IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 6 August 2022, accepted 14 September 2022, date of publication 20 September 2022, date of current version 27 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3208132

RESEARCH ARTICLE

Security Analysis of Gaussian and Discrete Modulations in FSO/CV-QKD Systems Employing LLO Under Phase and Amplitude Attacks

SARA AHMED[1], NANCY ALSHAER[2], (Member, IEEE), KHALED A. ALAGHBARI[3], (Member, IEEE), AND TAWFIK ISMAIL[1,4], (Senior Member, IEEE)

[1]Wireless Intelligent Networks Center (WINC), Nile University, Giza 12677, Egypt
[2]Department of Electronics and Electrical Communication, Faculty of Engineering, Tanta University, Gharbiya 31527, Egypt
[3]Institute of IR4.0, Universiti Kebangsaan Malaysia, Bangi, Selangor 43600, Malaysia
[4]National Institute of Laser Enhanced Sciences, Cairo University, Giza 12613, Egypt

Corresponding author: Tawfik Ismail (tismail@cu.edu.eg)

This work was supported by the Science, Technology, and Innovation Funding Authority (STIFA) of Egypt under Grant 38121.

ABSTRACT Continuous variable quantum key distribution (CV-QKD) using a local-local oscillator (LLO) is recently proposed to overcome security issues in conventional CV-QKD systems. However, Eve can manipulate the phase or amplitude of the phase reference pulse (PRP) transmitted over the insecure quantum channel, which has opened the door to new security issues. Maintaining optimal performance and preventing Eve's activities on the quantum channel depends on such a choice of modulation technique. In this paper, the performance of CV-QKD employing LLO over the free space optical (FSO) channel under weak turbulence conditions is investigated. Channel transmittance is introduced into the system model according to the log-negative Weibull distribution. We have adopted the trusted noise model and included the channel phase distortion in the excess noise calculations. We have also evaluated the secret key rate (SKR) using Gaussian modulation (GM) and discrete modulation (DM) protocols. We have reported the superiority of GM in achieving the highest SKR over long distances with the optimum choice of the modulation variance under Eve's attack on the PRP. Moreover, we analyzed phase and amplitude attacks on the PRP and showed that phase attacks are more severe and deteriorate the communication link more rapidly than amplitude attacks.

INDEX TERMS CV-QKD, local-local oscillator, transmitted local oscillator, FSO channel, air turbulence, Gaussian modulation, discrete modulation, amplitude attack, phase attack, trusted noise model.

I. INTRODUCTION

Quantum key distribution (QKD) is a promising alternative to classical cryptography algorithms for secure key sharing between two legitimate users, namely Alice and Bob, in the presence of a potential eavesdropper, namely Eve [1]. The two most common types of QKD systems are known as discrete variable QKD (DV-QKD) and continuous variable QKD (CV-QKD). The DV-QKD relies on counting photons with single photodetectors (SPDs) at Bob's receiver. This type has a limited transmission distance due to the low power of the single photon and a low data rate due to the dead time limitation of the SPDs [2]. For the CV-QKD counterpart, Bob employs coherent detection of In-phase/Quadrature (I/Q) modulated quantum signal (QS) using balanced detectors. Consequently, CV-QKD is more compatible with the existing optical communication systems while also having a higher data rate compared to DV-QKD [3], [4], [5]. However, coherent detection of CV-QKD requires a quite strong local oscillator (LO) pulse (as a phase reference) to overcome the shot-noise limitation at Bob's detectors, especially for lossy channels [6].

In conventional CV-QKD, Alice generates strong LO and weak QS, which are then co-transmitted to Bob through

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

an insecure quantum channel. This method is known as the transmitted local oscillator (TLO) scheme [7], [8], [9]. Unfortunately, the TLO scheme introduces several loopholes as Eve can develop numerous forms of attack on the LO, such as wavelength attack [10], [11], calibration attack [12], [13], and intensity fluctuation attack [14], [15]. Moreover, the necessary high intensity of the TLO imposes another limitation on the excess noise due to the considerable photon leakage from the LO to the QS [16], [17]. As a result, a new approach is required in order to overcome the earlier limitations. A revolutionary method called local-local oscillator (LLO) CV-QKD creates the LO locally at Bob's side rather than sending it via the quantum channel [18], [19]. However, Alice still sends a relatively strong phase reference pulse (PRP) with the QS, as it is impossible to lock the phase of two free-running lasers due to the finite linewidth of the laser sources. The intensity of the PRP is relatively larger than the QS but much weaker than the TLO. Although this approach eliminates several security issues, Eve can still manipulate the PRP and introduce new loopholes. Recently, authors in [16], [17], [20], [21], [22], and [23] have introduced two types of attack on the PRP over fiber quantum channel: phase attack and amplitude attack.

Free space optical (FSO) channels and fiber channels are of essential importance for a range of applications. These applications include radio astronomy, military services, disaster recovery, fiber failure, last-mile access, remote sensing, and backhaul for wireless cellular networks. Furthermore, the FSO channels offer more flexibility and cost-effectiveness than optical fiber channels for infrastructure deployment. Moreover, they provide a high data rate in the near-infrared (NIR) range. The increased demand for secure and high bandwidth communication links opens the door to employing QKD protocols over space links. However, atmospheric effects such as air turbulence deteriorate the performance of the FSO systems [24], [25]. In addition, the FSO channel suffers from fluctuating transmission properties. The propagation of the optical beam through the atmospheric channel is described using the transmittance probability distribution model that varies according to the turbulence strength [26], [27]. It is well known that the security proof for Gaussian modulation (GM) with coherent states is recognized for the collective attack, which is the most effective type of attack. However, recent research has shown that discrete modulation (DM) techniques that employ phase shift keying (PSK) outperform GM in terms of the communication distance and secret key rate (SKR). This is because the DM techniques have a high reconciliation efficiency even when the signal-to-noise ratio (SNR) is low [28], [29], [30], [31]. Unfortunately, the proof of security for DM coherent states is not yet established and is still being investigated. The 4-states and 8-states protocols are the most commonly used for DM [29], [30], [31], [32]. This is as a result of the performance measured in terms of distance, and SKR gets better when the number of states in the analysis is increased.

The main contributions of our work are (1) Studying the performance of the LLO-based CV-QKD protocol over the FSO channel under weak turbulence conditions. This is achieved by applying the log-negative Weibull distribution of the atmospheric transmission coefficient. (2) Developing an integrated, trusted noise model to represent the system's excess noise. The proposed model combines the effects of the noise sources of the transmitter, the channel, and the receiver. (3) Characterizing the wavefront aberrations by air turbulence in the FSO CV-QKD. This is accomplished by incorporating the intricate phase-screen calculations that establish the coherent efficiency. (4) Evaluating the CV-QKD SKR under PRP amplitude or phase attacks for both GM and DM using the channel transmittance model and the proposed integrated, trusted noise model. We show the system's robustness against amplitude attacks when reaching its maximum limit. (5) Ensuring the system's security and performance by adjusting Alice's modulation variance to an optimal value for different transmission distances, modulation techniques, and PRP attacks. (6) Quantifying and comparing the performance of GM and DM techniques in terms of SKR and reconciliation efficiency, showing the outstanding performance of the GM-based protocol compared to the DM.

The rest of the paper is organized as follows: In Section II, we introduce the LLO model, air channel model, and noise models. In Section III, the SKR is calculated under the existence of an eavesdropper. The results, including a comparative analysis of security in the GM and DM protocols under phase and amplitude attacks of the PRP, are presented in Section IV. Finally, we conclude our work in Section V.

II. CHANNEL AND NOISE MODELS

Fig. 1 shows the prepare and measure scheme employing LLO generated at Bob's side. In the preparation stage, Alice generates a train of coherent states with a repetition rate of $2/f$ and then splits it using an unbalanced beam splitter. Then, she performs amplitude and phase (I/Q) modulation on the weak pulses to produce QSs that carry the quantum information. In contrast, the relatively strong pulses are delayed by $1/f$ to represent the PRPs. Finally, she sends the QSs and PRPs over the air channel using a polarization-time multiplexing scheme. On the other side, Bob uses coherent detection during the measurement stage by employing homodyne detection for the QS, and heterodyne detection for phase estimation of the PRP as in [21]. He generates an LLO pulse train and then splits each pulse into two pulses using a balanced beam splitter. The first LLO pulse is used for heterodyne detection and quadrature measurement (X_R^B, P_R^B) of the PRP. The relative phase of the PRP θ_R, which is the phase difference between the reference and the LLO pulse $(\theta_R = \phi_{LO} - \phi_R)$, is estimated by [33] and [34]

