parameters to be used in the proposed encryption scheme. To overcome low secret-key rates of traditional scheme, dictated by the long coherence time T_c of turbulence channel, the proposed encryption scheme updates the parameters of gamma-gamma distribution, used to generate irradiance samples for cumulative distribution function-based determination of the key, every T_c seconds and as such the final key is shaped by the atmospheric turbulence channel. We also describe a scheme that randomly selects one of several available paths in which the simultaneously measured irradiance samples, after interleaving, are used to generate the raw key. The secret-key rates of the proposed schemes are orders of magnitude higher compared to corresponding traditional QKD and source type physical-layer security schemes and are comparable with the state-of-the-art optical communication data rates.

Index Terms: Physical-layer security, Quantum key distribution (QKD), Post-quantum cryptography, Information theoretic security, Computational security.

1. Introduction

The quantum key distribution (QKD) employs the concepts from quantum information theory, in particular no-cloning theorem and theorem on indistinguishability of arbitrary quantum states, to realize the distribution of keys whose security is guaranteed by the fundamentals physics' laws [1]-[4], rather than unproven mathematical assumptions used in computational security [5],[6]. The research in QKD gets expanded, with the first satellite-to-ground QKD demonstration [2] giving the momentum to this research. Nevertheless, there are several barriers that need to be overcome prior to its widespread applications. As an illustration, the secret-key rate (SKR) and achievable distance are both limited by the channel loss, which is dictated by the rate-loss tradeoff. To overcome these problems, among others, the following two approaches have become relevant: (i) introduction of the trusted relays concept [7] and (ii) quantum relays development [8]. Unfortunately, the trusted relays' concept assumes that the relay between any two nodes in the optical network can be trusted, which is difficult to ensure and verify in practical applications. On the other hand, the quantum relays require the employment of quantum memories of long-duration and entanglement distribution of high-fidelity.

As an alternative to QKD, the post-quantum cryptography (PQC) has been advocated in numerous papers [9]-[12] and various governmental agencies, such as [13]. The PQC algorithms are thought to be secure against attacks initiated by quantum computers. Unfortunately, similarly to computational security, there is no evidence that these algorithms cannot be breached by more sophisticated quantum algorithms. As an illustration lattice cryptography algorithms often employ the collision resistance hash functions, such as the following one: $\boldsymbol{u}=\mathbf{A}\boldsymbol{x}$, with $\boldsymbol{x}$ being Alice private vector, $\boldsymbol{u}$ being Alice public vector, and $\boldsymbol{A}$ being $m\times n$ public matrix describing the lattice, with columns representing the basis vectors of the lattice. Eve needs to perform an efficient quantum matrix inversion algorithm, similar to the Harrow-Hassidim-Lloyd (HHL) algorithm [14], to determine the Alice's private vector by $\boldsymbol{u}=\boldsymbol{A}^{-1}\boldsymbol{x}$ and thus break the PQC protocol. The HHL algorithm provides an exponential speed-up over corresponding classical algorithms. To overcome the main problems of both QKD and PQC protocols, someone may want to use the hybrid QKD-PQC protocols [15], however, the complexity of such approach is high.

The second alternative to full-scale QKD will be to employ the restricted eavesdropping concept introduced in [16]. This concept is applicable for terrestrial and satellite-to-satellite secure communications, but it is challenging to apply it in satellite-to-ground secure communication, because of large diffracted beam size at the ground station.

The third alternative would be to apply the physical-layer security (PLS) concepts [3], popular in both wireless communications [17],[18] and free-space optical (FSO) communications [19],[20]. In par-

ticular, secret key agreement (generation) protocols [21],[22] have similarity with QKD protocols [3]. Two types of models are typically considered for secret-key agreement [21]: (i) *source-type model*, wherein Alice and Bob observe the correlated outputs of the sources of randomness (not controlled by legitimate parties and Eve); and (ii) the *channel-type model*, in which Alice (or Bob) transmits random symbols to Bob (or Alice) with the help of a broadcast channel. The wireless channels themselves can serve as sources of common randomness [22]-[24]. On FSO communication side, the atmospheric turbulence channels themselves have been studied as the source of common randomness as well [25]-[28]. In [25] authors used the randomness in the phase change introduced by turbulent channel and reported secret-key rates in order of 10s bits/s. In [26],[27] authors use the fluctuations in beam intensity (scintillation) as the common source of randomness. Finally, in [28] authors also employ scintillation to generate secure key, employ channel state information to discard symbols being in deep fade, and demonstrate SKRs of few 10 kb/s. Given that SKR can be represented as the product of the secrecy fraction and raw key rate [3], which is ~$1/T_c$, with T_c being coherence time, the long coherence time limits the ultimate SKR. Because the coherence time of atmospheric turbulence channels ranges from few μs to 10 ms, the corresponding SKRs are orders of magnitudes lower than data rates used in contemporary optical digital communications [29].

