


Received December 25, 2017, accepted January 28, 2018, date of publication January 31, 2018, date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2800291

# Design and Security Analysis of Quantum Key Distribution Protocol Over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver

PHUC V. TRINH<sup>1</sup>, (Member, IEEE), THANH V. PHAM<sup>2</sup>, (Student Member, IEEE),  
NGOC T. DANG<sup>3</sup>, HUNG VIET NGUYEN<sup>4</sup>, (Member, IEEE),  
SOON XIN NG<sup>5</sup>, (Senior Member, IEEE), AND ANH T. PHAM<sup>2</sup> , (Senior Member, IEEE)

<sup>1</sup>Space Communications Laboratory, National Institute of Information and Communications Technology, Tokyo 184-8795, Japan

<sup>2</sup>Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan

<sup>3</sup>Department of Wireless Communications, Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

<sup>4</sup>5G Innovation Centre, University of Surrey, Guildford GU2 7XH, U.K.

<sup>5</sup>School of ECS, University of Southampton, Southampton SO17 1BJ, U.K.

Corresponding author: Anh T. Pham (pham@u-aizu.ac.jp)

This work was supported by the Telecommunications Advancement Foundation in Japan.

**ABSTRACT** This paper proposes a novel design and analyzes security performance of quantum key distribution (QKD) protocol over free-space optics (FSO). Unlike conventional QKD protocols based on physical characteristics of quantum mechanics, the proposed QKD protocol can be implemented on standard FSO systems using subcarrier intensity modulation binary phase shift keying and direct detection with a dual-threshold receiver. Under security constraints, the design criteria for FSO transmitter and receiver, in particular, the modulation depth and the selection of dual-threshold detection, respectively, is analytically investigated. For the security analysis, quantum bit error rate, ergodic secret-key rate, and final key-creation rate are concisely derived in novel closed-form expressions in terms of finite power series, taking into account the channel loss, atmospheric turbulence-induced fading, and receiver noises. Furthermore, Monte-Carlo simulations are performed to verify analytical results and the feasibility of the proposed QKD protocol.

**INDEX TERMS** Quantum key distribution (QKD), free-space optics (FSO), subcarrier intensity modulation (SIM), binary phase shift keying (BPSK), atmospheric turbulence-induced fading, dual-threshold direct detection.

## I. INTRODUCTION

With the rapid development of the Internet and recent advancements to the Internet of Things, the secure communications for sensitive information over the Internet plays a very crucial role. Conventional security relies solely on the secrecy of an encryption key based on cryptographic algorithms. To achieve unconditional security, two legitimate parties, namely Alice and Bob, must be able to share the secret key over publicly unsecured communication channels. This is also known as the key distribution problem. Unfortunately, conventional key distribution protocols relying on computational complexities are vulnerable to future advances in computer hardware and algorithms. Therefore, such protocols do not provide information-theoretic security, i.e. without any condition of computational assumptions [1]. Quantum key distribution (QKD), on the other hand,

promises the principle *unconditional security* by applying the law of quantum mechanics to securely distribute the key between two legitimate parties in the presence of eavesdropper(s), namely Yuen [2]. The first QKD protocol, widely known as BB84 protocol, was proposed by Bennett and Brassard [3], by which the legitimate sender (Alice) and receiver (Bob) can achieve the secret-key sharing with randomly generated signals encoded by two non-orthogonal quantum states.

Owing to how the information is encoded, there exists two major implementation methods of QKD protocols, namely discrete variable (DV) and continuous variable (CV). In DV-QKD systems, the key information is encoded onto the discrete state of a single photon, such as the phase or polarization [4]. The encoded photons are then transmitted over the quantum channel and detected by a single-photon

receiver. DV-QKD or single-photon based QKD has the advantage of enabling long-range key distribution, however, it requires the use of bulky and expensive single-photon detectors. In contrast, CV-QKD systems encode the key information on the continuous variables of coherent states conveyed by the amplitude and/or phase of weakly modulated light pulses [5]. Compared to DV-QKD, CV-QKD is much easier to implement as it is compatible with the standard optical telecommunication technologies and enables higher key generation rates by using heterodyne/homodyne detection instead of the single-photon counters. CV-QKD scheme has been theoretically studied and experimentally implemented both over optical fiber [6]- [10] and free-space optical (FSO) communication links [11]- [14].

The key implementation issue with CV-QKD system nevertheless arises from the heterodyne/homodyne detection receiver, which results in high cost due to the requirement of the sophisticated phase-stabilized local light at the receiver [15]. To avoid such issue and further simplify CV-QKD systems, intensity modulation with dual-threshold/direct detection (D-T/DD) over *fiber* CV-QKD systems has been recently proposed [16]. Specifically, two slightly intensity-modulated pulses, i.e. coherent states, employing on-off keying (OOK) are sent from the transmitter and directly detected by a PIN receiver with dual thresholds. The idea behind this dual-threshold detection is to mimic the sifting process of two non-orthogonal photon bases by adjusting two thresholds at high and low levels of two intensity-modulated signals with small amplitude difference. Due to quantum noise, signals arriving at the receiver exceed the thresholds randomly and uncorrelated for Eve and Bob. When thresholds are not exceeded, the coherent states are indistinguishable and Eve unavoidably introduces errors by randomly guessing the states. In this way, the QKD function can be achieved with simple configuration. To optimize the setting of dual thresholds, channel-state information (CSI) is required at the receiver. In optical fiber environments, CSI estimation can be easily achieved due to the *non-fading* channel characteristics.

Compared to optical fiber, nevertheless, FSO is more flexible and cheaper to implement, especially when there is an urgent need for quick deployment and/or re-deployment. In addition, FSO is able to provide fiber-like data rate of up to 10 Gbps [17], and is being considered for high-capacity, interference-immune, and resilient backhaul solutions in the fifth-generation (5G) mobile networks [18], [19]. More promisingly, with recent advances in quantum satellite communication over long-distance FSO link from a satellite to a ground station as well as inter-satellite communication, the possibility of a global QKD network for secure communication is practically highlighted [20], [21].

Motivated by the pioneer work in [16] and the fact that *free-space* QKD systems play an important role in future QKD networks, our goal in this paper is to design a CV-QKD protocol that can be feasibly and cost-effectively implemented on standard horizontal FSO systems while

satisfying necessary security constraints. Particularly, our contributions can be summarized as follows.

- We propose a novel *free-space* CV-QKD system using dual-threshold/direct detection (D-T/DD) with subcarrier intensity modulation binary phase shift keying (SIM/BPSK) signaling. Practically, CSI estimation for D-T settings over fading channels in case of OOK signaling is complicated due to the asymmetry of binary signals (e.g., noise variances are different in bits “0” and “1”). Therefore, the use of SIM/BPSK signaling whose signals of bit “0” and “1” are symmetric over the “zero” level will relax the CSI estimation over the atmospheric turbulence-induced fading channels.
- To confirm the feasibility and reliability of the proposed system, we analytically investigate the design criteria for FSO transmitter and receiver, especially, the modulation depth and the selection of values for D-T settings to maintain the security in the proposed free-space QKD system against a practical attacking strategy from the eavesdropper Eve (i.e., unauthorized receiver attack), with an assumption of fully trusted transmitting and receiving devices at Alice and Bob.
- In addition, we analytically study the secrecy performance of the proposed system by deriving, in newly accurate closed-form expressions, the quantum bit-error rate (QBER), ergodic secret-key rate, and final key-creation rate, taking into account effects of atmospheric channel and receiver noises. The well-known log-normal and Gamma-Gamma distributions are adopted to model the atmospheric turbulence in weak and moderate-to-strong regimes, respectively. Monte-Carlo (M-C) simulations are further implemented to confirm the validity of the analytical results.

The remainder of this paper is organized as follows. Section II provides basic concepts and describes the operation of conventional BB84 protocol over an FSO system. Section III then highlights the proposed design concept and system model. The atmospheric turbulence-induced fading channel is modeled and analyzed in Section IV. In Section V, the system secrecy performance metrics are theoretically investigated and derived in closed-form solutions in terms of finite power series. Finally, useful numerical results are discussed in Section VI, and the paper is concluded with summarized key points and future outlook in Section VII.

## II. CONVENTIONAL BB84 PROTOCOL OVER FSO

### A. BB84 PROTOCOL

In this subsection, we provide operational steps of the conventional BB84 protocol in support of the discussion in subsequent sections, which are summarized in four steps as follows [4].

*Step 1:* Alice randomly chooses between two linear polarization bases  $\otimes$  or  $\oplus$  (i.e., rectilinear or diagonal bases) for every bit that she wants to send. The two bases  $\otimes$  and  $\oplus$  constitute four polarization states ( $-45^\circ$ ,  $45^\circ$ ) and ( $0^\circ$ ,  $90^\circ$ ), respectively. For each chosen basis, Alice creates quantum

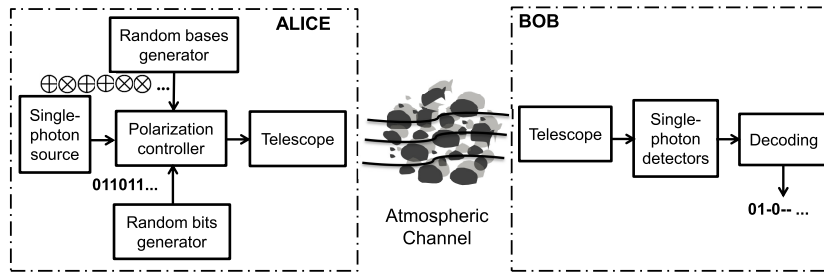


FIGURE 1. A simplified block diagram of the conventional BB84 QKD protocol over an FSO channel.

TABLE 1. An example of BB84 protocol.

Alice			Bob			
Bit	Basis	State	Basis	State	Bit	Sifted key
0	⊕	0°	⊕	0°	0	0
1	⊕	90°	⊕	90°	1	1
0	⊕	0°	⊗	-45°	0	discarded
1	⊕	90°	⊗	45°	1	discarded
0	⊗	-45°	⊕	0°	0	discarded
1	⊗	45°	⊕	90°	1	discarded
0	⊗	-45°	⊗	-45°	0	0
1	⊗	45°	⊗	45°	1	1

bits, or “qubits”, by encoding random bit values, “0” or “1”, using the following set of polarization codes

$$0 \rightarrow \begin{cases} 0^\circ & \text{if } \oplus \text{ was chosen,} \\ -45^\circ & \text{if } \otimes \text{ was chosen,} \end{cases} \quad (1)$$

$$1 \rightarrow \begin{cases} 90^\circ & \text{if } \oplus \text{ was chosen,} \\ 45^\circ & \text{if } \otimes \text{ was chosen.} \end{cases} \quad (2)$$

The encoded quantum bits are then transmitted over the unsecured channel as discrete single-photons to Bob’s receiver. An example of Alice’s qubits preparation can be seen in Table 1.

*Step 2:* At the receiver, Bob detects the encoded photons by a single-photon detector. To examine the encoded information, a basis,  $\otimes$  or  $\oplus$ , is randomly used to measure each photon in the corresponding polarization states. To this point, if Alice’s encoding and Bob’s decoding bases are the same, the corresponding bit value is read correctly with a high probability. Otherwise, if the two bases are different,<sup>1</sup> the received photon is measured by one of two polarization states of the used basis at Bob’s receiver. Thus, bits “0” and “1” are then decoded, corresponding to the measured polarization states. This is also known as the *sifting process* as illustrated in Table 1.

*Step 3:* After *Step 2*, the bit sequence detected by Bob and the corresponding bit sequence transmitted by Alice form their partially correlated *raw keys*. Through a public channel, Alice broadcasts her basis choice for each bit of her raw key, but not the bit value. Bob then reveals on which detected photons the same basis was used to measure (without

<sup>1</sup>When the wrong basis is used to measure, the measurement changes the original polarization state of the received photon to one of two polarization states of the wrong basis [4].

revealing the bit value he decoded on each one). They both discard photon measurements where Bob used a different basis, which is 50% on average, leaving the remaining bits as their *sifted key*, as shown in Table 1.