$$\widehat{\theta}_R = \arctan\left(\frac{P_R^B}{X_R^B}\right) \tag{1}$$

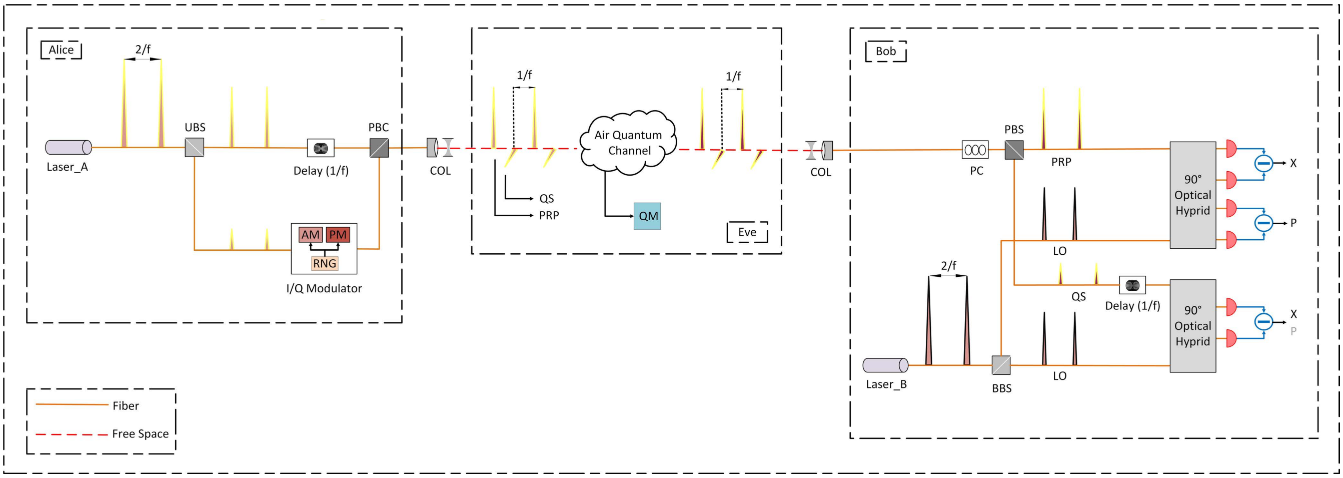


FIGURE 1. The system block diagram. PRP: Phase Reference Pulse, QS: Quantum Signal, LO: Local Oscillator, QM: Quantum Memory, UBS: Unbalanced Beam Splitter, BBS: Balanced Beam Splitter, PBC: Polarizing Beam Combiner, PBS: Polarizing Beam Splitter, PC: Polarization Controller, RNG: Random Number Generator, COL: Collimator.

Concurrently, the quadrature of the QS values (X_s^B, P_s^B) are measured by using the second LLO pulse as follows

$$X_s^B = \sqrt{\frac{T\eta}{\delta}}(\ X_s^A \cos\theta_s + P_s^A \sin\theta_s) + X_N \tag{2a}$$

$$P_s^B = \sqrt{\frac{T\eta}{\delta}}(-X_s^A \sin\theta_s + P_s^A \cos\theta_s) + P_N \tag{2b}$$

where X_N and P_N combine the excess noise sources and can be modeled as random Gaussian noises, δ depends on the type of detection of the QS; for homodyne detection, $\delta = 1$ and $\delta = 2$ for heterodyne detection. θ_s is the signal relative phase, which is the phase difference between the QS and the LLO pulse $(\theta_s = \phi_{\text{LO}} - \phi_s)$. Ideally, $\theta_s = 0$, but practically the free-running laser sources of Alice and Bob suffer from phase drift. Thus the measured quadratures (X_s^B, P_s^B) are phase rotated by $\theta_s \neq 0$. In order to restore the original quadratures, θ_s is estimated by the relative phase of the PRP $\widehat{\theta}_R$. In the reconciliation phase, either Alice or Bob rotates their quadratures by $-\widehat{\theta}_R$ according to the reconciliation scheme; reverse or direct [33]. The rotation matrix is given by

$$R_M = \begin{pmatrix} \cos\widehat{\theta}_R & -\sin\widehat{\theta}_R \\ \sin\widehat{\theta}_R & \cos\widehat{\theta}_R \end{pmatrix} \tag{3}$$

The process of rotating the quadratures is called quadrature remapping or phase correction/compensation scheme. This scheme is an alternative to employing complex phase-locking loops on Bob's LO [34], [35]. However, the rotation process is not perfect, and sources of excess noise come into the picture [36] as illustrated later.

A. CHANNEL MODEL

Channel transmission coefficient (T) is one of the key parameters of the insecure quantum channel. The main difference between the classical and quantum FSO channel models is the input-output relation of the transmission. For the FSO quantum channel, the input-output relation is defined according to the Glauber-Sudarshan P-function, where $(T \leq 1)$ to preserve the canonical commutation relations for the quantized optical field operators [37]. In terms of the Glauber-Sudarshan P-function, which is a quasi-probability as it may attain negativities, the relation between the input $P_{\text{in}}(\alpha)$ and output $P_{\text{out}}(\alpha)$ states can be written as [27]

$$P_{\text{out}}(\alpha) = \int_0^1 dT\ \text{P}(T) P_{\text{in}}(\frac{\alpha}{\sqrt{T}}), \tag{4}$$

where $\text{P}(T)$ is the probability distribution of the transmission coefficient (PDTC). Describing the transmission of quantum light across a turbulent atmosphere simply comes down to identifying this probability distribution. When the leading effect of the fluctuating losses in atmosphere is the beam wandering as the case for weak turbulence, the PDTC $\text{P}(T)$ is given by the log-negative generalized Rice distribution [26, eq. (9)]. The effect of the beam wandering is caused by the random fluctuation of beam-center position around a point at distance d from the center of the receiver's aperture [27]. In the particular case when the beam fluctuates around the aperture center, (i.e. $d = 0$), the generalized Rice distribution is reduced to the Weibull distribution and the PDTC is given by [26] and [38]

$$\begin{cases} \text{P}(T) \ = \dfrac{2}{\Gamma T}\left(\dfrac{R}{\sigma}\right)^2 \left[2\ln\dfrac{T_o}{T}\right]^{\frac{2}{\Gamma}-1} \times & \\ \exp\left[-\left(\dfrac{R}{\sigma\sqrt{2}}\right)^2 \left(2\ln\dfrac{T_o}{T}\right)^{\frac{2}{\Gamma}}\right], & \text{if } T \in [0, T_o] \\ 0, & \text{else} \end{cases} \tag{5}$$

The coordinates of the beam-center position follow a two dimensional Gaussian distribution with variance of σ^2 given by [39]

$$\sigma^2 = 1.919 \times C_n{}^2 L^3 (2\text{w}_0)^{-1/3}, \tag{6}$$

where $C_n{}^2$ is the refractive index structure parameter of the air, L is the transmission distance and w_0 is the beam radius at Alice's aperture. The transmission efficiency (T^2) of a Gaussian beam is given by [26]

$$T^2 = T_o^2 \exp\left[\left(\frac{-r}{R}\right)^{\Gamma}\right], \tag{7}$$

where the beam deflection distance r follows a Rice distribution with the parameters d and σ. T_o is the maximal transmission coefficient for the given beam-spot radius, R, and Γ are the scale and shape parameters, respectively. These last three parameters are obtained from the incomplete Weber integral in the forms [26], [38], [39]

$$T_o^2 = 1 - \exp\left[-2\left(\frac{a}{\mathrm{w}}\right)^2\right], \tag{8}$$

$$R = a\left[\ln\left(\frac{2T_o^2}{1-\exp\left[-(\frac{2a}{\mathrm{w}})^2\right]I_o\left[(\frac{2a}{\mathrm{w}})^2\right]}\right)\right]^{-\frac{1}{\Gamma}}, \tag{9}$$

$$\Gamma = 8\left(\frac{a}{\mathrm{w}}\right)^2 \frac{\exp\left[-(\frac{2a}{\mathrm{w}})^2\right]I_1\left[(\frac{2a}{\mathrm{w}})^2\right]}{1-\exp\left[-(\frac{2a}{\mathrm{w}})^2\right]I_o\left[(\frac{2a}{\mathrm{w}})^2\right]} \times \left[\ln\left(\frac{2T_o^2}{1-\exp\left[-(\frac{2a}{\mathrm{w}})^2\right]I_o\left[(\frac{2a}{\mathrm{w}})^2\right]}\right)\right]^{-1}, \tag{10}$$

where a is Bob's aperture radius and $I_n[.]$ is the modified Bessel function of the first kind of n-th order, and w is the received beam radius expressed as [39]

$$\mathrm{w} = \sqrt{\mathrm{w}_0^2 + \left(\frac{\Lambda L}{\pi \mathrm{w}_0}\right)^2}, \tag{11}$$

with Λ is the optical wavelength.

B. NOISE MODEL

In addition to the channel transmittance, excess noise ξ_{tot} is the 2^{nd} key parameter for analyzing the performance of the CV-QKD. In this part, we present the various noise sources that impact the entire system, as well as the effect of Eve's attack.

1) MODULATION NOISE

The finite dynamics of the AM add some noise to the quadratures of the QS due to the finite extension ratio of the AM [40]. This excess noise is quantified by [40] and [33]

$$\xi_{\mathrm{AM}} = E_{\mathrm{s,max}}^2 10^{-d_{\mathrm{dB}}/10} \tag{12}$$

where d_{dB} is the dynamics of the AM and $E_{\mathrm{s,max}} \approx \sqrt{10V_A}$ is the maximum signal amplitude to be modulated, with V_A is Alice's modulation variance.

2) PHOTON LEAKAGE NOISE

Polarizaion-multiplexing scheme was first proposed for conventional CV-QKD using TLO to reduce the leakage noise from the LO to the QS [7], [8], [9], but the noise level was still intolerant. Although LLO scheme has reduced this issue significantly, polarization- multiplexing is still preferable in many cases for further reduction of any probable leakage noise from the PRP to the QS. This is done by separating both the QS and PRP on different polarization directions. In this way the leakage will not occur at Alice's polarizing beam splitter (PBS). However, the finite extinction ration R_{po} of the PBS at Bob's side leads to some photon leakage. This excess noise is quantified by [40]

$$\xi_{\mathrm{LE}} = \frac{2E_R^2}{R_e + R_p} \tag{13}$$

where R_e is the finite extinction ratio of the pulse generation, which represents the ratio between the low and high level of the optical pulse, and R_p is the finite extinction ratio of the PBS.

