International Conference on Space Optics—ICSO 2018

Chania, Greece

9–12 October 2018

Edited by Zoran Sodnik, Nikos Karafolas, and Bruno Cugny

Effects of atmospheric turbulence and misalignment-induced fading on the secrecy performance of IM/DD free-space CV-QKD systems using a Gaussian beam

Phuc Trinh

Alberto Carrasco-Casado

Anh Pham

Morio Toyoshima

International Conference on Space Optics — ICSO 2018, edited by Zoran Sodnik,
Nikos Karafolas, Bruno Cugny, Proc. of SPIE Vol. 11180, 111801Y · © 2018 ESA
and CNES · CCC code: 0277-786X/18/$18 · doi: 10.1117/12.2535989

Effects of atmospheric turbulence and misalignment-induced fading on the secrecy performance of IM/DD free-space CV-QKD systems using a Gaussian beam

Phuc V. Trinh*[a], Alberto Carrasco-Casado[a], Anh T. Pham[b], Morio Toyoshima[a]
[a]Space Communications Laboratory, National Institute of Information and Communications Technology, 4-2-1 Nukui-Kitamachi, Koganei, Tokyo, Japan 184-8795; [b]Computer Communications Laboratory, The University of Aizu, Ikki-machi, Aizu-wakamatsu, Fukushima, Japan 965-8580

ABSTRACT

This paper explores the secrecy performance of the recently proposed intensity modulation/direct detection (IM/DD) terrestrial free-space quantum key distribution (QKD) system, by using a Gaussian-beam propagation model and considering the combined effects of atmospheric turbulence and legitimate transceivers' misalignment. Secrecy performance metrics including quantum bit error rate (QBER) and ergodic secret-key rate are newly derived in closed-form expressions, taking into account all combined effects of turbulence- and misalignment-induced fading channels, the eavesdropper's location relative to the legitimate receiver, and receiver noises. To satisfy security constraints, the system designs based on the intensity modulation depth and beam waist of the Gaussian beam at the transmitter, and dual-threshold (D-T) selection at the receiver, are comprehensively discussed under turbulence and misalignment conditions as well as different eavesdropper's locations. Monte-Carlo (M-C) simulations are also implemented to verify the analytical results. Remarkably, this paper also offers the first framework in the literature to evaluate the secrecy performance of free-space optical (FSO) systems considering the eavesdropper's location under the effect of misalignment between legitimate transceivers.

Keywords: Quantum key distribution, free-space optics, subcarrier intensity modulation, binary phase shift keying, atmospheric turbulence, misalignment, dual-threshold direct detection, Gaussian beam.

1. INTRODUCTION

Recent years have witnessed the exponential growth of computing technologies, which could potentially break the security of current confidential communications[1]. The confidential communications between two parties can be achieved using one-time-pad scheme, which requires a long random bit sequences, i.e. a secret "key", to be shared securely so that it can be used for the encryption and decryption of confidential messages. Conventional key distribution techniques are fundamentally insecure as they are solely based on computational complexities, which can be possibly solved by advanced computer hardware and algorithms, especially when large-scale quantum computers become available.

Fortunately, quantum key distribution (QKD) could guarantee secure key distribution by using single-photon transmissions. The security of QKD is based on the inviolability of the laws of quantum mechanics. Thus, a secret key can be securely shared between two legitimate parties, namely Alice and Bob, against an adversarial eavesdropper, namely Eve[2]. The implementation of QKD can be categorized into two schemes: discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD), corresponding to the key information being encoded on the polarization/phase of single photons, and the continuous variables of coherent states conveyed by amplitude and phase of weakly modulated pulses, respectively. From a practical perspective, CV-QKD is much more convenient to implement as it is compatible with standard telecommunication technologies by using heterodyne/homodyne detection receivers instead of dedicated single-photon counters. Nevertheless, the use of heterodyne/homodyne receivers requires a sophisticated phase-stabilized local light, which results in a higher implementation cost. To avoid such issue, differential-phase-shift-keying (DPSK)-based CV-QKD using a delay interferometer was developed[3]. To further simplify CV-QKD configurations, intensity modulation/direct detection (IM/DD) CV-QKD systems have been recently proposed for implementation over both

*pvtrinh@nict.go.jp; phone +81-42-327-5982; fax +81-42-327-6825; www.nict.go.jp optical fiber[4,5] and free-space optics (FSO)[6,7,8]. IM/DD systems do not require a delay interferometer and have been well-developed in standard optical communications.

QKD over FSO, or free-space QKD, plays an important role in bridging the gap to an eventual global quantum network as FSO platforms are highly secure and flexible, providing a wide range of applications for terrestrial, airborne, and satellite-based networks[9]. This paper further explores the secrecy performance of the recently proposed IM/DD free-space CV-QKD using subcarrier intensity modulation (SIM) binary phase shift keying (BPSK) with dual-threshold (D-T) avalanche photodiode (APD)-based receiver[8], under realistic terrestrial transmission environments including atmospheric turbulence- and legitimate transceivers' misalignment-induced fading channels. The atmospheric turbulence due to variations in the refractive index along the propagation path, which cause random temporal and spatial irradiance fluctuation in the optical beam, is modeled by a log-normal distribution. The legitimate transceivers' misalignment is studied by considering a Gaussian beam propagation model, taking into consideration the location of an adversary eavesdropper. To the best of authors' knowledge, there is no previous work in the literature offering a framework for analyzing the impact of different eavesdropper's locations under misalignment errors of FSO systems.

The contributions of this paper are therefore threefold. *Firstly*, a novel theoretical framework is analytically derived to investigate the combined effects of atmospheric turbulence- and misalignment-induced fading channels on the IM/DD terrestrial free-space CV-QKD system in the presence of an eavesdropper. Secrecy performance metrics including quantum bit error rate (QBER) and ergodic secret-key rate taking into consideration effects of composite fading channels and receiver noises are newly derived in closed-form expressions. *Secondly*, the system designs under security constraints are comprehensively discussed, based on the intensity modulation depth and beam waist of the Gaussian beam at the transmitter and D-T selection at the receiver, considering turbulence and misalignment conditions. In addition, Monte-Carlo (M-C) simulations are performed to confirm the validity of derived analytical results. *Finally*, this paper forms the first framework for analyzing the security of FSO systems considering the eavesdropper's location under the effect of misalignment between legitimate transceivers.

2. SYSTEM MODEL

2.1 System descriptions

2.1.1 System operation

In this section, we briefly repeat the operation overview of the recently proposed QKD protocol over free-space channels using SIM/BPSK signaling and D-T direct detection[8]. The operation steps are as follows. Firstly, Alice transmits SIM/BPSK intensity-modulated signals as coherent states with a relatively small modulation depth, denoted as $\delta\left(0<\delta<1\right)$, corresponding to binary random key bits "0" or "1" over the atmospheric channel. The two intensity-modulated signals representing binary bits are two coherent states that are nonorthogonal to each other, playing a similar role as nonorthogonal bases in conventional single-photon-based QKD protocols[10]. The transmitting modulated signals are then directly detected at Bob's receiver by using an avalanche photodiode (APD) and two detection thresholds.

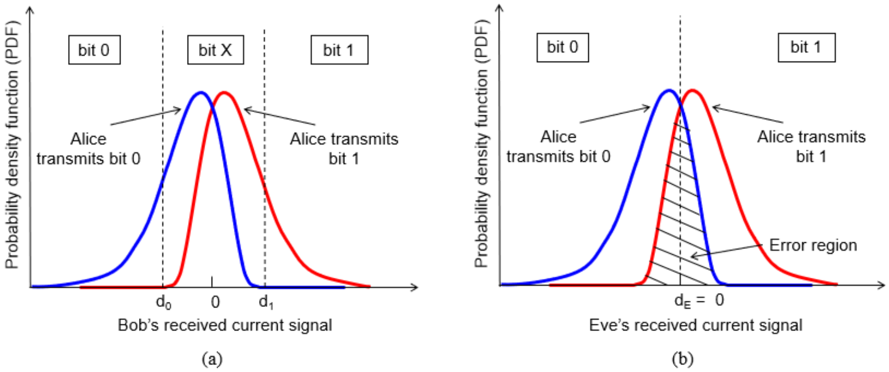


Figure 1. The probability density function of (a) Bob's received signal over fading channel with dual threshold detection, (b) Eve's received signal over fading channel with the optimal threshold detection.

