# Hybrid MPPM-BB84 Quantum Key Distribution Over FSO Channel Considering Atmospheric Turbulence and Pointing Errors

Nancy Alshaer, Mohamed E. Nasr, and Tawfik Ismail

***Abstract*—Nowadays, a high level of security is required for the transmission of critical information. Quantum Key Distribution (QKD) systems are considered the best option to protect such information. Many studies have shown the efficiency of the QKD optical fiber inspired by M-ary pulse position modulation (MPPM). Free-Space Optical (FSO) links provide an efficient and effective data transmission system. However, cumulative effects of laser beam divergence, misalignment, and turbulence-induced fading on the received irradiance in the FSO link might allow an external eavesdropper located near the authorized receiver to break the transmission under certain conditions. This paper introduces the development of an FSO system based on the MPPM and the BB84 protocol (MPPM-BB84) over the Gamma-Gamma (GG) turbulence channel with pointing errors. Time Binning is implemented using MPPM to increase system security and reduce the quantum bit error rate (QBER). The system security is investigated under photon number splitting attack and excess noise. Closed-form expressions for asymptotic expressions of the average symbol error probability (SER), raw key rate (RKR), and secret key rate (SKR) are introduced. Moreover, the Monte-Carlo simulations are then used to prove the validity of the analytical results. The optimal values for the average photon number per pulse (to achieve the maximum RKR and SKR) for each symbol length can guarantee the stability of the FSO system under different weather conditions. Smaller symbol lengths are more tolerant of detector loss. The proposed system supports linking distances from 1 km to 3 km while keeping the SKR almost constant.**

***Index Terms*—Quantum key distribution (QKD), M-ary pulse position modulation (MPPM), Gamma-Gamma turbulence, BB84 protocol, secret key, bosonic channel, poisson distribution, photon number splitting (PNS).**

## I. Introduction

FREE space optical (FSO) communication provides line-of-sight (LoS) connection between two fixed points (transmitter and receiver) using an optical carrier in the near-infrared (IR) band. So, it has a very high optical bandwidth, which allows for such high data rates. Other advantages include quick and easy deployment, license-free spectrum, lightweight, and low power requirements. FSO communication link is helpful in many situations, such as disaster recovery, last-mile access, and fiber failure, besides its application in military, remote sensing, radio astronomy, and backhaul for wireless cellular networks. The systems provide a variety of links either in Earth's atmosphere (terrestrial links) or between Earth and space (Earth-to-satellite/satellite-to-Earth links) and even in space (inter-satellite links). Despite the previously mentioned advantages, the performance of FSO systems is limited by atmospheric effects such as absorption, scattering, and turbulence besides pointing errors due to misalignment between the transmitter (Tx) and the receiver (Rx). Those effects deteriorate the quality of the optical signal, causing a decrease in the bit error rate (BER) performance, or sometimes result in complete link failure [1], [2]. Several statistical models have been proposed to represent the atmospheric turbulence, for example, k-distribution uses for strong turbulence condition, Gamma-Gamma distribution uses for moderate-to-strong turbulence, Log-Normal distribution represents weak-to-moderate turbulence and a general model known as Málaga [3].

The growing demand for high data and secure communication systems contributes to integration between FSO systems and quantum key distribution (QKD) protocols. In contrast to conventional cryptographic protocols, where the security is based on theoretical assumptions of computational complexity, the security of QKD protocols relies on quantum mechanics of physical laws that allow it to provide unconditional security. In QKD, two remote entities can establish and share a secret key over a quantum channel, which can be an optical fiber or free space. Once the key generated, it can be subsequently utilized in a symmetric cipher, such as the one-time pad or one of the modern symmetric ciphers, to transmit information over a public classical authenticated channel securely. The first QKD protocol known as BB84 was proposed by Bennett and Brassed in 1984 [4]. Since then, many QKD schemes have been proposed based on different coding techniques. Examples include phase coding [5], frequency coding [6], and time-coding [7].

The BB84 is classified as a discrete-variable quantum-key-distribution (DV-QKD) protocol where the critical information encodes by employing the discrete variables of a quantum state, such as the phase or polarization of a single photon and the detection is achieved using single-photon detection techniques. On the other hand, continuous-variable quantum-key-distribution (CV-QKD) protocol encodes the information onto the continuous variables such as phase and amplitude quadrature

Manuscript received August 24, 2021; revised October 4, 2021; accepted October 11, 2021. Date of publication October 14, 2021; date of current version October 28, 2021. This work was supported by Science, Technology & Innovation Funding Authority of Egypt under Grant 38121. *(Corresponding author: Tawfik Ismail.)*

Nancy Alshaer and Mohamed E. Nasr are with the Department of Electronics and Electrical Communication, Faculty of Engineering, Tanta University, Gharbiya 31527, Egypt (e-mail: n.a.alshaer@f-eng.tanta.edu.eg; mohamed.nasr@f-eng.tanta.edu.eg).

Tawfik Ismail is with the Department of Engineering Applications of Laser, National Institute of Laser Enhanced Sciences, Cairo University, Giza 12613, Egypt, and also with the Wireless Intelligent Networks Center, Nile University, Giza 16453, Egypt (e-mail: tismail@niles.cu.edu.eg).

Digital Object Identifier 10.1109/JPHOT.2021.3119767

of coherent states of light, and the detection is accomplished by coherent detection techniques (homodyne/heterodyne). So, CV-QKD is implemented much easier and cheaper than DV-QKD based on mature telecommunication components. It generates key rates higher than DV-QKD in low-loss channels [8]. The CV-QKD protocol was first described by Timothy Ralph in 1999, then Cerf, and Assche [9] have proposed several modifications. Unlike the previous two schemes, the distributed-phase-reference (DPR)-QKD uses the phase difference between two successive signal pulses or the photon arrival times to encode the critical information [10]. All these protocols are prepare and measure (PM) in the sense that the encoded pulses are sent from the Tx, Alice, to the Rx, Bob, who decodes the pulses as required by the determined protocol. Conversely, in entanglement-based (EB) protocols, Alice and Bob receive parts of entangled photons and execute appropriate measurements. Artur Ekert proposed the first EB protocol in 1991, Known as E91, based on Bell's theorem and employing entanglement photons rather than single photons [11].

M-ary pulse position modulation (MPPM) is one of the pulse time modulation techniques with superior power efficiency compared to other baseband modulation schemes. So, it appears to be the most suitable choice for a wide range of applications, especially those with handheld devices. In MPPM, there is no overlap between the pulses, so the MPPM symbols are orthogonal, which improves the system performance in terms of bit error rate (BER). In MPPM, the information is represented by the position of a pulse in a frame of fixed length ($M$-time slots), while the remaining slots are empty, and the data conveyed per frame is $\log_2 M$ bits [12]. So, MPPM provides advantages when implemented in BB84. First, it improves the utilization efficiency of weak laser pulses by also employing the empty pulses. Second, it allows retrieval of more than one bit from each detected photon, which increases the key generation rate. Poisson photon sources inherent in QKD systems limit its performance as multi-photon pulses reduce the connection security while the generation of single-photon pulses has low efficiency. MPPM is introduced as a promising solution to improve the efficiency of utilizing Poisson laser sources and hence the key generation rate [13], [14], [15]. Also, MPPM can eliminate the effects of detector dead time [16].