3) ADC QUANTIZATION NOISE

Quantization noise, ξ_{ADC}, is introduced by analog-to-digital converters (ADCs) at Bob's side. According to the research presented [16], this noise is constrained by the maximum amplitude of the signal that it can accommodate. The quantization noise can be represented as

$$\xi_{\mathrm{ADC}} = \frac{E_{\mathrm{s,max}}^2}{12 \times 2^n} \tag{14}$$

where n is the number of quantization bits. The previous noise sources can be lumped into one parameter ξ'

$$\xi' = \xi_o + \xi_{\mathrm{AM}} + \xi_{\mathrm{LE}} + \xi_{\mathrm{ADC}} \tag{15}$$

where ξ_o is the system excess noise from undefined or unprotected sources.

4) PHASE NOISE

Phase noise is caused by slow and fast drift of the optical phase leading to estimation error in the compensation process [40]. The slow drift is caused by the channel added noise on the QS and PRP during transmission. The variance of the channel phase noise is given by

$$V_{\mathrm{channel}} = \mathrm{var}(\phi_s^{\mathrm{ch}} - \phi_R^{\mathrm{ch}}) = 2\tau^2 \tag{16}$$

where ϕ_s^{ch} and ϕ_R^{ch} are the random accumulated phases on the QS and PRP by the channel and τ^2 is the variance of the phase distortion caused by air turbulence on any transmitted laser signal. The channel variance is modeled according to Monte-Carlo phase screen method using the Inverse Fast Fourier Transform (IFFT) [41]. The turbulence-induced phase is described using the Fourier series by

$$\theta(x, y) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} c_{mn} \exp[i2\pi(\kappa_{xm}x + \kappa_{xn}y)] \tag{17}$$

where c_{mn} donates the coefficients of Fourier series, κ_{xm} and κ_{xn} are the spatial frequencies in the x and y directions, respectively. According to Parseval's theorem, the power of the phase distortion is given by

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} |\theta(x, y)|^2 dxdy = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} |\Theta(x, y)|^2 d\kappa_x d\kappa_y \tag{18}$$

where $\Theta(x, y)$ is the power spectral density (PSD) of the phase distortion in the Cartesian coordinates, κ_x and κ_y donate the spatial frequencies in Cartesian representation. The PSD function is expressed by the pump spectral model in the polar coordinates as [39], [42]

$$\Theta(\kappa) = 0.49 r_o^{-5/3}\left[1 + 1.802\left(\frac{\kappa}{\kappa_l}\right) - 0.254\left(\frac{\kappa}{\kappa_l}\right)^{7/6}\right] \times \frac{\exp[-(\kappa/\kappa_l)^2]}{(\kappa^2+\kappa_o^2)^{11/6}} \tag{19}$$

where $\kappa = \sqrt{\kappa_x^2 + \kappa_y^2}$ is the spatial frequency in polar representation, $\kappa_l = 3.3/l_o$, $\kappa_o = 2\pi/L_o$ with l_o and L_o are the inner and outer scale of turbulence, respectively and $r_o = (0.423 \times C_n^2 L K^2)^{-3/5}$ is the coherence diameter with $K = 2\pi/\Lambda$ is the wavenumber. The c_{mn} are randomly generated according to Gaussian distribution with zero mean and variance obtained using Eq. (19). The variance of phase distortion $\tau^2 = \text{var}\big(\theta(x, y)\big)$ is obtained using the pre-calculated c_{mn} and after performing the IFFT as in Eq. (17).

The fast drift is the result of two components; the difference between the relative phases of the QS and PRP, as well as the estimation error of the PRP at Bob's detectors. The noise variance of the 1st component is given by [16], [33], [40]

$$\begin{aligned} V_{\text{drift}} &= \text{var}(\theta_s - \theta_R) \\ &= 2\pi(\Delta\upsilon_A + \Delta\upsilon_B)|t_R - t_s| \end{aligned} \tag{20}$$

where $\Delta\upsilon_A$ and $\Delta\upsilon_B$ are the linewidths of Alice and Bob's lasers and t_R and t_s are the emission times of the PRP and the QS, respectively. This noise is significant in the earlier pilot-sequential LLO schemes, where the PRP and the QS are generated sequentially from separate laser pulses [40]. In conventional TLO schemes, time-multiplexing is applied to eliminate the fast drift between the LO and the QS [7], [8], [9]. Similarly, time-multiplexing cancels this noise contribution in LLO scheme as a single laser pulse is splitted to instantaneously generate the QS and the PRP. Consequently, both pulses have the same initial phase ($\phi_s = \phi_R$). Thus, $t_R = t_s$ and $V_{\text{drift}} = 0$. The noise variance of the 2nd component of the fast drift is given by [16], [17], [33]

$$V_{\text{error}} = \text{var}(\theta_R - \widehat{\theta}_R) = \frac{\chi + 1}{E_R^2} \tag{21}$$

where E_R is the amplitude of the PRP and χ is the extra- added noise on the PRP, given by

$$\chi = \frac{1 - \langle T\rangle}{\langle T\rangle} + \frac{\chi_D^{\text{PRP}}}{\langle T\rangle} \tag{22}$$

with $\langle T\rangle$ represents the ensemble average of the transmittance. The 1st term of Eq. (22) stands for the loss-induced vacuum noise and the 2nd term is the generated noise during the imperfect detection of the PRP. In general, the detection noise referred to Bob's input is given by

$$\chi_D = \frac{\delta(1 + \upsilon_{\text{el}})}{\eta} - 1 \tag{23}$$

where η represents the detection efficiency and v_{el} is the electronic noise. In our system, we employ heterodyne detection to measure both quadratures of the PRP. Thus, $\chi_D^{\text{PRP}} = \chi_D|_{\delta=2}$. The total variance of the phase noise V_{phase} and the corresponding excess noise ξ_{phase} are approximated as [16], [33]

$$\begin{aligned} V_{\text{phase}} &= V_{\text{drift}} + V_{\text{channel}} + V_{\text{error}} \\ &\approx V_{\text{channel}} + V_{\text{error}} \end{aligned} \tag{24a}$$

$$\xi_{\text{phase}} = 2V_A\Big(1 - e^{-(V_{\text{phase}}/2)}\Big) \approx V_A V_{\text{phase}} \tag{24b}$$

and the total excess noise is given by

$$\xi_{\text{tot}} = \xi' + \xi_{\text{phase}} \tag{25}$$

The total channel added noise referred to the channel input is expressed as

$$\chi_{\text{line}} = \frac{1}{\langle T\rangle} - 1 + \xi_{\text{tot}} \tag{26}$$

and the total added noise imposed on the QS referred to the channel input is given by

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_D^{\text{QS}}}{\langle T\rangle} \tag{27}$$

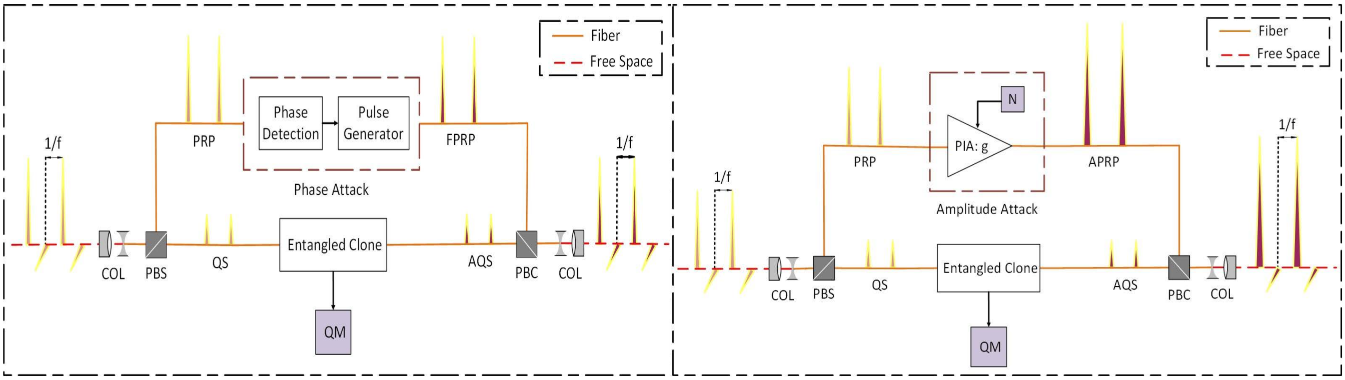
where $\chi_D^{\text{QS}} = \chi_D|_{\delta=1}$ represents the detection noise of the QS.

C. TRUSTED NOISE MODEL (TNM)

The detection of the PRP and QS was accomplished in a variety of studies using a single coherent detection stage [40]. Instead of a single detection stage, we employ two stages for the PRP and QS simultaneously [21], [40], as shown in Fig. 1. It is necessary to take into account the detection noise from the two stages. The detection of the PRP is addressed for by Eq. (22), while the detection of the QS is accounted by the 2nd term in Eq. (27). The detection process is characterized by the detection efficiency, η, and the electronic noise, v_{el}, as expressed in Eq. (23). According to the trusted noise model [16], [17], [23], the parameters η and v_{el} can be trusted and calibrated in the calculation of detection noise as long as Bob's detectors are not accessible to Eve. This is unlike the other untrusted noise sources, including channel noise, which Bob cannot easily calibrate. Therefore, part of the estimation error in Eqs. (21,22), which represents the detection noise of the PRP, can be trusted and the other parts are untrusted.

$$\begin{aligned} \chi &= \chi^U + \frac{\chi^T}{\langle T\rangle} \\ &= \left[\frac{1 - \langle T\rangle}{\langle T\rangle}\right]^U + \left[\frac{\chi_D^{\text{PRP}}}{\langle T\rangle}\right]^T \end{aligned} \tag{28a}$$

$$\begin{aligned} \xi_{\text{error}} &= V_A V_{\text{error}}^U + V_A V_{\text{error}}^T \\ &= \left[\frac{V_A}{E_R^2}(\chi^U + 1)\right]^U + \left[\frac{V_A}{E_R^2} \times \frac{\chi^T}{\langle T\rangle}\right]^T \\ &= \xi_{\text{error}}^U + \frac{\xi_{\text{error}}^T}{\langle T\rangle} \end{aligned} \tag{28b}$$



(a) Block diagram illustrates Eve's phase attack on the PRP.