*Step 4:* In practice, Bob’s sifted key may contain errors due to eavesdropping or channel/detector imperfections. To identify and remove the erroneous bits, Alice and Bob perform *information reconciliation* by publishing a random sample of their measurements over the public channel and using error correction techniques to correct the transmission errors, which ensures both keys are identical, forming their shared error-free *secret key*. In addition, to reduce Eve’s knowledge of the shared key, Alice and Bob apply the *privacy amplification* process by using their shared keys to produce a new, shorter key based on hash functions in such a way that Eve has only negligible information about the new key.

The security of BB84 protocol, according to the laws of quantum mechanics, lies in the fact that Alice encodes her information in *non-orthogonal* states  $\oplus$  or  $\otimes$  so that an eavesdropper Eve cannot sufficiently distinguish the two states and errors unavoidably occur when she eavesdrops [22].

## B. FREE-SPACE QKD USING BB84 PROTOCOL

Illustratively, Fig. 1 shows the simplified schematic diagram of a free-space QKD system employing the BB84 protocol.

At Alice’s side, a single-photon source is used to emit single photons, which could be ideally achieved with the help of a semiconductor quantum dot [23]. The single photons are then polarized by a polarization controller driven by two random streams of polarization bases and binary bits, which are respectively generated by the random bases generator and random bits generator [24]. The polarization controller encodes the binary bits into random bases according to the rules given in (1) and (2). The encoded photons are then transmitted over an atmospheric turbulence-induced fading channel to Bob. It is found that near-field atmospheric turbulence imposes a modest decrease in the sift probability and an increase in the conditional probability of error in BB84 [25].

At Bob’s side, a set of devices is invoked to measure the received photons, including a 50/50 ordinary beam splitter to provide a passive, random choice of polarization bases

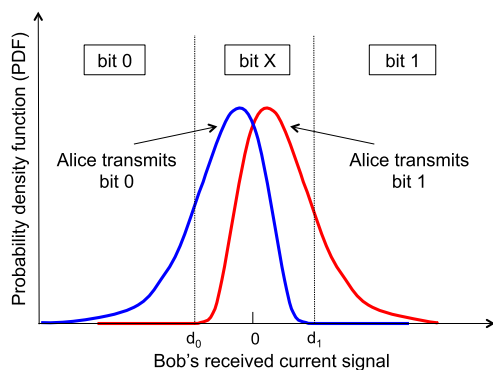
for a single photon, half-wave plates for converting the basis  $\oplus$  to  $\otimes$  and vice versa, and polarizing beam splitters for directing the incoming photons to the designated single-photon detector. A single-photon detector is a device used to detect the polarized photons. Recently, researchers have successfully developed a practical superconducting nanowire single-photon detector with record detection efficiency over 90% [26]. Based on the detection counted at the designated single-photon detectors of corresponding polarization states, the binary bits originally encoded by Alice on the polarization states could be decoded. Details of the decoding mechanism can be covered in [25] and [27].

### III. PROPOSED DESIGN CONCEPT AND SYSTEM MODEL

#### A. PROPOSED DESIGN CONCEPT

In this section, we describe the design concept for the implementation of the QKD protocol by using SIM/BPSK signaling and D-T/DD. Using the proposed QKD protocol, a CV-QKD function can be achieved and feasibly implemented on standard FSO systems, with simple configurations and sufficient security. Details are as follows.

*Step 1:* Alice transmits SIM/BPSK modulated signals, i.e. coherent states, with a small modulation depth ( $0 < \delta < 1$ ), corresponding to binary random bits “0” or “1” over the atmospheric channel. The two modulated signals representing binary bits are two coherent states that are nonorthogonal to each other. Thus, they play a similar role as nonorthogonal bases in BB84 protocol.



**FIGURE 2.** The probability density function of Bob’s received signal over atmospheric turbulence-induced fading channel,  $d_0$  and  $d_1$  are two levels of the dual thresholds.

*Step 2:* The transmitting modulated signals are then directly detected at Bob’s receiver using an avalanche photodiode (APD). Fig. 2 shows the probability density function (PDF) of Bob’s received BPSK signals influenced by the atmospheric turbulence-induced fading channel and receiver quantum noise, which are symmetric over the “zero” level. By obtaining the CSI, two levels of the D-T,  $d_0$  and  $d_1$ , can be selected symmetrically over the “zero” level. The distribution of the received signals has two peaks corresponding to Alice’s bit “0” and bit “1”, which overlap with each other as the modulation depth is small compared to noise

variances. For the detected value  $x$  of the received current signal, the detection rule can be expressed as

$$\text{Decision} = \begin{cases} 0 & \text{if } (x \leq d_0) \\ 1 & \text{if } (x \geq d_1) \\ X & \text{otherwise,} \end{cases} \quad (3)$$

where X represents the case that Bob creates no bit, which corresponds to the case of wrong basis selection in the BB84 protocol. It is noted that the random fluctuations in the received signals over the atmospheric channel result in random detection results of “0”, X, and “1” at the D-T. This randomness is uncorrelated with Eve’s one as it results from channel fading and quantum noises. It is practical and feasible to consider the signals arriving at Eve’s and Bob’s receivers experience uncorrelated fading as Eve’s receiver should be separated from Bob’s within distance in the order of meters for possible eavesdropping, whereas correlation appears when receivers’ separated spacing is in the order of centimeters [28].

*Step 3:* Using a classical public channel, Bob notifies Alice of the time instants he was able to create binary bits from detected signals. Alice then discards bit values at time instants that Bob created no bit. Now, Alice and Bob share an identical bit string, which is the *sifted key*. By obtaining the CSI estimation at the receiver,  $d_0$  and  $d_1$  can be adjusted, thus the probability of sift at Bob’s receiver can be controlled.

Table 3 illustrates a simple example of the proposed protocol according to the above-mentioned operational steps. Alice transmits bits “0” and “1” encoded onto SIM/BPSK modulated signals at different time instants, with  $i_0$  and  $i_1$  are intensity-modulated current signals of bits “0” and “1”, which are symmetric over the “zero” level and controlled by the modulation depth  $\delta$ ;  $d_0$  and  $d_1$  are two detection thresholds at Bob’s receiver, adjusted by obtaining the CSI estimation<sup>2</sup>, e.g. channel state  $h$  and noise variance  $\sigma_N^2$  (it is noted that noise variance is the same in bits “0” and “1” for BPSK signaling). At different time instants, depending on the decision rule in (3), bits “0”, “1”, and “X” (no bit) are created at Bob’s receiver. Over a public channel, Bob notifies Alice of the time instants he created no bits (e.g.,  $t_2, t_3, t_4, t_5$ ) so that Alice can discard key bits transmitted at the corresponding time instants, forming their shared sifted key.

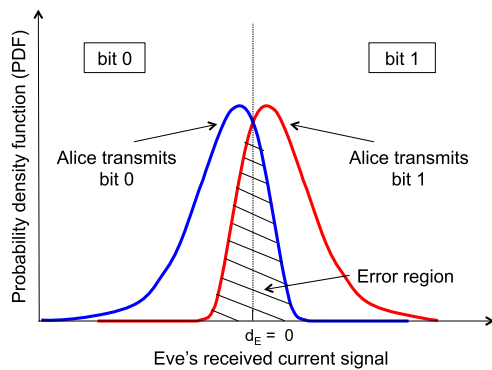
*Step 4:* Similar to the BB84 protocol, further *information reconciliation* and *privacy amplification* can then be implemented over the public channel to obtain the final *secret key*.

The security of this design concept can be explained as follows. *Firstly*, the modulation depth  $\delta$  of the SIM/BPSK signals is chosen to be small enough in order that Eve cannot fully distinguish the transmitted state. Eve can also try to use

<sup>2</sup>Here, it is assumed that perfect CSI can be obtained at Bob’s receiver. The CSI can be estimated by taking advantage of the slowly-varying nature of the FSO channel, i.e. fading remains constant over a large number of transmitted bits for a coherence time in the order of milliseconds [29]. For instance, a few pilot symbols may be transmitted from Alice to Bob so that Bob can estimate the CSI of the fading channel. The data symbols transmitted from Alice followed by the pilot symbols will experience similar channel fading.

**TABLE 2.** Comparison between different QKD technologies.

	DV-QKD [3]	CV-QKD [5]	Non-coherent CV-QKD (Proposed)
<b>Source</b>	Weak laser pulse (single-photon)	Laser	Laser
<b>Modulation</b>	Polarization	Amplitude & Phase	Intensity
<b>Detection</b>	Single-photon detection	Coherent detection	Direct detection
<b>System Complexity</b>	Very high	High	Low
<b>Implementation Cost</b>	Very high	High	Low
<b>Compatibility with Standard Technologies</b>	No	Yes	Yes
<b>Key Rate</b>	Low	High	High
<b>Free-Space Operation</b>	Near-field	Far-field	Far-field



**FIGURE 3.** The probability density function of Eve’s received signal over atmospheric turbulence-induced fading channel with the optimal threshold  $d_E$ .

**TABLE 3.** An example of the proposed protocol.

Alice			Bob			
Bit	Signals	Time	Thresholds	Time	Bit	Sifted key
0	$i_0$	$t_0$	$d_0$	$t_0$	0	0
1	$i_1$	$t_1$	$d_1$	$t_1$	1	1
0	$i_0$	$t_2$	$d_0$	$t_2$	X	discarded
1	$i_1$	$t_3$	$d_1$	$t_3$	X	discarded
0	$i_0$	$t_4$	$d_0$	$t_4$	X	discarded
1	$i_1$	$t_5$	$d_1$	$t_5$	X	discarded
0	$i_0$	$t_6$	$d_0$	$t_6$	0	0
1	$i_1$	$t_7$	$d_1$	$t_7$	1	1

D-T like Bob does, however, Eve’s signal fluctuation is uncorrelated to Bob’s one, thus the key bits created by Bob and Eve do not match, as mentioned in *Step 2*. If Eve tries to decode the key using the optimal threshold (which is  $d_E$  at “zero” as illustrated in Fig. 3), she obtains measurements where the two signals are strongly overlapped, thus she will suffer from a high error rate, thereby reducing the knowledge gained by Eve. *Secondly*, as mentioned in *Steps 2* and *3*, the probability of sift can also be controlled by Bob via the D-T setting. This means the amount of information shared between Alice and Bob can be controlled. As a result, we can guarantee a positive secrecy rate by properly adjusting the modulation depth and D-T setting so that the mutual information between Alice and Bob is always larger than that gained by Eve under various eavesdropping strategies. Details of the security analysis for

the transmitter/receiver design of the proposed system will be further discussed in Section VI.

Table 2 summarizes key characteristics of the proposed system, i.e. non-coherent CV-QKD, in comparison with DV-QKD and CV-QKD systems. The key features of the proposed system include simplicity and cost-efficiency, since phase-stabilized local laser or expensive single-photon detector is not required. In particular, Intensity Modulation/Direct Detection (IM/DD) systems are commercially available for high data rate, i.e., Gigabits per second (Gbps), and most advantageous for single-wavelength data transmission over short distances.

**B. SYSTEM MODEL**

Figure 4 presents a block diagram of the proposed free-space CV-QKD system using SIM/BPSK and D-T/DD receiver with an APD.

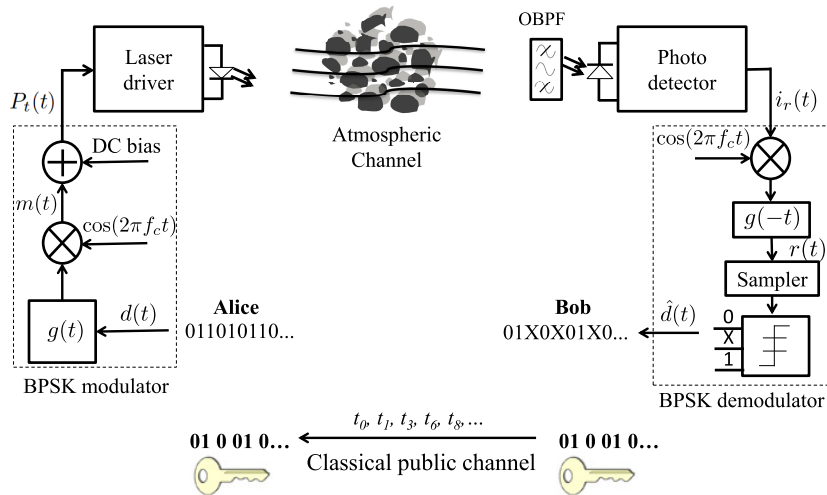
At the transmitter, the source data  $d(t)$  is first modulated onto a radio frequency (RF) subcarrier signal using BPSK scheme in which bits “0” and “1” are represented by two different phases  $180^\circ$  apart. The subcarrier signal  $m(t)$  is sinusoidal having both positive and negative values; therefore a DC bias is added to  $m(t)$  before it is used to modulate a continuous-wave laser beam. Let  $P_t(t)$  denote the transmitted power of the modulated laser beam, we have

$$P_t(t) = \frac{P}{2} [1 + \delta m(t)], \tag{4}$$

where  $P$  represents the peak transmitted power,  $\delta$  is the intensity modulation depth ( $0 < \delta < 1$ ) to avoid overmodulation ( $-1 < \delta m(t) < 1$ ).  $m(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$ , 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  $i$ th binary data. For the sake of simplicity, we normalize the power of  $m(t)$  to unity [30], [31].

