Secrecy Analysis of FSO Systems Considering Misalignments and Eavesdropper's Location

Phuc V. Trinh, *Member, IEEE,* Alberto Carrasco-Casado,

Anh T. Pham, *Senior Member, IEEE,* and Morio Toyoshima, *Member, IEEE*

Abstract

The use of free-space optical (FSO) systems as secure transmission media has recently attracted research efforts worldwide. However, their secrecy performance may be compromised by the presence of an adversarial eavesdropper. In addition, misalignments between transceivers could severely affect the legitimate FSO channel and increase eavesdropping risks. This paper, for the first time, offers a complete framework to analyze the impact of an eavesdropper's location on the secrecy performance of terrestrial FSO systems under generalized misalignments and atmospheric turbulence conditions. Particularly, the probability density functions (PDFs) of the eavesdropping channel are newly developed and presented in closed-form expressions. Capitalizing on the derived PDFs, secrecy performance metrics in the physical-layer security (PLS) and intensity modulation/direct detection (IM/DD) continuous-variable quantum key distribution (CV-QKD) systems can be analytically analyzed, incorporating all combined effects of the atmospheric turbulence, transceiver misalignments, receiver noises, and the eavesdropper's location. Monte-Carlo (MC) simulations are also implemented to corroborate the analytical results.

This paper was presented in part at the International Conference on Space Optics (ICSO), Chania, Greece, Oct. 2018.

P. V. Trinh, A. Carrasco-Casado, and M. Toyoshima are with the Space Communications Laboratory, National Institute of Information and Communications Technology, Tokyo 184-8795, Japan (e-mail: pvtrinh@nict.go.jp; alberto@nict.go.jp; morio@nict.go.jp).

A. T. Pham is with the Department of Computer and Information Systems, The University of Aizu, Aizuwakamatsu 965-8580, Japan (email: pham@u-aizu.ac.jp).

Index Terms

Physical-layer security, quantum key distribution, free-space optical systems, misalignments, eavesdropper's locations.

I. Introduction

Future wireless technologies embrace the use of radio frequency (RF) and free-space optical (FSO) systems [1]. Over the past decades, there have been extensive research efforts to secure these wireless systems. Conventionally, the classical cryptography based on the computational hardness of mathematical algorithms is used, thus referred to as the *computational security* [2]. However, its security might be threatened in the future, especially when large-scale powerful quantum computers become available [3]. To cope with this potential risk, cryptographic schemes that provide secure communications according to information theory, herein referred to as the *information-theoretic security (ITS)*, should be developed.

A. Background

Physical-layer security (PLS) may offer the ITS by exploiting the randomness in the physical-layer transmission media based on the laws of physics. PLS includes the keyless scheme (i.e. no secret keys are required for encryption but code designs and channel properties are exploited to achieve secrecy) and the secret-key scheme (i.e. a secret key is required for the encryption and decryption of confidential messages) [4]. On the one hand, the keyless scheme was pioneered by the work of Wyner in 1975, which considered a confidential transmission over a wiretap channel (WTC) between two legitimate parties, namely Alice and Bob, in the presence of an eavesdropper, namely Eve [5]. From this, the maximum transmission rate at which the eavesdropper is unable to decode any information, i.e. *secrecy capacity*, was formulated [5], [6]. Motivated by the problem of securing transmissions over wireless channels, the wireless counterpart of the WTC model was consequently developed by considering the impact of fading on the secrecy capacity [7].

On the other hand, the secret-key scheme is dated back in 1926, when the *one-time-pad* scheme was proposed by Vernam [8], using a random bit sequence as long as the confidential message, i.e. a *secret key*, that can be used only once for the encryption and decryption. This scheme was then proved to be secure according to information theory, i.e. ITS, by Shannon in 1949 [9]. In light of the developed knowledge for the WTC, the secret-key agreement (SKA) scheme was formulated in 1993 to share symmetric secret keys from the common randomness over a WTC [10]. Over the past decade, SKA has been extensively investigated for wireless channels in the RF domain by exploiting the common randomness from channels subject to the multipath scattering and fading [11].

Another way of realizing the ITS-proof secret-key scheme is to rely on optical quantum states based on the laws of quantum physics. By harnessing the inherent unpredictability in the quantum states, ***quantum key distribution (QKD)*** can be used to safely distribute the secret key. The first QKD protocol was proposed by Bennett and Brassard in 1984, i.e. BB84 protocol [12], which encodes the key information on the polarization states of photons. Afterwards, the implementation of QKD can be categorized into two schemes, namely the discrete-variable QKD (DV-QKD) [13] and the continuous-variable QKD (CV-QKD) [14]. Specifically, the DV-QKD encodes the key information on the polarization/phase of single photons, while CV-QKD utilizes the continuous variables of coherent states conveyed by the amplitude and phase of weakly modulated optical pulses. From a practical perspective, the CV-QKD is more convenient to implement as it is compatible with standard telecommunication technologies by using heterodyne/homodyne receivers instead of dedicated single-photon counters. Nevertheless, the use of heterodyne/homodyne receivers requires a sophisticated phase-stabilized local light, resulting in a higher deployment cost. To avoid such issue, the differential-phase-shift-keying (DPSK)-based CV-QKD using a delay interferometer was developed [15]. To further simplify CV-QKD configurations, intensity modulation/direct detection (IM/DD) CV-QKD systems have been recently proposed for both optical fiber [16], [17] and FSO systems [18]–[20], which do

not require the delay interferometer and are built upon off-the-shelf optical components. QKD over FSO systems, or *free-space QKD*, could offer secure connections for terrestrial, airborne, and satellite-based platforms, bridging the gap to an eventual global quantum network [21].

B. Motivations

Unlike the RF counterparts, the PLS for FSO systems is not mature since its eavesdropping scenarios are still under discussion, which can be classified into the active eavesdropping and the passive eavesdropping. In the active eavesdropping, Eve could actively send jamming optical signals to Bob to make his receiver congested with unwanted noises [22]. In the passive eavesdropping, Eve is assumed to passively intercept the legitimate channel near Alice's transmitter [23], in the middle of the communication link [24], and near Bob's receiver [23], [25]-[27]. This can also be extended to the mixed RF-FSO relaying networks where Eve is located near Bob in the FSO link [28], [29]. In practice, as the optical beam-width in FSO systems is very narrow and invisible, it is greatly challenging for Eve to intercept in the middle of the link. Therefore, it is practically reasonable to restrict Eve's physical ability to tap the FSO channel, hence modeling it as an FSO-WTC [30]. Specifically, Eve is assumed to be a fully passive eavesdropper located somewhere on Bob's receiver plane or further behind and tries to tap the side lobes of the divergent optical beam [30], [31]. This FSO-WTC model has been also applied for free-space QKD systems in the pursuit of higher secret-key rates (SKRs) [20], [32].

To accurately estimate the secrecy performance of FSO-WTC models in both PLS and QKD systems, it is crucial that all practical conditions including the atmospheric turbulence, misalignments, and especially the eavesdropper's exact location are taken into account. Recently, the eavesdropper's location is considered in the PLS analysis [33], by assuming a non-zero boresight misalignment model for the eavesdropping channel, given that a zero-boresight one is assumed for the legitimate channel. Unfortunately, this approach is inappropriate since there is no relation between Eve's location and the misaligned beam at Bob. In fact, this approach

inaccurately assumes two independent systems suffering from two different misaligned beams. To correctly address this problem, the fractions of collected powers at Bob and Eve must be respectively characterized by the misalignment vectors from their receivers to the center of the misaligned beam, which is governed by only one misalignment model.

C. Contributions

To the best of the authors' knowledge, our previous study in [34] was the first to tackle the aforementioned problem. Specifically, the impact of eavesdropper's locations on the IM/DD free-space CV-QKD system using a collimated Gaussian beam was analyzed under weak atmospheric turbulence conditions. In this paper, to offer a complete and generalized framework for analyzing the impact of all channel conditions considering the eavesdropper's location, the initial work in [34] has been substantially extended as follows.

- A complete framework is developed for determining the fractions of collected powers captured at Bob's and Eve's receivers. The crucial outcomes are the probability density functions (PDFs) characterizing Bob's and Eve's statistical channels impaired by the generalized misalignments modeled by a four-parameter Beckmann distribution and weak-to-strong atmospheric turbulence conditions modeled by the well-known log-normal (LN) and Gamma-Gamma (GG) distributions.
- For the most practical security analysis, the FSO-WTC model over a 7.8-km terrestrial link in [30], [31] is adopted. This model employs a divergent Gaussian beam that is considerably broadened over long distances, which makes the beam footprint much larger than the receiver size. Hence, Eve may tap the side lobes of the diverged beam by locating her receiver somewhere on or further behind Bob's receiver plane.
- Capitalizing on the derived PDFs and the FSO-WTC model, applications in the secrecy analysis of the PLS and IM/DD CV-QKD for FSO systems are presented. In particular, we newly derive the closed-form expressions of the outage secrecy capacity (OSC) and the

strictly positive secrecy capacity (SPSC) for the PLS analysis, and the quantum bit error rate (QBER) and the ergodic SKR for the IM/DD free-space CV-QKD system. As a result, all practical effects from the atmospheric turbulence, transceiver misalignments, receiver noises, and the eavesdropper's location can be comprehensively investigated. Furthermore, Monte-Carlo (MC) simulations are performed to confirm the validity of analytical results.

D. Organization

The remainder of this paper is organized as follows. Section II revisits the well-known atmospheric channel models that could be applied for both Bob and Eve. In Section III, the complete framework for obtaining the PDFs of the legitimate and eavesdropping channels considering the atmospheric turbulence and generalized misalignments is developed. Applications of the derived PDFs in analyzing the secrecy performance are then described for the PLS and the IM/DD free-space CV-QKD systems in Section IV and Section V, respectively. Finally, the paper is concluded in Section VI. For the sake of convenience, we provide a complete list of acronyms used in this paper in Appendix C.

II. Atmospheric Channel Models

A. Atmospheric Attenuation

The atmospheric attenuation caused by the molecular absorption and aerosol scattering suspended in the air can be described by Beer's law, which is given as

$$h_l = \exp(-\beta_l L), \tag{1}$$

where β_l is the attenuation coefficient and L is the transmission distance [35].

B. Atmospheric Turbulence-Induced Fading

Inhomogeneities in the temperature and pressure of eddies in the atmosphere lead to refractive-index variations along the transmission path, which is commonly known as *atmospheric turbu-*

lence. This results in intensity fluctuations of the optical beam observed at the receiver, i.e. *scintillation* or *fading*.