To overcome various problems of QKD, PQC, and PLS protocols, in this paper we propose a different strategy. Given the low raw key rates, dictated by long coherence time of atmospheric turbulence channels for source type secret-key generation (SKG) protocols, we propose to employ the atmospheric turbulence measurements as a source of randomness only to initialize the corresponding SKG protocol, while adjusting the parameters of the protocol based on time-varying FSO channel conditions. On such a way we are limited by long coherence time of turbulence channel only in initialization stage, which is used to initialize parameters for secret key generation. This SKG scheme updates the parameters of gamma-gamma distribution, used to generate irradiance samples for cumulative distribution function-based determination of the key, every T_c seconds, based on turbulence channel conditions, and as such the final key is shaped by the atmospheric turbulence channel. Similarly to the QKD, the secure key is dictated by the physics of the turbulent channel. We also describe the encryption scheme that employs multiple turbulence paths, randomly selected, to get the irradiance samples which are after interleaving used to create the raw key.

The paper is organized as follows. In Sec. 2, we describe the proposed atmospheric turbulence controlled SKG protocol. In Sec. 3, we describe the model and report some illustrative secret-key capacity results. The relevant concluding remarks are provided in Section 4.

2. Description of Proposed Atmospheric Turbulence-controlled SKG Protocol

The simplified version of the bidirectional FSO system to be used in proposed atmospheric turbulence-controlled secret-key generation protocol is provided in Fig. 1. Alice (Bob) sends the CW laser beam with the help of compressing telescope over the time-varying atmospheric turbulence channel. On receiver side, Bob (Alice) after the compressing telescope and beam splitter detects the received optical signal by using either direct detection or coherent detection receiver. With direct detection, the fluctuations in intensity (scintillation) can be used as the common source of randomness. With coherent detection variations in amplitude and phase difference can be both used as the sources of randomness and be selected in a random fashion. To facilitate explanations, let us describe the direct detection version of the setup with more details.

Because of the simultaneous transmission, the reciprocity principle will be satisfied, and Alice and Bob received signals in electrical domain can be represented, respectively, by:

$$\begin{aligned} r_A &= RP_{Tx}I + w_A, \\ r_B &= RP_{Tx}I + w_B, \end{aligned} \tag{1}$$

where I is the irradiance over FSO link, identical for both Alice and Bob; R is photodiode responsivity, P_{Tx} is the average transmitted power, and w_A (w_B) represents the noise sample in Alice (Bob) channel dominated by the transimpedance amplifier (TIA) used after the photodetector in optical receiver, which is a zero-mean white Gaussian noise of variance σ^2. The instantaneous electrical signal-to-noise ratio (SNR) is given by:

$$\gamma = \frac{P_{Tx}^2 R^2 I^2}{\sigma^2}. \tag{2}$$

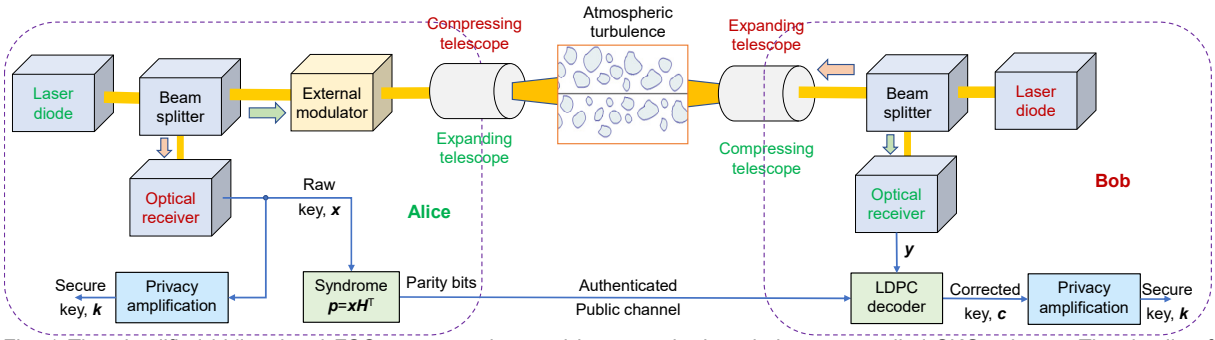

Fig. 1 The simplified bidirectional FSO system to be used in atmospheric turbulence-controlled SKG scheme. The details of postprocessing (information reconciliation and privacy amplification) are provided as well.