(b) Block diagram illustrates Eve's amplitude attack on the PRP.

FIGURE 2. The block diagrams illustrate the two types of attack on the PRP. COL: Collimator, PBS: Polarizing Beam Splitter, PBC: Polarizing Beam Combiner, PRP: Phase Reference Pulse, QS: Quantum Signal, AQS: Attacked Quantum Signal, QM: Quantum Memory, APRP: Amplified Phase Reference Pulse, FPRP: Forged phase reference pulse.

The 2nd term in Eq. (27) is modified to include the total trusted detection noise of the QS and the PRP

$$\chi_D^T = \frac{(1+\upsilon_{\text{el}})}{\eta} - 1 + \xi_{\text{error}}^T \tag{29}$$

and according to the TNM, only the untrusted parts of excess noise should be accounted for in Eq. (26) (i.e. $\xi_{\text{tot}}^U = \xi' + \xi_{\text{phase}}^U$). Thus, only the variances of untrusted noise sources are considered (i.e. $\xi_{\text{phase}}^U = V_A V_{\text{channel}} + \xi_{\text{error}}^U$) and Eq. (26) is modified to

$$\chi_{\text{line}} = \frac{1}{\langle T \rangle} - 1 + \xi_{\text{tot}}^U \tag{30}$$

and the total added noise in Eq. (27) is modified to

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_D^T}{\langle T \rangle} \tag{31}$$

It is worth to mention that χ_{tot} in Eq. (27) should remain unchanged even after applying the TNM in Eq. (31)

III. SECURITY ANALYSIS WITH ATTACKS

In this section, we investigate the SKR, as well as the security proof, for the PRP when it is subjected to attacks including both phase and amplitude.

A. PHASE ATTACK OF THE PRP

In this scenario, we study the phase attack on the PRP and its impact on the security analysis of the system model. This attack was initially presented in [21] and was further investigated in [22] and [20] over a fiber quantum channel. Fig. 2 illustrates the eavesdropping technique assuming that Eve is aware of the multiplexing pattern Alice sent. As a result, Eve can demultiplex and split this pattern into the PRP and QS. She first detects the phase of PRP and then generates a forged copy of PRP that contains additional noise. Since Bob receives the forged PRP with the added noise, he can view this signal manipulation as a direct attack on the phase of the PRP. However, this attack affects system security by significantly reducing the SKR over the transmission distance. To model this effect, we have assumed the added noise follows the Gaussian distribution with zero mean and variance of $V_{\text{attack}}^{\text{PRP}}$ [21], [22]. We can add the attack variance to the channel variance to lump the total noise variance directly affecting the phase during transmission over the FSO channel.

This type of attack is applied only to the PRP. On the other hand, Eve can apply the entangling cloner (EC) attack to the QS [43], in which she keeps the entangled QS in a Quantum Memory (QM) until Bob's detection or she can perform any collective attack for the more general case. Thus, to include the noise imposed on the QS and the PRP due to Eve's activity, we can modify ξ_{tot}^U in Eq. (30) to

$$\xi_{\text{tot}}^U = \xi' + V_A(V_{\text{channel}} + V_{\text{attack}}^{\text{PRP}}) + \xi_{\text{error}}^U + \xi_{\text{attack}}^{\text{QS}} \tag{32}$$

where $\xi_{\text{attack}}^{\text{QS}}$ refers to the collective attack on the QS.

B. AMPLITUDE ATTACK OF THE PRP

Another technique to attack the PRP is by amplifying its amplitude using a phase insensitive amplifier (PIA) [17], as illustrated in Fig. 2b. In this technique, Eve attempts to reduce the trusted noise ξ_{error}^T in Eq. (28b) after amplification. This reduction is given by

$$\Delta\xi_{\text{error}}^T = \frac{V_A \chi^T}{\langle T \rangle E_R^2} - \frac{V_A \chi^T}{g\langle T \rangle E_R^2} = \frac{\xi_{\text{error}}^T}{\langle T \rangle}\left(1 - \frac{1}{g}\right) \tag{33}$$

where g is the amplification factor, Eve can invest this reduction to hide the inevitable noise after performing any collective attack on the QS without affecting the total excess noise in order to deceive Bob. In this way, Bob should not consider the excess noise of the PRP's detection totally trusted. Otherwise, he will overestimate the actual ξ_{error}^T leading to a false SKR [17]. Moreover, Eve adds unavoidable amplification noise during amplitude manipulation. This additional noise is referred to the channel input, and it is given by

$$\xi_{\text{error}}^A = \frac{V_A \chi^A}{E_R^2} = \frac{V_A}{E_R^2} \times \frac{N(g-1)}{g\langle T \rangle} \tag{34}$$

where N is the noise variance of the PIA for the PRP mode and idler mode [44].

The reduction of ξ^{T}_{error} should compensate for the amplification noise and Eve's attack on the QS to keep Bob's measurement unaffected

$$\xi^{\text{QS}}_{\text{attack}} = \Delta\xi^{T}_{\text{error}} - \xi^{A}_{\text{error}} \tag{35}$$

In order to include Eve's noise into the total added noise, Eqs. (29,30) are modified to

$$\chi^{T}_{D} = \frac{(1+\upsilon_{\text{el}})}{\eta} - 1 + \xi^{T}_{\text{error}} - \langle T\rangle\xi^{\text{QS}}_{\text{attack}} \tag{36}$$

$$\chi_{\text{line}} = \frac{1}{\langle T\rangle} - 1 + \xi^{U}_{\text{tot}} + \xi^{\text{QS}}_{\text{attack}} \tag{37}$$

In this attack, Eve is not interested in manipulating the channel itself, but he manipulates the PRP's amplitude and hides his effect in the ξ^{T}_{error} term.

C. INTERRUPTION PROBABILITY

Free space optical transmission requires a high directivity of the laser beam. Therefore, the connectivity breakdown is possible when there is a significant angle-of-arrival fluctuation. Image jitter on a focal plane is the direct reflection of angle-of-arrival fluctuations on the receiving aperture plane. Communication is interrupted when the focus is not inside the receiving fiber core at this point. The interruption probability due to angle-of-arrival fluctuations is given as [45]:

$$P_{\text{inter}} = 1 - \int_{-d_{\text{cor}/2}}^{d_{\text{cor}/2}} \frac{1}{\sqrt{2\pi\langle\beta_a^2\rangle}F} \exp\left(\frac{-l^2}{2F^2\langle\beta_a^2\rangle}\right) dl, \tag{38}$$

where the fiber core diameter in meter is d_{cor} ranging between 8.3 and 10.5 μm for single mode fiber, the focal length of the collecting lens is F, and the variance of the arriving angle is $\langle\beta_a^2\rangle = \langle\Delta x_0^2\rangle/L^2$. For weak turbulence considered in this work, $\langle\Delta x_0^2\rangle = 0.33\ \mathrm{w}_0^2\ \sigma_R^2\ \Omega^{-7/6}$. $\sigma_R^2 = 1.23\ C_n^2\ K^{7/6}\ L^{11/6}$ is the Rytov variance. The Fresnel parameter is $\Omega = K\mathrm{w}_0^2/2L$.

D. SKR AND SECURITY PROOF UNDER PRP ATTACK

The security proof of CV-QKD mainly depends on which attack that Eve employs. This study focuses on the collective attack on the QS utilizing phase and amplitude attacks on the PRP. We apply the asymptotic calculations of the SKR, assuming the optimistic scenario with no accessibility to Bob's devices by Eve [32]. The security proof under collective attack is established upon the covariance matrix γ_{AB} that fully describes the quantum state ρ_{AB}

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{\text{AB}} \\ \sigma_{\text{AB}} & \gamma_B \end{pmatrix} = \begin{pmatrix} V\mathbf{I_2} & \sqrt{\langle T\rangle}Z\sigma_z \\ \sqrt{\langle T\rangle}Z\sigma_z & \langle T\rangle(V+X_{\text{line}})\mathbf{I_2} \end{pmatrix} \tag{39}$$

where $\mathbf{I_2}$ is 2×2 identity matrix, $\sigma_z = \text{diag}(1,-1)$ is the Pauli's z-matrix and Z is the correlation coefficient. The γ_{AB} is originally introduced for Gaussian modulated coherent states for the entanglement-based (EB) scheme. However, the calculations for the PM scheme are proved to be equivalent to the EB scheme. For Discrete modulated states, these calculations are applicable, if the covariance matrix for DM converges to the GM (i.e. $\gamma_{AB}^{\text{DM}} \approx \gamma_{AB}^{\text{GM}}, Z_{\text{DM}} \approx Z_{\text{GM}}$). To ensure the convergence, the condition $V_A^{\text{DM}} < 1$ should be satisfied [30], [46]. In our work, we compare the behavior of GM and the DM (with 4-states and 8-states). Accordingly, the calculations of Z depending on the modulation type are given by [20], [32], [46]

$$Z_{\text{GM}} = \sqrt{(V^2-1)} \tag{40a}$$

$$Z_4 = 2\alpha^2\sum_{k=1}^{3}\left(\lambda_{k-1}^{3/2}\lambda_k^{-1/2}\right) \tag{40b}$$