Figure 1(a) illustrates the probability density function (PDF) of Bob's received BPSK signals influenced by the atmospheric channel and receiver noises, which are symmetric over the "zero" level. It is seen that the distribution of the received signals has two peaks corresponding to Alice's bits "0" and "1", overlapping with each other due to the small modulation depth. To detect bits "0" and "1" on the received signals, Bob uses two detection thresholds d_0 and d_1 respectively at low and high levels, with decision rule on the detected value x of the received current signal can be expressed as

$$\text{Decision} = \begin{cases} 0 & \text{if } x \le d_0 \\ 1 & \text{if } x \ge d_1 \\ \text{X} & \text{otherwise} \end{cases}, \tag{1}$$

where X represents the case that Bob creates no bit, corresponding to the case of discarding wrong basis selection in conventional single-photon-based QKD protocols[10]. Then, using a classical public channel, Bob notifies Alice of the time instants he was able to infer binary bits from detected signals. Alice subsequently discards bits according to time instants that Bob inferred no bit. To this point, Alice and Bob share an identical bit string called *sifted key*. By obtaining the channel state information (CSI) estimation at the receiver to adjust D-T selection, the probability of sift at Bob's receiver can be easily controlled. Finally, Alice and Bob perform *information reconciliation* and *privacy amplification* over the public channel to obtain the final secret key.

2.1.2 Security constraints

In practice, as the optical beam width in FSO systems is very narrow and invisible, it is very challenging for Eve to intercept it in the middle of the transmission between Alice and Bob's main channel. Moreover, additional surveillance camera, radar, light detection and ranging (LIDAR) can be installed to alarm the system when Eve gets close to the main channel or Bob's receiver. To eavesdrop Alice's transmitted signal, one reasonable possibility is that Eve locates its passive receiver far behind Bob and tries to tap the side lobe of the laser beam[11]. Based on this assumption, we investigate in this paper the secrecy performance assuming that there is a "virtual" Eve which is close to Bob on the receiver plane, where the received signal intensity is always higher than that received by Eve's receiver located far behind Bob. In practice, we expect that Eve's location is somewhere meters away from Bob's receiver or kilometers behind Bob, thus the information loss to Eve in practice is always less than that to the "virtual" Eve as considered in this paper. This attacking scenario could serve as an effective upper bound estimation of the worst case of the leaked information to Eve[11]. In this way, it is reasonable to assume that the distance between Alice and Bob is equal to that between Alice and Eve, as the transmission distance is very large compared to the separation between Bob's and Eve's receivers. This separation should be sufficiently larger than the atmospheric coherence length so that the received signals at Bob's and Eve's receiver are uncorrelated. In this paper, we assume that Eve locates its passive receiver somewhere on the receiver plane near Bob's receiver and sets a threshold at the "zero" level since it is the optimal choice to decode the received signals[8], as illustrated in Figure 1(b). She will obtain measurements where the two signals representing bits "0" and "1" are strongly overlapped due to the small modulation depth controlled at Alice's transmitter, thus resulting in a high error rate.

2.2 System model

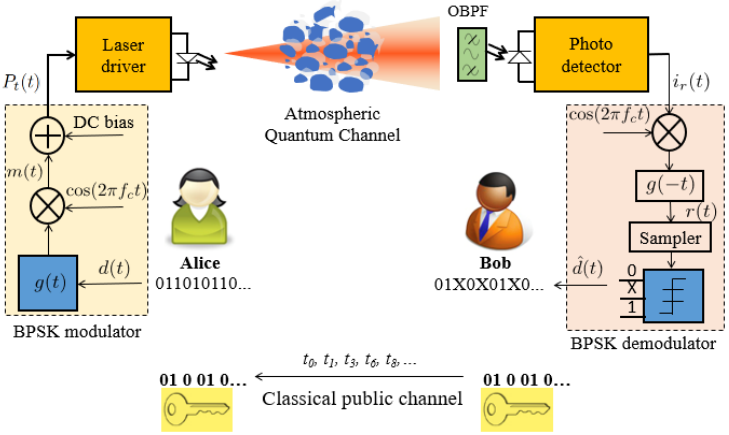


Figure 2. A block diagram of the considered free-space CV-QKD system using SIM/BPSK with a D-T receiver[8].

Figure 2 represents a block diagram of the considered free-space QKD system. The system model is analyzed as follows[8]. At the transmitter, the source data *d*(*t*) is modulated onto a radio frequency 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 power of the modulated laser beam can be expressed as $P_t(t) = P/2\left(1+\delta m(t)\right)$ where *P* represents the peak transmitted power, δ denotes the intensity modulation depth, and $m(t) = A(t)\,g(t)\cos\left(2\pi f_c t + a_i\pi\right)$ 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 *i*-th 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) before being converted into an electrical signal through direct detection at the 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 $i_r(t) = \Re\bar{g}\left(P/2\right)h(t)\left[1+\delta m(t)\right]+n(t)$, where $\Re = \eta q/\tilde{h}\, f_o$ is the responsivity of the APD with η is the quantum efficiency, *q* is the electron charge, $\tilde{h}$ is the Planck's constant, f_0 is the optical frequency; $\bar{g}$ is the average APD gain, and *n*(*t*) is the receiver noise. Since the fading channel gain *h*(*t*) varies slowly enough, the DC term $\Re\bar{g}\left(P/2\right)h(t)$ can be filtered out by the OBPF. The electrical signal $i_r(t)$ is then passed through the BPSK demodulator where the output signal *r*(*t*) is demodulated by the reference signal $\cos\left(2\pi f_c t\right)$ as

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

where i_0 and i_1 are the received current signals for bits "0" and "1", respectively. Assuming that the dark current is negligible, the receiver noises including the shot noise, background noise, and thermal noise can be modeled as additive white Gaussian noises (AWGN). Therefore, *n*(*t*) is the zero-mean AWGN with variance $\sigma_N^2 = \sigma_{sh}^2 + \sigma_b^2 + \sigma_{th}^2$ where $\sigma_{sh}^2, \sigma_b^2, \sigma_{th}^2$ are respectively the variances of shot noise, background noise, and thermal noise, calculated as $\sigma_{sh}^2 = 2q\bar{g}^2\Re F_A\left(\frac{1}{4}P\delta h\right)\Delta f$ with F_A denotes the excess noise factor, $\sigma_b^2 = 2q\bar{g}^2\Re F_A P_b \Delta f$ with P_b is the average received background radiation power, and $\sigma_{th}^2 = 4k_B T F_n \Delta f / R_L$ with F_n is the amplifier noise figure, *T* is the receiver temperature in Kelvin degree, R_L is the APD's load resistance. $\Delta f = R_b/2$ is the effective noise bandwidth for non-return-to-zero signal format, with R_b is the system bit rate. After demodulating process, the demodulated signals are sampled and then used to recover binary bits “0” and “1” using D-T detection rule in (1), forming Bob’s raw key. Bob then notifies Alice of the time instants that binary bits “0” and “1” were created so that Alice can discard the key bits transmitted at other time instants, forming the shared *sifted key*.

3. CHANNEL MODEL

3.1 Atmospheric attenuation

The attenuation of laser power through the atmosphere caused by molecular absorption and aerosol scattering suspended in the air can be described by the exponential Beers-Lambert Law as[12]

$$h_l = \exp\left(-\beta_l L\right), \tag{3}$$

where h_l is the loss over a propagation distance of length L in kilometer (km), β_l is the attenuation coefficient in dB/km. The attenuation h_l is considered as a constant scaling factor during a long period of time.