Because we used CW laser beam (unmodulated carrier), the transmitted power is constant. Given high directivity of the beam, and the employment of the expanding and compressing telescopes, we can control the beam size on receiver side, and we do not need to use the training sequence to estimate the channel, which is common in omnidirectional wireless links [22]. Based on intensity fluctuations, Alice and Bob can estimate the parameters of the channel such as scintillation index, coherence time T_c, parameters of the probability density function (PDF) of irradiance, etc. We further assume that Alice and Bob use cameras at their transceivers sides to ensure that Eve is not located on transmitter and receiver sides. Eve can still locate her receiver in close proximity of the building but will experience different turbulence conditions and her irradiance I_E will be different so that her signal can be represented by:

$$r_E = R_E a P_{Tx} I_E + w_E, \tag{3}$$

where R_E is the photodiode efficiency of Eve's photodetector, a is the attenuation coefficient to account for the high directivity of the beam used by Alice and Bob. To compensate for this Eve can employ better optical receiver (higher R_E and low noise TIA amplifier). Therefore, the electrical SNR ρ_E in Eve's channel will be different from that in Alice (Bob) channel. Moreover, Eve may even want to employ the semi-classical receiver. Clearly, this system is compatible with source-type SKG scenario [3],[21] since the turbulence channel is used as the source of common randomness. However, in this particular scenario Alice and Bob outcomes will be highly correlated, which is not true for Eve's outputs. After quantization, preferably the cumulative distribution function (CDF) based quantization, Alice and Bob's binary sequences will be highly correlated. Nevertheless, the Gaussian noise and quantization noise can still introduce the errors and Alice and Bob's sequences can still differ in certain number of bits. Alice and Bob should then perform error (information) reconciliation to get the same corrected common sequence. For instance, the spatially coupled LDPC coding-based information reconciliation scheme proposed in [15] is excellent candidate to be used for this purpose. In this scheme, Alice will use a systematic LDPC code to get the parity bits and can transmit them using the same FSO system shown in Fig.1, but an extra external modulator is needed. Given that Alice and Bob will get new intensity realization every T_c seconds, it is possible to use the same system for error reconciliation between these realizations. Even though the Eve's intensity sequence is not highly correlated with corresponding Alice and Bob's sequences, Alice and Bob should still perform privacy amplification, as described in [3], to ensure that their common sequence is secure. Contrary to the conventional SKG schemes, this common secure sequence will not be used as a common key, but instead to initialize the proposed cryptosystem. Our *basic cryptosystem* employs the best available random number generator (be generated in software or hardware) to create a truly random key, which is then used to encrypt data and then immediately destroyed, and this random number generator needs to be initialized. So the key idea is to use the secure sequence obtained as described above to initialize true random number generators used by Alice and Bob. Once the key is generated by Alice and Bob and used to encrypt arbitrary sequence to be transmitted, Alice and Bob will take next portion from the common secure sequence to re-initialize the random number generators for the next key. Periodically, Alice will send reference numbers obtained by encrypting a portion of the common secure sequence to re-

authenticate the communicating parties. This scheme assumes that synchronism between Alice and Bob is established before the protocol takes place. This can be done by transmitting the known reference sequence from Alice to Bob and by applying the cross-correlation method. The basic cryptosystem scheme's security is based on assumption that the best available random number generator is not deterministic. However, the basic scheme neither stores the keys nor exchanges them so it is significantly more difficult to break compared to the conventional encryption schemes.