1) Log-Normal Turbulence Model: For weak turbulence conditions, the fading channel coefficient is modeled as

$$h_t = \exp(2X), \tag{2}$$

where X is the log-amplitude of the optical intensity governed by a Gaussian distribution, i.e. *normal distribution*, with the mean μ_X and the variance σ_X^2. As a result, the PDF of intensity fluctuations can be described by an LN distribution as [35]

$$f_{h_t}(h_t) = \frac{1}{\sqrt{8\pi} h_t \sigma_X} \exp\left(-\frac{[\ln(h_t) - 2\mu_X]^2}{8\sigma_X^2} \right). \tag{3}$$

To ensure that the fading does not attenuate or amplify the average power, we normalize the fading coefficient so that $\mathbb{E}[h_t] = 1$, with $\mathbb{E}[\cdot]$ the statistical expectation. Doing so requires that $\mu_X = -\sigma_X^2$. The log-amplitude variance can be given as $\sigma_X^2 = 0.307 \left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2$, where λ is the wavelength and C_n^2 is the index of refraction structure parameter varying from 10^{-17} to 10^{-13} $\mathrm{m}^{-2/3}$ [36].

2) Gamma-Gamma Turbulence Model: For moderate-to-strong conditions, the fading channel coefficient is considered to arise from large-scale and small-scale atmospheric eddies, given as

$$h_t = Y_l Y_s, \tag{4}$$

where Y_l and Y_s represent the large-scale and small-scale fluctuations, which are assumed to be statistically independent. The large-scale fluctuation is widely accepted to be an LN amplitude [37], i.e. $Y_l = \exp(2\chi)$ with χ a Gaussian random variable. However, to avoid the infinite-range integral of the LN PDF, Y_l is approximated by a Gamma distribution due to its more favorable analytical structure. By assuming that Y_s also follows a Gamma distribution, the PDF of the fading channel coefficient can be modeled by a GG distribution, given as

$$f_{h_t}(h_t) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} (h_t)^{\frac{\alpha+\beta}{2}-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h_t}\right), \tag{5}$$

where $\Gamma(\cdot)$ represents the Gamma function defined as $\Gamma(w) \triangleq \int_0^\infty t^{w-1}e^{(-t)}dt$, $K_{\alpha-\beta}(\cdot)$ is the modified Bessel function of the second kind of order $(\alpha-\beta)$ [38]; $\alpha > 0$ and $\beta > 0$ are the effective numbers of large-scale and small-scale eddies, respectively expressed as [38]

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

where σ_R^2=$1.23\left(\frac{2\pi}{\lambda}\right)^{7/6}L^{11/6}C_n^2$ is the Rytov variance. For a Gaussian beam wave, weak fluctuations require $\sigma_R^2 < 1$ and $\sigma_R^2\Lambda^{5/6} < 1$, corresponding to the entire beam profile being less than unity. If either of these conditions fails, the fluctuations are considered as moderate to strong.

C. Channel Assumptions

When Eve is close to Bob on the same receiving plane, it is reasonable to assume that the atmospheric attenuation h_l and turbulence h_t parameters are the same for both Bob's and Eve's channels over a long transmission distance. In the rest of this paper, by applying the FSO-WTC model in [30], [31], the channel parameters are assumed as follows. With $\lambda = 1550$ nm, $\beta_l = 0.43$ dB/km, and $L = 7.8$ km, the values of C_n^2 with respect to the weak, moderate, and strong turbulence can be identified based on the Rytov variance, chosen as $C_n^2 = 3\times10^{-16}$, $C_n^2 = 10^{-15}$, and $C_n^2 = 5\times10^{-15}$ m$^{-2/3}$, respectively. To guarantee that there is no turbulence-induced fading correlation, i.e. independence between the legitimate and the eavesdropping channels, the distance between Bob's and Eve's receivers should be sufficiently separated. The relation between the channel correlation coefficient and the separation of receivers on the same plane was given in [39]. With the help of [39, (4)], we derive that separation distances of at least 17 cm, 18 cm, and 22 cm are required to guarantee the channel independence corresponding to the above-defined weak, moderate, and strong turbulence, respectively.

III. Combined Atmospheric Channel and Misalignment Models

In this section, the combined channel models characterizing the joint effects of atmospheric turbulence and misalignments at Bob's and Eve's receivers are respectively developed. In general,

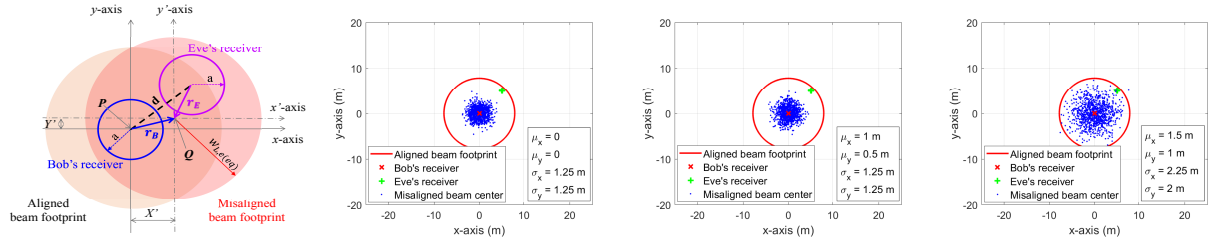


Fig. 1. (a) Bob's and Eve's locations on the receiver plane under misalignments, $F_0 = -10$ m, $w_0 = 0.01$ m; (b) Zero boresight misalignments; (c) Non-zero boresight misalignments; (d) Generalized misalignments.

the misalignments might be caused by the mechanical errors in the tracking system or vibrations of the transceiver due to strong winds, building sway, or light earthquakes, contributing to the signal fading at both receivers. Since the misalignment correlation time is on the order of a few seconds, which is much bigger than that of the atmospheric turbulence (e.g. 10-100 ms), it is practical and reasonable to consider that their fading coefficients are independent [40]. As shown in Fig. 1a, we assume in this paper that Eve's location is on the same receiving plane and at a distance d away from Bob, where Eve's received signal intensity is always higher than that when she is somewhere far behind Bob. This serves as the worst-case scenario and hence determines an effective upper bound of the worst possible leaked information to Eve.

A. Bob's Channel Model

When there are misalignments between Alice's transmitter and Bob's receiver, the normalized spatial distribution of the intensity of a divergent Gaussian beam at a distance L from the transmitter is given as $I_{beam}(\boldsymbol{\rho}, L) = \frac{2}{\pi w_{L,e}^2} \exp\left(-\frac{2\|\boldsymbol{\rho}\|^2}{w_{L,e}^2}\right)$, where $\boldsymbol{\rho}$ is the radial vector from the beam center with $\|\cdot\|$ is the norm of a vector [41]. The channel coefficient due to the geometric spread of the Gaussian beam with misalignment-error vector $\boldsymbol{r_B}$ with respect to Bob's receiver can be expressed as $h_{p,B}(\boldsymbol{r_B}; L) = \int_A I_{beam}(\boldsymbol{\rho} - \boldsymbol{r_B}; L)\, \mathrm{d}\boldsymbol{\rho}$, where $h_{p,B}(\boldsymbol{r_B}; L)$ also represents the fraction of the power collected at Bob's receiver with the receiver area A. Due to the

symmetry of the beam shape and the receiver area, the resultant $h_{p,B}(\boldsymbol{r_B}; L)$ depends only on the radial distance as shown in Fig. 1a, written as $r_B = \|\boldsymbol{r_B}\| = \left\| \begin{bmatrix} X' \\ Y' \end{bmatrix} \right\|$. Without the loss of generality, it is assumed that the radial distance is located along the x-axis. The fraction of collected power at Bob's receiver with the radius a is then approximated as [41]

$$h_{p,B}(\boldsymbol{r_B}; L) \cong A_0 \exp\left(-\frac{2r_B^2}{w_{L,e(eq)}^2}\right), \tag{7}$$

where $A_0 = (\text{erf}(\upsilon))^2$ is the fraction of collected power at $r_B = 0$, $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp(-t^2)\, \text{d}t$ is the Gauss error function, and $\upsilon = \frac{\sqrt{\pi}a}{\sqrt{2}w_{L,e}}$, $w_{L,e(eq)}^2 = w_{L,e}^2 \frac{\sqrt{\pi}\text{erf}(\upsilon)}{2\upsilon \exp(-\upsilon^2)}$ is the equivalent beam-width with $w_{L,e}$ the effective beam-width at a distance L from the transmitter, given as $w_{L,e} = w_L \sqrt{1 + 1.625\sigma_R^{12/5}\Lambda}$, where $w_L = w_0 \sqrt{(1 - \frac{L}{F_0})^2 + (\frac{2L}{kw_0^2})^2}$, $k = \frac{2\pi}{\lambda}$ is the optical wave number, w_0 is the transmitted beam radius, F_0 is the radius of curvature, and $\Lambda = \frac{2L}{kw_L^2}$ [35].

In the most general case, the elevation and horizontal displacements X' and Y' in the x and y directions can be considered as two independent Gaussian random variables with different non-zero means $\{\mu_x, \mu_y\}$ and variances $\{\sigma_x^2, \sigma_y^2\}$. As a result, the PDF of r_B can be characterized by a four-parameter Beckmann distribution as [42]

$$f_{r_B}(r_B) = \frac{r_B}{2\pi\sigma_x\sigma_y} \int_0^{2\pi} \exp\left(-\frac{(r_B\cos(\theta) - \mu_x)^2}{2\sigma_x^2} - \frac{(r_B\sin(\theta) - \mu_y)^2}{2\sigma_y^2}\right) \text{d}\theta. \tag{8}$$

Depending on some special cases of $\{\mu_x, \mu_y, \sigma_x^2, \sigma_y^2\}$, (8) reduces to several well-known and tractable distributions (e.g. Rayleigh distribution, Hoyt distribution, Rician distribution, and zero/non-zero mean single-sided Gaussian distributions), as specified in [42]. Since a closed-form solution for (8) is unknown, we utilize the result in [43] that the four-parameter Beckmann distribution can be accurately approximated by a modified Rayleigh distribution. Now, (8) can be expressed as

$$f_{r_B}(r_B) \cong \frac{r_B}{\sigma_{mod}^2} \exp\left(-\frac{r_B^2}{2\sigma_{mod}^2}\right), \quad r_B > 0, \tag{9}$$

where $\sigma_{mod}^2 = \left(\frac{3\mu_x^2\sigma_x^4 + 3\mu_y^2\sigma_y^4 + \sigma_x^6 + \sigma_y^6}{2}\right)^{1/3}$ is the approximated jitter variance of the misaligned beam. Figs. 1b, 1c, and 1d depict 1000 misaligned beam-center positions at $L = 7.8$ km governed by