3.2 Atmospheric turbulence-induced fading

An optical wave propagating through the atmosphere is affected by atmospheric turbulence, also known as *scintillation* or *fading*, which results in intensity fluctuations observed at the receiver. For weak turbulence conditions, the fading channel gain is modeled as

$$h_a = \exp\left(2X\right), \tag{4}$$

where X is the log-amplitude of the optical intensity following a Gaussian distribution with mean μ_X and variance σ_X^2. As a result, the intensity fluctuation PDF can be modeled as a log-normal distribution given by[13]

$$f_{h_a}\left(h_a\right) = \frac{1}{2h_a\sqrt{2\pi\sigma_X^2}} \exp\left(-\frac{\left(\ln h_a - 2\mu_X\right)^2}{8\sigma_X^2}\right). \tag{5}$$

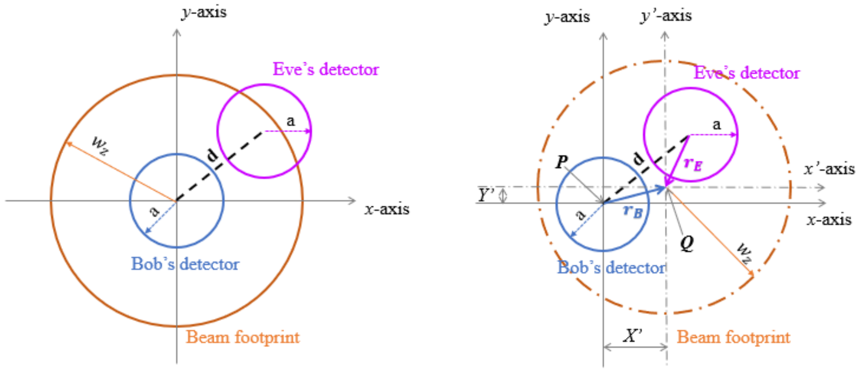
To ensure that the average power is not amplified by fading, the mean irradiance is normalized, i.e. $\mathrm{E}\left[h_a\right] = 1$ and $\mu_X = -\sigma_X^2$. Assuming a plane wave propagation, σ_X^2 is given as[12]

$$\sigma_X^2 \approx 0.307\left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2, \tag{6}$$

where λ is the wavelength, L is the transmission distance in meter (m), and C_n^2 varying from 10^{-17} m$^{2/3}$ to 10^{-12} m$^{2/3}$ stands for the index of refraction structure parameter. C_n^2 suffers strong variations with time, typically of several orders of magnitude during one day, when the turbulence strength changes from weak to strong depending on the time of the day. However, it is usually used as a specific value along the horizontal path according to the turbulence strength.

3.3 Fraction of collected power impaired by misalignment

The misalignment between the transmitter and receiver of an FSO system leads to pointing errors and considerably degrades the system performance. The transceiver misalignment might be caused by mechanical errors in the tracking system or vibrations of the mechanical transceiver due to strong winds, building sway, or light earthquakes. This results in additional fluctuation, i.e. fading, of the received signals at the receiver. For the sake of simplicity, the displacements of the laser beam along vertical (elevation) and horizontal (azimuth) directions are typically assumed to be independent Gaussian random variables[14]. Figure 3 illustrates Bob’s and Eve’s receivers on the receiver plane for two cases: (a) there is no misalignment between Alice’s transmitter and Bob’s receiver, and (b) there exists some misalignment between Alice’s transmitter and Bob’s receiver. Eve is assumed to locate its receiver at a distance *d* away from Bob’s receiver on the receiver plane to eavesdrop the signals transmitted from Alice, as described in Section 2.1.2. In this section, based on a Gaussian beam propagation model, we calculate the fraction of collected power at Bob’s and Eve’s receivers.



(a)
No misalignment

(b)
Misalignment

Figure 3. Alice's beam footprint at the receiver plane, (a) when there is no misalignment between Alice's transmitter and Bob's receiver, (b) when there exists misalignment between Alice's transmitter and Bob's receiver.

3.3.1 Bob's fraction of collected power

When there exists misalignment between Alice's transmitter and Bob's receiver, for a Gaussian beam, the normalized spatial distribution of the transmitted intensity at distance L from the transmitter is given by[14]

$$I_{\text{beam}}\left(\boldsymbol{\rho};L\right)=\frac{2}{\pi w_L^2}\exp\left(-\frac{2\left\|\boldsymbol{\rho}\right\|^2}{w_L^2}\right), \tag{7}$$

where $\boldsymbol{\rho}$ is the radial vector from the beam center, and w_L is the beam waist (radius calculated at e^{-2}) at distance L. The beam waist w_L of a Gaussian beam propagating in the atmosphere can be approximated as

$$w_L \approx w_0\left[1+\varepsilon\left(\frac{\lambda L}{\pi w_0^2}\right)^2\right]^{1/2}, \tag{8}$$

where w_0 is the beam waist at L = 0, $\varepsilon=\left(1+2w_0^2/\rho_0^2\left(L\right)\right)$ with $\rho_0\left(L\right)=\left(1.46C_n^2\left(2\pi/\lambda\right)^2 L\right)^{-3/5}$ is the coherence length of a plane wave propagation[15]. The attenuation due to geometric spread of the Gaussian optical beam with misalignment error vector $\boldsymbol{r_B}$ is expressed as

$$h_{p,B}\left(\boldsymbol{r_B};L\right)=\int_A I_{\text{beam}}\left(\boldsymbol{\rho}-\boldsymbol{r_B};L\right)\mathrm{d}\boldsymbol{\rho}, \tag{9}$$

where $h_{p,B}\left(\boldsymbol{r_B};L\right)$ represents the fraction of the power collected by the detector, with A is the detector area. When a misalignment error of $\boldsymbol{r_B}$ exists at Bob's receiver, $h_{p,B}$ is a function of the radial displacement and angle. Due to the symmetry of the beam shape and the detector area, the resultant $h_{p,B}\left(\boldsymbol{r_B};L\right)$ depends only on the radial distance $r_B=\left\|\boldsymbol{r_B}\right\|$, where $\left\|\cdot\right\|$ denotes the norm of a vector. Therefore, without loss of generality, we assume that the radial distance is located along the *x* axis. The fraction of the collected power at Bob's receiver of radius *a* in the transverse plane of the incident wave can be approximated as[14]

$$h_{p,B}\left(r_B;L\right)\approx A_0\exp\left(-\frac{2r_B{}^2}{w_{L_{eq}}^2}\right), \tag{10}$$

where $A_0 = \left[\operatorname{erf}\left(v\right)\right]^2$ is the fraction of the collected power at $r_B = 0$ with $\operatorname{erf}\left(\cdot\right)$ is the Gauss error function, $v = \left(\sqrt{\pi}a\right) \Big/ \left(\sqrt{2}w_L\right)$, and $w_{L_{eq}}^2 = w_L^2 \dfrac{\sqrt{\pi}\operatorname{erf}\left(v\right)}{2v\exp\left(-v^2\right)}$, where $w_{L_{eq}}$ is the equivalent beam width. Considering independent identical Gaussian distributions for the elevation and the horizontal displacements[14], the radial displacement r_B at Bob's receiver is modeled by a Rayleigh distribution,

$$f_{r_B}\left(r_B\right) = \frac{r_B}{\sigma_S^2}\exp\left(-\frac{{r_B}^2}{2\sigma_S^2}\right), \qquad r_B > 0, \tag{11}$$

where σ_S^2 is the jitter variance at Bob's receiver. Substituting (10) into (11), the PDF of $h_{p,B}$ can be given as

$$f_{h_{p,B}}\left(h_{p,B}\right) = \frac{\gamma^2}{A_0^{\gamma^2}} h_{p,B}^{\gamma^2-1}, \qquad 0 \le h_{p,B} \le A_0, \tag{12}$$