Now we describe another, advanced, *encryption scheme* that is *controlled by the atmospheric turbulence*. The initialization is the same as in basic encryption scheme, described in previous paragraph, but the common secure sequence is used to select the seeds to be used to generate the samples from gamma-gamma PDF, characterized by two parameters α and β, which will be described below. Every T_c seconds Alice and Bob get new channel realizations, which are used to determine the parameters of gamma-gamma distribution. Based on the seed taken from the common secure sequence, Alice and Bob generate samples from corresponding gamma-gamma distribution and use the CDF to determine the corresponding bit to be used for secure key. The samples get generated from this PDF until new channel realization is received, when generation continues but with new α and β parameters. Like in the basic scheme, Alice will send to Bob the reference numbers for authentication purpose. Once the secure key sequence of sufficient length is generated, it is used in one-time pad encryption and the key is immediately destroyed. The procedure is repeated for the new secure key. The key advantage of this protocol, compared to conventional approaches [26]-[28], is that it can operate at much higher rates, compatible with the state-of-the-art optical communications, but the key is shaped by the atmospheric turbulence channel. Similarly to entanglement assisted QKD schemes, the key is truly random, it is not known to either Alice or Bob until the sufficient number of measurements are performed on the turbulent channel. The security of this advanced scheme is comparable to that of QKD for individual (incoherent) attacks. The details of postprocessing steps, information (error) reconciliation and privacy amplification, are provided as well. Here we assume that the direct reconciliation is used. By using a systematic (n,k) LDPC code, the $(n-k,n)$ parity-check matrix $\boldsymbol{H}$ is used to get the parity bits by $\boldsymbol{p}=\boldsymbol{x}\boldsymbol{H}^{\mathrm{T}}$. The parity-bits get transmitted over an authenticated public channel. For instance, the same FSO link can be used for this purpose. Alternatively, given that for high code rates the number of parity-bits can be much smaller that the number of information bits, an RF link can be used for this purpose. On Bob's side, these parity bits will be combined with Bob's channel samples $\boldsymbol{y}$, and after LDPC decoding the corrected key $\boldsymbol{c}$ will be obtained. The corresponding modified LDPC decoder is provided in [3] (see page 129). Then both Alice and Bob perform privacy amplification (see Section 4.7 in ref. [3] for additional details) to remove any correlation with Eve's sequence and thus get the same secure key $\boldsymbol{k}$. The advanced encryption scheme can be combined with QKD as follows. We can use the QKD to initialize the protocol. Low key rate of QKD is not of concern anymore since it is used only in initialization stage.

Someone may claim that the use of the Gamma-Gamma PDF to generate the samples of irradiance, with parameters dictated by the FSO channel, may represent a security bottleneck. The need for generating the irradiance samples from PDF can be avoided by employing several alternative FSO paths. Namely, in addition to the line-of-sight path shown in Fig. 1 we can create the additional FSO paths with the help of properly selected mirrors. With the help of an optical space switch we can select the FSO path in random fashion, while still using one transceiver per participating party (Alice and Bob). For each path Alice and Bob will measure the instantaneous irradiance that will contribute to the raw key. Once sufficient number of raw bits get collected, Alice and Bob apply the same random interleaver followed by the conventional postprocessing steps as described in previous paragraph.

3. The Model and Illustrative Numerical Results

To describe the fluctuations in irradiance due to atmospheric turbulence, the gamma-gamma distribution is used in this paper, because it matches well experimental measurements, and is applicable to all turbulence regimes, ranging from the weak turbulence to the saturation regime [29]-[31]. Based on Eq. (2), by applying transforming random variable method, we obtain the following distribution of instantaneous SNR γ:

$$f(\gamma)=\frac{(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)}\left(\frac{\gamma}{\gamma_0}\right)^{\frac{\alpha+\beta}{4}-1}K_{\alpha-\beta}\left(2\sqrt{\alpha\beta\sqrt{\frac{\gamma}{\gamma_0}}}\right), \tag{4}$$

where α and β are the atmospheric turbulence parameters defined below, γ_0 is the average electrical SNR defined as:

$$\gamma_0=\frac{R^2P_{Tx}^2E[I]^2}{\sigma^2}=\frac{R^2P_{Tx}^2}{\sigma^2}, \tag{5}$$

where we used the fact that the irradiance *I* is normalized so that the expectation is one, i.e. *E*[*I*]=1. In Eq. (4), we use $\Gamma(\cdot)$ to denote the gamma function and $K_n(\cdot)$ to denote the *n*-th order modified Bessel function of the second kind. The atmospheric turbulence parameters α and β (for zero inner scale) are defined, respectively, as:

$$\alpha=\left\{\exp\left[\frac{0.49\sigma_R^2}{\left(1+1.11\sigma_R^{12/5}\right)^{7/6}}\right]-1\right\}^{-1},\ \beta=\left\{\exp\left[\frac{0.51\sigma_R^2}{\left(1+0.69\sigma_R^{12/5}\right)^{5/6}}\right]-1\right\}^{-1}, \tag{6}$$

wherein we use σ_R^2 to denote the Rytov variance, which is defined as:

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

with C_n^2 being the refractive structure parameter, *k* is the wave number ($k=2\pi/\lambda$, with λ being the wavelength), and *L* is the propagation distance. The Rytov variance is commonly used as an indicator of the atmospheric turbulence strength. The weak fluctuations are associated with $\sigma_R^2<1$, medium with $\sigma_R^2\approx 1$, the strong with $\sigma_R^2>1$, and the saturation regime is defined by $\sigma_R^2\to\infty$ [31]. The corresponding CDF of instantaneous SNR is given by :

$$CDF(\gamma)=\frac{1}{\Gamma(\alpha)\Gamma(\beta)}G_{1,3}^{2,1}\left(\alpha\beta\sqrt{\frac{\gamma}{\gamma_0}}\middle|\begin{matrix}1\\ \alpha,\ \beta,0\end{matrix}\right), \tag{8}$$

where $G_{c,d}^{a,b}(\cdot)$ is the Meijer's G-function [32],[33].

Let us first observe the cryptosystem in which the secret key is generated by using the atmospheric turbulence channel as the common source of randomness, which is used in initialization stage of our proposal. The corresponding secret-key capacity results, for one-way communication, are summarized in Fig. 2, for different turbulence strengths. We observe a realistic scenario when Eve faces similar turbulence conditions, but the parameters characterizing the turbulence might not be the same. The SNR in Alice (Bob) channel and in Eve's channel might not be the same as well. To characterize this, the ratio ρ in average SNRs for Alice (Bob) and Eve's channels is used as a parameter, which is defined as $\rho=\gamma_0/\gamma_{0,\mathrm{Eve}}$. Based on refs. [3],[21] the secret-key capacity C_{SK}, for one-way communication, is determined by:

$$C_{SK}=\max\left[I(X,Y)-I(X,Z),I(Y,X)-I(Y,Z)\right], \tag{9}$$

where X^N, Y^N, and Z^N are sequences (of length *N*) obtained by Alice, Bob, and Eve, respectively; by measuring the atmospheric turbulence channel.

The case with Rytov standard deviation $\sigma_R = 0.2$ (Rytov variance 0.04), provided in Fig. 2(a), is related to the weak turbulence regime, with the corresponding parameters of gamma-gamma distribution being α=51.913 and β=49.113. The case with Rytov standard deviation $\sigma_R = 1$, shown in Fig. 2(b), is related to the medium turbulence regime, while the corresponding parameters of gamma-gamma distribution are α=4.3939 and β=2.5636. Further, the case with Rytov standard deviation $\sigma_R = 3$ (Rytov variance 9), see Fig. 2(c), belongs to the strong turbulence regime, with the corresponding parameters of gamma-gamma distribution being α=5.485 and β=1.1156. Finally, the case with Rytov standard deviation $\sigma_R = 10$ (Rytov variance 100), provided in Fig. 2(d), is related to the saturation regime, while the corresponding parameters of gamma-gamma distribution are α=14.11 and β=1.0033. When the average SNR in Eve's channel is either higher or comparable to that that in Alice (Bob) channel, the turbulence helps a lot in improving secret-key capacity. On the other hand, when SNR in Eve's channel is 6 dB lower than that in Alice channel, the improvement is negligible. Eve's imperfect knowledge of Alice (Bob) turbulence condition does not help much in improving the secret key-rate, except for SNRs in Alice's channel higher than 8 dB, in weak and medium turbulence regimes.