At the receiver, the incoming optical field is passed through an optical bandpass filter (OBPF) before being converted into an electrical signal through DD at the APD. A standard RF coherent demodulator is employed to recover the source data  $\hat{d}(t)$ . Thus, the electrical signal at the output of the APD at the receiver can be written as

$$i_r(t) = \Re\left\{\frac{P}{2}h(t) [1 + \delta m(t)] + n(t)\right\}, \tag{5}$$



**FIGURE 4.** A block diagram of the proposed free-space QKD system using SIM/BPSK and D-T/DD with an APD receiver.

where  $\Re = \frac{\eta q}{h\nu}$  is the responsivity (in units of A/W) of the APD with  $\eta$  is the quantum efficiency,  $q$  is the electron charge,  $h$  is the Planck's constant,  $\nu$  is the optical frequency;  $\bar{g}$  is the average APD gain, and  $n(t)$  is the receiver noise. Since the turbulence-induced fading  $h(t)$  varies slowly enough, the DC term  $\{\Re \bar{g} \frac{P}{2} h(t)\}$  can be filtered out by the OBPF [32]. The electrical signal  $i_r(t)$  is then passed through the BPSK demodulator shown in Fig. 4, where the output signal  $r(t)$  is demodulated by the reference signal  $\cos(2\pi f_c t)$  as [32]

$$r(t) = \overline{i_r(t)\cos(2\pi f_c t)} = \begin{cases} i_0 = \frac{1}{4}\Re\bar{g}P\delta h(t) + n(t) \\ i_1 = \frac{1}{4}\Re\bar{g}P\delta h(t) + n(t) \end{cases}, \quad (6)$$

where  $i_0$  and  $i_1$  represent the received current signals for bits “0” and “1”, respectively. Assuming that the dark current is negligible, the receiver noises composing of shot noise, background noise, and thermal noise can be modeled as additive white Gaussian noises (AWGN) with high accuracy [32]. Thus,  $n(t)$  is the zero-mean AWGN with variance

$$\sigma_N^2 = \sigma_{sh}^2 + \sigma_b^2 + \sigma_{th}^2, \quad (7)$$

where  $\sigma_{sh}^2$ ,  $\sigma_b^2$ , and  $\sigma_{th}^2$  are respectively the variances of the APD shot noises caused by the received signal, background radiation, and receiver thermal noise, which can be subsequently expressed as

$$\sigma_{sh}^2 = 2q\bar{g}^2\Re F_A \left(\frac{1}{4}P\delta h\right) \Delta_f, \quad (8)$$

$$\sigma_b^2 = 2q\bar{g}^2\Re F_A P_b \Delta_f, \quad (9)$$

$$\sigma_{th}^2 = \frac{4k_B T F_n}{R_L} \Delta_f, \quad (10)$$

where  $F_A = k_A \bar{g} + \left(2 - \frac{1}{\bar{g}}\right) (1 - k_A)$  denotes the excess noise factor with  $k_A$  is the ionization factor,  $F_n$  is the amplifier noise figure,  $P_b$  is the average received background radiation power,  $\Delta_f = \frac{R_b}{2}$  with  $R_b$  is the system bit rate,  $T$  is the receiver temperature in Kelvin degree, and  $R_L$  is the APD's load resistance.

After demodulating process, the demodulated electrical signal is being sampled and then used to create binary bits “0”, “1”, and no bit (i.e., X), based on D-T/DD with decision rules as described in Section III-A, 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 the sifted key.

#### IV. ATMOSPHERIC CHANNEL MODELS

In our model, the channel coefficient  $h$  can be described as  $h = h^l h^t$ , where  $h^l$  is the channel loss including atmospheric attenuation and geometric spreading loss of the optical beam due to optical diffractions, and  $h^t$  is the atmospheric turbulence-induced fading.

##### A. CHANNEL LOSS

The channel loss induced by atmospheric attenuation described by the exponential Beer-Lambert's Law and geometric spreading loss can be formulated as

$$h^l = \frac{A}{\pi \left(\frac{\theta}{2}L\right)^2} \exp(-\beta_l L), \quad (11)$$

in which  $A = \pi(D/2)^2$  is the area of the receiver aperture with  $D$  is the diameter,  $\theta$  is the angle of divergence,  $\beta_l$  is the attenuation coefficient, and  $L$  is the transmission distance in kilometers [33].

##### B. ATMOSPHERIC TURBULENCE-INDUCED FADING

Inhomogeneities in the temperature and pressure of the atmosphere lead to refractive-index variations along the transmission path, which is commonly known as atmospheric turbulence. An optical wave propagating through the atmosphere is affected by atmospheric turbulence, leading to the irradiance (i.e., intensity) fluctuations, also known as *scintillation* or *fading*, observed at the receiver. To statistically characterize the atmospheric turbulence-induced fading,

log-normal (LN) and Gamma-Gamma (GG) distribution models have been widely used for characterizing weak and moderate-to-strong turbulence regimes, respectively.

### 1) LOG-NORMAL TURBULENCE MODEL

For weak turbulence conditions, the PDF of turbulence-induced fading coefficient  $h^t$ , governed by the LN distribution, can be expressed as [34]

$$f_{LN}(h^t) = \frac{1}{\sqrt{8\pi h^t \sigma_x}} \exp\left(-\frac{[\ln(h^t) - 2\mu_x]^2}{8\sigma_x^2}\right), \quad (12)$$

where  $\mu_x$  and  $\sigma_x^2$  are the mean and standard variance of log-amplitude fluctuation. 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  $\mathbb{E}[\cdot]$  denotes the statistical expectation. Doing so requires the choice of  $\mu_x = -\sigma_x^2$ . Assuming plane wave propagation,  $\sigma_x^2$  can be given as

$$\sigma_x^2 = 0.307 \left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2, \quad (13)$$

where  $\lambda$  is the wavelength and  $L$  is the transmission distance in meters.  $C_n^2$  stands for the refractive index structure coefficient, which varies from  $10^{-17}$  to  $10^{-13}$  [33].

### 2) GAMMA-GAMMA TURBULENCE MODEL

For moderate-to-strong turbulence conditions, the PDF of fading coefficient  $h^t$ , modeled by a GG distribution, is given as [35]

$$f_{GG}(h^t) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} (h^t)^{\frac{\alpha+\beta}{2}-1} \times K_{\alpha-\beta}(2\sqrt{\alpha\beta h^t}), \quad (14)$$

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  $(\alpha - \beta)$ ;  $\alpha > 0$  and  $\beta > 0$  are the effective numbers of small-scale and large-scale eddies of scattering environment, respectively. Assuming a plane wave propagation,  $\alpha$  and  $\beta$  are approximately expressed as

$$\alpha \cong \left[ \exp\left(\frac{0.49\sigma_R^2}{(1 + 1.11\sigma_R^{12/5})^{7/6}}\right) - 1 \right]^{-1}, \quad (15)$$

$$\beta \cong \left[ \exp\left(\frac{0.51\sigma_R^2}{(1 + 0.69\sigma_R^{12/5})^{5/6}}\right) - 1 \right]^{-1}, \quad (16)$$

where  $\sigma_R^2$  is the Rytov variance given as

$$\sigma_R^2 = 1.23 \left(\frac{2\pi}{\lambda}\right)^{7/6} L^{11/6} C_n^2. \quad (17)$$

The Rytov variance in (17) is used to characterize the strength of atmospheric turbulence. According to [36, Fig. 3], with  $\lambda = 1550$  nm, the changes in values of  $C_n^2$  and  $L$  classify  $\sigma_R^2$  into three categories,  $\sigma_R^2 < 1$ ,  $\sigma_R^2 \approx 1$ , and  $\sigma_R^2 > 1$  that respectively define weak, moderate, and strong turbulence conditions. As a result, having known  $C_n^2$  and  $L$ , one can determine the turbulence conditions accordingly.

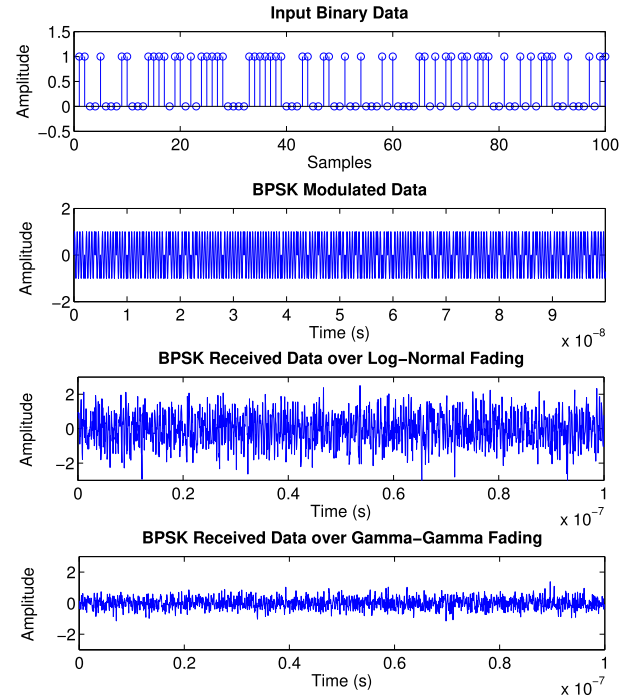


FIGURE 5. Impact of atmospheric turbulence-induced fading on electrical BPSK signal at the receiver.

## C. IMPACT OF ATMOSPHERIC TURBULENCE ON BPSK SIGNALING

To illustrate the impact of atmospheric turbulence-induced fading on electrical BPSK signaling at the receiver, Fig. 5 shows an example of transmitting 100 sample bits using BPSK-modulated signaling over an FSO link, with the data rate  $R_b = 1$  Gbps and transmission distance  $L = 1$  km, under the impact of weak and moderate-to-strong turbulence conditions modeled by LN (e.g.,  $C_n^2 = 10^{-15}$ ) and GG (e.g.,  $C_n^2 = 10^{-14}$ ) distributions, respectively. As is evident, the BPSK signaling received at the receiver suffers from fluctuations due to atmospheric turbulence. Especially, when turbulence becomes stronger, the electrical signal amplitude is severely fluctuated, which consequently results in highly noisy BPSK symbols in the constellation plane at the receiver, as shown in Fig. 6.

## V. SECRECY PERFORMANCE ANALYSIS

### A. QUANTUM BIT ERROR RATE

In BB84 protocol, the quantum bit error rate (QBER) can be defined as [4], [25]

$$\text{QBER} = \frac{P_{error}}{P_{sift}}, \quad (18)$$

where  $P_{error}$  and  $P_{sift}$  are the probabilities of error and sift, respectively. Specifically,  $P_{sift}$  is the probability that Bob uses the same bases as Alice's to measure the received photons, from which he decodes a string of bits called sifted key;  $P_{error}$  is the probability that there is a number of erroneous bits in the sifted key, caused by technical imperfections and/or

TABLE 4. Joint probabilities between Alice and Bob averaged over atmospheric turbulence-induced fading channels.