Time synchronization is one of the key challenges in implementing MPPM required (necessary) to reduce (eliminate) the timing offset between the Tx and Rx clocks. [17] concerned in achieving slot synchronization between MPPM pulses used in photon-limited optical channels via time estimation models considering both time and frequency modulation jitters. The proposed methods decreased the system probability of error. However, there was a trade-off between the complexity of the proposed estimation methods and the offset estimation accuracy. The inter-symbol guard times (ISGT) are utilized in deep space applications of optical MPPM communications to remove the back-to-back pulses, decreasing the hardware constraints. An estimation method depends on the ISGTs was proposed in [18] to infer the timing information. The ISGT synchronization method avoided the expense of the data rate for transmitting the pilot symbols compared with conventional methods. Considering asynchronous sampling at a sampling frequency of 1 slot of MPPM system [19] proposed a clock synchronization technique based on guard time. The proposed technique realized efficient synchronization within the scope of large timing offset, decreasing the system bit error rate.

Most of the existing studies of MPPM-QKD have considered the signal transmission over optical fiber rather than free space [13]–[20], [21], [22]. [14] proposed MPPM-BB84 protocol and evaluated its performance under different attack scenarios. In [15], the performance of the MPPM-QKD system has been analyzed, in terms of the raw key rate, using entanglement-photons taking into account photon transmission and detection losses. [21] introduced a novel phase-matching quantum key distribution (PM-QKD) protocol, named multiple pulses phase-matching (MPPM-QKD) protocol. The proposed protocol achieved a higher secret key generation performance over a 450 km fiber cable compared with round-robin differential phase shift quantum key distribution (RRDPS-QKD) with the same train (symbol) length and 200 km transmission distance. While [22] proposed and characterized the use of photon-added coherent states (PACS)-as a simple example of non-Gaussian states of light-in quantum (PPM) modulation. The proposed system exhibited improved performance in terms of error probability compared with a system employing classical states with the same energy and thermal noise. Given that the polarization encoding in fiber channels usually affects the phase encoding that induces briefing variations in the propagated signal [23], [24], [25]. These fluctuations cause a polarization drift, limiting the fiber reach and the transfer rate that meets performance conditions. Therefore, it could not be considered an efficient medium for discrete QKD protocols such as BB84, BBM92 and SARG04 that depend on modulating the information into the photon polarization state. So, it is more convenient to transmit the optical signal through free space instead of fiber when applying such protocols.

In this paper, we propose a complete system of BB84-MPPM over a terrestrial FSO channel. A combined effect of the turbulence channel and the quantum channel is demonstrated by integrating Gamma-Gamma and bosonic models. The Gamma-Gamma model is widely used in studying the impact of atmospheric turbulence, while the bosonic model describes the transmission of a light sent through space that loses energy in route from the transmitter to the receiver. We assumed that the two channels are independent, and therefore, we apply the superposition principles in the derived equations to calculate their effect. The bosonic channel model is responsible for computing the quantum channel effect on the transmitted qubits. The MPPM is also applied with the time bins concept to improve the performance of the transmission link by increasing the security and decreasing the quantum bit error rate. The MPPM has been considered as an effective power-efficient technique in optical communication systems. Due to the low energy transmitted by a weak laser source, which includes few photos, it is significant to improve the transmitted power to achieve 1) acceptable bit-error-rate, 2) longer distance, and 3) guaranteed secret key rate. In order to investigate the performance of the proposed system, closed-form expressions for 1) average and asymptotic symbol error rate and 2) raw key rate (RKR) and secret key rate (SKR) under photon number splitting (PNS) attack are derived. The effects of essential parameters such as transmit power, link distance, detector efficiency, modulation level, and weather conditions on the RKR and SKR are presented.

The rest of this paper is organized as follows. Section II represents the basic concepts and operation of the MPPM-BB84 protocol. The channel model and its related mathematical analysis are described in Section III, where the effect of two independent channels is assumed. The proposed system model is

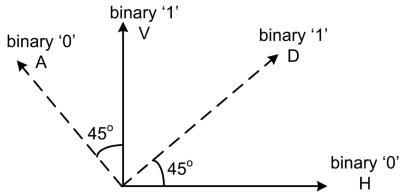


Fig. 1. BB84 polarization bases.

discussed in Section IV. In Section V, the proposed MPPM-BB84 FSO system metrics are theoretically analyzed, and closed-form expressions for raw key and secret key rates are derived under the PNS attack. Numerical results are expressed in Section VI. Finally, the paper is concluded in Section VII.

## II. Preliminaries

### A. BB84 Protocol

The BB84 protocol, based on the transmission of the quantum state of single photons, is the first protocol introduced to guarantee unlimited security. In this protocol, Alice prepares quantum bits (qubits) by encoding single photons into one of four orthogonal states horizontal (H), vertical (V), diagonal (D), and anti-diagonal (A). Whereas Alice randomly selects one of two conjugate bases to send classical bit values (e.g., 0 or 1) as shown in Fig. 1. Then she transmits the encoded qubit via the quantum channel to Bob. On the other side, Bob measures the photon using a randomly selected basis. If Bob measures the qubits in the same justification used by Alice, he will obtain a correct encoded bit. Otherwise, if he mismeasures the encoded bit providing an associate quantum bit error rate (QBER). This QBER is necessary to be introduced for such a system to determine the threshold of detecting an eavesdropper. Whereas, when an eavesdropper attempting to read qubits on the quantum channel, and because she does not know the encoding basis used by Alice and will try to guess and resend (intercept and resend attack), the value of QBER will increase. Therefore Alice and Bob will be able to know that Eve is attacking the quantum channel then they aborted the connection [4]. Furthermore, the perfect BB84 protocol (uses only single-photon) security against photon number splitting (PNS) attacks was guaranteed by the no-cloning theorem.

### B. Photon Number Splitting Attack

Security of the BB84-QKD protocol is highly dependent on the light source, which must be true single-photon. In the case of a single-photon transmission, Eve can not intercept individual photons sent from Alice to Bob due to the no-cloning theorem. On the other hand, in any practical device, multiple photons in a single pulse with some nonzero probability could be generated, which dramatic consequences on the security of the BB84 protocol [26]. The existence of more than one photon per pulse gives Eve a chance to gain information via a PNS attack and degrade the security of communication. In PNS, Eve could split and store a photon from a multi-photon pulse, and she performs measurement only after Bob and Alice have detected the corresponding basis information. This measurement technique is known as quantum non-demolition measurement (QND) that assumed to measure a number of photons without

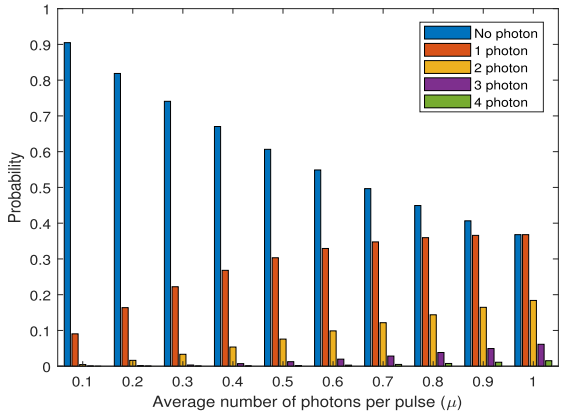


Fig. 2. Probability of photons generated per pulse.

disturbing the quantum state. In the presence of multi-photons, Eve can use an adjustable beam splitter and divide the photons into two parts one part follows Bob, and the other part is kept in her quantum memory. If Bob has access only to the average detection rate, not to the received photon statistics. Then, this attack will not introduce errors and hence can not be detected by Alice nor Bob, which completely violates the security of the system [27].