(9), for zero boresight, non-zero boresight, and generalized misalignments, respectively. This illustratively shows the scenarios where Eve might benefit from the misaligned beams with respect to her fixed location. With the help of (7), the PDF of $h_{p,B}$ can be finally derived as

$$f_{h_{p,B}}\left(h_{p,B}\right)=\frac{\varphi_{mod}^{2}}{A_{mod}^{\varphi_{mod}^{2}}}\left(h_{p,B}\right)^{\varphi_{mod}^{2}-1},\quad 0\leq h_{p,B}\leq A_{mod}, \tag{10}$$

where $\varphi_{mod}=\frac{w_{L,e(eq)}}{2\sigma_{mod}}$ is the ratio between the equivalent beam radius at Bob's receiver and the displacement standard deviation, $A_{mod}=A_0\Xi$, $\Xi=\exp\left(\frac{1}{\varphi_{mod}^2}-\frac{1}{2\varphi_x^2}-\frac{1}{2\varphi_y^2}-\frac{\mu_x}{2\sigma_x^2\varphi_x^2}-\frac{\mu_y}{2\sigma_y^2\varphi_y^2}\right)$, $\varphi_x=\frac{w_{L,e(eq)}}{2\sigma_x}$ and $\varphi_y=\frac{w_{L,e(eq)}}{2\sigma_y}$ are the jitter variances in the x and y directions, respectively [43]. From (10), the first moment of $h_{p,B}$ can be expressed as [42]

$$\mathbb{E}\left[h_{p,B}\right]=\frac{A_{mod}\varphi_{mod}^{2}}{1+\varphi_{mod}^{2}}. \tag{11}$$

The PDF of Bob's channel coefficient $h_B=h_l h_t h_{p,B}$ can be expressed as $f_{h_B}\left(h_B\right)=\int f_{h_B|h_t}\left(h_B|h_t\right)f_{h_t}\left(h_t\right)\mathrm{d}h_t$, where $f_{h_B|h_t}\left(h_B|h_t\right)$ is the conditional probability given a turbulence state h_t of Bob's channel. Under the weak atmospheric turbulence modeled by an LN distribution, Bob's channel PDF can be expressed in a closed-form expression as [41]

$$f_{h_B}\left(h_B\right)=\frac{\varphi_{mod}^{2}}{2\left(A_{mod}h_l\right)^{\varphi_{mod}^{2}}}\left(h_B\right)^{\varphi_{mod}^{2}-1}\mathrm{erfc}\left(\frac{\ln\left(\frac{h_B}{A_{mod}h_l}\right)+\mu_B}{\sqrt{8}\sigma_X}\right)\exp\left(2\sigma_X^2\varphi_{mod}^{2}\left(1+\varphi_{mod}^{2}\right)\right), \tag{12}$$

where $\mathrm{erfc}(x)=\frac{2}{\sqrt{\pi}}\int_x^{\infty}\exp(-t^2)\mathrm{d}t$ is the complementary error function, and $\mu_B=2\sigma_X^2(1+2\varphi_{mod}^2)$. Under the moderate-to-strong atmospheric turbulence modeled by a GG distribution, Bob's channel PDF can be expressed in a closed-form expression as [44]

$$f_{h_B}\left(h_B\right)=\frac{\varphi_{mod}^{2}}{\left(A_{mod}h_l\right)^{2}}\left(h_B\right)^{\varphi_{mod}^{2}-1}\sum_{i=1}^{N}a_i\xi_i^{\varphi_{mod}^{2}-\alpha}\Gamma\left(\alpha-\varphi_{mod}^{2},\frac{\xi_i}{A_{mod}h_l}h_B\right), \tag{13}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete Gamma function [45, (8.350.2)], $a_i=\frac{\theta_i}{\sum_{j=1}^{N}\theta_j\Gamma(\alpha)\xi_j^{-\alpha}}$, $\xi_i=\frac{\alpha\beta}{t_i}$, $\theta_i=\frac{(\alpha\beta)^{\alpha}\omega_i t_i^{-\alpha+\beta-1}}{\Gamma(\alpha)\Gamma(\beta)}$. N is the Gauss-Laguerre approximation order, ω_i and t_i are the weight factors and the abscissas of the Gauss-Laguerre quadrature [46, Table 25.9].

B. Eve's Channel Model

Let $\mathbf{P}$ denote the coordinate of Alice's optical beam center on the receiver plane with no misalignment. When there are misalignments between Alice's transmitter and Bob's receiver, we assume that the beam displacements X' and Y' are in the x-direction and y-direction on Bob's receiver plane as plotted in Fig. 1a. Hence, the position of the optical beam center on the receiver plane is given as $\mathbf{Q} = \begin{bmatrix} X' \\ Y' \end{bmatrix} + \mathbf{P}$, where $\mathbf{Q}$ is the center of the misaligned beam footprint. Assuming a distance d between Eve's and Bob's positions on the receiver plane, we have $\|\mathbf{P}\|^2 = d^2 = \text{constant}$. The radial distance $r_E = \|\boldsymbol{r_E}\|$ between the beam center and Eve's aperture center can be presented as $r_E^2 = \|\mathbf{Q}\|^2 = \underbrace{\left\| \begin{bmatrix} X' \\ Y' \end{bmatrix} \right\|^2}_{r_B^2} + 2 \begin{bmatrix} X' \\ Y' \end{bmatrix}^T \mathbf{P} + \underbrace{\|\mathbf{P}\|^2}_{d^2}$, where $[\cdot]^T$ denotes the transpose of a matrix. Thus, the fraction of collected power at Eve's receiver with the radius a can be approximated as

$$h_{p,E}\left(r_E; L\right) \cong A_{mod} \exp\left(-\frac{2r_B^2}{w_{L,e(eq)}^2}\right) \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp\left(-U\right), \tag{14}$$

where $U = \frac{4}{w_{L,e(eq)}^2} \begin{bmatrix} X' \\ Y' \end{bmatrix}^T \mathbf{P}$. It should be noted that the independent Gaussian random variables X' and Y' with means $\{\mu_x, \mu_y\}$ and variances $\{\sigma_x^2, \sigma_y^2\}$ are approximated by two Gaussian random variables with zero means and variances $\sigma_x^2 = \sigma_y^2 = \sigma_{mod}^2$ [43], then U is also a Gaussian random variable with zero mean and variance $\sigma_U^2 = \frac{16\sigma_{mod}^2 d^2}{w_{L,e(eq)}^4}$. Eve's channel coefficient can then be expressed as

$$h_E = h_l h_t h_{p,E}. \tag{15}$$

Theorem 1. *Under the weak atmospheric turbulence modeled by an LN distribution, the PDF of Eve's channel coefficient can be expressed in a closed-form expression as*

$$f_{h_E}\left(h_E\right) = \frac{B_1 \exp\left(\frac{2d^2\varphi_{mod}^2}{w_{L,e(eq)}^2}\right)}{\left(A_{mod}h_l\right)^{\varphi_{mod}^2}} \left(h_E\right)^{\varphi_{mod}^2 - 1} \operatorname{erfc}\left(\frac{\ln\left(\frac{h_E}{A_{mod}h_l}\right) + \frac{2d^2}{w_{L,e(eq)}^2} + B_2}{\sqrt{2}\sigma_G}\right), \tag{16}$$

where $B_1 = \frac{\varphi_{mod}^2}{2}\exp\left(\frac{\varphi_{mod}^4\sigma_G^2}{2} - \varphi_{mod}^2\mu_G\right)$ *and* $B_2 = (\varphi_{mod}^2\sigma_G^2 - \mu_G)$, *with* μ_G *and* σ_G^2 *the mean and variance of a Gaussian random variable* G *given as* $\mu_G = -2\sigma_X^2$ *and* $\sigma_G^2 = \left(4\sigma_X^2 + \frac{16\sigma_{mod}^2 d^2}{w_{L,e(eq)}^4}\right)$.

Proof: Please see Appendix A. ■

Theorem 2. *Under the moderate-to-strong atmospheric turbulence modeled by a GG distribution, the PDF of Eve's channel coefficient can be expressed in a closed-form expression as*

$$f_{h_E}(h_E) = \frac{\sqrt{2}\sigma_{G'}B_1'\exp\left(-\varphi_{mod}^2 B_2'\right)}{\Gamma(\beta)}\sum_{k=1}^{M} C_k (D_k)^{\beta}\exp\left(-D_k h_E\right)(h_E)^{\beta-1}, \tag{17}$$

where $B_1' = \frac{\varphi_{mod}^2}{2}\exp\left(\frac{\varphi_{mod}^4\sigma_{G'}^2}{2} - \varphi_{mod}^2\mu_{G'}\right)$ *with* $\mu_{G'}$ *and* $\sigma_{G'}^2$ *the mean and variance of a Gaussian random variable* G' *given as* $\mu_{G'} = -\frac{1}{2}\ln\left(\frac{\alpha+1}{\alpha}\right)$ *and* $\sigma_{G'}^2 = \left(\ln\left(\frac{\alpha+1}{\alpha}\right) + \frac{16\sigma_{mod}^2 d^2}{w_{L,e(eq)}^4}\right)$. M *is the Gauss-Hermite approximation order,* $C_k = \mathrm{w}_k \mathrm{erfc}(x_k)\exp\left(x_k^2 + \sqrt{2}\sigma_{G'}\varphi_{mod}^2 x_k\right)$ *and* $D_k = \frac{\beta}{A_{mod}h_l\exp\left(\sqrt{2}\sigma_{G'}x_k - \frac{2d^2}{w_{L,e(eq)}^2} - B_2'\right)}$, *with* $B_2' = (\varphi_{mod}^2\sigma_{G'}^2 - \mu_{G'})$, w_k *and* x_k *are respectively the weight factors and the zeros of the Gauss-Hermite polynomial [46, Table 25.10].*

Proof: Please see Appendix B. ■

IV. Applications in Physical-Layer Security

A. System Model

Considering the FSO-WTC model, we assume a communications link using the IM/DD with on-off keying (OOK) modulation, in which the received electrical signals at Bob and Eve, respectively denoted as y_B and y_E, can be expressed as

$$y_B = h_B R_B x + n_B, \;\; y_E = h_E R_E x + n_E, \tag{18}$$

where $x \in \{0, 2P_t\}$ is the transmitted intensity taken as symbols drawn equiprobably from an OOK constellation, P_t is the average transmitted optical power, R_B and R_E are the responsivities of Bob's and Eve's receivers, n_B and n_E are the corresponding signal-dependent additive white

Gaussian noises (AWGNs) [41]. Hence, the received electrical signal-to-noise ratios (SNRs) at Bob and Eve for the OOK signaling over a fading channel can be respectively defined as

$$\mathrm{SNR}(h_B) = \frac{2P_t^2 R_B^2 h_B^2}{\sigma_{n,B}^2} = 4\gamma_B h_B^2, \ \mathrm{SNR}(h_E) = \frac{2P_t^2 R_E^2 h_E^2}{\sigma_{n,E}^2} = 4\gamma_E h_E^2, \tag{19}$$

where γ_B and γ_E denote the electrical SNRs in the absence of fading.