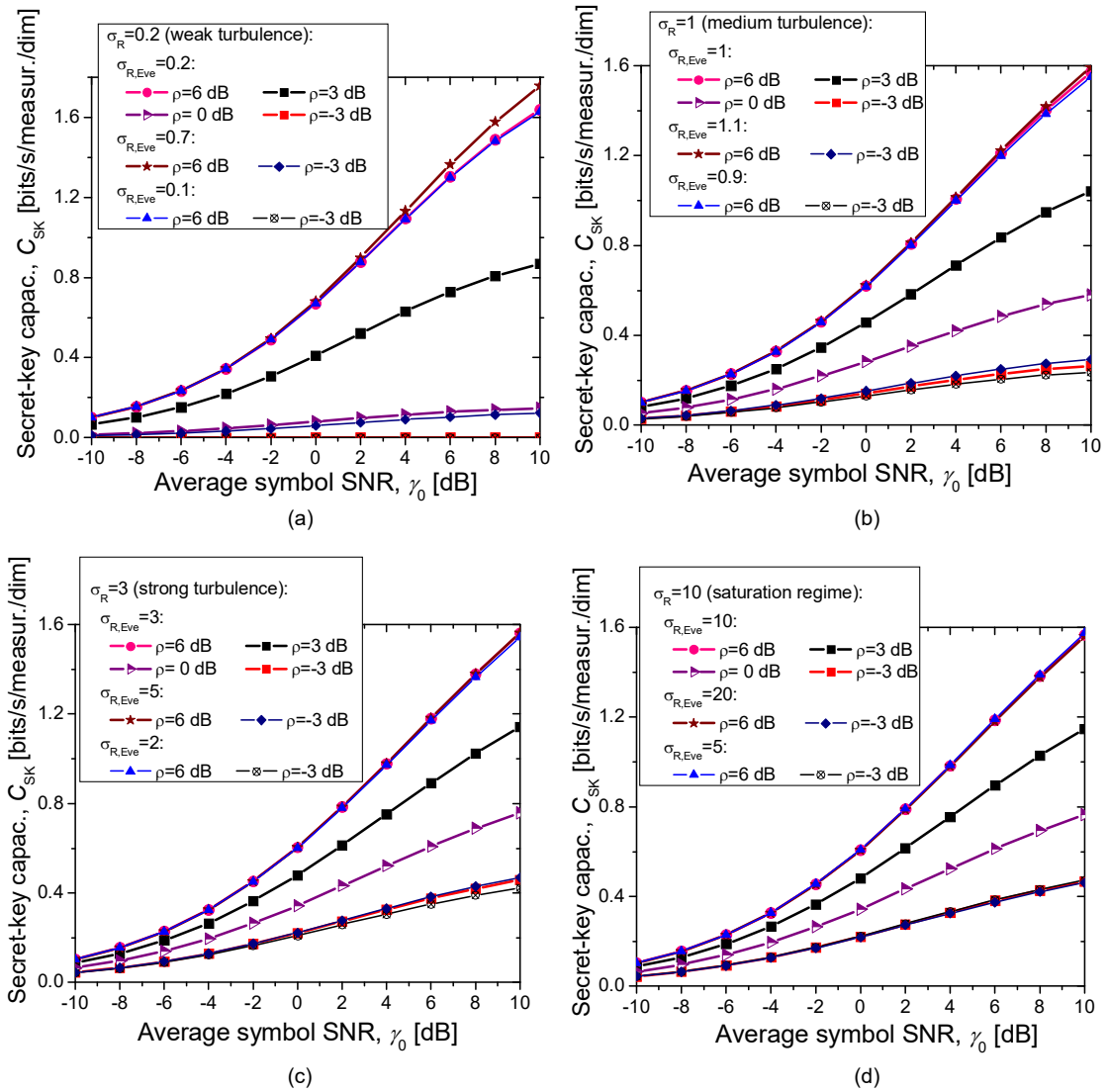

Fig. 2 The secret-key capacity results when atmospheric turbulence channel is used as the common source of randomness, for different turbulence strengths: (a) weak turbulence, (b) medium turbulence, (c) strong turbulence, and (d) saturation regime.

After initialization, in the proposed atmospheric turbulence condition controlled cryptosystem, the measured intensity fluctuations are used only to determine gamma-gamma distribution parameters α and β, while the corresponding irradiance sequences generated by Alice and Bob, denoted by $\{I_A\}$ and $\{I_B\}$, are highly correlated given that they use the same seed from common secret sequence obtained in initialization stage. The correlation coefficient between Alice and Bob, therefore, tends to 1, namely:

$$\rho_{AB} = \frac{E(I_A I_B) - E(I_A)E(I_B)}{\sigma_A \sigma_B}\bigg|_{I_A = I_B = I} = \frac{E(I^2) - E(I)^2}{\sigma_A^2} = \frac{1 + \frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\alpha\beta} - 1}{\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\alpha\beta}} = 1, \tag{10}$$

where we used the following two expressions derived from gamma-gamma PDF:

$$E(I^2) = 1 + \frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\alpha\beta}, \quad \sigma_I^2 = \frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\alpha\beta}. \tag{11}$$

On the other hand, given that Eve $\{I_E\}$ and Alice's $\{I_A\}$ irradiance sequences are independent we have that $E\{I_A I_E\} = E\{I_A\}\, E\{I_E\}$ yielding to the zero-correlation coefficient, that is:

$$\rho_{AE} = \frac{E(I_A I_E) - E(I_A)E(I_B)}{\sigma_A \sigma_E} = \frac{E(I_A)E(I_B) - E(I_A)E(I_B)}{\sigma_A \sigma_E} = 0. \tag{12}$$

This indicates that the secret-key rate in the proposed scheme is comparable to the achievable information rate over the corresponding channel Allice and Bob communicate with the common encrypted key. Alice and Bob can use the fiber-optics channel to exchange their encrypted data to get ultra-high data rates. In this case the secret-key rate will be determined by the available electronics.