In practice, a single-photon source is not available, and it is often replaced by a weak laser source, which can be described as a coherent state. Whereas Alice generates a coherent state pulse, encodes its information, and randomizes each train pulse. The pulses emerged from the weak laser source follows a Poisson distribution as follow

$$P_i = e^{-\mu} \times \frac{\mu^i}{i!} \tag{1}$$

where $i$ is the photon number and $\mu$ is the mean photon number (the light intensity). The pulses can be categorized into two types: empty pulses (with zero photons) and nonempty pulses (with one or more photons) see Fig. 2. So, the weak laser sources are usually working at ($\mu < 0.5$) such that the probability of multi-photon pulses (two and more) is reduced [14], [28].

Due to weak coherent sources (multi-photon), the BB84 protocol is vulnerable to the PNS attack. The decoy-state method is more robust against the PNS attack. Therefore, it is applied as a countermeasure against vulnerabilities caused using coherent states of light for QKD protocols. Formal security proof of the decoy-state method against all possible attacks was introduced in [29], besides comparing two widely known attacks on multi-photon pulses: photon-number splitting and beam splitting. A key-rate optimization approach for the decoy-state BB84 QKD protocol is presented in [30] considering quantum channels with a significant amount of noise. The authors followed a more rigorous approach combining several linear and nonlinear programs to derive tighter protocol parameters and better key rates than previous approaches relying on heuristic assumptions.

### C. Key Distribution With MPPM Scheme

The average number of photons per pulse received by Bob affects by two main factors, namely, photon transmission losses (happen during photon propagation or PNS) and detection losses (due to detector imperfection). In the Poisson regime, the number of photons sent per channel is very low. The Poisson statistics

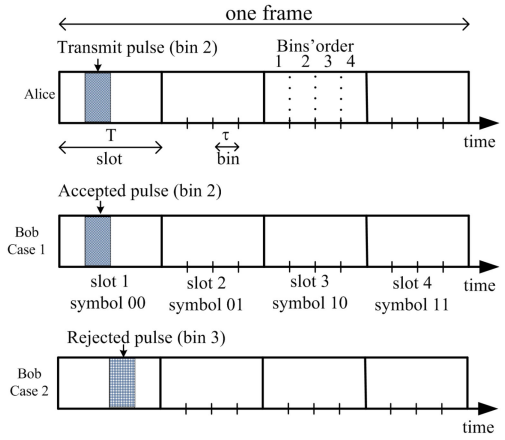


Fig. 3. The concept of time bins. A frame of length M = 4 slots and each slot has four bins.

effectively limit the channel output to a finite alphabet. However, even without any noise (dark current) or also if quantum-optical measurements are used rather than photon detection, the capacity still limited [13], [31]. MPPM is represented as a way to aid the task of coding such channels, which helps improve its finite capacity [15].

In MPPM, one frame has $M$ time slots, the occupied slot represents $\log_2 M$ bits, and the pulse occupies only one slot [32]. The time slot itself is divided into many sub-slots called bins to reduce the probability of attack success from Eve [33]. This requires reducing the pulse width to accommodate the bin time $\tau$ rather than the slot time $T$. This reduction in the pulse width, compared with a traditional frame, results in increased pulse power, enabling longer link distance. The procedure for generating the raw key is as follows. The frame number is used to communicate between Alice and Bob. The pulse (the photon) detected within a slot in a particular frame is utilized to generate a raw key of $\log_2 M$ bits, provided that it has the same bin number at Alice and Bob. The concept of time bins is presented in Fig. 3, where the pulse is assumed to compress by 25%. Consequently, it will occupy only a quarter of the time slot $T$. Therefore, the time slot has been divided into four bins. Assuming Alice sent her pulse in bin #2 if Bob detected the pulse in the same time bin as shown in Fig. 3(b), they will accept this transmission. However, if Bob detected the pulse at another time-bin (assuming bin #3) as shown in Fig. 3(c), they will discard this transmission. Finally, the raw keys are generated by the slot numbers of the accepted bins in the chosen frames [33], [34]. Such dynamic bin allocation and the increase in the energy of the pulse per time reduce the quantum bit error rate (QBER).

## III. Proposed System Model

The block diagram of the proposed FSO system with BB84-MPPM is shown in Fig. 4. The figure is divided into three parts, the transmitter, the channel, and the receiver. We describe the transmitter and the receiver in the following subsections, while the channel will be presented in detail in Section IV.

### A. The Transmitter

The data bit stream emits from the digital source at Alice is converted into MPPM symbols. Each symbol contains only one pulse located in different time slots within the symbol of length $M$. The slots are divided into bins, whereas the pulse compressed inside a time-bin rather than a time slot. This will increase the pulse power and decrease the opportunity of Eve to get data. The compressed pulse is directed pseudo-randomly to one of the four outputs of the demultiplexer. This output is used to modulate the intensity of the laser source. The driver circuit provides the driving current of the laser source and satisfies the non-negative condition of the signal. The attenuator in each path is tuned to weaken the power of the optical signal such that the average number of photons emitted per pulse is less than 0.5. The photon in the pre-selected path is polarized in one of two non-orthogonal bases (horizontal/vertical and $\pm 45^\circ$ shown in Fig. 1), where the half-wave plate (HWP) will shift the direction of the linearly polarized photons by $45^\circ$. The Tx telescope is used to adjust the beam waist and the divergence angle. Also, it helps to produce a parallel optical beam to be transmitted over space. Finally, the polarized photons are sent to Bob through the quantum channel.

### B. The Receiver

At the receiver, a telescope is used to capture the optical signal that will be divided by the non-polarizing beam splitter (NPBS) by a certain percentage without affecting the polarization states. The polarization of the received photon is measured using a polarized beam splitter (PBS). The optical signal is amplified using Photomultiplier tube (PMT) with gain from $10^6$ to $10^7$ and then converted to an electrical signal via the avalanche photodetector (APD). Then, it passed to the pulse decompress by the multiplexer, and finally, it is demodulated. The MPPM demodulator output is used to form the raw key.

## IV. Channel Model

This section studies two channel models (Bosonic Channel and Gamma-Gamma Turbulence Channel) that are assumed to simultaneously affect the propagation of single photons in free space.

### A. Bosonic Channel Theory and Model

There are several types of bosonic channels, for example, loss channels, linear channels, Gaussian dilatable channels, photon-added lossy channels, and photon-added amplifier channels [35, Fig. 2]. The operation of bosonic channels can be divided into two modes based on the input average energy constraints: single-mode and multi-mode. In a multi-mode scenario, the channel acts on a collection of many input Bosonic modes, and the single-mode scenario operates on only one input Bosonic mode [36].