B. Secrecy Performance Metrics

Since the atmospheric turbulence and misalignments lead to a slowly varying channel, the fading can be considered constant over a large number of transmitted bits [40]. Hence, the capacity in the Shannon case does not exist and the probability of OSC stands out as a useful metric to probabilistically reflect how the instantaneous secrecy capacity is below a targeted rate C_T [27]. We assume that Eve is a purely passive eavesdropper, thus no channel state information (CSI) about Eve's channel is available to Alice and Bob. In this case, Alice has no choice but to set her secrecy rate to a constant C_T. Then, the probability of OSC can be defined as $\mathrm{OSC} = \Pr\left\{C_S\left(\gamma_B, \gamma_E\right) < C_T\right\}$, where $C_S\left(\gamma_B, \gamma_E\right)$ denotes the secrecy capacity written as

$$C_S\left(\gamma_B, \gamma_E\right) = \max\left\{B\log_2\left(1+4\gamma_B h_B^2\right) - B\log_2\left(1+4\gamma_E h_E^2\right), 0\right\}, \tag{20}$$

where B is the channel bandwidth [47]. Thus, the probability of OSC can be expressed as

$$\mathrm{OSC} = \Pr\left\{\log_2\left(\frac{1+4\gamma_B h_B^2}{1+4\gamma_E h_E^2}\right) < C_T\right\} = \int_0^\infty F_{h_B}\left(\sqrt{\frac{2^{C_T}\left(1+4\gamma_E h_E^2\right)-1}{4\gamma_B}}\right) f_{h_E(h_E)}\mathrm{d}h_E, \tag{21}$$

where $F_{h_B}(\cdot)$ denotes the cumulative distribution function (CDF) of Bob's channel. Since an exact closed-form solution for (21) is difficult to obtain, we thus aim to derive a lower bound for the OSC, which can be written as

$$\mathrm{OSC}_{LB} = \int_0^\infty F_{h_B}\left(2^{\frac{C_T}{2}}\sqrt{\frac{\gamma_E}{\gamma_B}}h_E\right) f_{h_E(h_E)}\mathrm{d}h_E. \tag{22}$$

Considering the atmospheric turbulence modeled by the GG distribution, with the help of [44, (18)] and Theorem 2, after some simple mathematical manipulations, (22) can be rewritten as

$$\mathrm{OSC}_{LB} = (I_1 + I_2), \tag{23}$$

where

$$I_1 = \frac{\sqrt{2}\sigma_{G'} B_1' \exp\left(-\varphi_{mod}^2 B_2'\right)}{\Gamma(\beta)(A_{mod}h_l)^{\varphi_{mod}^2}} \left(\frac{2^{C_T}\gamma_E}{\gamma_B}\right)^{\frac{\varphi_{mod}^2}{2}} \sum_{i=1}^{N}\sum_{k=1}^{M} a_i \xi_i^{-\alpha+\varphi_{mod}^2} C_k (D_k)^{\beta} \times \int_0^{\infty} h_E^{\varphi_{mod}^2+\beta-1} \exp(-D_k h_E)\Gamma\left(\alpha-\varphi_{mod}^2, \Upsilon_i h_E\right) \mathrm{d}h_E, \tag{24}$$

$$I_2 = \frac{\sqrt{2}\sigma_{G'} B_1' \exp\left(-\varphi_{mod}^2 B_2'\right)}{\Gamma(\beta)} \sum_{i=1}^{N}\sum_{k=1}^{M} a_i \xi_i^{-\alpha} C_k (D_k)^{\beta} \int_0^{\infty} h_E^{\beta-1} \exp(-D_k h_E)\gamma(\alpha, \Upsilon_i h_E) \mathrm{d}h_E, \tag{25}$$

where $\gamma(\cdot,\cdot)$ is the lower incomplete Gamma function defined in [45, (8.350.1)] and $\Upsilon_i = \frac{\xi_i}{A_{mod}h_l}\sqrt{\frac{2^{C_T}\gamma_E}{\gamma_B}}$. By applying [45, (6.455.1)] in (24) and [45, (6.455.2)] in (25), we derive the following closed-form expressions

$$I_1 = \frac{\sqrt{2}\sigma_{G'}\Gamma(\alpha+\beta) B_1' \exp\left(-\varphi_{mod}^2 B_2'\right)}{\left(\varphi_{mod}^2+\beta\right)\Gamma(\beta)(A_{mod}h_l)^{\alpha}} \left(\frac{2^{C_T}\gamma_E}{\gamma_B}\right)^{\frac{\alpha}{2}} \sum_{i=1}^{N}\sum_{k=1}^{M} \frac{a_i C_k (D_k)^{\beta} {}_2F_1\left(1, \alpha+\beta; \varphi_{mod}^2+\beta+1; \frac{D_k}{\Upsilon_i+D_k}\right)}{(\Upsilon_i+D_k)^{\alpha+\beta}}, \tag{26}$$

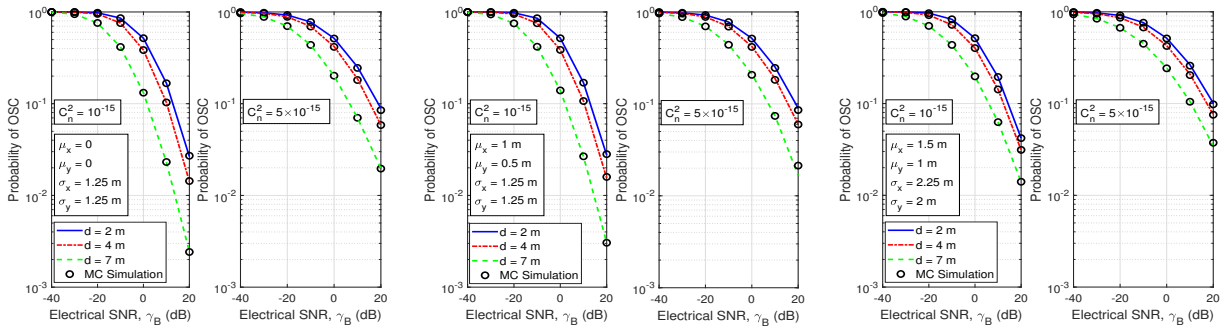
$$I_2 = \frac{\sqrt{2}\sigma_{G'}\Gamma(\alpha+\beta) B_1' \exp\left(-\varphi_{mod}^2 B_2'\right)}{\alpha\Gamma(\beta)(A_{mod}h_l)^{\alpha}} \left(\frac{2^{C_T}\gamma_E}{\gamma_B}\right)^{\frac{\alpha}{2}} \sum_{i=1}^{N}\sum_{k=1}^{M} \frac{a_i C_k (D_k)^{\beta} {}_2F_1\left(1, \alpha+\beta; \alpha+1; \frac{\Upsilon_i}{\Upsilon_i+D_k}\right)}{(\Upsilon_i+D_k)^{\alpha+\beta}}, \tag{27}$$

where ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ denotes the Gauss hypergeometric function defined in [45, (9.14)]. Plugging (26) and (27) into (23), a closed-form expression of the lower bound of the OSC can be obtained.

Another important benchmark to emphasize the existence of a secure communication is the probability of SPSC defined as [47]

$$\text{SPSC} = \Pr\left\{C_S\left(\gamma_B, \gamma_E\right) > 0\right\} = 1 - \text{OSC}|_{C_T=0}. \tag{28}$$

From (21), it is deduced that the lower bound of OSC becomes the exact form when $C_T = 0$. Thus, the exact closed-form expression of SPSC can be attained by substituting (26) and (27) into (28) and setting $C_T = 0$.



(a) (b) (c)

Fig. 2. Probability of OSC for different Eve's locations and channel conditions, $F_0 = -10$ m, $w_0 = 0.01$ m, $a = 5$ cm, $\gamma_E = 0$ dB, $C_T = 0.5$ bits/channel use, $N = 10$, $M = 40$. (a) Zero boresight misalignments; (b) Non-zero boresight misalignments; (c) Generalized misalignments.

C. Numerical Results

To investigate the impact of Eve's locations on the instantaneous secrecy capacity with respect to the targeted rate C_T, Fig. 2 depicts the probability of OSC versus γ_B under different misalignments and turbulence conditions. MC simulations are also performed to confirm the accuracy of the derived closed-form expressions. Regarding the OSC analysis, we will highlight four main observations. Firstly, for all misalignments and turbulence conditions, the probability of OSC always increases when Eve is closer to Bob. However, the gain of OSC depends on the severity of misalignments. It is seen that the gain of OSC in Figs. 2a and 2b when Eve moves from $d = 7$ m to $d = 4$ m increases more quickly than that in Fig. 2c. This indicates that Eve should move closer to Bob to achieve a better gain under less severe misalignments. Secondly, at the same distance d and turbulence conditions, the probability of OSC in Fig. 2c is higher than that in Figs. 2a and 2b. This is because Eve is more likely to benefit from the misaligned beam under more severe misalignments, especially at a further distance d. Thirdly, it is interesting to observe that the stronger turbulence actually helps to reduce the probability OSC when $\gamma_B \ll \gamma_E$, however it becomes the adverse factor when $\gamma_B \geq \gamma_E$, regardless of

the severity of misalignments. Finally, the OSC is more likely to happen when $\gamma_B \ll \gamma_E$. For instance, when $\gamma_B = -20$ dB and $\gamma_E = 0$ dB, the probability of OSC is roughly more than 70% for all cases. Based on (28) and the results from Fig. 2, similar conclusions can be drawn for the SPSC by understanding that a higher probability of OSC corresponds to a lower probability of SPSC (i.e. a secure communications is less likely to exist) and vice versa. The results of SPSC are not shown due to the space limitation.