where $\gamma = w_{L_{eq}} \big/ 2\sigma_S$ is the ratio between the equivalent beam radius at Bob's receiver and the misalignment error displacement standard deviation. The first moment of $h_{p,B}$ is given as[15]

$$\mathsf{E}\left[h_{p,B}\right] = \frac{A_0\gamma^2}{1+\gamma^2}. \tag{13}$$

When there is no misalignment between Alice's transmitter and Bob's receiver, the fraction of collected power at Bob's receiver can be calculated by substituting $r_B = 0$ into (10) as[16]

$$h_{p,B}\left(0;L\right) \approx A_0. \tag{14}$$

3.3.2 Eve's fraction of collected power

When there exists misalignment between Alice's transmitter and Bob's receiver, let $\boldsymbol{P}$ denote the coordinate of Alice's transmit beam center in the receiver plane with no misalignment. Assume a beam displacement X' in the *x*-direction and Y' in the *y*-direction at Bob's receiver plane as in Figure 3(b). Now, the position of the transmit beam center when there exists misalignment is

$$\boldsymbol{Q} = \begin{bmatrix} X' \\ Y' \end{bmatrix} + \boldsymbol{P}, \tag{15}$$

where $\boldsymbol{Q}$ is the center of the footprint. With d denotes the distance between Eve's and Bob's receivers on the receiver plane, we have $\left\|\boldsymbol{P}\right\|^2 = d^2 = \text{constant}.$ The distance $r_E = \left\|\boldsymbol{r_E}\right\|$ between the beam center and Eve's aperture center is

$$r_E^2 = \left\|\boldsymbol{Q}\right\|^2 = \underbrace{\left(\begin{bmatrix} X' \\ Y' \end{bmatrix}\right)^2}_{r_B^2} + 2\begin{bmatrix} X' \\ Y' \end{bmatrix}^T \boldsymbol{P} + \underbrace{\left\|\boldsymbol{P}\right\|^2}_{d^2}, \tag{16}$$

where r_B is the magnitude of the displacement between Alice's beam center and Bob's aperture center defined in Section 3.3.1. With the help of (16), the fraction of the collected power at Eve's receiver of radius *a* in the transverse plane of the incident wave can be approximated as

$$h_{p,E}\left(r_E;L\right) \approx A_0\exp\left(-\frac{2{r_E}^2}{w_{L_{eq}}^2}\right) \approx A_0\exp\left(-\frac{2{r_B}^2}{w_{L_{eq}}^2}\right)\exp\left(-\frac{2d^2}{w_{L_{eq}}^2}\right)\exp\left(-U\right), \tag{17}$$

where $U = \frac{4}{w_{L_{eq}}^2}\begin{bmatrix} X' \\ Y' \end{bmatrix}^T \boldsymbol{P}$. It should be noted that since both X' and Y' are independent Gaussian random variables with zero mean and variance σ_S^2, then U is also a Gaussian random variable with mean $\mu_U = 0$ and variance $\sigma_U^2 = 16\sigma_S^2 d^2 \big/ w_{L_{eq}}^4$. When there is no misalignment between Alice's transmitter and Bob's receiver, the fraction of collected power at Eve's receiver can be simply calculated as

$$h_{p,E}\left(d;L\right) \approx A_0 \exp\left(-\frac{2d^2}{w_{L_{eq}}^2}\right). \tag{18}$$

3.4 Channel statistical model

In this section, the channel statistical model is developed, taking into account the atmospheric attenuation, atmospheric turbulence- and misalignment-induced fading. It is noted that the channel statistics when there is no misalignment was previously reported[8].

3.4.1 Bob's channel statistical model

The PDF of Bob's channel gain $h_B = h_{l,B} h_{a,B} h_{p,B}$ can be expressed as[14]

$$f_{h_B}\left(h_B\right) = \int f_{h_B|h_{a,B}}\left(h_B \left| h_{a,B}\right.\right) f_{h_{a,B}}\left(h_{a,B}\right) \mathrm{d}h_{a,B}, \tag{19}$$

where $f_{h_B|h_{a,B}}\left(h_B \left| h_{a,B}\right.\right)$ is the conditional probability given a turbulence state $h_{a,B}$ of Bob's channel. With the help of (12), the resulting conditional distribution calculated at Bob's receiver can be expressed as

$$f_{h_B|h_{a,B}}\left(h_B \left| h_{a,B}\right.\right) = \frac{1}{h_{a,B} h_{l,B}} f_{h_{p,B}}\left(\frac{h_B}{h_{a,B} h_{l,B}}\right) = \frac{\gamma^2}{A_0^{\gamma^2} h_{a,B} h_{l,B}}\left(\frac{h_B}{h_{a,B} h_{l,B}}\right)^{\gamma^2 - 1}, \quad 0 \le h_B \le A_0 h_{a,B} h_{l,B}. \tag{20}$$

Substituting (20) into (19), we have

$$f_{h_B}\left(h_B\right) = \frac{\gamma^2}{\left(A_0 h_{l,B}\right)^{\gamma^2}} h_B^{\gamma^2 - 1} \int_{h_B / A_0 h_{l,B}}^{\infty} h_{a,B}^{-\gamma^2} f_{h_{a,B}}\left(h_{a,B}\right) \mathrm{d}h_{a,B}. \tag{21}$$

Plugging (5) into (21) and after some mathematical manipulations, the closed-form expression of $f_{h_B}\left(h_B\right)$ can be readily given as[14]

$$f_{h_B}\left(h_B\right) = \frac{\gamma^2}{2\left(A_0 h_{l,B}\right)^{\gamma^2}} h_B^{\gamma^2 - 1} \mathrm{erfc}\left(\frac{\ln\left(\frac{h_B}{A_0 h_{l,B}}\right) + 2\sigma_X^2\left(1 + 2\gamma^2\right)}{\sqrt{8}\sigma_X}\right) \exp\left(2\sigma_X^2 \gamma^2 \left(1 + \gamma^2\right)\right). \tag{22}$$

3.4.2 Eve's channel statistical model

With the help of (3), (4) and (17), Eve's channel gain can be mathematically expressed as

$$h_E = h_{l,E} h_{a,E} h_{p,E} = A_0 h_{l,E} \exp\left(-\frac{2{r_B}^2}{w_{L_{eq}}^2}\right) \exp\left(-\frac{2d^2}{w_{L_{eq}}^2}\right) \exp\left(\hat{X} - U\right), \tag{23}$$

where $\hat{X} = 2X$ with X is the log-amplitude of the optical intensity defined in Section 3.2. Thus, we have $\mu_{\hat{X}} = 2\mu_X = -2\sigma_X^2$ and $\sigma_{\hat{X}}^2 = 4\sigma_X^2$. Let $\exp(G) = \exp(\hat{X} - U)$, where G is also Gaussian distributed with mean $\mu_G = \mu_{\hat{X}} = -2\sigma_X^2$ and $\sigma_G^2 = \sigma_{\hat{X}}^2 + \sigma_U^2 \approx 1.23\left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2 + \frac{16\sigma_S^2 d^2}{w_{L_{eq}}^4}$. The channel gain in (23) is then simplified to

$$h_E = A_0 h_{l,E} \exp\left(-\frac{2d^2}{w_{L_{eq}}^2}\right) \exp(G - T), \tag{24}$$

where $T = 2{r_B}^2 \big/ w_{L_{eq}}^2$ is an exponential random variable with a PDF given by $f_T(t) = \gamma^2 \exp(-\gamma^2 t)$, with γ is already defined in (12). Now, let $V = G - T$, the PDF of V can be expressed in a closed-form expression as[17]

$$\begin{aligned} f_V(v) &= \int_0^\infty f_{V|T}(v|t)\, f_T(t)\,\mathrm{d}t = \int_0^\infty \frac{1}{\sqrt{2\pi}\sigma_G} \exp\left(-\frac{\left(v - (\mu_G - t)\right)^2}{2\sigma_G^2}\right) \gamma^2 \exp\left(-\gamma^2 t\right) \mathrm{d}t, \\ &= B_1 \exp\left(\gamma^2 v\right) \mathrm{erfc}\left(\frac{v + B_2}{\sqrt{2}\sigma_G}\right), \end{aligned} \tag{25}$$

where $B_1 = \frac{\gamma^2}{2} \exp\left(\gamma^4 \frac{\sigma_G^2}{2} - \gamma^2 \mu_G\right)$ and $B_2 = \gamma^2 \sigma_G^2 - \mu_G$. Substituting (24) into (25) and after some mathematical manipulations, the PDF of the channel gain at Eve's receiver can be finally expressed as

$$f_{h_E}(h_E) = \frac{B_1 \exp\left(2d^2\gamma^2 \big/ w_{L_{eq}}^2\right)}{\left(A_0 h_{l,E}\right)^{\gamma^2}} h_E^{\gamma^2 - 1} \mathrm{erfc}\left(\frac{\ln\left(h_E \big/ A_0 h_{l,E}\right) + 2d^2 \big/ w_{L_{eq}}^2 + B_2}{\sqrt{2}\sigma_G}\right). \tag{26}$$