$$Z_8 = 2\alpha^2\sum_{k=1}^{7}\left(\lambda_{k-1}^{3/2}\lambda_k^{-1/2}\right) \tag{40c}$$

with $V = V_A + 1, \alpha = \sqrt{V_A/2}$, where λ is described in details in *Appendix* for each type of modulation. The asymptotic calculations of the lower bound of the SKR are based on the reverse reconciliation scheme, which is proved to be more efficient in CV-QKD protocols and obtained as [7]:

$$\text{SKR} \geq (1 - P_{\text{inter}}) \int \text{P}(T)\left[\beta I_{\text{AB}} - \chi_{\text{BE}}\right] dT \tag{41}$$

where I_{AB} is the mutual information between Alice and Bob, χ_{BE} is the Holevo bound that stands for the maximum Eve's information on Bob's information, and β represents the reconciliation efficiency. Using Shannon's equation, I_{AB} is calculated using Bob's measured variance V_B and the conditional variance $V_{B|A}$ as [20]:

$$I_{\text{AB}} = \frac{\delta}{2}\log_2\left(\frac{V_B}{V_{B|A}}\right) = \frac{\delta}{2}\log_2(1+\text{SNR}) \tag{42}$$

with $\text{SNR} = V_A/(1+\chi_{\text{tot}})$ represents the Signal to Noise Ratio. For more practical scenario β is evaluated as a function of the SNR that varies with the transmission distance as in [44]

$$\beta = \left(\frac{\log_{10}(1+\text{SNR}^{1.2})}{1.29\log_{10}(1+\text{SNR})}\right) + 0.02 \tag{43}$$

χ_{BE} is calculated and derived using γ_{AB} in Eq. (39)

$$\chi_{\text{BE}} = \sum_{i=1}^{2} G\left(\frac{\nu_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\nu_i - 1}{2}\right) \tag{44}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$ and the symplectic eigenvalues $\nu_i (i = 1, 2, \ldots, 5)$ are given by

$$\nu_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}) \tag{45a}$$

$$\nu_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}) \tag{45b}$$

and $\nu_5 = 1$, with

$$\begin{aligned} A &= \det(\gamma_A) + \det(\gamma_B) + 2\det(\sigma_{AB}) \\ &= V^2 + (\langle T\rangle(V + \chi_{\text{line}}))^2 - 2\langle T\rangle Z^2 \end{aligned} \tag{46a}$$

$$B = \det(\gamma_{AB}) = \left(\langle T\rangle(V^2 + V\chi_{\text{line}} - Z^2)\right)^2 \tag{46b}$$

TABLE 1. **The fixed simulation parameters [16], [17], [20], [40]. All variances and noises are in SNU.**

Parameter	Symbol	Value
Refractive index structure parameter	C_n^2	$10^{-16}\text{m}^{-2/3}$
The optical wavelength	Λ	1.55 μm
Bob's aperture radius	a	0.075 m
Inner scale of turbulence	l_o	0.01 m
Outer scale of turbulence	L_o	10 m
Detection effeciency	η	50%
Electronic noise	ν_{el}	0.1
System excess noise from unprotected sources	ξ_o	0.01
Amplitude of the PRP	E_R	$\sqrt{200}$
Finite extinction ratio of the pulse generation	R_e	50 dB
Finite extinction ratio of the PBS	R_p	30 dB
Dynamics of the AM	d_{dB}	80 dB
Number of quantization bits	n	8
Noise variance of the PIA	N	1
Fiber core diameter	d_{cor}	9 μm

and for homodyne detection

$$C_{\text{hom}} = \frac{A\chi_D + V\sqrt{B} + c_1}{c_1 + \chi_D} \tag{46c}$$

$$D_{\text{hom}} = \frac{V\sqrt{B} + B\chi_D}{c_1 + \chi_D} \tag{46d}$$

with $c_1 = \langle T \rangle (V + \chi_{\text{line}})$ [30], [32], [47].

IV. RESULTS AND DISCUSSION

In this section, the security analysis and SKR calculations are presented. These analysis and calculations are based on the channel and noise models that were described in Section II and are presented under the phase and the amplitude attacks of the PRP over the FSO channel with fluctuating transmittance as stated in Section III. The values of the simulation parameters are listed in Table 1 [16], [17], [20], [40].

A. CHANNEL NOISE VARIANCE

The Monte Carlo simulation is used to generate 1000 phase screens to calculate the channel noise variance V_{channel}. The simulation uses a grid size of $M \times M$ with $M = 2\text{w}/\Delta$, where $\Delta = 2.92 \times 10^{-4}$ m is the grid spacing. Each point on the screen represents the accumulated phase ϕ_{ch} at a specific (x, y) location on the laser beam at a certain distance. Then, the average phase screen is obtained, and its variance is calculated, as shown in Fig. 3. We have performed these calculations for distances up to 20 km. This process is repeated many times, and the average variances at each distance are obtained for better fitting, as shown in Fig. 4. For the optimal coupling of the laser beam into Bob's aperture, the ratio between the received beam radius and the radius of Bob's aperture (w$/a$) is adjusted in the range [1.1 $-$ 2.3] across the distance range up to 20 km. This is practically achieved using optical lenses to collimate the laser beam. The initial beam radius at Alice's side $\text{w}_0 \in [0.12 - 6.26]$ cm is obtained after numerically solving Eq. (11) for w_0.

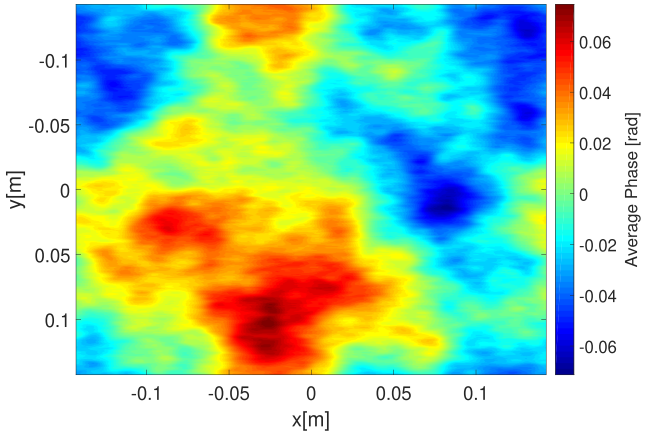


FIGURE 3. **The average phase screen at 1200 m with variance of 8.0855 x 10^{-4} rad^2.**

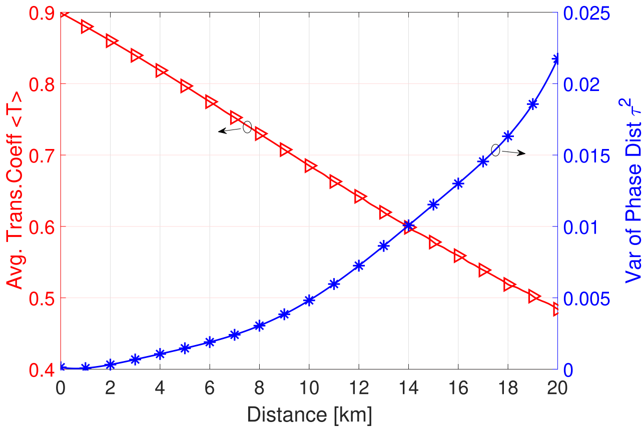


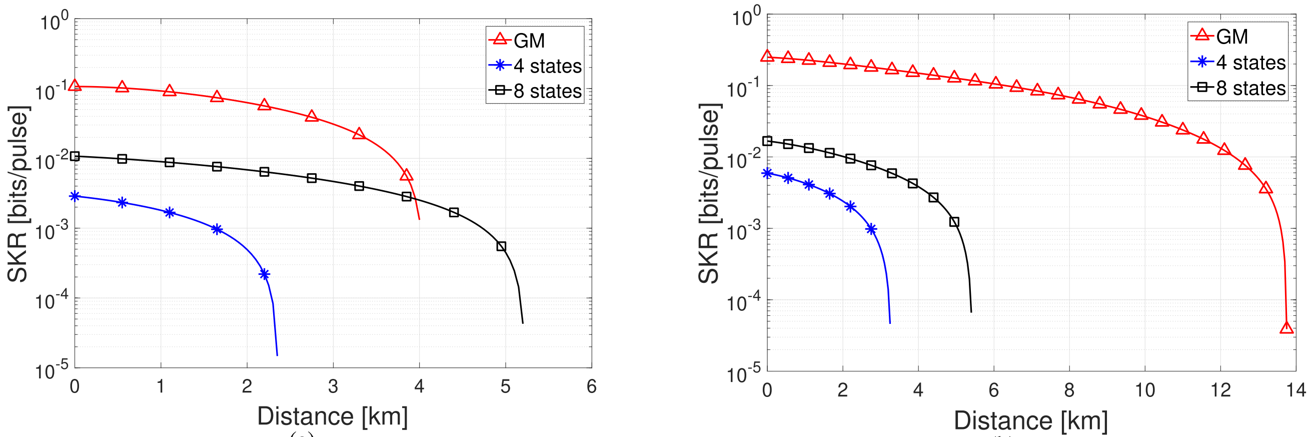
FIGURE 4. **Avg. transmission coefficient $\langle T \rangle$ (left y-axis) and Phase distortion variance τ^2 (right y-axis) v.s. distance.**

B. AVERAGE TRANSMISSION COEFFICIENT

We have obtained the average transmission coefficient $\langle T \rangle$ for the calculations of the SKR as described in the CV-QKD by using the previously computed w_o and Eqs. (5-10) . In the first step, we used the Rice distribution to generate 1000 points as a random variable for the beam deflection distance r. The noncentrality and the scale parameters are set to $d = 0$ and σ in Eq. (6), respectively. Then, Eqs. (7-10) are used to calculate $\langle T \rangle$ according to the PDTC of the log-negative Weibull distribution in Eq. (5) as a function of the transmission distance, as shown in Fig. 4.