In quantum communication, one of the most practical channels is the lossy bosonic channel. It consists of a collection of bosonic modes that lose energy during propagation from the transmitter to the receiver. The lossy bosonic channel provides an appropriate method to model photons' propagation in free space, as shown in Fig. 5. The bosonic channel has one parameter $(0 < \eta_b \leq 1)$ known as the transmissivity of the channel that represents the percentage of photons that arrive at the receiver through the channel. If the channel input is a coherent state $|\mu\rangle$, then the coherent state at the output is $|\eta_b \mu\rangle$. So, the bosonic channel preserves the Poisson statistics of the photon count [13], [37].

A schematic of the model of the lossy bosonic channel is shown in Fig. 6, [38]. Each left-to-right line represents the

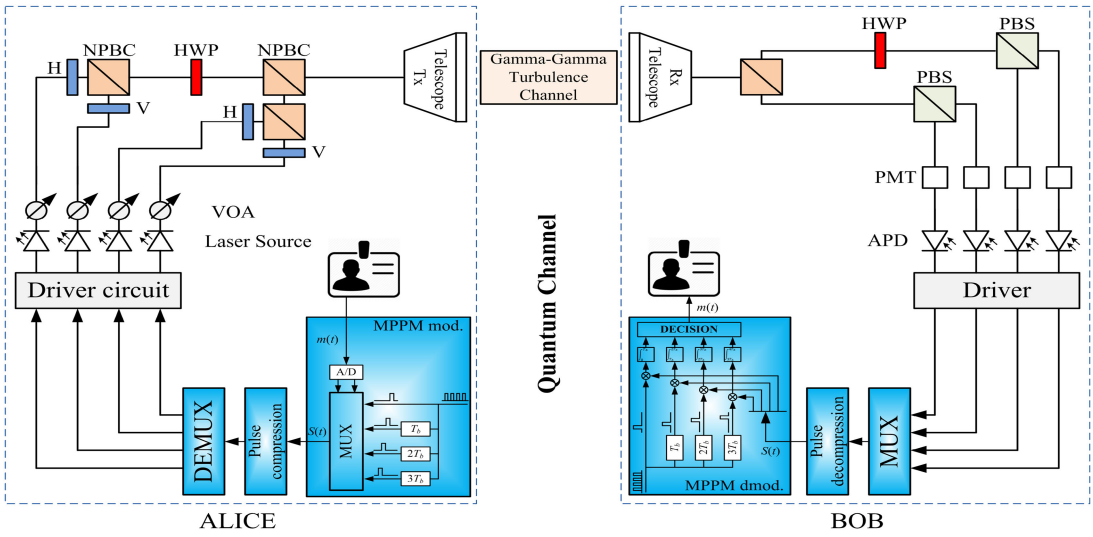


Fig. 4. Block diagram of the proposed MPPM-BB84 FSO system. VOA:Variable optical attenuator; NPBC:Non-polarizing beam combiner; HWP: Half wave plate; PBS: Polarizing beam splitter; PMT: Photonmultiplier tube; APD: Avalanche photo detector.

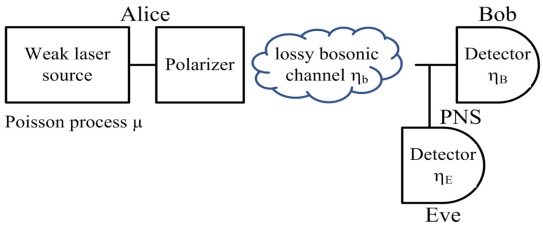


Fig. 5. Polarized photons' transmission over the bosonic channel.


Fig. 6. A schematic of the model of lossy Bosonic channel.

input mode that indicates one use of the channel. The dashed top-bottom line represents the environment mode. Each input mode interacts with the corresponding environment mode through a beam splitter that simulates the channel influence. For an integer $n$, the Bosonic channel operation is defined over a set of $n$ input Bosonic oscillators, with canonical variables $\{q_k, p_k\},\ k = 1, \ldots n$. The environment effect is represented by a collection of ancillary modes $\{Q_k, P_k\},\ k = 1, \ldots n$. In the Heisenberg picture the channel transforms the input field variables as [39]:

$$q'_k = \sqrt{\eta_b}\, q_k + \sqrt{1-\eta_b}\, Q_k,$$
$$p'_k = \sqrt{\eta_b}\, p_k + \sqrt{1-\eta_b}\, P_k, \qquad (2)$$

where $k$ is an integer label the sequential channel uses. At the $k$th use, the $k$th mode of the environment is linearly mixed with the $k$th input mode through a beam splitter with a transmissivity $\eta_b$. For DV-QKD protocols, the lossy Bosonic channel must be analyzed as a discrete-time channel.

The free space transmittance can be simulated based on the probability distribution of the transmittance (PDT) given in [40, Eq. (2)], considering the propagation of a Gaussian beam along the $z$ axis s onto the aperture plane at distance $z = L$. The transmittance of the circular Gaussian beam with an effective spot-radius $W_{\text{eff}}$ can be accurately (provided beam ellipticity is small) approximated by [40] [41]:

$$\eta_b(\upsilon, \phi) = \eta_0 \exp\left\{ -\left[ \frac{r_0/a}{\mathrm{R}\left(\frac{2}{W_{\text{eff}}(\phi-\varphi_0)}\right)} \right]^{\Lambda\left(\frac{2}{W_{\text{eff}}(\phi-\varphi_0)}\right)} \right\}, \qquad (3)$$

where $\eta_b(\upsilon, \phi)$ is assumed to be mainly impacted by distortion of the spot shape and size, and beam wandering. $\eta_0$ is transmittance of the beam in the center of the aperture, $a$ the radius of the receiving aperture, and $\Lambda(\psi), \mathrm{R}(\psi)$ are the shape and scale functions, respectively [40].

### *B. Gamma-Gamma Turbulence Channel*

In FSO communications, the Gamma-Gamma (GG) distribution is widely used to represent moderate-to-strong turbulence. It has a probability density function (PDF), defined in [42], which represents only the effect of atmospheric turbulence. A complete model including the combined effects of atmospheric attenuation and pointing errors (misalignment fading) over the Gamma-Gamma channel was derived in [43] as:

$$f(h) = \frac{\alpha\beta\gamma^2}{A_0 h_a \Gamma(\alpha)\Gamma(\beta)} \left( \frac{\alpha\beta h}{A_0 h_a} \right)^{\frac{(\alpha+\beta)}{2}-1}$$
$$\times\, G_{1,3}^{3,0}\left[ \frac{\alpha\beta}{A_0 h_a} h \middle| \begin{matrix} 1-\frac{\alpha+\beta}{2}+\gamma^2 \\ -\frac{\alpha+\beta}{2}+\gamma^2, \frac{\alpha-\beta}{2}, \frac{\beta-\alpha}{2} \end{matrix} \right], \qquad (4)$$

where $\Gamma(.)$ is the gamma function; $\alpha$ and $\beta$ are the effective number of large-scale and small-scale cells of the scattering

process [42], [44]. Both $\alpha$ and $\beta$ depend on the Rytov variance $\sigma_R^2$ given as $\sigma_R^2 = 1.23\, C_n^2\, (2\pi/\lambda)^{7/6}\, L^{11/6}$, where $C_n^2$ is the refraction index structure parameter, $\lambda$ is the light source wavelength, and $L$ is the propagation distance [45]. The fraction of the collected power at the photodetector center is $A_0$, and $\gamma = (w_{zeq}/2\sigma_s)$ is the ratio between the equivalent beam width and jitter standard division that measures the severity of the pointing error effect [46]. The atmospheric attenuation is $h_a$, which determined by Beers-Lambert Law as $h_a = \exp(-\sigma L)$, where $\sigma$ is the weather-dependent attenuation coefficient (km$^{-1}$), and $L$ is the transmission distance. The channel state $h$ represents the optical intensity fluctuations resulting from the atmospheric turbulence, atmospheric attenuation, and PE effects [43]. Whereas G is the Meijer G-function defined in [47].