Alice's bit $a$	Bob's bit $b$	Joint probability averaged over the fading channel $P_{A,B}(a, b)$
0	0	$\frac{1}{2} \int_0^\infty Q\left(\frac{i_0-d_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
0	X	$\frac{1}{2} - \frac{1}{2} \int_0^\infty Q\left(\frac{i_0-d_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t - \frac{1}{2} \int_0^\infty Q\left(\frac{d_1-i_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
0	1	$\frac{1}{2} \int_0^\infty Q\left(\frac{d_1-i_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
1	0	$\frac{1}{2} \int_0^\infty Q\left(\frac{i_1-d_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
1	X	$\frac{1}{2} - \frac{1}{2} \int_0^\infty Q\left(\frac{d_1-i_1}{\sigma_N}\right) f_{h^t}(h^t) dh^t - \frac{1}{2} \int_0^\infty Q\left(\frac{i_1-d_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
1	1	$\frac{1}{2} \int_0^\infty Q\left(\frac{d_1-i_1}{\sigma_N}\right) f_{h^t}(h^t) dh^t$

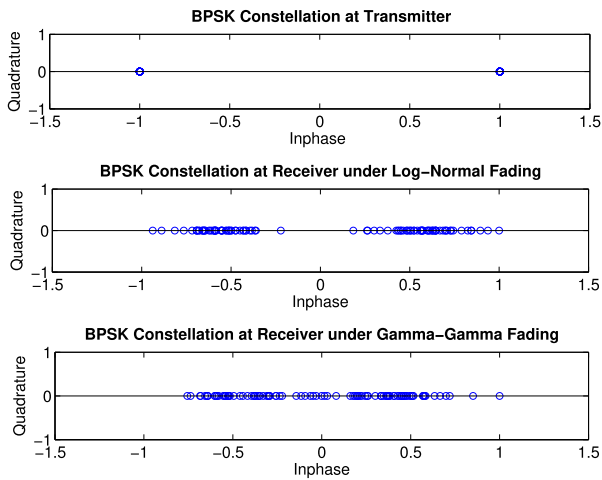


FIGURE 6. Impact of atmospheric turbulence-induced fading on electrical BPSK constellation at the receiver.

Eve's intervention. Thus, QBER reflects the percentage of bit errors in the sifted key. These errors are on the order of a few percent, hence QBER strongly contrasts with the  $10^{-9}$  commonly known in optical communications [4]. As a result, the name QBER is used to clearly distinguish it from the bit error rate (BER) used in standard optical communications.

Similar to BB84 protocol, we use the metric QBER in (18) with the same purpose of reflecting the bit error rate in the sifted key. Particularly in our proposed system,  $P_{sift}$  corresponds to the probability that Bob can detect bits "0" and "1" using the dual-threshold detection, and  $P_{error}$  is the probability that Bob mistakenly decides "0" when "1" was transmitted and vice versa. These probabilities can be calculated through the joint probabilities between Alice and Bob, respectively given as

$$P_{sift} = P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1), \tag{19}$$

$$P_{error} = P_{A,B}(0,1) + P_{A,B}(1,0). \tag{20}$$

From (19) and (20), QBER can be derived as in (18). Let us denote  $P_{A,B}(a, b)$  ( $a, b \in \{0, 1\}$ ) as the joint probability that Alice's bit "a" coincides with Bob's bit "b", defined as

$$P_{A,B}(a, b) = P_A(a)P_{B|A}(b|a), \tag{21}$$

where  $P_A(a) = \frac{1}{2}$  is the probability that Alice sends bit "a" ( $a \in \{0, 1\}$ ), since "1" and "0" are equally likely to be transmitted from Alice.  $P_{B|A}(b|a)$  is the conditional probability that Bob creates bit "b" when Alice sends bit "a". Using two detection thresholds  $d_0$  and  $d_1$  and decision rule in (3), the joint probabilities between Alice and Bob, averaged over the fading channel, are listed in Table 4.

From Table 4, the joint probabilities when Alice transmits bits "0" and "1", averaged over the fading channel, can be respectively expressed as

$$P_{A,B}(a, 0) = \frac{1}{2} \int_0^\infty Q\left(\frac{i_a - d_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t, \tag{22}$$

$$P_{A,B}(a, 1) = \frac{1}{2} \int_0^\infty Q\left(\frac{d_1 - i_a}{\sigma_N}\right) f_{h^t}(h^t) dh^t, \tag{23}$$

where  $a \in \{0, 1\}$ ,  $i_0 = -\frac{1}{4}\Re\{\bar{g}P\delta h^t\}$  and  $i_1 = -i_0$ .  $Q(\cdot) \triangleq \frac{1}{\sqrt{2\pi}} \int_0^\infty \exp(-t^2/2) dt$  is the Gaussian Q-function.

To determine  $d_0$  and  $d_1$  in (22) and (23), we propose the D-T selections as follows

$$d_0 = \mathbb{E}[i_0] - \zeta \sqrt{\sigma_N^2} \text{ and } d_1 = \mathbb{E}[i_1] + \zeta \sqrt{\sigma_N^2}, \tag{24}$$

where  $\zeta$  is the dual-threshold scale coefficient to adjust  $d_0$  and  $d_1$ .  $\sigma_N^2$  is the noise variance defined in (7).  $\mathbb{E}[i_0]$  and  $\mathbb{E}[i_1]$  are the mean values of  $i_0$  and  $i_1$ , respectively. Thus,  $\mathbb{E}[i_0] = -\frac{1}{4}\Re\{\bar{g}P\delta h^t\}$  and  $\mathbb{E}[i_1] = \frac{1}{4}\Re\{\bar{g}P\delta h^t\}$  as  $\mathbb{E}[h] = \mathbb{E}[h^t h^t] = h^t$  with  $\mathbb{E}[h^t] = 1$  as the mean irradiance is normalized to unity [30]. It is deduced from (24) that the D-T selections depend on two parameters, which are the modulation depth  $\delta$  and D-T scale coefficient  $\zeta$ . By adjusting  $\delta$  and  $\zeta$ , we are able to control  $P_{sift}$ ,  $P_{error}$ , and QBER of the QKD system.

### 1) QBER OVER LOG-NORMAL CHANNELS

The joint probabilities in (22) and (23), over LN channels, can be respectively derived in closed-form expressions as

$$P_{A,B}(a, 0) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k, i \neq 0}^k \omega_i Q\left(\frac{\mp \frac{1}{4}\Re\{\bar{g}P\delta h^t\} e^{2\sqrt{2}\sigma_{x,x}+2\mu_x} - d_0}{\sigma_{N-i}}\right), \tag{25}$$

$$P_{A,B}(a, 1) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k, i \neq 0}^k \omega_i Q\left(\frac{d_1 \pm \frac{1}{4}\Re\{\bar{g}P\delta h^t\} e^{2\sqrt{2}\sigma_{x,x}+2\mu_x}}{\sigma_{N-i}}\right), \tag{26}$$



where

$$\sigma_{N-i} = \sqrt{2qF_A \bar{g}^2 \Re \left[ \frac{1}{4} P \delta h^l e^{2\sqrt{2}\sigma_x x_i + 2\mu_x} + P_b \right] \Delta f + \frac{4k_b TF_n}{R_L} \Delta f}, \quad (27)$$

$$d_0 = \mathbb{E}[i_0] - \zeta \sqrt{\sigma_{N-i}^2}, \quad (28)$$

$$d_1 = \mathbb{E}[i_1] + \zeta \sqrt{\sigma_{N-i}^2}. \quad (29)$$

Here,  $k$  is the order of approximation,  $\{\omega_i\}$  and  $\{x_i\}$  ( $i = -k, -k + 1, \dots, -1, 1, 2, \dots, k$ ) are weight factors and zeros of the Hermite polynomial, respectively [37]. The proof of (25) and (26) can be found in Appendix VII. By plugging (25) and (26) into (19) and (20), the closed-form solution for the QBER in (18) can be obtained. It is noted that  $k = 10$  gives accurate results for this approximation [34].

## 2) QBER OVER GAMMA-GAMMA CHANNELS

The joint probabilities in (22) and (23), over GG channels, can be respectively derived in closed-form expressions as

$$P_{A,B}(a, 0) \approx \frac{1}{2} \sum_{i=1}^N \sum_{l=1}^M a_i \xi_i^{-b_i} \nu_l \tau_l^{b_l-1} Q \left( \frac{\mp \frac{1}{4\xi_i} \Re \bar{g} P \delta h^l \tau_l - d_0}{\sigma_{N-i,l}} \right), \quad (30)$$

$$P_{A,B}(a, 1) \approx \frac{1}{2} \sum_{i=1}^N \sum_{l=1}^M a_i \xi_i^{-b_i} \nu_l \tau_l^{b_l-1} Q \left( \frac{d_1 \pm \frac{1}{4\xi_i} \Re \bar{g} P \delta h^l \tau_l}{\sigma_{N-i,l}} \right), \quad (31)$$

where

$$\sigma_{N-i,l} = \sqrt{2qF_A \bar{g}^2 \Re \left[ \frac{1}{4\xi_i} P \delta h^l \tau_l + P_b \right] \Delta f + \frac{4k_b TF_n}{R_L} \Delta f}, \quad (32)$$

$$d_0 = \mathbb{E}[i_0] - \zeta \sqrt{\sigma_{N-i,l}^2}, \quad (33)$$

$$d_1 = \mathbb{E}[i_1] + \zeta \sqrt{\sigma_{N-i,l}^2}. \quad (34)$$

Here,  $a_i$ ,  $b_i$ , and  $\xi_i$  are parameters of a mixture-Gamma (MG) distribution chosen to approximate the GG distribution, with  $N$  is the number of mixture components [38].  $\nu_l$  and  $\tau_l$  are weight factors and abscissas of the Laguerre polynomials, with  $M$  is the number of iteration to numerically approximate Laguerre integration [37, Table 25.9]. The detailed proof of (30) and (31) is provided in Appendix VII. By plugging (30) and (31) into (19) and (20), the closed-form solution for the QBER in (18) can be derived. It is noted that  $N = M = 10$  gives accurate results for this approximation [38].

## B. ERGODIC SECRET-KEY RATE & FINAL KEY-CREATION RATE

To validate the security of the proposed system, we analyze the *ergodic secret-key rate*, denoted as  $S$ , over the atmospheric fading channels. If  $S$  is positive, it is theoretically possible that the amount of information gained by Eve can be decreased through the process of privacy

amplification [39]. When  $S$  is negative, Bob must be able to detect Eve’s intervention with Eve is limited solely by laws of physics [40]. After sharing key bit information and performing error correction, Alice and Bob estimate the amount of information leaked to Eve, and exclude it by means of privacy amplification to obtain the final key. From the information theoretical viewpoint, we denote  $H(B)$  and  $H(E)$  as the information entropies of Bob and Eve, respectively. The conditional entropies of Bob-Alice and Eve-Alice are denoted as  $H(B|A)$  and  $H(E|A)$ , respectively. The mutual information  $I(A; B)$  and  $I(A; E)$  are defined as the estimation of the amount of information shared between Alice and Bob, and that shared between Alice and Eve, respectively expressed as

$$I(A; B) = H(B) - H(B|A), \quad (35)$$

$$I(A; E) = H(E) - H(E|A), \quad (36)$$

in which the key is said to be secure if  $I(A, B)$  is higher than  $I(A, E)$  [41]. As a result, we define the ergodic secret-key rate as the maximum transmission rate at which the eavesdropper is unable to decode any information, given as [41]

$$S = I(A; B) - I(A; E). \quad (37)$$

It is noted that the expression of  $S$  in (37) 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 (in order for him to error-correct his data) and eavesdropped by Eve. Thus, the leaked amount of information from Alice to Eve, i.e.  $I(A; E)$ , should be excluded to obtain a secure key. Other types of error correction protocols, e.g. bidirectional or reverse reconciliation [16], [42], can also be employed, however, they are not considered in this paper for the sake of conciseness. In practice, the error correction efficiency should be taken into account in investigating  $I(A; B)$ , nevertheless, we assume perfect error correction efficiency, i.e. 100%, as an upper bound evaluation of the system performance [16].