V. Applications in IM/DD Free-Space CV-QKD System

A. System Operation

In conventional QKD protocols, e.g. BB84 protocol, the key information is encoded by Alice in four states of photon polarizations, forming two non-orthogonal bases, and transmitted to Bob. Alice and Bob then communicate over a public channel, and if Alice's encoding and Bob's decoding bases are the same, the corresponding key bit is read. Otherwise, the measurements are discarded, leaving the remaining bits as the *sifted key*. Alice and Bob may further perform the *information reconciliation* and *privacy amplification* to produce a shorter key about which Eve has only negligible information [12]. By mimicking the concept of BB84, however, utilizing two non-orthogonal coherent states of optical pulses, the IM/DD free-space CV-QKD system using subcarrier intensity modulation (SIM)/binary phase shift keying (BPSK) with dual-threshold (DT) detection has been recently proposed in [20]. Specifically, Alice transmits SIM/BPSK intensity-modulated signals as coherent states with a modulation depth δ ($0 < \delta < 1$), corresponding to binary random key bits "0" or "1", over the atmospheric channel. Due to the relatively small δ, the two signals are partially overlapped, being non-orthogonal to each other. To detect bits "0" and "1" on the received signals, Bob sets two detection thresholds d_0 and d_1 at low and high levels, respectively, based on a decision rule as $x = \begin{cases} 0 & \text{if} \quad x_d \leq d_0, \\ 1 & \text{if} \quad x_d \geq d_1, \\ \text{X} & \text{otherwise}, \end{cases}$ where x denotes the

transmitted signal, x_d is the detected value of x, and "X" represents the case that Bob creates no bit, i.e. the detected signal is discarded. Then, using a classical public channel, Bob notifies Alice of the time instants he was able to infer key bits from detected signals. Alice subsequently discards bits according to time instants that Bob inferred no bit. As a result, Alice and Bob share an identical bit string, i.e. *sifted key*. By obtaining the CSI estimation, the thresholds d_0 and d_1 can be adjusted, thus the probability of sift at Bob's receiver can be controlled. Although Eve may try to use the DT as Bob does, the fluctuations in the signals received by Bob and Eve are different due to the independent fading channels and receivers' quantum noises, hence resulting in different sifted key bits [20]. Therefore, to receive as much information as possible, Eve is assumed to set the "hard" threshold at $d_E = 0$, which is the optimal one to detect symmetric BPSK signaling[1]. Eve's error probability is hence dependent on how much the two transmitted signals from Alice is overlapped. For the secrecy analysis, the important system design criteria for the legitimate transceivers would be the modulation depth δ at Alice's transmitter and the DT scale coefficient at Bob's receiver (namely ζ, introduced later in Section V-C1) to adjust d_0 and d_1 with respect to the mean values of received signals.

B. System Model

Figure 3 presents a block diagram of the considered free-space CV-QKD system. At the transmitter, the source data $d(t)$ is modulated onto an RF subcarrier signal using BPSK scheme in which bits "0" and "1" are represented by two different phases 180° apart. The subcarrier signal $m(t)$ is sinusoidal having both positive and negative values, thus a direct current (DC) bias is added to $m(t)$ before it is used to modulate a continuous-wave laser beam. The transmitted

[1]It is noted that more sophisticated detection schemes could be also considered. For example, Eve may apply soft-information measurements which could possibly yield higher (or equal) information rate compared to the hard measurement case [17]. Nevertheless, our proposed analytical framework can be straightforwardly applied for further investigations with more powerful assumptions on Eve's detection schemes.

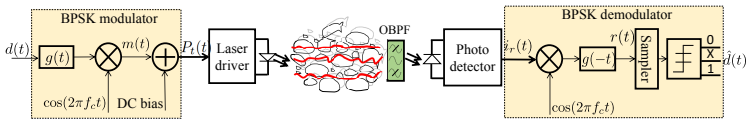


Fig. 3. A block diagram of the considered free-space CV-QKD system using SIM/BPSK with a DT receiver.

power thus can be expressed as $P_t(t) = \frac{P}{2}[1 + \delta m(t)]$, where P represents the peak transmitted power, and δ is the intensity modulation depth. Considering a single symbol duration, $m(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$, where $A(t)$ is the subcarrier amplitude, $g(t)$ is the rectangular pulse shaping function, f_c is the subcarrier frequency, and $a_i \in [0, 1]$ represents the ith binary data. For the sake of simplicity, $m(t)$ is normalized to unity.

At the receiver, the incoming optical field is passed through an optical bandpass filter (OBPF) to limit the amount of background radiation noise before being converted into an electrical signal through the direct detection at an avalanche photodiode (APD). A standard coherent demodulator is employed to recover the source data $\hat{d}(t)$. As a result, the electrical signal at the output of the APD at Bob's receiver can be expressed as $i_r(t) = R\bar{g}\frac{P}{2}h(t)[1 + \delta m(t)] + n(t)$, where $R = \frac{\eta q}{\widetilde{h}\mathrm{v}}$ is the responsivity of the APD with η the quantum efficiency, q the electron charge, $\widetilde{h}$ the Planck's constant, v the optical frequency; $\bar{g}$ is the average APD gain, and $n(t)$ is the receiver noise. Since the fading channel coefficient $h(t)$ varies slowly enough, the DC component can be filtered out. The electrical signal $i_r(t)$ is then passed through the BPSK demodulator. The output signal $r(t)$ is demodulated by the reference signal $\cos(2\pi f_c t)$ as

$$r(t) = \overline{i_r(t)\cos(2\pi f_c t)} = \begin{cases} i_0 = -\frac{1}{4}R\bar{g}P\delta h(t) + n(t) \\ i_1 = \ \ \frac{1}{4}R\bar{g}P\delta h(t) + n(t) \end{cases}, \tag{29}$$

where i_0 and i_1 represent the received current signals for bits "0" and "1", respectively. The receiver noise $n(t)$ is modeled as the zero-mean AWGN [48], with the variance $\sigma_N^2 = \sigma_{sh}^2 + \sigma_b^2 + \sigma_{th}^2$, where σ_{sh}^2, σ_b^2, and σ_{th}^2 are respectively the variances of the APD shot noises caused by the received signal, background noise, and receiver thermal noise, calculated as $\sigma_{sh}^2 =$

$2q\bar{g}^2RF_A\left(\frac{1}{4}P\delta h\right)\Delta_f$, $\sigma_b^2 = 2q\bar{g}^2RF_AP_b\Delta_f$, $\sigma_{th}^2 = \frac{4k_BTF_n}{R_L}\Delta_f$, where $F_A = k_A\bar{g} + \left(2 - \frac{1}{\bar{g}}\right)(1 - k_A)$ denotes the excess noise factor with k_A the ionization factor, F_n is the amplifier noise figure, P_b is the average received background radiation power, $\Delta_f = \frac{R_b}{2}$ is the effective noise bandwidth with R_b the system bit rate, T is the receiver temperature, and R_L is the APD's load resistance [49]. After the demodulating process, the demodulated electrical signals are sampled and then used to recover binary bits "0" and "1" based on the decision rule, forming Bob's raw key. Bob then notify Alice of the time instants that only bits "0" and "1" were created so that Alice can discard the key bits transmitted at other time instants, forming their shared *sifted key*.

C. Secrecy Performance Metrics

1) Quantum Bit Error Rate: The QBER is defined as [12]

$$\text{QBER} = \frac{P_{error}}{P_{sift}} = \frac{P_{A,B}(0,1) + P_{A,B}(1,0)}{P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1)}, \tag{30}$$

where P_{sift} is the probability that Bob can infer bits "0" and "1" from the detection thresholds, and P_{error} is the probability of error in all detected bits. $P_{A,B}(a,b)$ $(a,b \in \{0,1\})$ is the joint probability that Alice's bit "a" coincides with Bob's bit "b". These joint probabilities, averaged over the fading channel, can be expressed as

$$P_{A,B}(a,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{i_a - d_0}{\sigma_N}\right) f_{h_B}(h_B)\,\mathrm{d}h_B, \tag{31}$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_1 - i_a}{\sigma_N}\right) f_{h_B}(h_B)\,\mathrm{d}h_B, \tag{32}$$

where $a \in \{0,1\}$, $i_0 = -\frac{1}{4}R\bar{g}P\delta h_l h_t h_{p,B}$ and $i_1 = -i_0$. $Q(\cdot) \triangleq \frac{1}{\sqrt{2\pi}}\int_0^\infty \exp(-t^2/2)\mathrm{d}t$ is the Gaussian Q-function. At the DT receiver, d_0 and d_1 are given as

$$d_0 = \mathbb{E}[i_0] - \zeta\sqrt{\sigma_N^2}, \quad \text{and} \quad d_1 = \mathbb{E}[i_1] + \zeta\sqrt{\sigma_N^2}, \tag{33}$$

where ζ is the *DT scale coefficient* to adjust the detection levels of d_0 and d_1, σ_N^2 is the receiver noise variance. $\mathbb{E}[i_0]$ and $\mathbb{E}[i_1]$ are the mean values of i_0 and i_1, respectively. With $\mathbb{E}[h_t] = 1$

and $\mathbb{E}[h_{p,B}]$ given in (11), $\mathbb{E}[i_0]$ and $\mathbb{E}[i_1]$ can be respectively calculated as

$$\mathbb{E}[i_0] = -\frac{1}{4} R\bar{g} P \delta h_l \left(\frac{A_{mod}\varphi_{mod}^2}{1+\varphi_{mod}^2} \right), \quad \text{and} \quad \mathbb{E}[i_1] = -\mathbb{E}[i_0]. \tag{34}$$

Applying Theorem 1 in (31) and (32), making a change of variables then using Gauss-Hermite polynomial approximation [46, Table 25.10], under the weak atmospheric turbulence modeled by an LN distribution, (31) and (32) can be expressed in closed-form expressions as

$$P_{A,B}(a,0) = \frac{\varphi_{mod}^2 \sigma_X \exp\left(-2\sigma_X^2 \varphi_{mod}^4\right)}{\sqrt{2}} \sum_{k=1}^{M} \mathrm{w}_k \mathrm{erfc}\left(x_k\right) \exp\left(x_k^2 + \sqrt{8}\sigma_X \varphi_{mod}^2 x_k\right) Q\left(\frac{i_a(k) - d_0}{\sigma_{N(k)}}\right), \tag{35}$$

$$P_{A,B}(a,1) = \frac{\varphi_{mod}^2 \sigma_X \exp\left(-2\sigma_X^2 \varphi_{mod}^4\right)}{\sqrt{2}} \sum_{k=1}^{M} \mathrm{w}_k \mathrm{erfc}\left(x_k\right) \exp\left(x_k^2 + \sqrt{8}\sigma_X \varphi_{mod}^2 x_k\right) Q\left(\frac{d_1 - i_a(k)}{\sigma_{N(k)}}\right), \tag{36}$$

where $\sigma_{N(k)} = \sqrt{2qF_A\bar{g}^2R\left[\frac{1}{4}P\delta A_{mod}h_l \exp\left(\sqrt{8}\sigma_X x_k - 2\sigma_X^2\left(1+2\varphi_{mod}^2\right)\right) + P_b\right]\Delta_f + \frac{4k_BTF_n}{R_L}\Delta_f}$, $i_a(k) = \mp\frac{1}{4}R\bar{g}P\delta A_{mod}h_l \exp\left(\sqrt{8}\sigma_X x_k - 2\sigma_X^2\left(1+2\varphi_{mod}^2\right)\right)$. Similarly, applying Theorem 2 in (31) and (32), making a change of variables then using Gauss-Hermite polynomial approximation [46, Table 25.10] with the help of [45, (8.351.4) and (9.210.2)], under the moderate-to-strong atmospheric turbulence modeled by a GG distribution, (31) and (32) can be expressed in closed-form expressions as