To obtain LoS in terrestrial FSO communication systems, the transceivers are often located on the top of tall buildings. Pointing error is the slow fluctuation of the LoS component due to thermal expansion of the building (boresight displacement), dynamic wind loads, or/and building sway and vibration (jitter). The pointing error results from the displacement of the laser beam along vertical (elevation) and horizontal (azimuth) directions. It represents the misalignment (radial displacement) between the beam footprint center and the center of the detection plane as shown in ([46], Fig. 2). The radial displacement that defines the pointing errors follows a Beckmann distribution [48]. This paper considers pointing errors with jitter displacement and zero boresight displacement. In this case, Beckmann distribution is specialized to Rayleigh distribution [49].

### C. Average and Asymptotic Symbol Error Rate for MPPM Over GG Channel

A closed-form expression of the average symbol error rate ASER of MPPM FSO system considering the combined effect of atmospheric turbulence and PE has been deduced in [45] as:

$$P_s = \frac{(M-1)\, 2^{\alpha+\beta-4}}{\pi^{\frac{3}{2}}\, \Gamma(\alpha)\Gamma(\beta)}\, \gamma^2 \times G_{7,4}^{2,6}\left( \frac{16\, M \log_2 M\, \overline{\text{SNR}} A_0^2}{\alpha^2 \beta^2} \right. \\ \left. h_a^2 \left| \begin{matrix} \frac{1-\gamma^2}{2}, \frac{2-\gamma^2}{2}, \frac{1-\alpha}{2}, \frac{2-\alpha}{2}, \frac{1-\beta}{2}, \frac{2-\beta}{2}, 1 \\ 0, \frac{1}{2}, \frac{-\gamma^2}{2}, \frac{1-\gamma^2}{2} \end{matrix} \right. \right), \tag{5}$$

where $M$ is the number of time slots per symbol. $\overline{\text{SNR}}$ is the average signal-to-noise ratio (SNR) defined in [45] as:

$$\overline{\text{SNR}} = \left( \frac{\Re P_T G_T G_R \eta_T \eta_R \lambda^2}{32\, \pi^2\, L^2\, \sigma_n} \right)^2,$$

where $\Re$ is the photodetector responsivity, $P_T$ is the optical transmit power at the telescope aperture. $G_T = (\pi D_T/\lambda)^2$, $G_R = (\pi D_R/\lambda)^2$, $\eta_T$ and $\eta_R$ are the telescope gains and optical efficiencies of the transmitter (Tx) and the receiver (Rx), respectively. $\lambda$ is the wavelength of the laser source. $D_T$ and $D_R$ are aperture diameter of the Tx and Rx, respectively.

The variance of the channel Gaussian noise $\sigma_n^2$ is [50]:

$$\sigma_n^2 = \sigma_{sh}^2 (1 + \eta_D \langle \eta_b \rangle \varepsilon + v_{el}), \tag{6}$$

where $\sigma_{sh}^2$ is the shot noise variance [51], $\eta_D$ is the detection efficiency, $\langle \eta_b \rangle$ is the mean of the channel transmittance, $\varepsilon$ is the excess noise, and $v_{el}$ is the electronic noise [52].

At asymptotically high SNR, the ASER of a communication system over a fading channel is precisely approximated as $P_s^{\infty} = (G_c.\overline{\text{SNR}})^{-G_d}$, where $G_d$ and $G_c$ are the diversity order the coding gain [53]. At high SNR the channel PDF in (4) can be approximated as in [49] by $\lim_{h\to 0} f(h) = ah^t + g_t(h)$, where $g_t(h)$ validates $\lim_{h\to 0}[g_t(h)/h^t] = 0$ and the constant $t$ is defined by the channel PDF. Now, it is straight forward to deduce the diversity order $G_d = (\alpha+\beta)/4$ and the coding gain is obtained as:

$$G_c = \xi \left[ \frac{(2\alpha\beta)^{\frac{\alpha+\beta}{2}} \gamma^2\, \Gamma(\frac{\alpha+\beta+2}{4})}{\sqrt{\pi}(A_0 h_a)^{\frac{\alpha+\beta}{2}} \Gamma(\alpha)\Gamma(\beta)(\alpha+\beta)} \right]^{-\frac{4}{\alpha+\beta}}, \tag{7}$$

where $\xi$ is a positive constant depends on the modulation scheme. It is derived for MPPM to be $(M-1)/2$. The asymptotic SER of MPPM FSO system over GG channel with PE and atmospheric attenuation is derived as:

$$P_s^{\infty} = \left(\xi\, \overline{\text{SNR}}\right)^{-\frac{\alpha+\beta}{4}} \left[ \frac{(2\alpha\beta)^{\frac{\alpha+\beta}{2}} \gamma^2 \Gamma(\frac{\alpha+\beta+2}{4})}{\sqrt{\pi}(A_0 h_a)^{\frac{\alpha+\beta}{2}} \Gamma(\alpha)\, \Gamma(\beta)(\alpha+\beta)} \right]. \tag{8}$$

## V. Raw Key and Secret Key Rates

This section discusses the raw key and secret key rates of the proposed system. Considering, the probability of a pulse with i photons is $P_i = e^{-\mu}\mu^i/i!$ while $i \geq 0$ and the probability of a pulse with zero photons is $P_0 = e^{-\mu}$. Therefore, the probability of generating a frame with pulse having $i$ photons can be obtained using Binomial distribution as [15]:

$$P_{\text{i, MPPM}} = \binom{M}{1} P_i\, P_0^{(M-1)} \tag{9}$$

The raw key rate (RKR) per frame determines by the photon detection efficiency at Bob and channel attenuation is given in [14, Eq. (2)]. It is modified to accomodate the beam propagation in free space atmospheric channel such that:

$$R_{\text{raw}} = \frac{1}{2} \frac{\log_2 M}{M} \sum_{i\geq 1} P_{\text{i, MPPM}} [1 - (1 - \langle \eta_b \rangle \eta_D)^i], \tag{10}$$

where $\eta_D$ is the detector efficiency assuming similarity at Bob and Eve detectors such that $\eta_B = \eta_E = \eta_D$. In this paper, the bosonic channel effect is taken into account such that the average number of photons arrived at Bob is $\eta_b \mu$.