C. SKR CALCULATIONS AND SECURITY ANALYSIS

Choosing the modulation variance V_A is extremely important for maintaining a high SKR over long distances. In the first step, we calculated the SKR by considering that V_A is equal to 18.9, 0.35, and 0.5 for GM, 4-states, and 8-states, respectively, as mentioned in [21], [22], and [20]. We did this while assuming that no existence of Eve's attack on the QS and the PRP as in Fig. 5a. After that, we optimized V_A with respect to the distance, and the results are shown in Fig. 5b. The optimal values of V_A throughout the distances that are acceptable for secure transmission are [1.2$-$6.3], [0.45$-$0.5],



(a)

(b)

FIGURE 5. SKR v.s. Distance without introducing attack on the QS and the PRP. (a) V_A is set to 18.9, 0.35 and 0.5 for GM, 4-states and 8-states, respectively as in [21], [22], [20]. (b) The optimal ranges of V_A based on the transmission distance for optimal security, $V_A \in [1.2 - 6.3]$, $V_A \in [0.45 - 0.5]$ and $V_A \in [0.6 - 0.9]$ for GM, 4-states and 8-states, respectively.

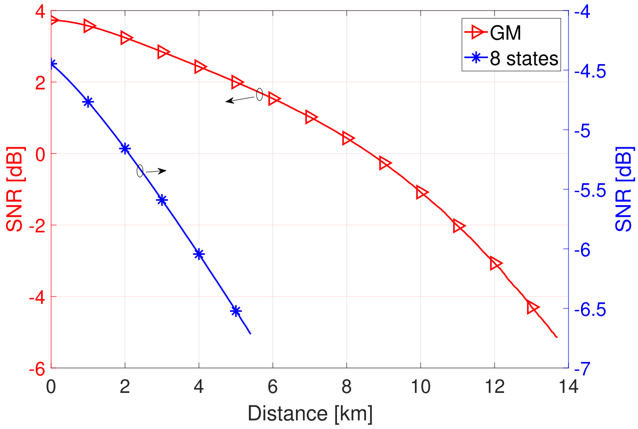


FIGURE 6. SNR v.s. Distance for GM (left y-axis) and 8-states (right y-axis).

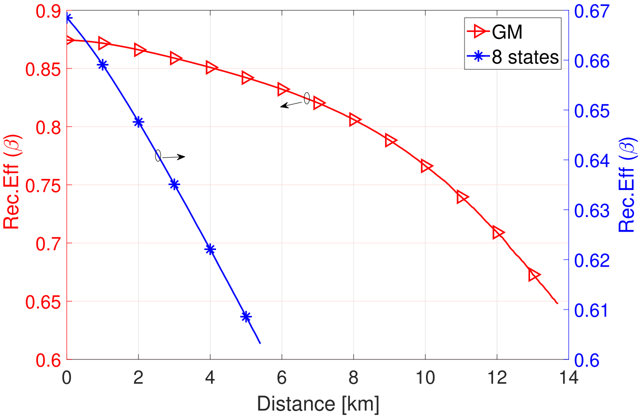


FIGURE 7. Reconciliation efficiency (β) v.s. Distance for GM (left y-axis) and 8-states (right y-axis).

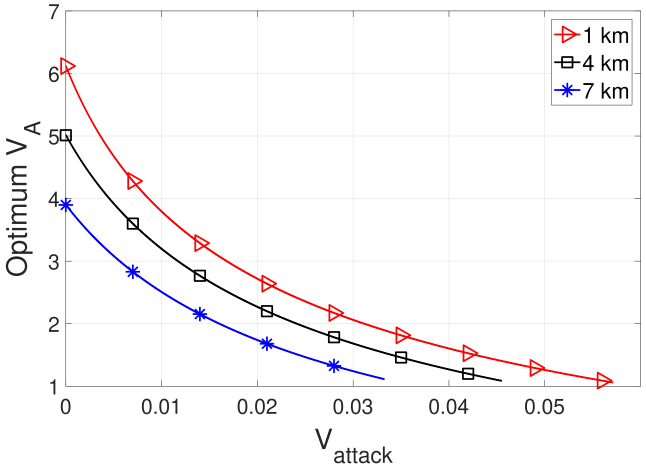


FIGURE 8. Optimum V_A v.s. Eve's variance attack, V_{attack}, at different transmission distances for GM under phase attack.

and [0.6 – 0.9] for GM, 4-states, and 8-states, respectively. Although GM shows higher SKR with extended distances compared to DM when employing the optimal V_A at each distance point, the SNR required to maintain this performance for GM is very high compared to DM, as seen in Fig. 6. This requires a significant amount of signal power in order to keep the SKR for GM at its optimal level. In contrast to GM, the DM with 8-states can still provide secure communication at SNR lower than −3dB for distances less than 6km. This illustrates that DM protocols can provide security at very low signal power. According to Eq. (43), the calculations of the reconciliation efficiency β provide that GM is more efficient compared to DM, as shown in Fig. (7).

In the case of eavesdropping using the phase attack, increasing the variance of attack, V_{attack}, changes the optimal value of V_A as well as the optimum SKR during the transmission. According to [39], Eve's attack on the QS, $\xi^{\text{QS}}_{\text{attack}}$, is set to 0.001. In the event, the V_A and SKR in GM or 8-states modulations are highly affected by increasing V_{attack}. As V_{attack} and the transmission distance increases, the optimal V_A rapidly decreases, as shown in Fig. 8 and Fig. 9 for GM and DM (8-states), respectively. This causes a significant drop in the SKR with the transmission distance as presented in Fig. 10 and Fig. 11 for GM and DM (8-states), respectively. In addition, increasing the

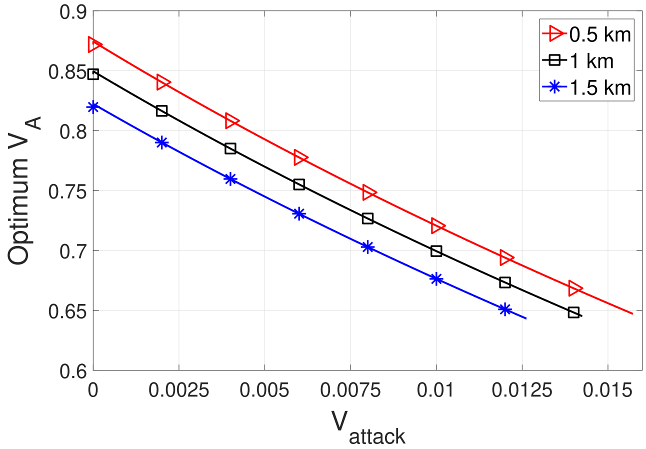


FIGURE 9. Optimum V_A v.s. Eve's variance attack, V_{attack}, at different transmission distances for DM (8-states) under phase attack.

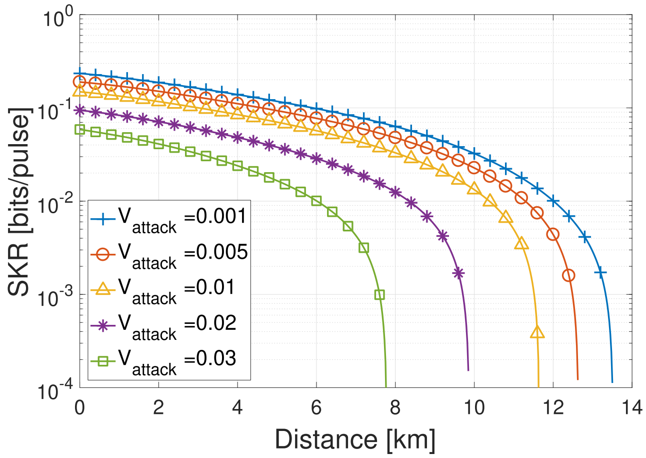


FIGURE 10. SKR v.s. transmission distance using optimum V_A for GM under phase attack.

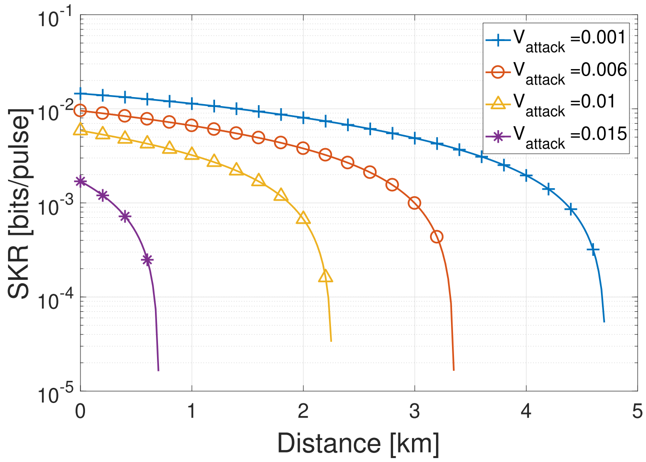


FIGURE 11. SKR v.s. transmission distance using optimum V_A for DM (8-states) under phase attack.

transmission distance necessitates a decrease in the value of V_A in order to maintain the highest possible SKR before dropping, as shown in Fig. 8 and Fig. 9 for GM and DM (8-states), respectively.