$$P_{A,B}\left(a,0\right) = \frac{\varphi_{mod}^2}{2} \sum_{i=1}^{N} \sum_{k=1}^{M} a_i \xi_i^{-\alpha} \mathrm{w}_k x_k^{\varphi_{mod}^2 - 1} \Psi_i\left(x_k\right) Q\left(\frac{i_a(k) - d_0}{\sigma_{N(k)}}\right), \tag{37}$$

$$P_{A,B}\left(a,1\right) = \frac{\varphi_{mod}^2}{2} \sum_{i=1}^{N} \sum_{k=1}^{M} a_i \xi_i^{-\alpha} \mathrm{w}_k x_k^{\varphi_{mod} - 1} \Psi_i\left(x_k\right) Q\left(\frac{d_1 - i_a(k)}{\sigma_{N(k)}}\right), \tag{38}$$

where $i_a(k) = \mp\frac{1}{4\xi_i}R\bar{g}P\delta A_{mod}h_l x_k$, $\Psi_i(x_k) = \Gamma(\alpha - \varphi_{mod}^2)\,{}_1F_1(1-\alpha+\varphi_{mod}^2, 1-\alpha+\varphi_{mod}^2; x_k) + \frac{\Gamma\left(\varphi_{mod}^2 - \alpha\right)x_k^{(\alpha-\varphi_{mod}^2)}}{\Gamma\left(1-\alpha+\varphi_{mod}^2\right)}\,{}_1F_1(1, 1+\alpha-\varphi_{mod}^2; x_k)$ with ${}_1F_1\left(\cdot,\cdot;\cdot\right)$ the confluent hypergeometric function defined in [45, (9.210.1)]. The closed-form expression for QBER at Bob's receiver can be straightforwardly derived by applying (35) to (38) in (30).

2) Ergodic Secret-Key Rate: To validate the security of the considered system, we investigate the ergodic (i.e. average) SKR denoted as S, over the atmospheric channel. If S is positive, it is concluded that the system is secured as the amount of information gained by Eve can be theoretically decreased through the privacy amplification. Otherwise, the system is vulnerable to Eve's intervention as she obtains a larger amount of information compared to Bob. The ergodic SKR, defined as the maximum transmission rate at which the eavesdropper is unable to decode any information, is given as

$$S = I(A;B) - I(A;E), \tag{39}$$

where the mutual information $I(A;B)$ and $I(A;E)$ are defined as the estimations of the amount of information shared between Alice and Bob, and that shared between Alice and Eve, respectively[2] [13]. $I(A;B)$ and $I(A;E)$ can be calculated as $I(A;B) = H(B) - H(B|A)$, and $I(A;E) = H(E) - H(E|A)$, where $H(B)$ and $H(E)$ are the information entropies of Bob and Eve, $H(B|A)$ and $H(E|A)$ are the conditional entropies of Bob-Alice and Eve-Alice, respectively. As Alice and Bob share information over the binary erasure channel (BEC) with errors, the mutual information $I(A;B)$ is readily given as $I(A;B) = p\log_2(p)+(1-p-q)\log_2(1-p-q)-\left(\frac{p}{2}+\frac{(1-p-q)}{2}\right)\log_2\left(\frac{p}{2}+\frac{(1-p-q)}{2}\right)-\left(\frac{(1-p-q)}{2}+\frac{p}{2}\right)\log_2\left(\left(\frac{(1-p-q)}{2}+\frac{p}{2}\right)\right)$, where the probabilities of transmitting bits "0" and "1" are assumed to equally likely occur, p and q are the conditional probabilities corresponding to $P_{B|A}(b,a)$ with $a \in \{0,1\}$ and $b \in \{0,1,\mathrm{X}\}$ [20]. The closed-form expressions for these probabilities can be straightforwardly derived using (35) to (38). On the other hand, Eve obtains a bit string by eavesdropping the signals using the optimal detection

[2]It is noted that (39) corresponds to the uni-directional error-correction protocol in the information reconciliation process, in which the error-correcting information is sent from Alice through the public channel to Bob. Although other types of error-correction protocols, e.g. bidirectional or reverse reconciliation, can also be employed [15], [16], they are not considered for the sake of conciseness. In practice, the error-correction efficiency should be considered, nevertheless, we assume in this paper the perfect efficiency, serving as an upper bound evaluation of the system performance.

threshold $d_E = 0$, whose bit values are partially identical to Alice's. Thus, Alice and Eve share some information via the binary symmetric channel (BSC), for which the mutual information can be given as

$$I(A;E) = 1 + P_E \log_2(P_E) + (1 - P_E)\log_2(1 - P_E), \tag{40}$$

where $P_E = P_{A,E}(0,1) + P_{A,E}(1,0)$ is Eve's error probability with $P_{A,E}(0,1)$ and $P_{A,E}(1,0)$ the joint probabilities that Eve falsely detects Alice's transmitted bits using the threshold d_E. $P_{A,E}(0,1)$ and $P_{A,E}(1,0)$ with $d_E = 0$ averaged over the fading channel can be expressed as

$$P_{A,E}(0,1) = P_{A,E}(1,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{i_E}{\sigma_{N,E}}\right) f_{h_E}(h_E)\,\mathrm{d}h_E, \tag{41}$$

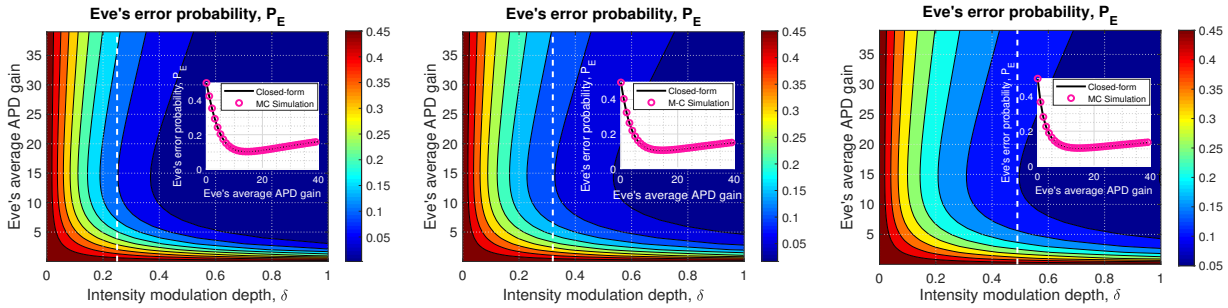
where $i_E = \frac{1}{4}R\bar{g}P\delta h_E$, $\sigma^2_{N,E}$ is the noise variance at Eve's receiver. Applying Theorem 1 in (41), making a change of variables then using Gauss-Hermite polynomial approximation [46, Table 25.10], under the weak atmospheric turbulence modeled by an LN distribution, (41) can be expressed in a closed-form expression as

$$P_{A,E}(0,1)=P_{A,E}(1,0)=\frac{\sigma_G B_1 \exp(-\varphi^2_{mod}B_2)}{\sqrt{2}}\sum_{k=1}^{M} \mathrm{w}_k \mathrm{erfc}(x_k)\exp\left(x_k^2+\sqrt{2}\sigma_G\varphi^2_{mod}x_k\right)Q\left(\frac{i_E(i,k)}{\sigma_{N,E(k)}}\right), \tag{42}$$

where $\sigma_{N,E(k)} = \sqrt{2qF_A\bar{g}^2R\left[\frac{1}{4}P\delta A_{mod}h_l\exp\left(\sqrt{2}\sigma_G x_k - \frac{2d^2}{w^2_{L,e(eq)}} - B_2\right) + P_b\right]\Delta_f + \frac{4k_BTF_n}{R_L}\Delta_f}$, $i_E(i,k) = \frac{1}{4}R\bar{g}P\delta A_{mod}h_l\exp\left(\sqrt{2}\sigma_G x_k - \frac{2d^2}{w^2_{L,e(eq)}} - B_2\right)$. Similarly, applying Theorem 2 in (41) making a change of variables, then using Gauss-Laguerre polynomial approximation [46, Table 25.9], under the moderate-to-strong atmospheric turbulence modeled by a GG distribution, (41) can be expressed in a closed-form expression as

$$P_{A,E}(0,1) = P_{A,E}(1,0) = \frac{\sigma_{G'}B_1'\exp(-\varphi^2_{mod}B_2')}{\sqrt{2}\Gamma(\beta)}\sum_{i=1}^{N}\sum_{k=1}^{M} C_k\omega_i t_i^{\beta-1}Q\left(\frac{i_E(i,k)}{\sigma_{N,E(i,k)}}\right), \tag{43}$$

where $i_E(i,k) = \frac{1}{4D_k}R\bar{g}P\delta t_i$, $\sigma_{N,E(i,k)}=\sqrt{2qF_A\bar{g}^2R\left(\frac{P\delta t_i}{4D_k}+P_b\right)\Delta_f+\frac{4k_BTF_n}{R_L}\Delta_f}$. The final closed-form expression for (40) can be straightforwardly derived by utilizing (42) and (43). Based on (35) to (43), the closed-form expression of the ergodic SKR in (39) can be readily obtained.



(a) (b) (c)

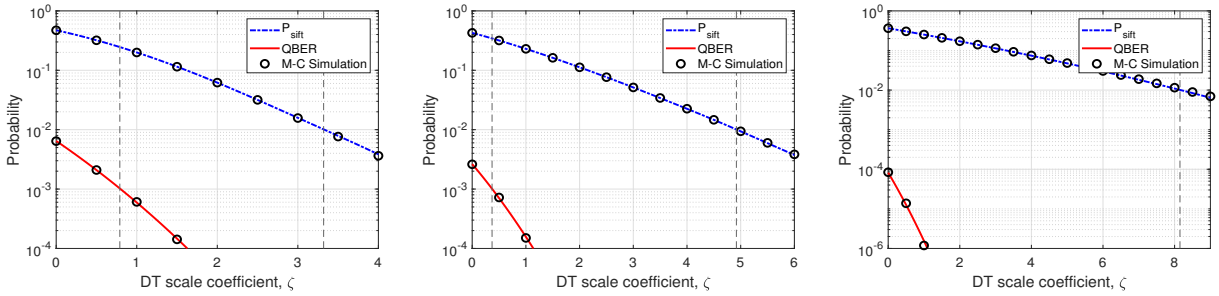
Fig. 4. (a) Weak turbulence $C_n^2 = 3 \times 10^{-16}$, $d = 0.17$ m; (b) Moderate turbulence $C_n^2 = 10^{-15}$, $d = 0.18$ m; (c) Strong turbulence $C_n^2 = 5 \times 10^{-15}$, $d = 0.22$ m. Closed-form approximation order $N = M = 100$.