From (37), the useful bit rate, namely *final key-creation rate*, after error correction and privacy amplification to exclude the amount of information leaked to Eve from that shared between Alice and Bob, denoted as  $R_f$ , can be derived as

$$R_f = R_s(I(A; B) - I(A; E)), \quad (38)$$

where  $R_s$  is the sifted-key rate or raw-key rate, i.e. the length of the raw key that can be produced per unit time that contains the sifting factor, given as  $R_s = P_{sift} R_b$  with  $R_b$  is the system bit rate [43].

To obtain  $S$  and  $R_f$ , the mutual information  $I(A; B)$  and  $I(A; E)$  over both LN and GG atmospheric turbulence channels are derived as follows.

### 1) MUTUAL INFORMATION BETWEEN ALICE AND BOB, $I(A; B)$

Alice and Bob share information over the channel as depicted in Fig. 7, where  $x_i$  ( $i \in \{1, 2\}$ ) represents bit “0” or “1”,

TABLE 5. Joint probabilities between Alice and Eve averaged over atmospheric turbulence-induced fading channels.

Alice's bit $a$	Eve's bit $c$	Joint probability averaged over the fading channel $P_{A,E}(a, c)$
0	0	$\frac{1}{2} - \frac{1}{2} \int_0^\infty Q\left(\frac{d_E - i_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
0	1	$\frac{1}{2} \int_0^\infty Q\left(\frac{d_E - i_0}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
1	0	$\frac{1}{2} \int_0^\infty Q\left(\frac{i_1 - d_E}{\sigma_N}\right) f_{h^t}(h^t) dh^t$
1	1	$\frac{1}{2} - \frac{1}{2} \int_0^\infty Q\left(\frac{i_1 - d_E}{\sigma_N}\right) f_{h^t}(h^t) dh^t$

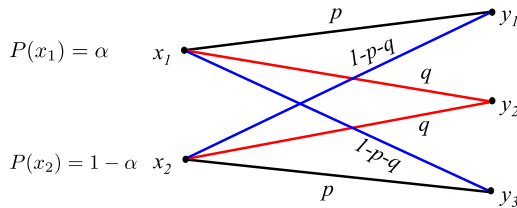


FIGURE 7. Diagram of the binary erasure channel (BEC) with errors between Alice and Bob.

and  $y_j$  ( $j \in \{1, 2, 3\}$ ) denotes bit “0”,  $X$ , or “1”, respectively.  $p$  and  $q$  are the channel transition probabilities.  $\alpha$  and  $(1 - \alpha)$  are the probabilities of transmitting bits “0” and “1”. We refer to this type of channel as the binary erasure channel (BEC) with errors [44]. Hence, the mutual information  $I(A; B)$  can be derived as

$$\begin{aligned}
 I(A; B) &= p \log_2(p) + (1 - p - q) \log_2(1 - p - q) \\
 &\quad - (\alpha p + (1 - \alpha)(1 - p - q)) \log_2(\alpha p + (1 - \alpha)(1 - p - q)) \\
 &\quad - (\alpha(1 - p - q) + (1 - \alpha)p) \log_2(\alpha(1 - p - q) + (1 - \alpha)p).
 \end{aligned} \tag{39}$$

The detailed proof of (39) can be found in Appendix VII. In our system, we have  $\alpha = 0.5$  since the probabilities of transmitting bits “0” and “1” are equally likely to occur.  $p$ ,  $q$ , and  $(1 - p - q)$  are respectively the conditional probabilities that Bob creates bit  $y_j$  when Alice sends bit  $x_i$ , which can be deduced from the joint probabilities derived in Section V-A.

2) MUTUAL INFORMATION BETWEEN ALICE AND EVE,  $I(A; E)$

In our system, Eve obtains a bit string through eavesdropping using the optimal detection threshold  $d_E = 0$ , whose bit values are partially identical to Alice’s. Thus, we can consider that Alice and Eve share some information via binary symmetric channel (BSC). As a result, the mutual information  $I(A; E)$  can be given as [4], [41]

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

where  $p_e$  is the transition probability that Eve correctly detects the transmitted bits. Let  $e$  be Eve’s error probability, which is defined as

$$e = P_{A,E}(0, 1) + P_{A,E}(1, 0), \tag{41}$$

with  $P_{A,E}(0, 1)$  and  $P_{A,E}(1, 0)$  are the joint probabilities that Eve falsely detects Alice’s transmitted bits using threshold

detection  $d_E = 0$ , respectively expressed as

$$P_{A,E}(0, 1) = \frac{1}{2} \int_0^\infty Q\left(\frac{d_E + \frac{1}{4} \Re \bar{g} P \delta h^l h^t}{\sigma_N}\right) f_{h^t}(h^t) dh^t, \tag{42}$$

$$P_{A,E}(1, 0) = \frac{1}{2} \int_0^\infty Q\left(\frac{\frac{1}{4} \Re \bar{g} P \delta h^l h^t - d_E}{\sigma_N}\right) f_{h^t}(h^t) dh^t. \tag{43}$$

Similar to Section V-A, the joint probabilities between Alice and Eve, averaged over the fading channel, are summarized in Table 5. Following the same approach as presented in Section V-A, the joint probabilities  $P_{A,E}(0, 1)$ ,  $P_{A,E}(1, 0)$ , and Eve’s probability of error  $e$  can also be derived in closed-form expressions as in (44) and (45) (over LN channels); (46) and (47) (over GG channels), respectively.

$$P_{A,E}(0, 1) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k, i \neq 0}^k \omega_i Q\left(\frac{d_E + \frac{1}{4} \Re \bar{g} P \delta e^{2\sqrt{2}\sigma_x x_i + 2\mu_x}}{\sigma_{N-i}}\right), \tag{44}$$

$$P_{A,E}(1, 0) \approx \frac{1}{2\sqrt{\pi}} \sum_{i=-k, i \neq 0}^k \omega_i Q\left(\frac{\frac{1}{4} \Re \bar{g} P \delta e^{2\sqrt{2}\sigma_x x_i + 2\mu_x} - d_E}{\sigma_{N-i}}\right). \tag{45}$$

$$P_{A,E}(0, 1) \approx \frac{1}{2} \sum_{i=1}^N \sum_{l=1}^M a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} Q\left(\frac{d_E + \frac{1}{4\xi_i} \Re \bar{g} P \delta h^l \tau_l}{\sigma_{N-i,l}}\right), \tag{46}$$

$$P_{A,E}(1, 0) \approx \frac{1}{2} \sum_{i=1}^N \sum_{l=1}^M a_i \xi_i^{-b_i} \nu_l \tau_l^{b_i-1} Q\left(\frac{\frac{1}{4\xi_i} \Re \bar{g} P \delta h^l \tau_l - d_E}{\sigma_{N-i,l}}\right). \tag{47}$$

All notations in (44)-(47) are already defined in Section V-A. Plugging (44)-(47) into (41), closed-form expressions for Eve’s probability of error can be derived over both LN and GG channels.

VI. NUMERICAL RESULTS

A. SECURITY ANALYSIS

The appeal of QKD protocols mainly comes from the fact that it can provide *unconditional security*, which means that the security can be proved without imposing any restriction on the computational resources or the manipulation techniques that are available to the eavesdropper acting on the signal [43]. This should not be considered as a synonym for *absolute security*, which does not exist in any key distribution scheme with security dependent on physical characteristics

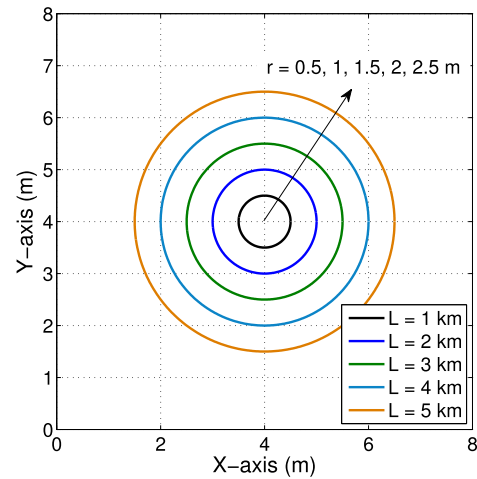
due to system imperfections and eavesdropper’s attacks. The definition of security is indeed a quantitative issue, and there is yet no true valid quantification of QKD security under all possible attacks [2]. As our proposed QKD protocol is based on standard FSO systems with classical signals, simple physical-layer eavesdropping is the most powerful strategy. Several important attacks in quantum cryptography, such as collective attacks and coherent attacks, cannot be beyond the eavesdropping strategy for classical signals [45].

In standard FSO systems, the physical-layer security was analyzed, both theoretically and experimentally, under several popular Eve’s attacking strategies [46]- [48]. Particularly, based on the same concept of D-T/DD receiver as in [49], the security analysis was comprehensively performed for *two-way* free-space QKD systems, under unauthorized receiver attack (URA), beam-splitting attack (BSA), and intercept-resend attack (IRA) [48]. In [49], it is confirmed that the proposed *one-way* free-space QKD system using SIM/BPSK and D-T/DD was secured against IRA with high probability of detecting Eve (more than 99%) over short key length, and some initial results under URA were also discussed. As the optical beamwidth in FSO systems is very narrow and invisible, it is extremely difficult for Eve to intercept in the middle of the transmission between Alice and Bob to perform IRA. In addition, surveillance cameras can be installed at Alice to prevent Eve from performing BSA by locating its receiver near Alice as theoretically assumed in [47] and [48]. Therefore, the most practical attacking strategy for Eve is the URA, by locating its unauthorized receiver within the beam footprint near and/or behind Bob’s receiver, since the optical beam experiences geometric spreading as analyzed in Section IV-A.

In this paper, we aim to prove that our proposed QKD protocol, with proper transmitter and receiver settings, is able to achieve positive ergodic secret-key rate ( $S > 0$ ) in the presence of Eve, thus a secure key can be shared between Alice and Bob. Eve is assumed to be equipped with an APD at her receiver and perform URA near and/or behind Bob’s receiver. Transmitting/receiving devices at Alice and Bob are fully trusted. Illustratively, Fig. 8 shows the beam footprints with corresponding radiuses  $r$  (m) affected by geometric spreading after transmitting over a distance of  $L$  (km), with angle of divergence  $\theta = 10^{-3}$  rad. This figure serves as a reference for the possible positions that Eve can locate her unauthorized receiver within the beam footprint near and/or behind Bob’s receiver.

**B. SYSTEM DESIGN CRITERIA**

In this section, we investigate the criteria for Alice’s transmitter and Bob’s receiver settings to maintain the security of the proposed system under URA. Secrecy performance metrics are analytically analyzed and in a good agreement with M-C simulations. The system parameters and constants used in the analysis are shown in Table 6. For a transmission distance of 1 km, the values of  $C_n^2 = 10^{-15}$ ,  $C_n^2 = 5 \times 10^{-14}$ , and  $C_n^2 = 10^{-13}$  correspond to the weak, moderate, and strong



**FIGURE 8.** Beam footprint with radius  $r$  (m) at distance  $L$  (km) away from Alice’s transmitter, with angle of divergence  $\theta = 10^{-3}$  rad.

**TABLE 6.** System Parameters and Constants [16], [32], [34].

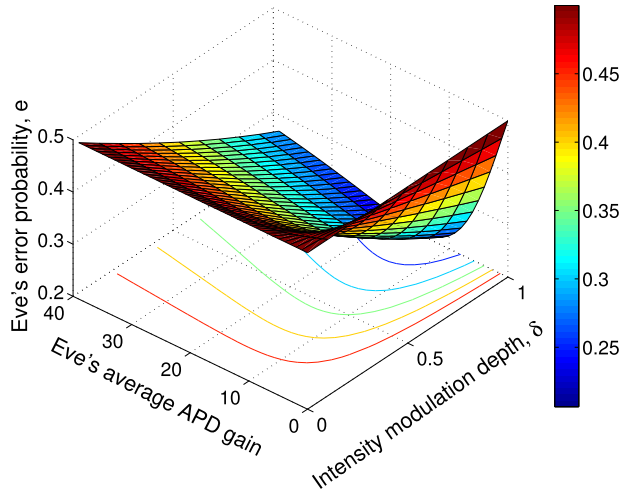
Name	Symbol	Value
Boltzmann’s constant	$k_B$	$1.38 \times 10^{-23}$ W/K/Hz
Planck’s constant	$\hbar$	$6.626 \times 10^{-34}$
Electron charge	$q$	$1.6 \times 10^{-19}$ C
Load resistor	$R_L$	1000 $\Omega$
Receiver temperature	$T$	300 K
Quantum efficiency	$\eta$	0.62
Ionization factor	$k_A$	0.7 (InGaAs APD)
Receiver’s aperture diameter	$D$	0.02 m
Angle of divergence	$\theta$	$10^{-3}$ rad
Amplifier noise figure	$F_n$	2
Atmospheric attenuation coefficient	$\beta_i$	0.43 dB/km
Wavelength	$\lambda$	1550 nm
Average background power	$P_b$	-40 dBm
Bit rate	$R_b$	1 Gbps

turbulence conditions. LN and GG models are used to characterize weak and moderate-to-strong turbulence, respectively.  $L_{A,B}$  and  $L_{E,A}$  are the transmission distances between Alice-Bob and Eve-Alice, respectively.