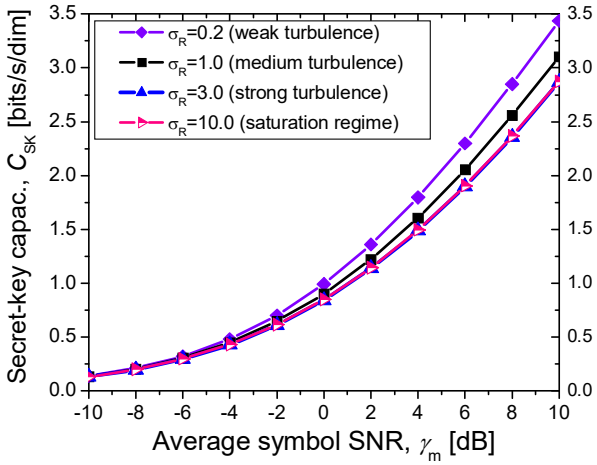

Fig. 3 The secret-key capacity over FSO channel against the SNR in the main channel, when the proposed encryption scheme is used, for different turbulence strengths.

If Alice and Bob decide to use the same FSO channel as in Fig. 1 to transmit their encrypted data (with corresponding external modulators being inserted), the secret-key rates that needed to be generated should follow the Fig. 3. Clearly, significantly higher secret-key capacities are possible when the proposed atmospheric turbulence-controlled cryptosystem is used, when compared to the traditional approaches.

4. Concluding Remarks

To overcome various problems of QKD, PQC, and PLS protocols, we have proposed to employ the source type PLS scheme, utilizing the turbulent channel as the source of randomness, only in initialization stage.

Given the low raw key rates, dictated by long coherence time of atmospheric turbulence channels for source type secret-key generation protocols, we have proposed to adjust the parameters of the protocol based on time-varying FSO channel conditions. After the coherence time T_c elapses, Alice and Bob receive new channel realizations, which are further used to determine the parameters of gamma-gamma distribution. This gamma-gamma PDF is used to generate irradiance samples for CDF-based determination of the key. The irradiance samples get generated from this gamma-gamma PDF until new channel realization is received, when generation continues but with updated gamma-gamma PDF parameters. The proposed encryption has not been limited by the long coherence time of turbulence channel, while secret key between Alice and Bob has been shaped by the atmospheric turbulence channel. We have also described a scheme that randomly selects one of several available paths in which the simultaneously measured irradiance samples, after interleaving, have been used to generate the raw key. This scheme does not require the PDF to generate the raw key. The achievable secret key rates, for the proposed cryptosystem, are orders of magnitude higher than that in corresponding QKD and PLS schemes.

In addition to the optical channels, this concept is applicable in mm-wave and THz channels, as well as in 5G/6G systems employing highly directive links achieved by massive MIMO approaches.

References

[1] G. van Assche, Quantum Cryptography and Secrete-Key Distillation. Cambridge-New York: Cambridge University Press, 2006.

[2] S.-K. Liao, *et al*., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[3] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer, 2019.

[4] Z. Qu, I. B. Djordjevic, "Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels," *IEEE Photonics Journal*, vol. 9, no. 6, p. 7600408, Dec. 2017.

[5] B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. Indianapolis, IN: John Wiley & Sons, 2015.

[6] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, Second Edition. Boca Raton, FL: CRC Press, 2015.

[7] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, Apr. 2014.

[8] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, Nov. 2001.

[9] D. J. Bernstein, J. Buchmann, E. Dahmen, *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009.

[10] D. J. Bernstein, "Grover vs. McEliece,'" in *Post-Quantum Cryptography–PQCrypto* (Lecture Notes in Computer Science), vol. 6061, N. Sendrier, Eds. Berlin, Germany: Springer, 2010.