D. Numerical Results

In this section, the design criteria at Alice and Bob (i.e. intensity modulation depth δ and DT scale coefficient ζ, respectively) that guarantee a positive ergodic SKR S of the IM/DD free-space CV-QKD system can be determined. The system parameters used in the analysis, unless otherwise noted, include $F_0 = -10$ m, $w_0 = 0.01$ m, $P = 23$ dBm, $\mu_x = \mu_y = 0$, $\sigma_x = \sigma_y = 1.25$ m, $R_b = 1$ Gbps, and $a = 5$ cm for both Bob's and Eve's receivers. Other receiver noise parameters are taken from [20].

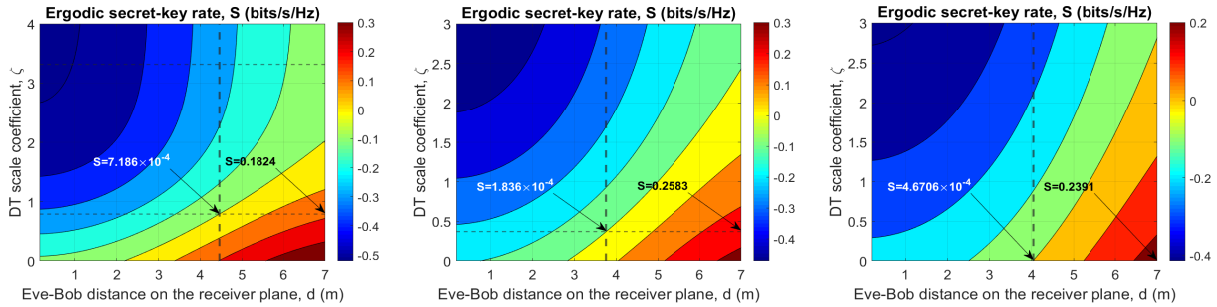
Figure 4 illustrates Eve's error probability P_E to discover the proper selection of δ at Alice's transmitter so that P_E is sufficiently high, e.g. $P_E \geq 0.1$. It is seen from Fig. 4 that Alice should respectively select $\delta \leq 0.25$, $\delta \leq 0.32$, and $\delta \leq 0.49$, under weak, moderate, and strong turbulence so that $e \geq 0.1$ even when Eve sets the optimal APD gain $\bar{g} = 15$. The insets in Fig. 4 show e versus $\bar{g}$ for different turbulence conditions with the corresponding maximum values of δ that limit $P_E \cong 0.1$. An excellent agreement between closed-form results and MC simulations can be observed.

Based on the δ chosen at Alice's transmitter, Fig. 5 shows QBER and P_{sift} versus the DT scale coefficient ζ to find out the selection range guaranteeing $P_{sift} \geq 10^{-2}$ (e.g. to receive



(a) (b) (c)

Fig. 5. (a) Weak turbulence $C_n^2 = 3\times10^{-16}$, $\delta = 0.25$; (b) Moderate turbulence $C_n^2 = 10^{-15}$, $\delta = 0.32$; (c) Strong turbulence $C_n^2 = 5\times10^{-15}$, $\delta = 0.49$. Closed-form approximation order $N = M = 100$.



(a) (b) (c)

Fig. 6. (a) Weak turbulence $C_n^2 = 3\times10^{-16}$, $\delta = 0.25$; (b) Moderate turbulence $C_n^2 = 10^{-15}$, $\delta = 0.32$; (c) Strong turbulence $C_n^2 = 5\times10^{-15}$, $\delta = 0.49$. Closed-form approximation order $N = M = 100$.

sufficient key bits) and QBER$\leq 10^{-3}$ (e.g. to feasibly correct bit errors using error-correction codes in the information reconciliation process) [20]. As seen in Figs. 5a, 5b, and 5c, the selection ranges for ζ corresponding to weak, moderate, and strong turbulence conditions are respectively as $0.79 \leq \zeta \leq 3.32$, $0.37 \leq \zeta \leq 4.92$, and $0 \leq \zeta \leq 8.15$. MC simulations are additionally performed and a good agreement with analytical results can be confirmed.

Finally, it is able to observe in Fig. 6 how the ergodic SKR S changes from negative to positive, indicating when Eve gains more or less information depending on eavesdropping locations. The final key-creation rates can be straightforwardly derived as $R_f = P_{sift}R_bS$ [20]. It is necessary to

select the smallest value of ζ so that a positive S can be guaranteed with Eve's closest location to Bob, e.g. $\zeta = 0.79$, $\zeta = 0.37$, and $\zeta = 0$ under weak, moderate, and strong turbulence, respectively. Here, P_{sift} corresponding to the selected ζ can be extracted from results in Fig. 3 as 0.246, 0.344, and 0.365, respectively. With these selections, the smallest positive S in Figs. 6a, 6b, and 6c are 7.186×10^{-4}, 1.836×10^{-4}, and 4.6706×10^{-4} bits/s/Hz[3], if Eve's locations d are 4.46 m, 3.76 m, and 4.04 m, respectively. This means our system can always generate a secret key if a security distance of about 4.5 m from Bob's receiver could be guaranteed.

The SKR would be much higher if Eve is further away from Bob. For instance, when Eve's location is $d = 7$ m, the ergodic SKRs S are about 0.1824, 0.2583, and 0.2391 bits/s/Hz corresponding to R_f at roughly 44.87, 88.85, and 87.27 Mbps under weak, moderate, and strong turbulence, respectively. It is noted that these key rates correspond to the worst-case scenario in the considered FSO-WTC model. The key rate can be significantly enhanced up to hundreds of Mbps, if a fine-pointing system is installed or Eve is further behind Bob. In practice, our system requires a channel monitoring mechanism to adapt the transmitter's δ and receiver's ζ to different turbulence regimes.

VI. Conclusion

This paper is marked as the first framework in the literature for the secrecy analysis of a terrestrial FSO system under all channel conditions considering the eavesdropper's location. The important results of this framework are the PDFs of the legitimate and eavesdropping channels considering the atmospheric turbulence and generalized misalignments. By applying the proposed PDFs, all combined effects of the atmospheric turbulence, transceiver misalignments, receiver noises, and the eavesdropper's location were comprehensively analyzed for the PLS and IM/DD

[3]The information rate can be expressed in terms of spectral bandwidth efficiency in bits/s/Hz if the frequency response of the channel is known [50]. In this paper, the given bandwidth is 1 GHz which is equal to the system bit rate $R_b = 1$ Gbps.

free-space CV-QKD systems. Finally, MC simulations further confirmed the correctness of the derived analytical results.

APPENDIX A
PROOF OF THEOREM 1

Plugging (1), (2), and (14) into (15), Eve's channel coefficient can be expressed as

$$h_E = A_{mod} h_l \exp\left(-\frac{2r_B^2}{w_{L,e(eq)}^2}\right) \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp\left(\hat{X} - U\right), \tag{44}$$

where $\hat{X} = 2X$ with X is the log-amplitude of the optical intensity given in (2). As a result, we have $\mu_{\hat{X}} = 2\mu_X = -2\sigma_X^2$ and $\sigma_{\hat{X}}^2 = 4\sigma_X^2$. Let $\exp(G) = \exp\left(\hat{X} - U\right)$, where G is also Gaussian distributed with mean $\mu_G = \mu_{\hat{X}} = -2\sigma_X^2$ and $\sigma_G^2 = \sigma_{\hat{X}}^2 + \sigma_U^2 \cong 1.23\left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2 + \frac{16\sigma_{mod}^2 d^2}{w_{L,e(eq)}^4}$. The channel coefficient in (44) is then simplified to

$$h_E = A_{mod} h_l \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp(G - T), \tag{45}$$

where $T = \frac{2r_B^2}{w_{L,e(eq)}^2}$ is an exponential random variable with a PDF given by $f_T(t) = \varphi_{mod}^2 \exp(-\varphi_{mod}^2 t)$. Now, let $V = G - T$, the PDF of V can be expressed in a closed-form expression as [51, (21)]

$$f_V(v) = B_1 \exp\left(\varphi_{mod}^2 v\right) \operatorname{erfc}\left(\frac{v + B_2}{\sigma_G}\right), \tag{46}$$

where $B_1 = \frac{\varphi_{mod}^2}{2} \exp\left(\varphi_{mod}^4 \frac{\sigma_G^2}{2} - \varphi_{mod}^2 \mu_G\right)$ and $B_2 = (\varphi_{mod}^2 \sigma_G^2 - \mu_G)$. Substituting (45) into (46) and making a change of variables completes the proof.

APPENDIX B
PROOF OF THEOREM 2

Plugging (1), (4), and (14) into (15), Eve's channel coefficient can be expressed as

$$h_E = A_{mod} h_l \exp\left(-\frac{2r_B^2}{w_{L,e(eq)}^2}\right) \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp(-U)\, Y_l Y_s, \tag{47}$$

For the sake of mathematical derivation, we consider Y_l as an LN random variable while keeping Y_s as the Gamma random variable. It is noteworthy that assuming Y_l as an LN random variable

inherently aligns with the nature of large-scale fluctuations. To reflect the impact of moderate-to-strong turbulence characterized by the GG model, the LN random variable Y_l is approximated with a Gamma one using the moment matching method. As a result, Eve's channel coefficient in (47) can be rewritten as

$$h_E = A_{mod} h_l \exp\left(-\frac{2r_B^2}{w_{L,e(eq)}^2}\right) \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp\left(\hat{\chi} - U\right) Y_s, \tag{48}$$

where $\hat{\chi}$ is a Gaussian random variable with $\mu_{\hat{\chi}} = -\frac{1}{2}\ln\left(\frac{\alpha+1}{\alpha}\right)$ and $\sigma_{\hat{\chi}}^2 = \ln\left(\frac{\alpha+1}{\alpha}\right)$. Let $\exp\left(G'\right) = \exp\left(\hat{\chi} - U\right)$, where G' is also Gaussian distributed with mean $\mu_{G'} = \mu_{\hat{\chi}}$ and variance $\sigma_{G'}^2 = \sigma_{\hat{\chi}}^2 + \sigma_U^2 = \left(\ln\left(\frac{\alpha+1}{\alpha}\right) + \frac{16\sigma_{mod}^2 d^2}{w_{L,e(eq)}^4}\right)$. The channel coefficient in (47) is then simplified to

$$h_E = A_{mod} h_l \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp\left(G' - T\right) Y_s, \tag{49}$$

where $T = \frac{2r_B^2}{w_{L,e(eq)}^2}$ is an exponential random variable with a PDF given by $f_T(t) = \varphi_{mod}^2 \exp(-\varphi_{mod}^2 t)$. Let $Z = A_{mod} h_l \exp\left(-\frac{2d^2}{w_{L,e(eq)}^2}\right) \exp\left(G' - T\right)$, then the PDF of Z, i.e. $f_Z(z)$, follows Theorem 1 and that of Y_s follows a Gamma distribution as $f_{Y_s}(y_s) = \frac{\beta^\beta y_s^{\beta-1}}{\Gamma(\beta)} \exp(-\beta y_s)$. The PDF of Eve's channel coefficient is now expressed as

$$f_{h_E}\left(h_E\right) = \int f_{h_E|Y_s}\left(h_E|Y_s\right) f_{Y_s}\left(y_s\right) \mathrm{d}y_s = \int \frac{1}{y_s} f_Z\left(\frac{h_E}{y_s}\right) f_{Y_s}\left(y_s\right) \mathrm{d}y_s. \tag{50}$$

Making a change of variables and applying Hermite polynomial approximation $\int_{-\infty}^{\infty} g\left(x\right) \mathrm{d}x \approx \sum_{k=1}^{M} \mathrm{w}_k g\left(x_k\right) \exp\left(x_k^2\right)$ [46, Table 25.10] completes the proof.