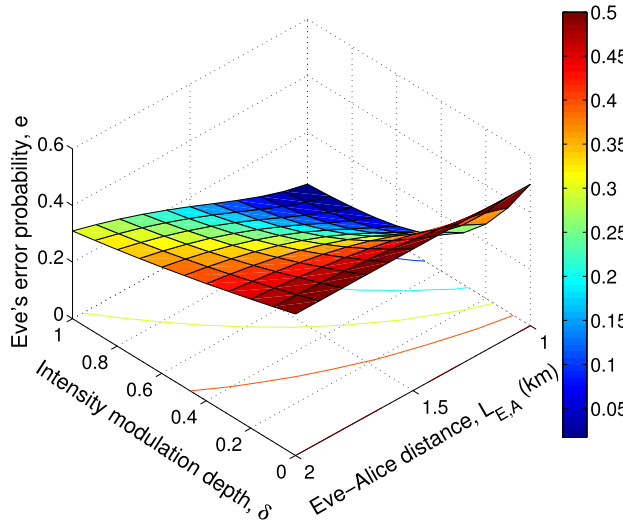
**1) ALICE’S TRANSMITTER DESIGN**

In URA, Eve tries to steal information by tapping the transmitted signal within the beam footprint near and/or behind Bob’s receiver. To defend against this attack, Alice chooses a small value of modulation depth  $\delta$  at the transmitter so that Eve will suffer from a high error rate with  $d_E = 0$ . Assuming that  $L_{A,B} = 1$  km and Eve is close to Bob’s receiver, e.g.  $L_{E,A} = 1$  km, Fig. 9 investigates Eve’s error rate  $e$ , under weak turbulence condition, to find out the proper selection of  $\delta$  to guarantee that  $e$  is sufficiently high, e.g.  $e > 0.1$ , while Eve tries to lower  $e$  by choosing its optimal average APD gain  $\bar{g}$ . It is seen that the chosen values for  $\delta$  should be  $\delta \leq 0.4$ , thus,  $e > 0.1$  is always guaranteed even when Eve selects its optimal  $\bar{g} = 15$ .

In Fig. 10, with  $\bar{g} = 15$  and  $L_{A,B} = 1$  km, we confirm the selection of  $\delta$  by letting Eve locate its receiver within 1 km behind Bob’s receiver. The turbulence parameter is set at



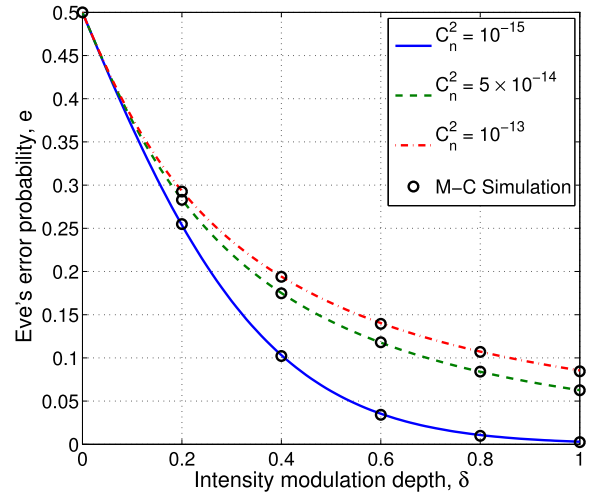
**FIGURE 9.** Eve's error probability ( $e$ ) versus intensity modulation depth ( $\delta$ ) and average APD gain ( $\bar{g}$ ).  $L_{E,A} = 1$  km,  $P = 0$  dBm,  $C_n^2 = 10^{-15}$  (LN model).



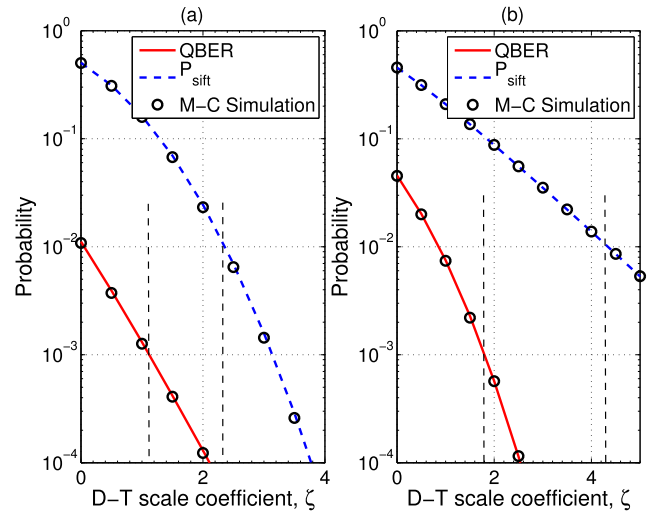
**FIGURE 10.** Eve's error probability ( $e$ ) versus intensity modulation depth ( $\delta$ ) and Eve's distance from Alice ( $L_{E,A}$ ).  $\bar{g} = 15$ ,  $P = 0$  dBm,  $C_n^2 = 10^{-14}$  (GG model).

$C_n^2 = 10^{-14}$  so that Eve will experience moderate-to-strong turbulence conditions as  $L_{E,A}$  increases. It is seen that when Eve moves further, the received signal at Eve's receiver suffers from stronger turbulence-induced fading, which results in higher  $e$ . Therefore, with  $\delta \leq 0.4$ , it is confirmed that  $e > 0.1$  while Eve performs URA near and/or behind Bob's receiver.

Furthermore, in Fig. 11, when  $L_{E,A} = 1$  km, we investigate the impact of different turbulence conditions on Eve's error probability along with the selection of modulation depth  $\delta$ . It is observed that by choosing  $\delta \leq 0.4$ , Eve's error probability is always higher than 0.1 under all turbulence conditions. It is noted that the modulation depth should not be too small as it considerably increases the bit errors at Bob, which might be unable to correct using error-correction codes. In this paper, for further performance analysis,  $\delta = 0.4$  is chosen.



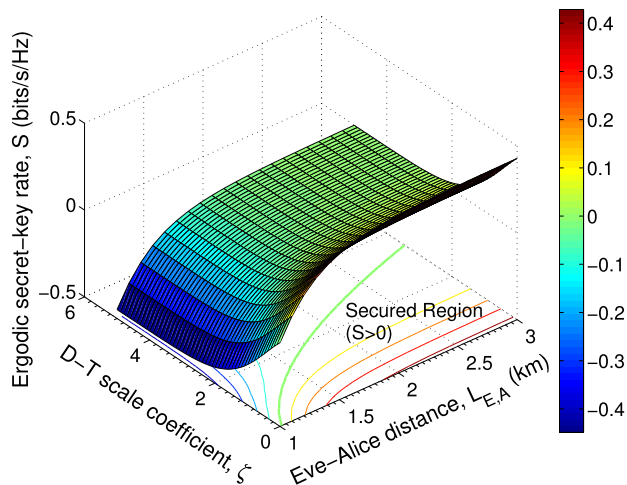
**FIGURE 11.** Eve's error probability ( $e$ ) versus intensity modulation depth ( $\delta$ ).  $\bar{g} = 15$ ,  $L_{E,A} = 1$  km,  $P = 0$  dBm,  $C_n^2 = 10^{-15}$  (LN model),  $C_n^2 = 5 \times 10^{-14}$  and  $C_n^2 = 10^{-13}$  (GG model).



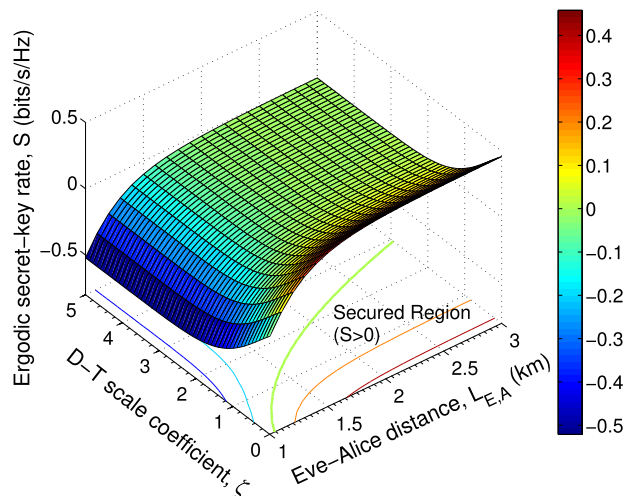
**FIGURE 12.** Bob's QBER and  $P_{sift}$  versus the D-T scale coefficient ( $\zeta$ ), under (a) weak ( $C_n^2 = 10^{-15}$ , modeled by LN), and (b) strong ( $C_n^2 = 10^{-13}$ , modeled by GG) turbulence conditions.  $\delta = 0.4$ ,  $L_{A,B} = 1$  km,  $\bar{g} = 15$ ,  $P = 0$  dBm.

## 2) BOB'S RECEIVER DESIGN

Regarding the criteria for receiver design, we can control QBER and  $P_{sift}$  by adjusting  $d_0$  and  $d_1$  through  $\zeta$ , as shown in Fig. 12. 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 (e.g., to achieve at least a sifted-key rate at Mbps with typical transmission rates at Gbps of standard FSO systems). At the same time, we also want to keep QBER  $\leq 10^{-3}$  so that errors can be feasibly corrected at Mbps sifted-key rate by error-correction codes. After performing error correction to correct errors in the sifted key and privacy amplification to remove Eve's information, Alice and Bob can then share a shorter key, i.e. final secure key. Doing so requires the choice of  $1.2 \leq \zeta \leq 2.35$  under weak turbulence



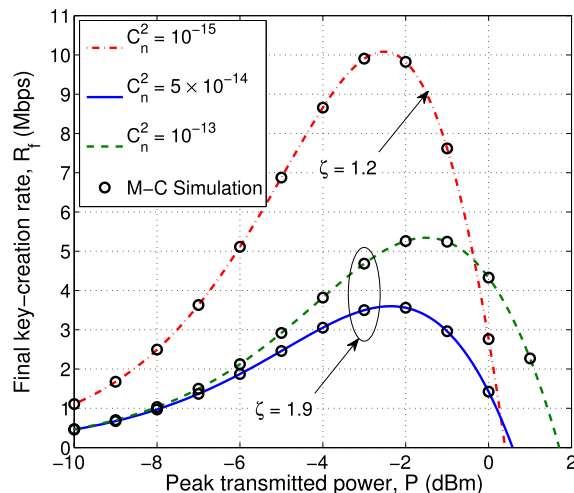
**FIGURE 13.** Ergodic secret-key rate ( $S$ ) versus D-T scale coefficient ( $\zeta$ ) and Eve-Alice distance ( $L_{E,A}$ ) in km.  $\delta = 0.4$ ,  $L_{A,B} = 1$  km,  $\bar{g} = 15$ ,  $P = 0$  dBm,  $C_n^2 = 10^{-14}$  (modeled by GG).



**FIGURE 14.** Ergodic secret-key rate ( $S$ ) versus D-T scale coefficient ( $\zeta$ ) and Eve-Alice distance ( $L_{E,A}$ ) in km.  $\delta = 0.4$ ,  $L_{A,B} = 1$  km,  $\bar{g} = 15$ ,  $P = 0$  dBm,  $C_n^2 = 10^{-15}$  (modeled by LN).

conditions (Fig. 12(a)), and  $1.9 \leq \zeta \leq 4.35$  under strong turbulence conditions (Fig. 12(b)).