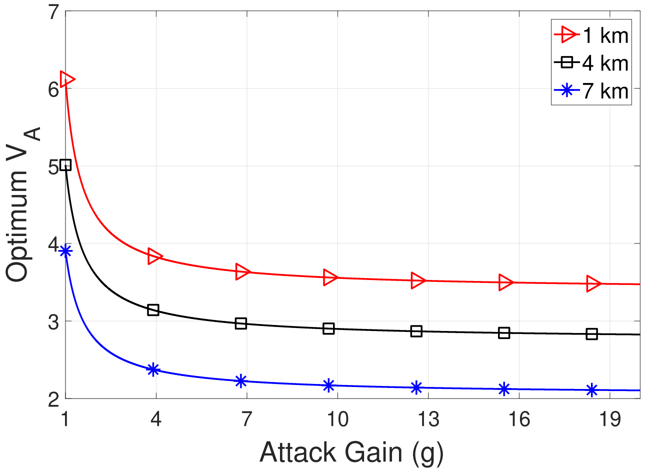


FIGURE 12. Optimum V_A v.s. Eve's attack gain, g, at different distances for GM under amplitude attack.

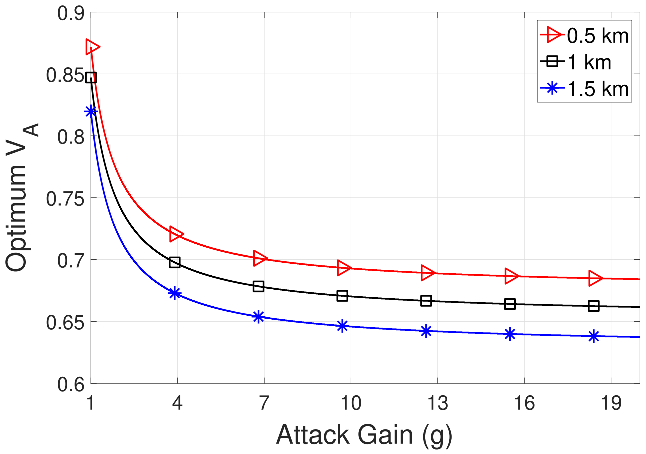


FIGURE 13. Optimum V_A v.s. Eve's attack gain, g, at different distances for DM (8-states) under amplitude attack.

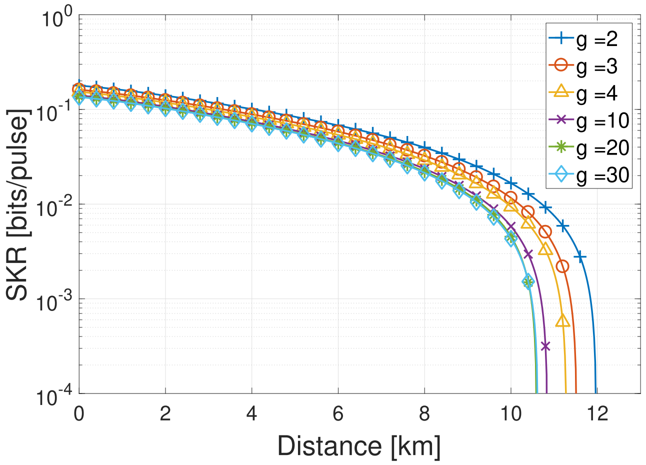


FIGURE 14. SKR v.s. transmission distance using optimum V_A for GM under amplitude attack.

In the case of eavesdropping employing the amplitude attack by attack gain (g), an increase in g affects the optimal value of V_A as well as the optimum SKR during the transmission. Fig. 12 illustrates the impact of increasing the attack

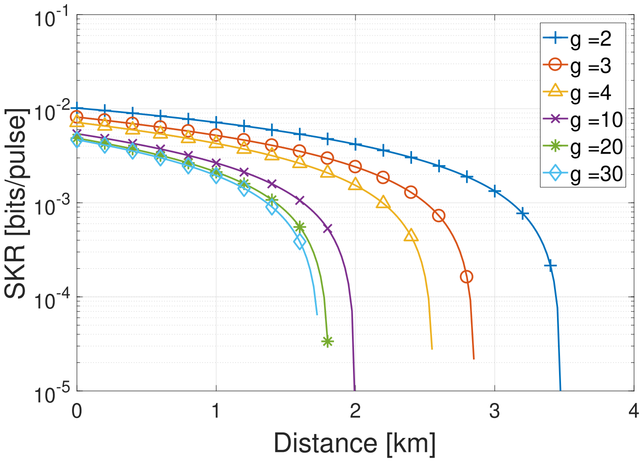


FIGURE 15. SKR v.s. transmission distance using optimum V_A for DM (8-states) under amplitude attack.

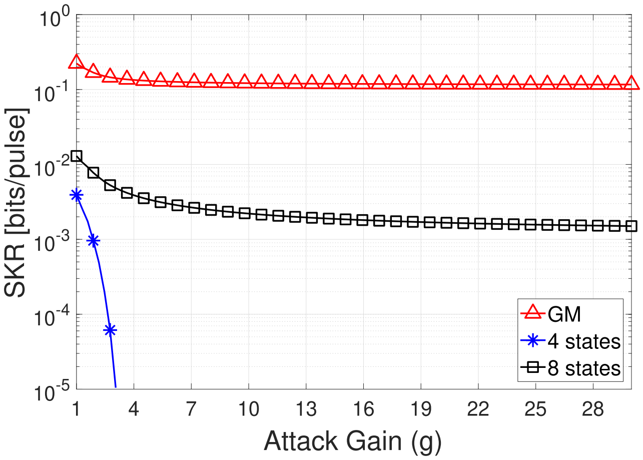


FIGURE 17. SKR v.s. Eve's attack on the PRP using the optimum V_A at 1200 m under amplitude attack.

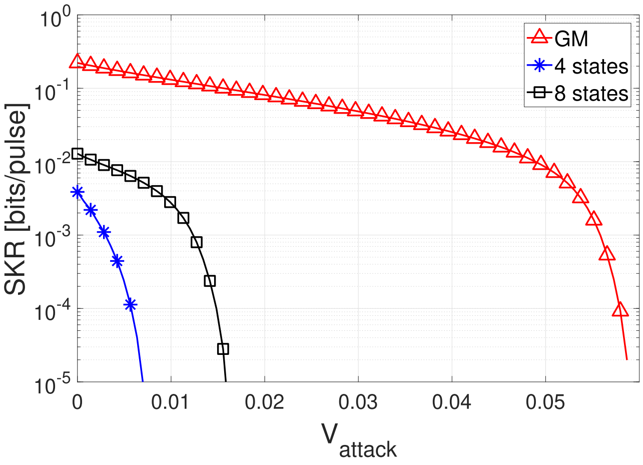


FIGURE 16. SKR v.s. Eve's attack on the PRP using the optimum V_A at 1200 m under phase attack.

gain on the optimal value of V_A while using GM. As can be seen, when attack gain changes in the range $[1-4]$, the optimal V_A decreases significantly. For $(g > 4)$, the optimal V_A slightly decreases until it almost saturates for a high gain value. The effect of attack gain on the optimal V_A using DM (8-states) is shown in Fig. 13, whereas the optimal V_A decreases significantly when the attack gain changes in the range $[1-10]$ while slightly affected for $(g > 10)$. We can still observe that longer distances require lower values of the optimal V_A, as seen in Fig. 12 and Fig. 13. The effect of increasing the transmission distance on the SKR at different values of g for GM and DM (8-states) is shown in Fig. 14 and Fig. 15, respectively, while maintaining the value of V_A optimal according to the applied distance. The saturation of the optimum SKR and V_A under the amplitude attack is due to the increment of $\Delta\xi^T_{\text{error}}$ with increasing g until reaching $\xi^T_{\text{error}}/\langle T\rangle$, from Eq.(33). In this case, the trusted noise model will return to the untrusted model, and the amount of the PRP's trusted detection noise will be inconsiderable. This is due to the large amplitude of the PRP after Eve's amplification, but the communication link is still secured for shorter distances.

Finally, the GM shows higher resistivity to Eve's attack than the DM since it keeps a higher SKR for a wider range of attacks, especially phase attacks. This is illustrated in the SKR v.s Eve's calculations at a fixed distance of 1200m, as shown in Fig. 16 and Fig. 17 for phase and amplitude attack, respectively. Furthermore, we can observe the minimal diversity of the curves in the case of the amplitude attack compared to the phase attack, as presented in Fig. 10 and Fig. 14 for GM and Fig. 11 and Fig. 15 for DM (8-states). Thus, we can ensure the system robustness under amplitude attack and consider the effect of the phase attack more severe on the communication link.

V. CONCLUSION

This work developed an integrated, trusted noise model of the LLO-based CV-QKD scheme over an atmospheric quantum channel. We have included the effect of the fluctuating transmittance assuming weak turbulence by applying the log-negative Weibull distribution model. In order to evaluate the phase distortion caused by atmospheric turbulence, the Monte-Carlo phase screen method has been utilized. Eve's attack on either the amplitude or phase of the PRP has been included in the SKR calculations. The optimal value of Alice's states that satisfy the maximum SKR is quantified for each transmission distance. Consequently, the system security is compared for GM and DM with 4 and 8 -states considering all the previous assumptions. The numerical results have confirmed the out-performance of the GM compared to DM protocols regarding achievable SKR, transmission distance, and reconciliation efficiency. However, the analysis has revealed that this performance of GM is restricted by the availability of relatively high levels of SNR compared to that required in DM. Moreover, it is found that the SKR has exhibited great stability under amplitude attack with increasing the gain of the PIA at Eve's side. On the contrary, phase attack causes a severe reduction of the SKR with increasing phase noise variance due to Eve's activity on the PRP. As future work, we could investigate the possibility of detecting Eve's attack by presenting a comprehensive setup for monitoring the amplitude of the PRP as well as the phase noise of the QS and the PRP. Additionally, this will enable precisely determining several types of attacks.