[11] M. Baldi, F. Chiaraluce, and M. Bianchi, "Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes," *IET Inf. Secur.*, vol. 7, no. 3, pp. 212–220, Sep. 2013.

[12] P. Branco, P. Mateus, C. Salema, A. Souto, "Using Low-Density Parity-Check codes to improve the McEliece cryptosystem," *Information Sciences*, vol. 510, pp. 243-255, Feb. 2020,

[13] NIST, Post-quantum cryptography PQC, available at: https://csrc.nist.gov/projects/post-quantum-cryptography

[14] A. W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for solving linear systems of equations," *Phys. Rev. Lett.*, vol. 103, Art. no. 150502, Mar. 2009.

[15] I. B. Djordjevic, "Joint QKD-Post-Quantum Cryptosystems," *IEEE Access*, vol. 8, pp. 154708–154712, 24 August 2020.

[16] Z. Pan, K. P. Seshadreesan, W. Clark, M. R. Adcock, I. B. Djordjevic, J. H. Shapiro, S. Guha, "Secret-Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping," *Physical Review Applied*, vol. 14, no. 2, Article ID 024044, 2020. (Published 17 August 2020.)

[17] H. V. Poor, R. F. Schaefer, "Wireless physical layer security," *PNAS*, vol. 114, no. 1, pp. 19-26, 2017.

[18] X. Zhou, L. Song, Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton·London·New York: CRC Press, 2014.

[19] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, Art. ID 7901014, Apr. 2015.

[20] X. Sun, I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, Art. ID 7901110, Feb. 2016.

[21] R. Ahlswede I Csiszár, "Common randomness in information theory and cryptography-part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39 no. 4, pp. 1121–1132, 1993.

[22] L. Lai, Y. Liang, H. V. Poor, W. Du, “Key generation from wireless channels,” in X. Zhou, L. Song, Y. Zhang (Eds.), *Physical Layer Security in Wireless Communications*, Boca Raton·London·New York: CRC Press, pp. 47-68, 2014.
[23] R. Wilson, D. Tse, R. A. Scholtz, “Channel identification: Secret sharing using reciprocity in ultrawideband channels,” *IEEE Trans. Inf. Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.
[24] C. Ye, S. Mathur, A. Reznik, W. Trappe, and N. Mandayam, “Information theoretic key generation from wireless channels,” *IEEE Trans Inf. Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.
[25] M. D. Drake, C. F. Bas, D. R. Gervais, P. F. Renda, D. Townsend, J. J. Rushanan, J. Francoeur, N. C. Donnangelo, M. D. Stenner, “Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance,” *Opt. Eng.*, vol. 52, no. 5, Art ID. 055008, 29 May 2013.
[26] N. Wang, X. Song, J. Cheng, and V. C. Leung, “Enhancing the security of free-space optical communications with secret sharing and key agreement,” *J. Opt. Commun. Netw.*, vol. 6, no. 12, pp. 1072–1081, 2014.
[27] C. Chen and H. Yang, “Shared secret key generation from signal fading in a turbulent optical wireless channel using common-transverse-spatial-mode coupling,” *Opt. Express*, vol. 26, pp. 16422-16441, 2018.
[28] H. Endo, M. Fujiwara, M. Kitamura, O. Tsuzuki, R. Shimizu, M. Takeoka, M. Sasaki, “Free-space optical secret key agreement with post-selection based on channel state information,” *Proc. SPIE 11153, Environmental Effects on Light Propagation and Adaptive Systems II*, Article ID 111530K, 9 October 2019.
[29] I. B. Djordjevic, *Advanced Optical and Wireless Communications Systems*. Cham, Switzerland: Springer International Publishing, 2017.
[30] M. A. Al-Habash, L. C. Andrews, R. L. Phillips, “Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media,” *Opt. Eng.*, vol. 40, no. 8, pp. 1554-1562, 2001.
[31] L. C. Andrews, R. L. Philips, *Laser Beam Propagation through Random Media*, 2nd Ed. Bellingham, Washington: SPIE Press, 2005.
[32] M. Petkovic, G. T. Djordjevic and I. B. Djordjevic, “Analysis of mixed RF/FSO system with imperfect CSI estimation,” in Proc. *2017 19th International Conference on Transparent Optical Networks (ICTON)*, Article ID Mo.C2.1, Girona, 2017, pp. 1-7.
[33] I. Gradshteyn and I. Ryzhik, *Table of Integrals, Series, and Products*, 5th ed. New York, NY, USA: Academic, 1994.