4. SECRECY PERFORMANCE ANALYSIS

In this section, the secrecy performance metrics of the considered IM/DD free-space CV-QKD system are derived in closed-form expressions considering all effects of turbulence- and misalignment-induced fading channels and receiver noises. It is noteworthy that the closed-form expressions for the secrecy performance metrics when there is no misalignment can be similarly derived, however, it is omitted here for the sake of conciseness.

4.1 Quantum bit error rate

The quantum bit error rate (QBER) is defined as[8]

$$\text{QBER}=\frac{P_{error}}{P_{sift}} = \frac{P_{A,B}(0,1) + P_{A,B}(1,0)}{P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1)}, \tag{27}$$

where $P_{A,B}(a,b)\left(a,b \in \{0,1\}\right)$ is the joint probability that Alice's bit "a" coincides with Bob's bit "b". The joint probabilities when Alice transmits bits "0" and "1", averaged over the log-normal fading channel can be respectively expressed as[8]

$$P_{A,B}(a,0) = \frac{1}{2}\int_0^\infty Q\left(\frac{i_a - d_0}{\sigma_N}\right) f_{h_B}(h_B)\,\mathrm{d}h_B, \tag{28}$$

$$P_{A,B}(a,1) = \frac{1}{2}\int_0^\infty Q\left(\frac{d_1 - i_a}{\sigma_N}\right) f_{h_B}(h_B)\,\mathrm{d}h_B, \tag{29}$$

where $a \in \{0,1\}$, $Q(\cdot) \square \frac{1}{\sqrt{2\pi}} \int_{0}^{\infty} \exp\left(-t^2/2\right) \mathrm{d}t$ is the Gaussian Q-function, $i_0 = -\frac{1}{4}\Re \overline{g} P \delta h_B = -\frac{1}{4}\Re \overline{g} P \delta h_{l,B} h_{a,B} h_{p,B}$ and $i_1 = -i_0$. d_0 and d_1 are the D-T thresholds given as

$$d_0 = \mathsf{E}\left[i_0\right] - \zeta \sqrt{\sigma_N^2}, \tag{30}$$

$$d_1 = \mathsf{E}\left[i_1\right] + \zeta \sqrt{\sigma_N^2}, \tag{31}$$

where ζ is the *D-T scale coefficient* to adjust the thresholds, σ_N^2 is the noise variance defined in Section 2.2. $\mathsf{E}\left[i_0\right]$ and $\mathsf{E}\left[i_1\right]$ are the mean values of i_0 and i_1. With $\mathsf{E}\left[h_{a,B}\right] = 1$ and $\mathsf{E}\left[h_{p,B}\right]$ given in (13), $\mathsf{E}\left[i_0\right]$ and $\mathsf{E}\left[i_1\right]$ can be respectively calculated as

$$\mathsf{E}\left[i_0\right] = -\frac{1}{4}\Re \overline{g} P \delta h_{l,B} \mathsf{E}\left[h_{p,B}\right] = -\frac{1}{4}\Re \overline{g} P \delta h_{l,B} \left(\frac{A_0 \gamma^2}{1+\gamma^2}\right) \tag{32}$$

$$\mathsf{E}\left[i_1\right] = \frac{1}{4}\Re \overline{g} P \delta h_{l,B} \mathsf{E}\left[h_{p,B}\right] = \frac{1}{4}\Re \overline{g} P \delta h_{l,B} \left(\frac{A_0 \gamma^2}{1+\gamma^2}\right). \tag{33}$$

With the help of (22), the joint probabilities in (28) and (29) can be respectively derived in closed-form expressions by applying some mathematical manipulations and using Hermite polynomial approximation formula[18] $\int_{-\infty}^{\infty} g(x) \mathrm{d}x \approx \sum_{i=1}^{N} \omega_i g(x_i) \exp\left(x_i^2\right)$, which can be respectively expressed as

$$\begin{aligned} P_{A,B}(a,0) = {} & \frac{\gamma^2 \sigma_X \exp\left(-2\sigma_X^2 \gamma^4\right)}{\sqrt{2}} \sum_{i=1}^{N} \omega_i \operatorname{erfc}(x_i) \exp\left(x_i^2 + \sqrt{8}\sigma_X \gamma^2 x_i\right) \\ & \times Q\left(\frac{\mp \frac{1}{4}\Re \overline{g} P \delta A_0 h_{l,B} \exp\left(\sqrt{8}\sigma_X x_i - 2\sigma_X^2\left(1+2\gamma^2\right)\right) - d_0}{\sigma_{N(i)}}\right), \end{aligned} \tag{34}$$

$$\begin{aligned} P_{A,B}(a,1) = {} & \frac{\gamma^2 \sigma_X \exp\left(-2\sigma_X^2 \gamma^4\right)}{\sqrt{2}} \sum_{i=1}^{N} \omega_i \operatorname{erfc}(x_i) \exp\left(x_i^2 + \sqrt{8}\sigma_X \gamma^2 x_i\right) \\ & \times Q\left(\frac{d_1 \pm \frac{1}{4}\Re \overline{g} P \delta A_0 h_{l,B} \exp\left(\sqrt{8}\sigma_X x_i - 2\sigma_X^2\left(1+2\gamma^2\right)\right)}{\sigma_{N(i)}}\right), \end{aligned} \tag{35}$$

where

$$\sigma_{N(i)} = \sqrt{2qF_A \overline{g}^2 \Re\left[\frac{1}{4}P\delta A_0 h_{l,B} \exp\left(\sqrt{8}\sigma_X x_i - 2\sigma_X^2\left(1+2\gamma^2\right)\right) + P_b\right] \Delta f + \frac{4k_b T F_n}{R_L} \Delta f}, \tag{36}$$

$$d_0 = \mathsf{E}\left[i_0\right] - \zeta \sqrt{\sigma_{N(i)}^2}, \tag{37}$$

$$d_1 = \mathsf{E}\left[i_0\right] + \zeta \sqrt{\sigma_{N(i)}^2}. \tag{38}$$

Here, N is the order of Hermite polynomial approximation, $\{\omega_i\}$ and $\{x_i\}$ are the weight factors and zeros of the Hermite polynomial, respectively. The first hundred values of $\{\omega_i\}$ and $\{x_i\}$ are well tabulated[19].