In Figs. 13 and 14, we look at another aspect of the performance metric in receiver design by showing the ergodic secret-key rate  $S$  versus  $\zeta$  and Eve-Alice distance  $L_{E,A}$  under moderate-to-strong (Fig. 13) and weak (Fig. 14) turbulence conditions. It is known from Fig. 12(b) that the setting range for  $\zeta$  is  $1.9 \leq \zeta \leq 4.35$  under strong turbulence conditions. Thus, by applying this constraint in Fig. 13, it is seen that the QKD system is secured (i.e.,  $S > 0$ ) when Eve is located at least 1.7 km away from Alice when  $\zeta = 1.9$ . Similarly, under weak turbulence conditions (Fig. 14), the QKD system is secured when Eve is located at least 1.5 km away from Alice when  $\zeta = 1.2$ . As a result, to guarantee positive secret-key rates, it is necessary to select the smallest possible  $\zeta$  in the selection ranges corresponding to each turbulence conditions.



**FIGURE 15.** Final key-creation rate ( $R_f$ ) versus peak transmitted power ( $P$ ) in dBm.  $\delta = 0.4$ ,  $L_{A,B} = 1$  km,  $L_{E,A} = 1.5$  km,  $\bar{g} = 15$ ,  $C_n^2 = 10^{-15}$  (modeled by LN),  $C_n^2 = 5 \times 10^{-14}$  and  $C_n^2 = 10^{-13}$  (modeled by GG).

Finally, the final key-creation rate  $R_f$  is investigated versus the peak transmitted power  $P$  in Fig. 15 with system settings ( $\delta = 0.4$ ,  $\zeta = 1.2$ ) for weak turbulence and ( $\delta = 0.4$ ,  $\zeta = 1.9$ ) for moderate-to-strong turbulence. Eve’s location is fixed at  $L_{E,A} = 1.5$  km (i.e., 500 m behind Bob’s receiver). As expected, the setting of  $\zeta$  imposes an explicit effect on  $R_f$ , as it controls  $P_{sift}$ . Consequently, under weak turbulence condition ( $C_n^2 = 10^{-15}$ ) with  $\zeta = 1.2$ ,  $R_f = 10$  Mbps can be achieved at  $P = -2.5$  dBm. It is noteworthy that increasing  $P$  more than  $-2.5$  dBm leads to a reduction in  $R_f$ , since it increases the mutual information between Alice and Eve  $I(A; E)$ . On the other hand, under moderate and strong turbulence conditions ( $C_n^2 = 5 \times 10^{-14}$  and  $C_n^2 = 10^{-13}$ , respectively), with  $\zeta = 1.9$ ,  $R_f$  is reduced since Bob’s  $P_{sift}$  is smaller. To maximize  $R_f$ , choosing appropriate values of  $P$  becomes crucial, i.e.,  $P = -2$  dBm and  $P = -1.5$  dBm under moderate and strong turbulence conditions, respectively. It is also seen that  $R_f$  at optimal  $P$  under strong turbulence is higher than that under moderate turbulence, e.g., up to 5.2 Mbps compared to 3.6 Mbps, respectively. This is logical as  $I(A; E)$  is reduced when turbulence becomes stronger under the same setting of  $\zeta$ .

## VII. CONCLUSIONS AND FUTURE OUTLOOK

We proposed a novel QKD protocol using SIM/BPSK and D-T/DD receiver with an APD, which can be feasibly implemented on standard FSO systems. The design criteria under practical security constraints for FSO transmitter and receiver, in particular, the modulation depth and the setting for dual-threshold selection, were comprehensively discussed. For performance analysis, important secrecy metrics including QBER, ergodic secret-key rate, and final key-creation rate were analytically derived in novel closed-form expressions in terms of finite power series, considering the impact of atmospheric channel and receiver noises. Finally, analytical results were further verified by M-C simulations.

The results in this paper proved that QKD function can be achieved based on the pulse-based signal level of a laser beam as in standard optical systems. This helps to reduce the deployment cost of future secured networks since standard telecommunication devices can be used, instead of costly and sophisticated single-photon equipment. Consequently, performance analysis and improvement techniques inherited from the rich literature of standard FSO systems can be straightforwardly applied on the proposed free-space QKD system. In the future, it is promising to experimentally implement the proposed QKD protocol in practical FSO systems to verify its feasibility and security efficiency over both horizontal and space communication links. Further physical impairments such as pointing errors and weather effects should also be taken into account. Different improvement techniques (e.g. diversity and relaying techniques) and various error correction methods (e.g. bidirectional or reverse reconciliation) could be investigated to improve the secrecy performance and final key-creation rate of the future QKD systems.

**Appendix**

**A PROOF OF THE JOINT PROBABILITIES IN (25) AND (26)**

Substituting (11) and (12) into (22) with  $a = 0$ , we obtain the expression for  $P_{A,B}(0, 0)$  as

$$P_{A,B}(0, 0) = \frac{1}{2} \int_0^\infty Q\left(\frac{-\frac{1}{4}\Re\bar{g}P\delta h^l h^t - d_0}{\sigma_N}\right) \times \frac{1}{\sqrt{8\pi h^t \sigma_x}} \exp\left(-\frac{[\ln(h^t) + 2\sigma_x^2]^2}{8\sigma_x^2}\right) dh^t. \quad (48)$$

Making the change of variable  $y = \frac{(\ln(h^t) + 2\sigma_x^2)}{\sqrt{8\sigma_x^2}}$ , (48) can be rewritten as

$$P_{A,B}(0, 0) = \frac{1}{2\sqrt{\pi}} \int_{-\infty}^\infty Q\left(\frac{-\frac{1}{4}\Re\bar{g}P\delta h^l e^{2\sqrt{2}\sigma_x y + 2\mu_x} - d_0}{\sigma_{N(y)}}\right) \times \exp(-y^2) dy, \quad (49)$$

where

$$\sigma_{N(y)} = \sqrt{2qF_A \bar{g}^2 \Re\left[\frac{1}{4}P\delta h^l e^{2\sqrt{2}\sigma_x y + 2\mu_x} + P_b\right] \Delta f + 4 \frac{k_b T}{R_L} \Delta f}, \quad (50)$$

$$d_0 = \mathbb{E}[i_0] - \zeta \sqrt{\sigma_{N(y)}^2}. \quad (51)$$

Using the Gauss-Hermite quadrature formula [37]

$$\int_{-\infty}^\infty g(y) \exp(-y^2) dy \approx \sum_{i=-k, i \neq 0}^k \omega_i g(x_i), \quad (52)$$

where  $k$  is the order of approximation,  $\{\omega_i\}$  and  $\{x_i\}$  ( $i = -k, -k + 1, \dots, -1, 1, 2, \dots, k$ ) are the weight factors and the zeros of the Hermite polynomial, respectively, we obtain the closed-form solution for  $P_{A,B}(0, 0)$ . By following similar procedures, closed-form solutions for  $P_{A,B}(a, 0)$  and  $P_{A,B}(a, 1)$ ,  $a \in \{0, 1\}$ , can be derived as in (25) and (26), respectively.

**A PROOF OF THE JOINT PROBABILITIES IN (30) AND (31)**

Substituting (11) and (14) into (22) with  $a = 0$ , we obtain the expression for  $P_{A,B}(0, 0)$  as

$$P_{A,B}(0, 0) = \frac{1}{2} \int_0^\infty Q\left(\frac{-\frac{1}{4}\Re\bar{g}P\delta h^l h^t - d_0}{\sigma_N}\right) \times \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} (h^t)^{\alpha+\beta-1} K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h^t}\right) dh^t. \quad (53)$$

To facilitate our calculation, the PDF of GG distribution in (53) can be efficiently approximated by an MG distribution, as recently proposed in [38]. Thus, (53) can be rewritten as

$$P_{A,B}(0, 0) = \frac{1}{2} \sum_{i=1}^N a_i \int_0^\infty Q\left(\frac{-\frac{1}{4}\Re\bar{g}P\delta h^l h^t - d_0}{\sigma_N}\right) \times (h^t)^{b_i-1} \exp(-\xi_i h^t) dh^t, \quad (54)$$

where  $N$  is the number of mixture components;  $a_i$ ,  $b_i$ , and  $\xi_i$  are the parameters of an MG distribution approximating a GG distribution, readily given as [38]

$$a_i = \frac{\theta_i}{\sum_{j=1}^N \theta_j \Gamma(b_j) \xi_j^{-b_j}}, \quad b_i = \alpha, \quad (55)$$

$$\xi_i = \frac{\alpha\beta}{t_i}, \quad \theta_i = \frac{(\alpha\beta)^\alpha w_i t_i^{-\alpha+\beta-1}}{\Gamma(\alpha)\Gamma(\beta)}. \quad (56)$$

Making the change of variable  $y = \xi_i h^t$ , (54) can be expressed as

$$P_{A,B}(0, 0) = \frac{1}{2} \sum_{i=1}^N a_i \xi_i^{-b_i} \int_0^\infty Q\left(\frac{-\frac{1}{4\xi_i}\Re\bar{g}P\delta h^l y - d_0}{\sigma_{N(y)}}\right) \times y^{b_i-1} \exp(-y) dy, \quad (57)$$

where

$$\sigma_{N(y)} = \sqrt{2qF_A \bar{g}^2 \Re\left[\frac{1}{4\xi_i}P\delta h^l y + P_b\right] \Delta f + \frac{4k_b T F_n}{R_L} \Delta f}, \quad (58)$$

$$d_0 = \mathbb{E}[i_0] - \zeta \sqrt{\sigma_{N(y)}^2}. \quad (59)$$

Now, applying the Gaussian-Laguerre quadrature method [37]

$$\int_0^\infty g(y) \exp(-y) dy \approx \sum_{l=1}^M v_l g(\tau_l), \quad (60)$$

where  $v_l$  and  $\tau_l$  are the weight factors and abscissas of the Laguerre polynomials, with  $M$  is the number of iteration to numerically approximate Laguerre integration [37, Table 25.9];  $g(y) = Q\left(\frac{-\frac{1}{4\xi_i}\Re\bar{g}P\delta h^l y - d_0}{\sigma_{N(y)}}\right) y^{b_i-1}$ , we obtain the closed-form solution for  $P_{A,B}(0, 0)$ . By following similar procedures, closed-form solutions for  $P_{A,B}(a, 0)$  and  $P_{A,B}(a, 1)$ ,  $a \in \{0, 1\}$ , can be derived as in (30) and (31), respectively.

### A PROOF OF THE MUTUAL INFORMATION $I(A; B)$ IN (39)

First, the matrix of transmission probabilities of the considered BEC with errors can be expressed as

$$[P(B|A)] = \begin{bmatrix} p & q(1-p-q) \\ (1-p-q)q & p \end{bmatrix}. \quad (61)$$

The output probabilities can be calculated from the input probabilities and the channel matrix as follows

$$\begin{aligned} [P(B)] &= [P(A)][P(B|A)] \\ &= [\alpha \ 1-\alpha] \begin{bmatrix} p & q(1-p-q) \\ (1-p-q)q & p \end{bmatrix} \\ &= [\Psi_1 \ q \ \Psi_2], \end{aligned} \quad (62)$$

where

$$\Psi_1 = \alpha p + (1-\alpha)(1-p-q), \quad (63)$$

$$\Psi_2 = \alpha(1-p-q) + (1-\alpha)p. \quad (64)$$

On the other hand, the joint probability matrix  $[P(A, B)]$  can be calculated as

$$\begin{aligned} [P(A, B)] &= \begin{bmatrix} \alpha & 0 \\ 0 & 1-\alpha \end{bmatrix} [P(B|A)] \\ &= \begin{bmatrix} \alpha p & \alpha q & \alpha(1-p-q) \\ (1-\alpha)(1-p-q)q & (1-\alpha)p & \end{bmatrix}. \end{aligned} \quad (65)$$

From (62) and (65), the entropy of the channel output  $H(B)$  and the conditional entropy  $H(B|A)$  can be derived as

$$\begin{aligned} H(B) &= -\sum_{j=1}^3 P(y_j) \log_2 P(y_j) \\ &= -\Psi_1 \log_2 \Psi_1 - q \log_2 q - \Psi_2 \log_2 \Psi_2. \quad (66) \\ H(B|A) &= -\sum_{j=1}^3 \sum_{i=1}^2 P(x_i, y_j) \log_2 P(y_j|x_i) \\ &= H(B) + p \log_2 p + q \log_2 q + (1-p-q) \log_2 (1-p-q). \quad (67) \end{aligned}$$

Finally, the expression of  $I(A; B)$  in (39) can be derived by  $I(A; B) = H(B) - H(B|A)$ , with  $H(B)$  and  $H(B|A)$  are from (66) and (67), respectively.