Now, the RKR of MPPM-BB84 over the Gamma-Gamma channel is derived using (5) and (10) as:

$$R_{\text{raw,GG}} = R_{\text{raw}} \times \left(1 - \frac{P_s}{\log_2 M}\right) \tag{11}$$

To deduce an expression for the secret key rate (SKR) of MPPM-BB84 over the Gamma-Gamma channel, PNS attack is considered. In the attack scenario, Eve will split one photon if the received pulse has more than one photon (multi-photon) and the measurement will be performed after Alice and Bob have revealed the corresponding bases information. The data gained by Eve is:

$$R_{\text{Eve,GG}} = \frac{1}{2} \frac{\log_2 M}{M} \sum_{i\geq 2} P_{\text{i, MPPM}}\, \eta_D \times \left(1 - \frac{P_s}{\log_2 M}\right) \tag{12}$$

TABLE I
SYSTEM AND SIMULATION PARAMETERS, NOISES ARE IN SHOT-NOISE UNITS (SNU)

| Parameter | Symbol | Value |
|---|---|---|
| Link distance | $L$ | $1-4$ km |
| Structure parameter - moderate | $C_n^2$ | $5\times10^{-14}m^{-2/3}$ |
| Structure parameter - strong | $C_n^2$ | $3.5\times10^{-13}m^{-2/3}$ |
| Transmitter diameter | $D_T$ | 0.15 m |
| Receiver diameter | $D_R$ | 0.35 m |
| Transmission rate | $R_b$ | 500 Mbps |
| Wavelength | $\lambda$ | 1550 nm |
| Optical transmit power | $P_T$ | $-90$ to $-70$ dBm |
| Tx optics efficiency | $\eta_T$ | 0.8 |
| Rx optics efficiency | $\eta_R$ | 0.8 |
| Detector efficiency | $\eta_D$ | 0.8 |
| Responsivity | $\Re$ | 0.5 A/W |
| Number of time slots | $M$ | 4, 8 and 16 |
| Attenuation coefficient | $\sigma$ | 2 and 18.3 dB/km |
| mean channel transmittance | $\langle\eta_b\rangle$ | 0.9 |
| Jitter standard devision | $\sigma_s$ | 0.1 m |
| Beam divergence angle | $\theta$ | 2 mrad |
| Excess noise | $\varepsilon$ | 0.065 SNU |
| Electronic noise | $v_{el}$ | 0.01 SNU |

The SKR of MPPM-BB84 over the Gamma-Gamma channel is obtained using (11) and (12) as:

$$R_{\text{SKR,GG}} = R_{\text{raw,GG}} - R_{\text{Eve,GG}} \tag{13}$$

The final key creation rate $\text{R}_f$ is given by:

$$R_f = R_{\text{SKR,GG}}\, R_b\ , \tag{14}$$

where $\text{R}_b$ is the system bit rate.

## VI. RESULTS AND DISCUSSION

This section evaluates the performance of the proposed MPPM-BB84 system numerically over the Gamma-Gamma turbulence channel, taking into account the deterioration effects of atmospheric turbulence and misalignment. The impact of critical system parameters, such as transmission distance, excess noise, weather conditions, detector efficiency, and the average number of photons, is studied. Simulation results are presented, and the Monte-Carlo simulations are then used to prove the validity of the analytical results. The key parameters used in the numerical simulation and analysis of the proposed expressions are presented in Table I, [14], [45], [50], [52].

In the reported results, the system performance is evaluated in terms of the RKR and SKR of MPPM-BB84, which are calculated in the equations (11) and (13), respectively. Fig. 7 shows the raw and secret key rates of the proposed MPPM-BB84 protocol concerning the average number of photons per pulse $\mu$ and for different symbol, at moderate turbulence ($c_n^2 = 5\times10^{-14}$) and very light mist atmosphere ($\beta_l = 2$ dB/km). From the figure, we can observe that the optimal values of $\mu$, that satisfies maximum RKR and SKR, for $M = 4, 8$, and 16 are $0.29, 0.15$, and $0.07$, respectively. Moreover, the raw and secret key rates decreases with the increase of symbol lengths at optimal $\mu$. It clearly demonstrates that the system's security level is determined by the difference between the RKR and SKR values. This difference increases the severity of the PNS attack and, therefore, the security of the system decreases. The $M = 16$ modulation order guarantees (maximizes) system security at a tradeoff of lower SKR.

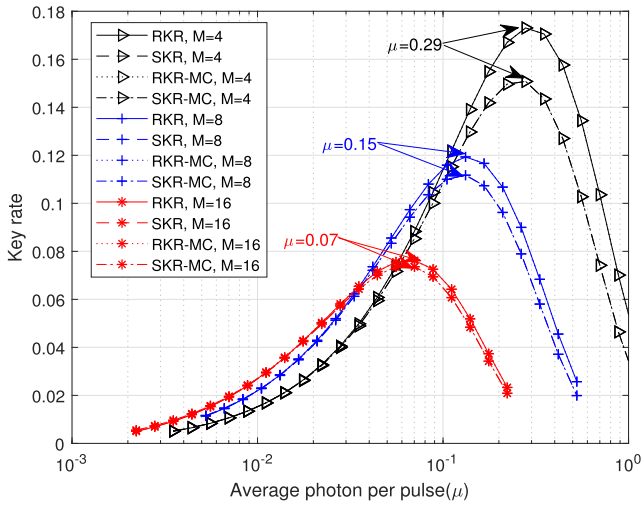


Fig. 7. Raw key rate and secret key rate versus $\mu$ at different $M$, $L = 1$ km, at Moderate Turbulence.

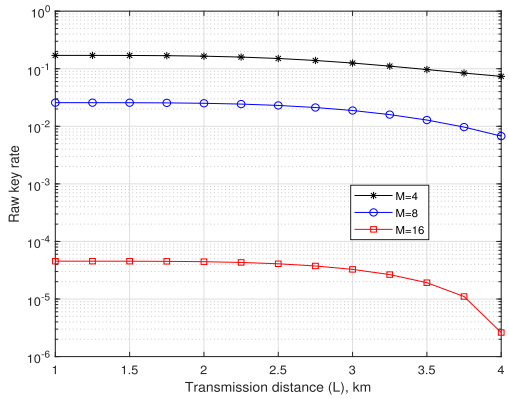


Fig. 8. Raw key rate versus link distance $L$ at Moderate Turbulence (with optimal value of $\mu$ and for $M = 4, 8$ and 16).

The performance of the proposed system in terms of RKR versus the link distance is shown in Fig. 8. For different symbol lengths, the RKR is almost the same at 1 km$< L <$ 2.5 km, a slight degradation occurs at 2.5 km$< L <$ 3.5 km while a significant decrease appears at $L > 3.5$ km, especially at $M = 16$. Therefore, this system satisfies stable performance in terms of RKR at modulation orders $M = 4, 8$, and 16 for propagation distance up to 2.5 km. It is clear from Fig. 7 and Fig. 8 that, for moderate turbulence and very light mist atmosphere if $\mu > 0.01$, the optimum symbol length which satisfies maximum key rates is $M = 4$ as it has the highest symbol efficiency compared with $M = 8$ and $M = 16$. The numerical results of the average number of photons per pulse as a function of the weak laser source power is shown in Fig. 9 for different symbol lengths. This figure helps to control by reducing the probability of multi-photon pulses (two and more) by keeping $\mu < 0.5$ as concluded from Fig. 2. For example, if the system design criteria are $\mu$=0.3, the laser source power must be kept at $-71.1$ dBm, $-72.8$ dBm, and $-74.1$ dBm for $M = 4, 8$, and 16, respectively. This can be implemented in the transmitter circuit using the variable optical attenuator (VOA) as depicted in the system block diagram of Fig. 4.