4.2 Ergodic secret-key rate

To validate the security of the considered system, we investigate the ergodic secret-key rate, denoted as *S*, over the atmospheric turbulence- and misalignment-induced fading channels. 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 privacy amplification. Otherwise, the system is vulnerable to Eve's intervention as she obtains a larger amount of information compared to Bob. The ergodic secret-key rate *S* is defined as the maximum transmission rate at which the eavesdropper is unable to decode any information, given as[8]

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

where *I*(*A*;*B*) and *I*(*A*;*E*) are the mutual information defined as the estimations of the amount of information shared between Alice and Bob, and that shared between Alice and Eve, respectively. *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[8]

$$\begin{aligned} I\left(A;B\right) = {} & p\log_2 p + \left(1-p-q\right)\log_2\left(1-p-q\right) - \left(\alpha p + \left(1-\alpha\right)\left(1-p-q\right)\right)\log_2\left(\alpha p + \left(1-\alpha\right)\left(1-p-q\right)\right) \\ & -\left(\alpha\left(1-p-q\right) + \left(1-\alpha\right)p\right)\log_2\left(\alpha\left(1-p-q\right) + \left(1-\alpha\right)p\right), \end{aligned} \tag{40}$$

where α and $\left(1-\alpha\right)$ are probabilities of transmitting bits "0" and "1" with $\alpha = 0.5$ as they are equally likely to occur, p and q are the conditional probabilities corresponding to $P_{B|A}\left(b|a\right)$ with $a \in \{0,1\}$ and $b \in \{0,1,X\}$. The closed-form expressions for these probabilities can be derived from the results in Section 4.1. On the other hand, Eve obtains a bit string through eavesdropping the signals using the optimal detection threshold $d_E = 0$, whose bit values are partially identical to Alice's. Thus, Alice and Eve share some information via binary symmetric channel (BSC), for which the mutual information can be given as[8]

$$I\left(A;E\right) = 1 + e\log_2 e + \left(1-e\right)\log_2\left(1-e\right), \tag{41}$$

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

$$P_{A,E}\left(0,1\right) = P_{A,E}\left(1,0\right) = \frac{1}{2}\int_0^\infty Q\left(\frac{\frac{1}{4}\Re\bar{g}P\delta h_E}{\sigma_{N,E}}\right) f_{h_E}\left(h_E\right)\mathrm{d}h_E, \tag{42}$$

With the help of (26) and following the footsteps in Section 4.1, the joint probabilities $P_{A,E}\left(0,1\right)$ and $P_{A,E}\left(1,0\right)$ can be also derived in closed-form expressions by applying some mathematical manipulations and using Hermite polynomial approximation formula[18] $\int_{-\infty}^{\infty} g\left(x\right)\mathrm{d}x \approx \sum_{i=1}^{N} \omega_i g\left(x_i\right)\exp\left(x_i^2\right)$, which can be expressed as

$$P_{A,E}\left(0,1\right)=P_{A,E}\left(1,0\right)=\frac{B_1\sigma_G\exp\left(-\gamma^2B_2\right)}{\sqrt{2}}\sum_{i=1}^{N}\omega_i\operatorname{erfc}\left(x_i\right)\exp\left(x_i^2+\sqrt{2}\sigma_G\gamma^2x_i\right)$$
$$\times Q\left(\frac{\frac{1}{4}\Re\bar{g}P\delta A_0h_{l,E}\exp\left(\sqrt{2}\sigma_Gx_i-\frac{2d^2}{w_{L_{eq}}^2}-B_2\right)}{\sigma_{N,E(i)}}\right), \tag{43}$$

where

$$\sigma_{N,E(i)}=\sqrt{2qF_A\bar{g}^2\Re\left[\frac{1}{4}P\delta A_0h_{l,E}\exp\left(\sqrt{2}\sigma_Gx_i-\frac{2d^2}{w_{L_{eq}}^2}-B_2\right)+P_b\right]\Delta f+\frac{4k_bTF_n}{R_L}\Delta f}. \tag{44}$$

5. NUMERICAL RESULTS

In this section, we investigate the design criteria for Alice's transmitter (i.e. intensity modulation depth δ and Gaussian beam waist at transmitter output w_0) and Bob's receiver (i.e. D-T scale coefficient ζ) to maintain the secrecy performance of the system under security constraints discussed in Section 2.1.2. For security analysis, two performance metrics, QBER and ergodic secret-key rate S (bits/s/Hz), are analyzed and confirmed by M-C simulations with a very good accuracy. Some setup parameters include the atmospheric attenuation coefficient β_l = 0.43 dB/km, the transmission distance L = 1000 m, the operating wavelength $\lambda = 1550$ nm, the peak transmitted power P = 0 dBm, and the system bit rate R_b = 1 Gbps. Bob and Eve are assumed to use the same APD-based receiver with aperture radius a = 0.01 m. From the setup parameters, the coherence length of the plane wave propagation in (8) is derived as $\rho_0 \approx 0.05$ m. Applying the security constraints, we assume d > 0.05m so that there is no correlation between the signals received at Bob's and Eve's receiver[15]. In this section, d is investigated at different values for $d \geq 0.06$ m. The secrecy performance is investigated for two cases, when there exists (i) no misalignment, and (ii) misalignment with the jitter variance at Bob's receiver is set at $\sigma_S^2 = 5a = 0.05$ m.

5.1 No misalignment

5.1.1 Alice's transmitter design

In Figure 4, Eve's error probability e is investigated to find out the proper selection of δ at Alice's transmitter to guarantee that e is sufficiently high, e.g. $e \geq 0.1$, while Eve tries to lower e by choosing its optimal average APD gain $\bar{g}$. It is seen from Figure 4 that the chosen value of δ should be $\delta \leq 0.062$ so that $e \geq 0.1$ is always guaranteed even when Eve selects its optimal $\bar{g} = 15$.

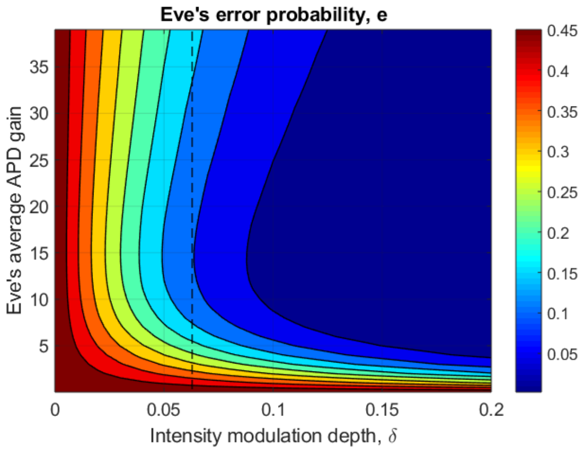


Figure 4. Eve's error probability versus Eve's average APD gain and intensity modulation depth. $C_n^2 = 6\times10^{-15}$, Eve-Bob distance on the receiver plane $d = 0.1$ m, beam waist at transmitter output $w_0 = 0.1$ m.

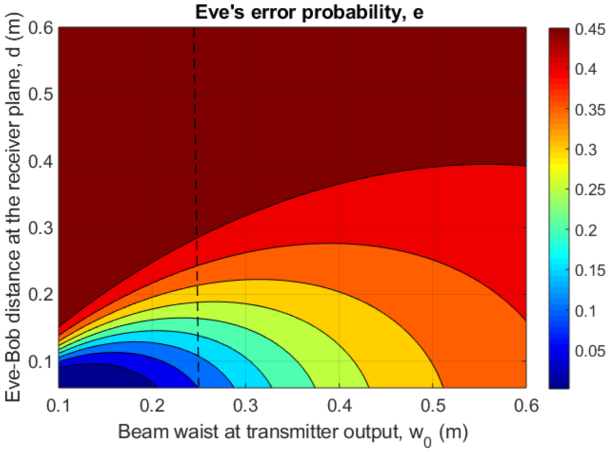


Figure 5. Eve's error probability versus Eve-Bob distance on the receiver plane *d*, and beam waist at transmitter output w_0. $C_n^2 = 6\times10^{-15}$, $\delta = 0.062$, $\bar{g} = 15$.

In Figure 5 Eve's error probability *e* is investigated to find out the suitable Gaussian beam waist at Alice's transmitter that satisfies $e \geq 0.1$ for different Eve's locations on the receiver plane characterized by *d*. With the chosen value of intensity modulation depth $\delta = 0.062$ from Figure 4, Alice should choose the Gaussian beam waist at her transmitter output at $w_0 = 0.25$ m to guarantee that $e \geq 0.1$ for all Eve's possible eavesdropping locations on the receiver plane.