APPENDIX C
LIST OF ACROYMS

APD Avalanche photodiode

AWGN Additive white Gaussian noise

BEC Binary erasure channel

BPSK Binary phase shift keying

BSC Binary symmetric channel

CDF Cumulative distribution function

CSI Channel state information

CV-QKD Continuous-variable quantum key distribution

DPSK Differential phase shift keying

DV-QKD Discrete-variable quantum key distribution

DC Direct current

DT Dual threshold

FSO Free-space optical

GG Gamma-Gamma

IM/DD Intensity-modulation/direct-detection

ITS Information theoretical security

LN Log-normal

MC Monte-Carlo

OBPF Optical bandpass filter

OOK On-off keying

OSC Outage secrecy capacity

PDF Probability density function

PLS Physical layer security

QBER Quantum bit error rate

QKD Quantum key distribution

RF Radio frequency

SIM Subcarrier intensity modulation

SKA Secret-key agreement

SKR Secret-key rate

SNR Signal-to-noise ratio

SPSC Strictly positive secrecy capacity

REFERENCES

[1] H. Dahrouj *et al.*, "Cost-effective hybrid RF/FSO backhaul solution for next generation wireless systems," *IEEE Wireless Commun.,* vol. 22, no. 5, pp. 98–104, Oct. 2015.

[2] W. Stallings, *Cryptography and network security: principles and practice,* 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.

[3] L. Gomes, "Quantum computing: both here and not here," *IEEE Spectr.,* vol. 55, no. 4, pp. 42–47, Apr. 2018.

[4] A. Mukherjee *et al.*, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Commun. Surveys Tuts.,* vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.,* vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory,* vol. 24, no. 3, pp. 339–348, May 1978.

[7] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Inform. Theory,* vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[8] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Trans. Am. Inst. Electr. Eng,* vol. XLV, pp. 295–301, Jan. 1926.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.,* vol. 28, no. 4, pp. 656–715, Oct. 1949.

[10] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Inform. Theory,* vol. 39, no. 3, pp. 733–742, May 1993.

[11] J. Zhang *et al.*, "Key generation from wireless channels: a review," *IEEE Access,* vol. 4, pp. 614–626, Mar. 2016.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.,* Bangalore, India, Dec. 1984, pp. 175–179.

[13] N. Gisin *et al.*, "Quantum cryptography," *Rev. Modern Phys.,* vol. 74, no. 1, pp. 145–195, Jan. 2002.

[14] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.,* vol. 88, Feb. 2002, Art. no. 057902.

[15] T. Kukita, H. Takada, and K. Inoue, "Macroscopic differential phase shift quantum key distribution using an optically pre-amplified receiver," *Jpn. J. Appl. Phys.,* vol. 49, Dec. 2010, Art. no. 122801.

[16] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise," *New J. Phys.,* vol. 18, Jan. 2016, Art. no. 013018.

[17] T. A. Eriksson, P. V. Trinh, H. Endo, M. Takeoka, and M. Sasaki, "Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks," *OSA Opt. Express,* vol. 26, no. 16, pp. 20409–20419, Aug. 2018.

[18] P. V. Trinh *et al.*, "Performance of free-space QKD systems using SIM/BPSK and dual-threshold/direct-detection," in *Proc. IEEE Globecom Workshops (GC Wkshps),* Washington, DC, USA, Dec. 2016, pp. 1–6.

[19] P. V. Trinh and A. T. Pham, "Design and secrecy performance of novel two-way free-space QKD protocol using standard FSO systems," in *Proc. IEEE Int. Conf. Commun. (ICC),* Paris, France, May 2017, pp. 1–6.

[20] P. V. Trinh *et al.*, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access,* vol. 6, pp. 4159–4175, Feb. 2018.

[21] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nat. Photon.,* vol. 11, pp. 502–508, Aug. 2017.

[22] P. Paul, M. R. Bhatnagar, and A. Jaiswal, "Jamming in free space optical systems: mitigation and performance evaluation," *IEEE Trans. Commun. (Early Access),* Dec. 2019.

[23] 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, Apr. 2015, Art. no. 7901014.

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

[25] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," *IEEE Photon. J.,* vol. 7, no. 5, pp. 1–18, Oct. 2015, Art. no. 7903418.

[26] H. Endo *et al.*, "Free-space optical channel estimation for physical layer security," *OSA Opt. Express,* vol. 24, no. 8, pp. 8940–8955, Apr. 2016.

[27] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over Málaga turbulence channels," *IEEE Wireless Commun. Lett.,* vol. 6, no. 2, pp. 274–277, Apr. 2017.

[28] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "On secrecy analysis of DF based dual hop mixed RF-FSO systems," *IEEE Access,* vol. 7, pp. 66725–66730, Jun. 2019.

[29] D. R. Pattanayak *et al.*, "Physical layer security of a two way relay based mixed FSO/RF networks in the presence of multiple eavesdroppers," *Optics Commun.,* vol. 463, May 2020, Art. no. 125429.

[30] M. Fujiwara *et al.*, "Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link," *OSA Opt. Express,* vol. 26, no. 15, pp. 19513–19523, Jul. 2018.

[31] H. Endo *et al.*, "Free-space optical secret key agreement," *OSA Opt. Express,* vol. 26, no. 18, pp. 23305–23332, Sep. 2018.

[32] M. Legre and B. Huttner, "Quantum-enhanced physical layer cryptography: a new paradigm for free-space key distribution," in *Proc. Int. Conf. Quantum Crypto. (QCRYPT),* Cambridge, UK, Sept. 2017, pp. 1–3.

[33] R. Boluda-Ruiz, A. Garcia-Zambrana, B. Castillo-Vazquez, and K. Qaraqe, "Secure communication for FSO links in the presence of eavesdropper with generic location and orientation," *OSA Opt. Express,* vol. 27, no. 23, pp. 34211–34229, Nov. 2019.

[34] P. V. Trinh, A. Carrasco-Casado, A. T. Pham, and M. Toyoshima, "Effects of atmospheric turbulence and misalignment-induced fading on the secrecy performance of IM/DD free-space CV-QKD systems using a Gaussian beam," in *Proc. Int. Conf. Space Opt. (ICSO),* Chania, Greece, Oct. 2018, pp. 1–18.

[35] L. C. Andrews and R. L. Phillips, *Laser beam propagation through random media*, 1st ed. Bellingham, WA: SPIE 1998.

[36] S. Karp *et al.*, *Optical channels: fibers, clouds, water and the atmosphere,* New York, NY, USA: Springer, 1988.

[37] J. H. Churnside and S. F. Clifford, "Log-normal Rician probability-density function of optical scintillations in the turbulent atmosphere," *OSA J. Opt. Soc. Am. A,* vol. 4, no. 10, pp. 1923–1930, Oct. 1987.

[38] M. A. Al-Habash, L. C. Andrews, and R. L. Phillips, "Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media," *OSA Opt. Eng.,* vol. 40, no. 8, pp. 1554–1562, Aug. 2001.

[39] P. V. Trinh, T. V. Pham, and A. T. Pham, "Free-space optical systems over correlated atmospheric fading channels: spatial diversity or multihop relaying?," *IEICE Trans. Commun.,* vol. E101-B, no. 9, pp. 2033–2046, Sep. 2018.

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

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

[42] H. AlQuwaiee, H. -C. Yang, and M. -S. Alouini, "On the asymptotic capacity of dual-aperture FSO systems with generalized pointing error model," *IEEE Trans. Wireless Commun.,* vol. 15, no. 9, pp. 6502–6512, Sep. 2016.

[43] R. Boluda-Ruiz, A. Garcia-Zambrana, C. Castillo-Vazquez, and B. Castillo-Vazquez, "Novel approximation of misalignment fading modeled by Beckmann distribution on free-space optical links," *OSA Opt. Express,* vol. 24, no. 20, pp. 22635–22649, Oct. 2016.

[44] H. G. Sandalidis, N. D. Chatzidiamantis, and G. K. Karagiannidis, "A tractable model for turbulence- and misalignment-induced fading in optical wireless systems," *IEEE Commun. Lett.,* vol. 20, no. 9, pp. 1904–1907, Sep. 2016.

[45] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products,* 7th ed., New York, NY, USA: Academic 2008.

[46] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables,* 9th ed., New York, NY, USA: Dover 1972.

[47] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory,* vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[48] X. Song, F. Yang, and J. Cheng, "Subcarrier intensity modulated optical wireless communications in atmospheric turbulence with pointing errors," *IEEE/OSA J. Opt. Commun. Netw.,* vol. 5, no. 4, pp. 349–358, Apr. 2013.

[49] M. I. Petkovic, D. N. Milic, and G. T. Djordjevic, "Optimisation of subcarrier intensity modulation binary phase-shift keying free space optical link with avalanche photodiode receiver influenced by gamma-gamma atmospheric turbulence and pointing errors," *IET Commun.,* vol. 10, no. 12, pp. 1473–1479, Apr. 2016.

[50] J. A. Anguita, I. B. Djordjevic, M. A. Neifeld, and B. V. Vasic, "Shannon capacities and error-correction codes for optical atmospheric turbulent channels," *OSA J. Opt. Netw.,* vol. 4, no. 9, pp. 586–601, Sept. 2005.

[51] A. A. Farid and S. Hranilovic, "Outage capacity for MISO intensity-modulated free-space optical links with misalignment," *IEEE J. Opt. Commun. Netw.,* vol. 3, no. 10, pp. 780–789, Oct. 2011.