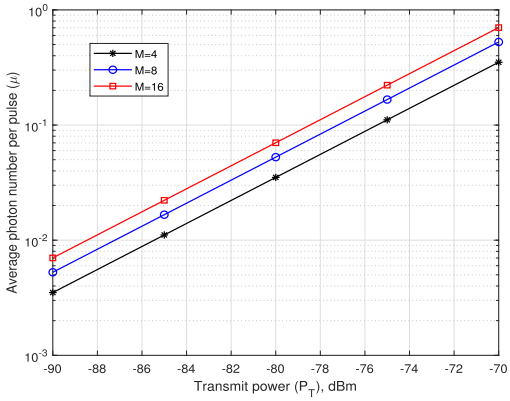


Fig. 9. Average number of photons per pulse versus transmit power for $M = 4, 8$ and 16, and $L = 1$ km, at Moderate Turbulence.

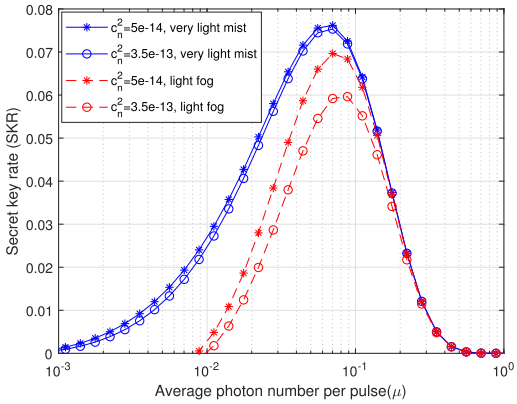


Fig. 10. Secret key rate versus $\mu$ with different weather conditions and atmospheric turbulence at $M = 16$ and $L = 1$ km.

Fig. 10 shows the influence of varying weather conditions and atmospheric turbulence on the rate of generating the secret key for modulation order $M = 16$. It is clear that the weather condition has a dominant effect on the SKR compared with the atmospheric turbulence. The maximum SKR that can be achieved at $M = 16$ is at $\mu \approx 0.07$. In good weather, the variation of the turbulence from moderate ($c_n^2 = 5 \times 10^{-14}$) to strong ($c_n^2 = 3.5 \times 10^{-13}$) does not nearly affect the SKR. While for bad weather (foggy), the SKR reduces by about 0.01 from the maximum value as the turbulence changes from moderate to strong. The results show that with $M = 16$ and $\mu \approx 0.07$, the QKD link considers stable under different weather conditions (moderate and strong) with SKR $\geq 0.06$.

In order to show the effect of the time bins on the SKR, Fig. 11 is presented. When the weather is foggy, more time bins give a higher SKR. For example, at time bins $= 4$, the SKR increased twice compared to time bins $= 2$. Furthermore, in bad weather conditions, four-time bins introduce nearly the same SKR as in very light mist weather conditions with only a one-time bin. Hence the system can introduce a reliable performance in bad weather. We believe that the analysis and simulation of the proposed system provide a good reference that supports a secure-efficient QKD system over free space and optimizes the available parameters to satisfy the design objectives.

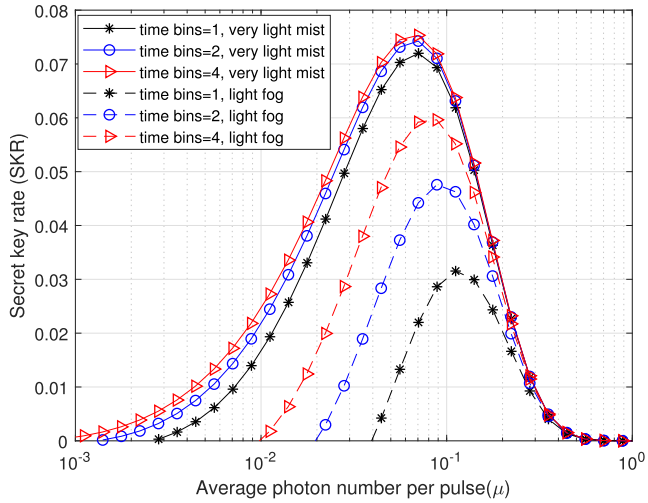


Fig. 11. Raw key rate versus $\mu$ with different number of time bins and weather conditions for strong turbulence at $M = 16$ and $L = 1$ km.

## VII. Conclusion

In this paper, we showed the benefits of integrating FSO systems and MPPM-QKD protocol to provide high data rates and secure systems. This work has proposed the design and analysis of the MPPM-BB84 FSO system, using the Poisson photon source. A Gamma-Gamma distribution is assumed, and the combined effects of atmospheric attenuation, atmospheric turbulence, and misalignment are considered. The system performance is evaluated under the PNS attack in terms of RKR and SKR. According to the assumed parameters, it is found that when the average number of photons $\mu > 0.1$, then the symbol of length $M = 4$ will give the maximum SKR. Also, for each symbol length $M$, there is a corresponding optimal value for $\mu$ that satisfies the highest SKR. Where the VOA at the transmitter can be adjusted to satisfy the optimal $\mu$ for the operating symbol length. In the proposed system, the link distance can be varied from 1 km to 3 km without significant variation in the RKR. The degradation of system performance due to variations in weather conditions can be avoided by operating the system at an optimum value of $\mu$ for each $M$. The proven expressions of RKR and SKR can be used as a guide for any similar systems with different values of system and channel parameters.

## References

[1] H. Kaushal and G. Kaddoum, "Optical communication in space: Challenges and mitigation techniques," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 57–96, Jan.–Mar. 2017.

[2] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surv. Tut.*, vol. 16, no. 4, pp. 2231–2258, Oct.–Dec. 2014.

[3] K. Anbarasi, C. Hemanth, and R. Sangeetha, "A review on channel models in free space optical communication systems," *Opt. Laser Technol.*, vol. 97, pp. 161–171, 2017.

[4] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Proc. Workshop Theory Appl. Cryptographic Techn.*, 1984, pp. 475–480.

[5] K. Balygin, A. Klimov, I. Bobrov, K. Kravtsov, S. Kulik, and S. Molotkov, "Inherent security of phase coding quantum key distribution systems against detector blinding attacks," *Laser Phys. Lett.*, vol. 15, no. 9, pp. 1–6, 2018.

[6] Z. Chang-Hua, P. Chang-Xing, Q. Dong-Xiao, G. Jing-Liang, C. Nan, and Y. Yun-Hui, "A new quantum key distribution scheme based on frequency and time coding," *Chin. Phys. Lett.*, vol. 27, no. 9, pp. 090301.1–090301.4, 2010.

[7] S. Ali, "Time-polarization coding in quantum cryptography," *Opt. Quantum Electron.*, vol. 48, no. 12, pp. 558–568, 2016.

[8] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[9] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, pp. 1–5, 2001.

[10] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. Yuan, and A. J. Shields, "Manipulating photon coherence to enhance the security of distributed phase reference quantum key distribution," *Appl. Phys. Lett.*, vol. 111, no. 26, pp. 1–5, 2017.

[11] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[12] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling With Matlab*, Boca Raton, FL, USA: CRC Press, 2019.