5.1.2 Bob's receiver design

Based on the parameters chosen in Alice's transmitter design ($\delta = 0.062$ and $w_0 = 0.25$ m), we now investigate the design criteria for Bob's receiver. We can control QBER and P_{sift} by adjusting d_0 and d_1 through the D-T scale coefficient ζ at Bob's receiver, as shown in Figure 6. Our target is to control $P_{sift} \geq 10^{-2}$ so that the probability of sift is sufficient for Bob to receive information from Alice. At the same time, we also want to keep QBER $\leq 10^{-3}$ so that errors can be feasibly corrected by error-correcting codes. Doing so requires the choice of $0.57 \leq \zeta \leq 2.7$.

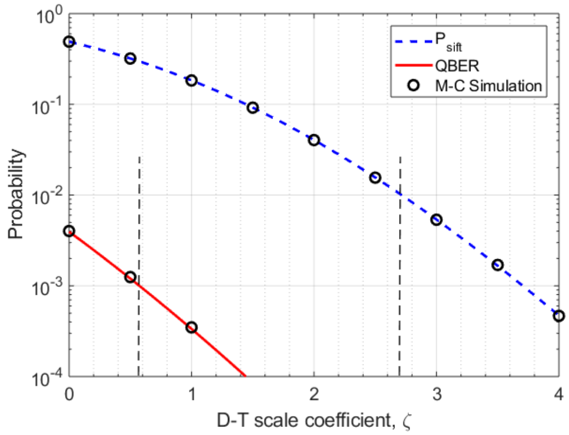


Figure 6. Bob's probability of sift and QBER versus Bob's D-T scale coefficient ζ. $C_n^2 = 6\times10^{-15}$, $\delta = 0.062$, w_0 = 0.25 m, $\bar{g} = 15$.

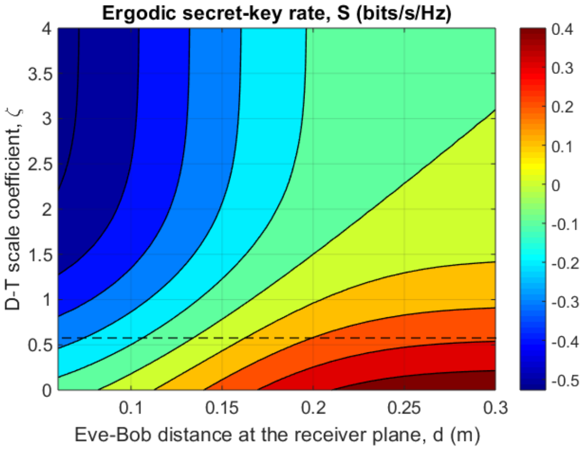


Figure 7. Bob's ergodic secret-key rate versus Eve-Bob distance at the receiver plane *d* and D-T scale coefficient ζ. $C_n^2 = 6\times10^{-15}$, $\delta = 0.062$, $w_0 = 0.25$ m, $\bar{g} = 15$.

Figure 7 shows the ergodic secret-key rate *S* to find out the optimal choice of ζ that guarantee positive *S* under security constraints. By applying the constraint of selection range $0.57 \le \zeta \le 2.7$, it is seen that the system is secured with $\zeta \ge 0.57$ when $d \ge 0.13$ m. Thus, to achieve the highest possible S when Eve tries to get closer to Bob's receiver, it is necessary to select the smallest possible value of ζ, i.e. $\zeta = 0.57$. From *S*, the final key rate, denoted as R_f can be derived as $R_f = P_{sift} R_b S$, and with $\delta = 0.062$ and $\zeta = 0.57$ we can respectively estimate the key rate as $R_f \approx 4$ Mbps, when Eve locates its receiver 30 cm away from Bob. It can be concluded from Figure 7 that the best eavesdropping strategy for Eve, when there is no misalignment, is to try to get closer to Bob's receiver to gain more information.

5.2 Misalignment

5.2.1 Alice's transmitter design

Figure 8 illustrates Eve's error probability *e* to discover the proper selection of δ at Alice's transmitter so that *e* is sufficiently high, e.g. $e \ge 0.1$, when Eve locates its receiver relatively close to Bob, e.g. $d = 0.1$ m, on the receiver plane. It is seen that Alice should select $\delta \le 0.084$ at her transmitter to always guarantee $e \ge 0.1$. From Figure 8, different optimal values of w_0 at Alice's transmitter which minimizes Eve's error rate can be respectively found. It is necessary to avoid using these values to always guarantee that Eve will suffer from the worst possible error rate.

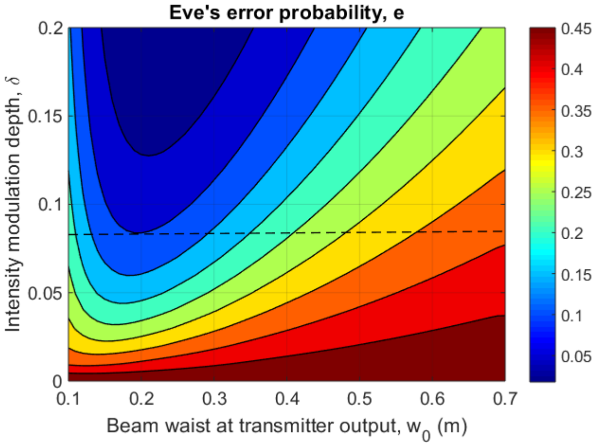


Figure 8. Eve's error probability versus intensity modulation depth and beam waist at the transmitter output. $C_n^2 = 6\times10^{-15}$, $\bar{g} = 15$, $d = 0.1$ m.

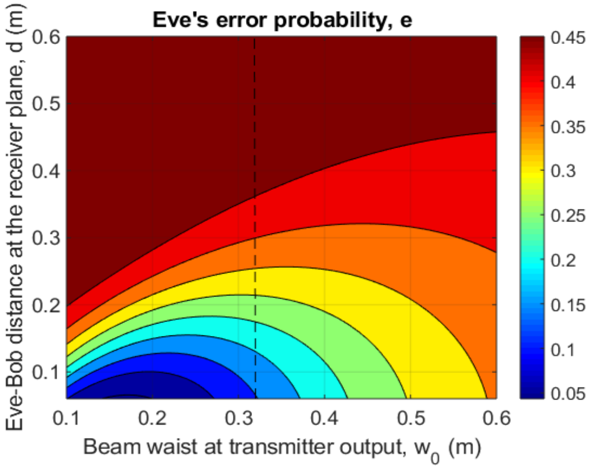


Figure 9. Eve's error probability versus Eve-Bob distance at the receiver plane d, and beam waist at transmitter output w_0, $C_n^2 = 6\times10^{-15}$, $\delta = 0.084$, $\bar{g} = 15$.

In Figure 9, Eve's error probability e is investigated to find out the proper selection of w_0 at Alice's transmitter for different locations of Eve on the receiver plane. With the chosen value of intensity modulation depth $\delta = 0.084$ from Figure 8, Alice should choose the Gaussian beam waist at her transmitter output at w_0 = 0.32 m to guarantee that $e \geq 0.1$ for all possible Eve's positions.

5.2.2 Bob's receiver design

Based on the parameters chosen in Alice's transmitter design ($\delta = 0.084$ and w_0 = 0.32 m), we now investigate the design criteria for Bob's receiver. Figure 10 shows QBER and P_{sift} versus the D-T scale coefficient ζ to find out the selection range of ζ in order that the conditions $P_{sift} \geq 10^{-2}$ and QBER $\leq 10^{-3}$ are met. To do so, Bob should choose ζ in the range $1.6 \leq \zeta \leq 2.56$.