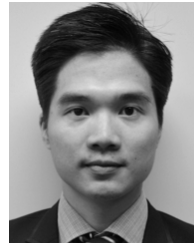
### ACKNOWLEDGMENT

Phuc V. Trinh would like to thank Dr. Wojciech Roga from Department of Physics, University of Strathclyde, UK for fruitful discussions. This paper was presented in part at the IEEE Global Communications Conference, and the Workshop on Quantum Communications and Information Technology, Washington, DC, USA, Dec. 2016 [49].”

### REFERENCES

- [1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *NPJ Quantum Inf.*, vol. 2, May 2016, Art. no. 16025.
- [2] H. P. Yuen, “Security of quantum key distribution,” *IEEE Access*, vol. 4, pp. 724–749, 2016.
- [3] 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.
- [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Modern Phys.*, vol. 74, p. 145, Mar. 2002.
- [5] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, Feb. 2002, Art. no. 057902.
- [6] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution,” *Nature Photon.*, vol. 7, pp. 378–381, Apr. 2013.
- [7] X. Wang, J. Liu, X. Li, and Y. Li, “Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution,” *IEEE J. Quantum Electron.*, vol. 51, no. 6, Jun. 2015, Art. no. 5200206.
- [8] B. Korzh *et al.*, “Provably secure and practical quantum key distribution over 307 km of optical fibre,” *Nature Photon.*, vol. 9, no. 3, pp. 163–168, 2014.
- [9] D. Huang, P. Huang, D. Lin, and G. Zeng, “Long-distance continuous-variable quantum key distribution by controlling excess noise,” *Sci. Rep.*, vol. 6, Jan. 2016, Art. no. 19201.
- [10] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, “Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects,” *Phys. Rev. A*, vol. 93, no. 2, 2016, Art. no. 022315.
- [11] T. Schmitt-Manderbach *et al.*, “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” *Phys. Rev. Lett.*, vol. 98, no. 1, 2011, Art. no. 010504.
- [12] B. Heim *et al.*, “Atmospheric continuous-variable quantum communication,” *New J. Phys.*, vol. 16, Nov. 2014, Art. no. 113018.
- [13] N. Hosseini-dehaj and R. Malaney, “Quantum key distribution over combined atmospheric fading channels,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7413–7419.
- [14] X. Sun, I. B. Djordjevic, and M. A. Neifeld, “Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels,” *IEEE Photon. J.*, vol. 8, no. 3, Jun. 2016, Art. no. 7904713.
- [15] T. Hirano, H. Yamanaka, M. Ashikaga, T. Koshini, and R. Namiki, “Quantum cryptography using pulsed homodyne detection,” *Phys. Rev. A*, vol. 68, no. 4, Oct. 2003, Art. no. 042331.
- [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] P. V. Trinh, N. T. Dang, and A. T. Pham, “All-optical relaying FSO systems using EDFA combined with optical hard-limiter over atmospheric turbulence channels,” *IEEE/OSA J. Lightw. Technol.*, vol. 33, no. 19, pp. 4132–4144, Oct. 1, 2015.
- [18] A. T. Pham, P. V. Trinh, V. V. Mai, N. T. Dang, and T. C. Thang, “Hybrid free-space optics/millimeter-wave architecture for 5G mobile backhaul networks,” in *Proc. 20th Opto-Electron. Commun. Conf.*, Jul. 2015, pp. 1–3.
- [19] P. V. Trinh, T. C. Thang, and A. T. Pham, “Mixed mmWave RF/FSO relaying systems over generalized fading channels with pointing errors,” *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 5500414.
- [20] K. Günthner *et al.*, “Quantum-limited measurements of optical signals from a geostationary satellite,” *Optica*, vol. 4, no. 6, pp. 611–616, Jun. 2017.
- [21] H. Takenaka, A. C.-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite,” *Nature Photon.*, vol. 11, pp. 502–508, Jul. 2017.
- [22] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.
- [23] A. V. Kuhlmann *et al.*, “Transform-limited single photons from a single quantum dot,” *Nature Commun.*, vol. 6, Sep. 2015, Art. no. 8204.
- [24] T. Lunghi *et al.*, “Self-testing quantum random number generator,” *Phys. Rev. Lett.*, vol. 114, no. 15, Apr. 2015, Art. no. 150501.
- [25] J. H. Shapiro, “Near-field turbulence effects on quantum-key-distribution,” *Phys. Rev. A*, vol. 67, no. 2, Feb. 2003, Art. no. 022309.
- [26] W. Zhang *et al.*, “NbN superconducting nanowire single photon detector with efficiency over 90% at 1550 nm wavelength operational at compact cryocooler temperature,” *Sci. China Phys. Mech. Astron.*, vol. 60, no. 12, Dec. 2017, Art. no. 120314.
- [27] H. V. Nguyen *et al.*, “Network coding aided cooperative quantum key distribution over free-space optical channels,” *IEEE Access*, vol. 5, pp. 12301–12317, 2017.

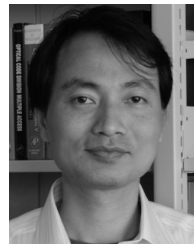
- [28] G. Yang, M. A. Khalighi, S. Bourennane, and Z. Ghassemlooy, "Fading correlation and analytical performance evaluation of the space-diversity free-space optical communications system," *J. Opt.*, vol. 16, Feb. 2014, Art. no. 035403.
- [29] N. D. Chatzidiamantis, D. S. Michalopoulos, E. E. Kriezis, G. K. Karagiannidis, and R. Schober, "Relay selection protocols for relay-assisted free-space optical systems," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 1, pp. 92–103, Jan. 2013.
- [30] W. O. Popoola and Z. Ghassemlooy, "BPSK subcarrier intensity modulated free-space optical communications in atmospheric turbulence," *IEEE/OSA J. Lightw. Technol.*, vol. 27, no. 8, pp. 967–973, Apr. 15, 2009.
- [31] 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.
- [32] D. A. Luong, T. C. Thang, and A. T. Pham, "Effect of avalanche photodiode and thermal noises on the performance of binary phase-shift keying-subcarrier-intensity modulation/free-space optical systems over turbulence channels," *IET Commun.*, vol. 7, no. 8, pp. 738–744, Mar. 2013.
- [33] S. Karp, *Optical Channels: Fibers, Clouds, Water and the Atmosphere*. New York, NY, USA: Plenum, 1988.
- [34] H. T. T. Pham, P. V. Trinh, N. T. Dang, and A. T. Pham, "A comprehensive performance analysis of PPM-based FSO systems with APD receiver in atmospheric turbulence," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2012, pp. 357–361.
- [35] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. Bellingham, WA, USA: SPIE, 2005.
- [36] P. V. Trinh, N. T. Dang, T. C. Thang, and A. T. Pham, "Performance of all-optical amplify-and-forward WDM/FSO relay systems over atmospheric dispersive turbulence channels," *IEICE Trans. Commun.*, vol. E99-B, no. 6, pp. 1255–1264, Jun. 2016.
- [37] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1972.
- [38] 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.
- [39] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
- [40] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," *Phys. Rev. Lett.*, vol. 93, Sep. 2004, Art. no. 120501.
- [41] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.
- [42] 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. 93, no. 12R, 2004, Art. no. 120501.
- [43] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.
- [44] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley, 2006.
- [45] T. Tomaru, "Secret key distribution protocol for practical optical channels using a pre-shared key and phase fluctuations," *Jpn. J. Appl. Phys.*, vol. 49, Jul. 2010, Art. no. 074401.
- [46] H. Endo et al., "Free-space optical channel estimation for physical layer security," *Opt. Exp.*, vol. 24, no. 8, Apr. 2016, Art. no. 259736.
- [47] 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.
- [48] 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. Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 929–934.
- [49] P. V. Trinh, T. V. Pham, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Performance of free-space QKD systems using sim/psk and dual-threshold/direct-detection," in *Proc. IEEE Global Commun. (GLOBECOM)*, Dec. 2016, pp. 1–6.



**PHUC V. TRINH** (S'13–M'17) received the B.E. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam, in 2013, and the M.Sc. and Ph.D. degrees in computer science and engineering from The University of Aizu, Aizuwakamatsu, Japan, in 2015 and 2017, respectively. He is currently a Researcher with the Space Communications Laboratory, National Institute of Information and Communications Technology, Tokyo, Japan. His current research interests include the area of optical wireless communications, modulation techniques, coding, channel modeling and simulation, and performance analysis. He is a member of IEICE. His study in Japan was fully funded by a Japanese government scholarship (MonbuKagaku-sho).



**THANH V. PHAM** (S'13) received the B.E. and M.E. degrees in computer network systems from The University of Aizu, Japan, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree. His research interests include the area of free space optics, relay networks, and visible light communications. He is a Student Member of IEICE. His study in Japan was funded by the Japanese Government Scholarship (MonbuKagakusho).



**NGOC T. DANG** received the B.E. degree in electronics and telecommunications from the Hanoi University of Technology, Hanoi, Vietnam in 1999, the M.E. degree in electronics and telecommunications from the Posts and Telecommunications Institute of Technology (PTIT), Hanoi, in 2005, and the Ph.D. degree in computer science and engineering from The University of Aizu, Aizuwakamatsu, Japan, in 2010. He was an Invited Researcher with FOTON

ENSSAT Lab., Université de Rennes 1, France, in 2011, and a Research Fellow with Computer Communications Lab., The University of Aizu, Japan, in 2012, 2013, 2015, and 2017. He is currently an Associate Professor/Head with the Department of Wireless Communications, PTIT. His current research interests include the area of communication theory with a particular emphasis on modeling, design, and performance evaluation of optical CDMA, RoF, and optical wireless communication systems.



**HUNG VIET NGUYEN** received the B.Eng. degree in electronics and telecommunications from the Hanoi University of Science and Technology, Hanoi, Vietnam, in 1999, the M.Eng. degree in telecommunications from the Asian Institute of Technology, Bangkok, Thailand, in 2002, and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2013. Since 1999, he has been a Lecturer with the Posts and Telecommunications Institute of Technology, Vietnam. He is involved in the OPTIMIX and CONCERTO European as well as EPSRC funded projects. He is currently a Research Fellow with the 5G Innovation Centre, University of Surrey, U.K. His research interests include cooperative communications, channel coding, network coding, and quantum communications.





**SOON XIN NG** (S'99–M'03–SM'08) received the B.Eng. degree (Hons.) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a Post-Doctoral Research Fellow focused on collaborative European research projects such as SCOUT, NEWCOM, and PHOENIX. Since 2006, he has been a Member of Academic Staff with the School

of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently an Associate Professor in telecommunications with the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes, and joint wireless-and-optical-fibre communications. He has authored over 200 papers and co-authored two John Wiley/IEEE Press books in this field. He is a Chartered Engineer and a fellow of the Higher Education Academy in the UK.



**ANH T. PHAM** (M'00–SM'11) received the B.E. and M.E. degrees in electronics engineering from the Hanoi University of Technology, Vietnam, in 1997 and 2000, respectively, and the Ph.D. degree in information and mathematical sciences from Saitama University, Japan, in 2005. From 1998 to 2002, he was with NTT Corporation, Vietnam. Since 2005, he has been a Faculty Member with The University of Aizu, where he is currently a Professor and the Head of the Com-

puter Communications Laboratory, Division of Computer Engineering. His research interests include the broad areas of communication theory and networking with a particular emphasis on modeling, design, and performance evaluation of wired/wireless communication systems and networks. He has authored/co-authored over 160 peer-reviewed papers on these topics. He is a member of IEICE and OSA.

• • •