[13] Y. Kochman and G. W. Wornell, "On high-efficiency optical communication and key distribution," in *Proc. Inf. Theory Appl. Workshop*, 2012, pp. 172–179.

[14] Y. Zhang and I. B. Djordjevic, "Generalized ppm-based bb84 QKD protocol," in *Proc. 16th Int. Conf. Transparent Opt. Netw.*, 2014, pp. 1–4.

[15] H. Zhou and G. Wornell, "Adaptive pulse-position modulation for high-dimensional quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory*, 2013, pp. 359–363.

[16] Y. Zhang, I. B. Djordjevic, and M. A. Neifeld, "Efficient quantum key distribution based on pulse-position modulation," in *Emerg. Technol. Secur. Defence II; Quantum-Phys.-Based Inf. Secur. III*, vol. 9254, pp. 1–7, 2014.

[17] M. S. Bashir and S. S. Muhammad, "Time synchronization in photon-limited deep space optical communications," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 1, pp. 30–40, Feb. 2020.

[18] X. Wang, Y. Wang, Z. Yao, X. Chen, X. Zhu, and X. Zhang, "Timing offset estimation of ppm signal for deep space optical communications," in *Proc. Signal Inf. Process., Netw. Comput.*, Berlin, Germany: Springer, 2020, pp. 444–452.

[19] J. Xiang, X. X. Chen, P. Zhang, and Y. Jia, "Clock synchronization technology for pulse position modulation with guard time at sampling frequency of 1 slot," *Chin. J. Lasers*, vol. 45, no. 10, pp. 10–16, 2018.

[20] M. Nazarathy, "Quantum key distribution over a fiber-optic channel by means of pulse position modulation," *Opt. Lett.*, vol. 30, no. 12, pp. 1533–1535, 2005.

[21] G. Chen *et al.*, "Multiple pulses phase-matching quantum key distribution," pp. 1–13, 2019.

[22] S. Guerrini, M. Chiani, M. Z. Win, and A. Conti, "Quantum pulse position modulation with photon-added coherent states," in *Proc. IEEE Globecom Workshops*, 2019, pp. 1–5.

[23] H. Z. A. Muller and N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre," *Europhysics Lett.*, vol. 33, no. 5, pp. 713–725, 1996.

[24] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, *Quantum Cryptography Over Underground Optical Fibers*, N. Koblitz, Ed. Berlin, Heidelberg, Germany: Springer, 1996.

[25] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, "Active polarization stabilization in optical fibers suitable for quantum key distribution," *Opt. Exp.*, vol. 15, no. 26, pp. 17928–17936, 2007.

[26] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack," *New J. Phys.*, vol. 4, no. 44, pp. 1–9, 2002.

[27] A. Gaidash, V. Egorov, and A. Gleim, "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices," *J. Phys.: Conf. Ser.*, vol. 735, no. 1, pp. 1–6, 2016.

[28] V. Savu, L. Frunzio, and D. E. Prober, "Enhancing the energy resolution of a singles photon STJ spectrometer using diffusion engineering," *IEEE Trans. Appl. Supercond.*, vol. 17, no. 2, pp. 324–327, Jun. 2007.

[29] A. S. Trushechkin, E. O. Kiktenko, D. A. Kronberg, and A. K. Fedorov, "Security of the decoy state method for quantum key distribution," *Phys.-Uspekhi*, vol. 64, no. 1, pp. 88–102, 2021.

[30] T. Attema, J. W. Bosman, and N. M. Neumann, "Optimizing the decoy-state bb84 QKD protocol parameters," *Quantum Inf. Process.*, vol. 20, no. 4, pp. 1–26, 2021.

[31] A. Lapidoth and S. M. Moser, "On the capacity of the discrete-time Poisson channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 303–322, Jan. 2009.

[32] J. G. Proakis and M. Salehi, *Digital Communications.* New York, NY, USA: McGraw-Hill, 2001, vol. 4.

[33] X. Liu *et al.*, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km," *Appl. Phys. Lett.*, vol. 114, no. 14, pp. 141104–141109, 2019.

[34] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," *Phys. Rev. Lett.*, vol. 98, no. 6, pp. 1–4, 2007.

[35] L. Lami, K. K. Sabapathy, and A. Winter, "All phase-space linear bosonic channels are approximately gaussian dilatable," *New J. Phys.*, vol. 20, no. 11, pp. 1–26, 2018.

[36] F. Caruso, V. Giovannetti, and A. S. Holevo, "One-mode bosonic gaussian channels: A full weak-degradability classification," *New J. Phys.*, vol. 8, no. 12, pp. 1–23, 2006.

[37] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[38] V. Giovannetti and S. Mancini, "Bosonic memory channels," *Phys. Rev. A*, vol. 71, no. 6, pp. 1–6, 2005.

[39] C. Lupo, O. V. Pilyavets, and S. Mancini, "Capacities of lossy bosonic channel with correlated noise," *New J. Phys.*, vol. 11, no. 6, pp. 1–17, 2009.

[40] I. Derkach, V. C. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels," *New J. Phys.*, vol. 22, no. 5, pp. 1–11, 2020.

[41] D. Vasylyev, A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Phys. Rev. Lett.*, vol. 117, no. 9, pp. 1–18, 2016.

[42] L. C. Andrews, R. L. Phillips, R. J. Sasiela, and R. Parenti, "PDF models for uplink to space in the presence of beam wander," in *Proc. SPIE*, vol. 6551, 2007, pp. 1–12.

[43] H. G. Sandalidis, T. A. Tsiftsis, and G. K. Karagiannidis, "Optical wireless communications with heterodyne detection over turbulence channels with pointing errors," *J. Lightw. Technol.*, vol. 27, no. 20, pp. 4440–4445, 2009.

[44] K. Kiasaleh, "Channel estimation for FSO channels subject to gamma-gamma turbulence," in *Proc. Int. Conf. Space Opt. Syst. Appl.*, Corsica, France, 9-12, 2012, pp. 1–7.

[45] T. Ismail, E. Leitgeb, Z. Ghassemlooy, and M. Al-Nahhal, "Performance improvement of FSO system using multi-pulse pulse position modulation and simo under atmospheric turbulence conditions and with pointing errors," *IET Netw.*, vol. 7, no. 4, pp. 165–172, 2018.

[46] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *J. Lightw. Technol.*, vol. 25, no. 7, pp. 1702–1710, 2007.

[47] Mathematica, Accessed: Jul. 19, 2018. [Online]. Available: http://functions.wolfram.com/Hypergeometric/Functions/MeijerG/

[48] P. Beckmann and A. Spizzichino, *The Scattering of Electromagnetic Waves From Rough Surfaces*. Norwood, MA, USA: Artech House, 1987.

[49] F. Yang, J. Cheng, and T. A. Tsiftsis, "Free-space optical communication with nonzero boresight pointing errors," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 713–725, Feb. 2014.

[50] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, "Parameter estimation of atmospheric continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 99, no. 3, pp. 1–12, 2019.

[51] G. P. Agrawal, *Fiber-Optic Communication Systems*. Hoboken, NJ, USA: Wiley, 2012.

[52] F. Laudenbach *et al.*, "Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, pp. 1–37, 2018.

[53] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1389–1398, Aug. 2003.