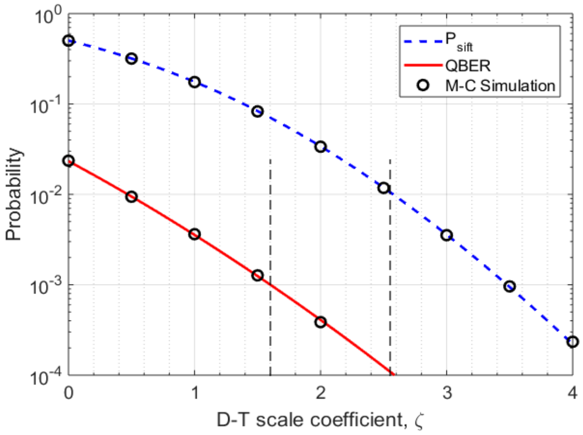


Figure 10. Bob’s probability of sift and QBER versus Bob’s D-T scale coefficient. $C_n^2 = 6\times10^{-15}$, $\delta = 0.084$, w_0 = 0.32 m, $\bar{g} = 15$.

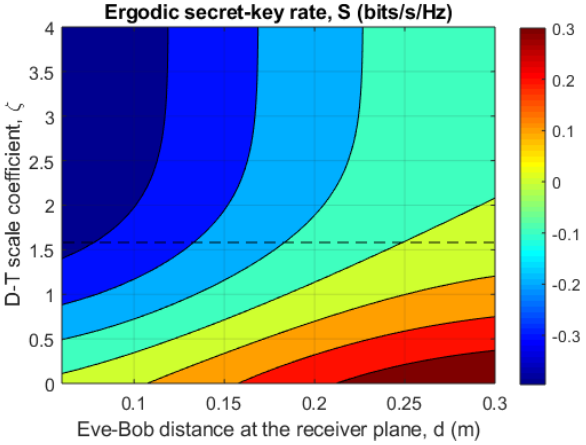


Figure 11. Bob’s ergodic secret-key rate versus Eve-Bob distance at the receiver plane d and D-T scale coefficient. $C_n^2 = 6\times10^{-15}$, $\delta = 0.084$, w_0 = 0.32 m, $\bar{g} = 15$.

In Figure 11, the ergodic secret-key rate *S* is investigated to find out the optimal choice of ζ that guarantee positive *S* under security constraints. By applying the constraint of selection range $1.6 \le \zeta \le 2.56$, it is seen that the system is secured with $\zeta \ge 1.6$ when $d \ge 0.25$ m. Thus, to achieve the highest possible *S* when Eve tries to get closer to Bob’s receiver, it is necessary to select $\zeta = 1.6$. Similar to Figure 7, with $\delta = 0.084$ and $\zeta = 1.6$, we can infer the final key rate as $R_f \approx 2.9$ Mbps, when Eve locates its receiver 30 cm away from Bob. It can be concluded from Figure 11 that the achievable ergodic secret-key rate is considerably reduced by the negative effects of misalignments combined with atmospheric turbulence. In addition, Eve is able to gain key information by locating its receiver within 0.25 m away from Bob, which is 0.12 m further compared to the case when there is no misalignment in Figure 7.

6. CONCLUSIONS

The combined effects of atmospheric turbulence- and misalignment-induced fading on the secrecy performance of IM/DD free-space CV-QKD systems using SIM/BPSK signaling with D-T APD-based receiver were investigated. The atmospheric turbulence was modeled by a log-normal fading distribution and the misalignment was analyzed based on a Gaussian beam propagation model. Under security constraints, the design criteria for Alice’s transmitter (i.e. intensity modulation depth and beam waist of the Gaussian beam) and Bob’s receiver (i.e. D-T scale coefficient selection) were comprehensively analyzed. For performance analysis, the QBER and ergodic secret-key rate were analytically derived in accurate closed-form expressions considering all effects of composite fading channels and receiver noises. Furthermore, M-C simulations additionally confirmed the correctness of derived analytical results. This paper was also marked as the first framework in the literature for analyzing the secrecy performance of FSO systems considering the eavesdropper's location on the receiver plane under the effect of misalignment between legitimate transceivers.

7. ACKNOWLEDGMENT

This work is a part of "Research and Development of the Quantum Cryptography Technology for Satellite Communications" in "Research and Development of Information and Communications Technology" of Ministry of Internal Affairs and Communication (MIC), Japan and this work is supported by MIC.

REFERENCES

[1] Cheng, C., Lu, R., Petzoldt, A., and Takagi, T., "Securing the internet of things in a quantum world," IEEE Commun. Mag., 55(2), 116-120 (2017).

[2] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H., "Quantum cryptography," Rev. Mod. Phys., 74(1), 145-195 (2002).

[3] Kukita, T., Takada, H., and Inoue, K., "Macroscopic differential phase shift quantum key distribution using an optically pre-amplified receiver", Jpn. J. Appl. Phys., 49, 122801 (2010).

[4] Ikuta, T. and Inoue, K., "Intensity modulation and direct detection quantum key distribution based on quantum noise," New J. Phys., 18, 013018 (2016).

[5] Eriksson, T. A., Trinh, P. V., Endo, H., Takeoka, M., and Sasaki, M., "Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks," OSA Opt. Express, 26(16), 20409-20419 (2018).

[6] Trinh, P. V., Pham, T. V., Nguyen, H. V., Ng, S. X., and Pham, A. T., "Performance of free-space QKD systems using SIM/BPSK and dual-threshold/direct-detection," Proc. IEEE Global Commun. Conf. (Globecom), QCIT Workshop, 1-6 (2016).

[7] Trinh, P. V. and Pham, A. T., "Design and secrecy performance of novel two-way free-space QKD protocol using standard FSO systems," Proc. IEEE Int. Conf. Commun. (ICC), 929-934 (2017).

[8] Trinh, P. V., Pham, T. V., Dang, N. T., Nguyen, H. V., Ng, S. X., and Pham, A. T., "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," IEEE Access, 6, 4159-4175 (2018).

[9] Takenaka, H., Carrasco-Casado, A., Fujiwara, M., Kitamura, M., Sasaki, M., and Toyoshima, M., "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," Nature Photon., 11, 502-508 (2017).

[10] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Comput. Syst. Signal Process., 175-179 (1984).

[11] Fujiwara, M., Ito, T., Kitamura, M., Endo, H., Tsuzuki, O., Toyoshima, M., Takenaka, H., Takayama, Y., Shimizu, R., Takeoka, M., Matsumoto, R., and Sasaki, M., "Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link," OSA Opt. Express, 26(15), 19513-19523 (2018).

[12] Karp, S., [Optical channels: fibers, clouds, water and the atmosphere], New York, NY, USA: Plenum (1988).

[13] Pham, H. T. T., Trinh, P. V., Dang, N. T., and Pham, A. T., "A comprehensive performance analysis of PPM-based FSO systems with APD receiver in atmospheric turbulence," Proc. IEEE Int. Conf. Adv. Technol. Commun. (ATC), 357-361 (2012).

[14] Farid, A. A. and Hranilovic, S., "Outage capacity optimization for free-space optical links with pointing errors," IEEE/OSA J. Lightw. Technol., 25(7), 1702-1710 (2007).

[15] AlQuwaiee, H., Yang, H. -C., and Alouini, M. -S., "On the asymptotic capacity of dual-aperture FSO systems with generalized pointing error model," IEEE Trans. Wireless Commun., 15(9), 6502-6512 (2016).

[16] Pham, H. T. T., Trinh, P. V., Dang, N. T., and Pham, A. T., "Secured relay-assisted atmospheric optical code-division multiple-access systems over turbulence channels," IET Optoelectron., 9(5), 241-248 (2015).

[17] Farid, A. A. and Hranilovic, S., "Outage capacity for MISO intensity-modulated free-space optical links with misalignment," IEEE/OSA J. Opt. Commun. Netw., 3(10), 780-789 (2011).

[18] Abramowitz, M. and Stegun, I. A., [Handbook of Mathematical Functions with Fomulas, Graphs, and Mathematical Tables], 9th ed. New York, USA: Dover Publications (1972).

[19] "Nodes and Weights of Gauss-Hermite Calculator," http://keisan.casio.com/exec/system/1281195844.