APPENDIX

For n-state system, the density matrix is given by [20], [32], [46]

$$\rho_n = \sum_{i=0}^{n-1} \lambda_i |\phi_i\rangle\langle\phi_i| \tag{V.1}$$

For $n = 4$

$$\lambda_{0,2} = \frac{1}{2} e^{-\alpha^2}(\cosh\alpha^2 \pm \cos\alpha^2) \tag{V.2a}$$

$$\lambda_{1,3} = \frac{1}{2} e^{-\alpha^2}(\sinh\alpha^2 \pm \sin\alpha^2) \tag{V.2b}$$

For $n = 8$

$$\lambda_{0,4} = \frac{1}{4} e^{-\alpha^2}\left(\cosh\alpha^2 + \cos\alpha^2 \pm 2\cos\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\right) \tag{V.3a}$$

$$\lambda_{1,5} = \frac{1}{4} e^{-\alpha^2}\Big(\sinh\alpha^2 + \sin\alpha^2 \pm \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}} \pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\Big) \tag{V.3b}$$

$$\lambda_{2,6} = \frac{1}{4} e^{-\alpha^2}\left(\cosh\alpha^2 - \cos\alpha^2 \pm 2\sin\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}}\right) \tag{V.3c}$$

$$\lambda_{3,7} = \frac{1}{4} e^{-\alpha^2}\Big(\sinh\alpha^2 - \sin\alpha^2 \mp \sqrt{2}\cos\frac{\alpha^2}{\sqrt{2}}\sinh\frac{\alpha^2}{\sqrt{2}} \pm\sqrt{2}\sin\frac{\alpha^2}{\sqrt{2}}\cosh\frac{\alpha^2}{\sqrt{2}}\Big) \tag{V.3d}$$

REFERENCES

[1] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[2] I. B. Djordjevic, "Discrete variable (DV) QKD," in *Physical-Layer Security and Quantum Key Distribution*. Cham, Switzerland: Springer, 2019, pp. 267–322.

[3] M. Zou, Y. Mao, and T.-Y. Chen, "Phase estimation using homodyne detection for continuous variable quantum key distribution," *J. Appl. Phys.*, vol. 126, no. 6, Aug. 2019, Art. no. 063105.

[4] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, and B. Xu, "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," *Commun. Phys.*, vol. 5, no. 1, pp. 1–10, Dec. 2022.

[5] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, no. 1, pp. 1800011.1–1800011.37, 2018.

[6] S. P. Kish, E. Villasenor, R. Malaney, K. A. Mudge, and K. J. Grant, "Use of a local local oscillator for the satellite-to-earth channel," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2021, pp. 1–6.

[7] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 4, Oct. 2007, Art. no. 042305.

[8] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," *Phys. Rev. A*, vol. 76, no. 5, pp. 052323-1–052323-9, Nov. 2007.

[9] 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.

[10] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 5, pp. 052309.1–052309.9, May 2013.

[11] X. Tan, Y. Guo, L. Zhang, J. Huang, J. Shi, and D. Huang, "Wavelength attack on atmospheric continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 103, no. 1, Jan. 2021, Art. no. 012417.

[12] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 87, no. 6, pp. 062313.1–062313.7, Jun. 2013.

[13] Y. Mao, Y. Wang, W. Huang, H. Qin, D. Huang, and Y. Guo, "Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 101, no. 6, pp. 062320.1–062320, Jun. 2020.

[14] D. A. Kronberg and Y. V. Kurochkin, "Role of intensity fluctuations in quantum cryptography with coherent states," *Quantum Electron.*, vol. 48, no. 9, pp. 843–848, Sep. 2018.

[15] C. Li, L. Qian, and H.-K. Lo, "Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources," *Npj Quantum Inf.*, vol. 7, no. 1, pp. 1–8, Dec. 2021.

[16] Y. Shao, H. Wang, Y. Pi, W. Huang, Y. Li, J. Liu, J. Yang, Y. Zhang, and B. Xu, "Phase noise model for continuous-variable quantum key distribution using a local local oscillator," *Phys. Rev. A, Gen. Phys.*, vol. 104, no. 3, pp. 032608.1–032608.25, Sep. 2021.

[17] Y. Shao, Y. Li, H. Wang, Y. Pan, Y. Pi, Y. Zhang, W. Huang, and B. Xu, "Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator," *Phys. Rev. A, Gen. Phys.*, vol. 105, no. 3, Mar. 2022, Art. no. 032601.

[18] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," *Opt. Lett.*, vol. 40, no. 16, pp. 3695–3698, Aug. 2015.

[19] B. Qi and C. C. W. Lim, "Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator," *Phys. Rev. A, Gen. Phys.*, vol. 9, no. 5, pp. 1–10, May 2018.

[20] K. A. Alaghbari, K. Rumyantsev, T. Eltaif, O. Elmabrok, and H.-S. Lim, "Adaptive modulation for continuous-variable quantum key distribution with real local oscillators under phase attack," *IEEE Photon. J.*, vol. 13, no. 5, pp. 1–7, Oct. 2021.

[21] B. Huang, Y. Zhu, P. Tang, Y. Huang, and Z. Peng, "Practical security of the continuous-variable quantum key distribution with locally-generated local oscillators," *J. Appl. Math. Phys.*, vol. 7, no. 11, pp. 2751–2759, 2019.

[22] B. Huang, Y. Huang, and Z. Peng, "Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack," *Opt. Exp.*, vol. 27, no. 15, pp. 20621–20631, 2019.

[23] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 36, no. 3, pp. 7–15, 2019.

[24] N. Alshaer, M. E. Nasr, and T. Ismail, "Hybrid MPPM-BB84 quantum key distribution over FSO channel considering atmospheric turbulence and pointing errors," *IEEE Photon. J.*, vol. 13, no. 6, pp. 1–9, Dec. 2021.

[25] N. Alshaer, A. Moawad, and T. Ismail, "Reliability and security analysis of an entanglement-based QKD protocol in a dynamic ground-to-UAV FSO communications system," *IEEE Access*, vol. 9, pp. 168052–168067, 2021.

[26] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, no. 22, pp. 220501.1–220501.13, Jun. 2012.

[27] D. Vasylyev, A. A. Semenov, and W. Vogel, "Atmospheric quantum channels with weak and strong turbulence," *Phys. Rev. Lett.*, vol. 117, no. 9, pp. 090501.1–090501.18, Aug. 2016.

[28] I. B. Djordjevic, ''On the discretized Gaussian modulation (DGM)-based continuous variable-QKD,'' *IEEE Access*, vol. 7, pp. 65342–65346, 2019.

[29] I. B. Djordjevic, ''Optimized-eight-state CV-QKD protocol outperforming Gaussian modulation based protocols,'' *IEEE Photon. J.*, vol. 11, no. 4, pp. 1–10, Aug. 2019.

[30] Y. Guo, R. Li, Q. Liao, J. Zhou, and D. Huang, ''Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier,'' *Phys. Lett. A*, vol. 382, no. 6, pp. 372–381, Feb. 2018.

[31] Z. Qu, I. B. Djordjevic, and M. A. Neifeld, ''RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection,'' *Opt. Lett.*, vol. 41, no. 23, pp. 5507–5510, Dec. 2016.

[32] M. Li and M. Cvijetic, ''Continuous-variable quantum key distribution with self-reference detection and discrete modulation,'' *IEEE J. Quantum Electron.*, vol. 54, no. 5, pp. 1–8, Oct. 2018.

[33] A. Marie and R. Alléaume, ''Self-coherent phase reference sharing for continuous-variable quantum key distribution,'' *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 1, pp. 012316.1–012316.22, Jan. 2017.

[34] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, ''Generating the local oscillator 'locall' in continuous-variable quantum key distribution based on coherent detection,'' *Phys. Rev. X*, vol. 5, no. 4, pp. 041009.1–041009.12, Oct. 2015.

[35] R. Corvaja, ''Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection,'' *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 2, pp. 022315.1–022315.7, Feb. 2017.

[36] P. Huang, D.-K. Lin, D. Huang, and G.-H. Zeng, ''Security of continuous-variable quantum key distribution with imperfect phase compensation,'' *Int. J. Theor. Phys.*, vol. 54, no. 8, pp. 2613–2622, Aug. 2015.

[37] D. Vasylyev, W. Vogel, and A. A. Semenov, ''Theory of atmospheric quantum channels based on the law of total probability,'' *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 6, pp. 063852.1–063852.14, Jun. 2018.

[38] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, ''Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 881–919, 1st Quart., 2019.

[39] M. Li and T. Wang, ''Continuous-variable quantum key distribution over air quantum channel with phase shift,'' *IEEE Access*, vol. 8, pp. 39672–39677, 2020.

[40] T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, ''Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator,'' *Phys. Rev. A, Gen. Phys.*, vol. 97, no. 1, pp. 012310.1–012310.11, Jan. 2018.

[41] J. D. Schmidt, *Numerical Simulation of Optical Wave Propagation: With Examples in MATLAB*. Bellingham, Washington USA: SPIE, 2010.

[42] M. Li, M. Cvijetic, Y. Takashima, and Z. Yu, ''Evaluation of channel capacities of OAM-based FSO link with real-time wavefront correction by adaptive optics,'' *Opt. Exp.*, vol. 22, no. 25, pp. 31337–31346, 2014.

[43] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, ''Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables,'' 2003, *arXiv:quant-ph/0306141*.

[44] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, ''Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers,'' *J. Phys. B, At., Mol. Opt. Phys.*, vol. 42, no. 11, pp. 114014.1–114014.11, May 2009.

[45] S. Wang, P. Huang, T. Wang, and G. Zeng, ''Atmospheric effects on continuous-variable quantum key distribution,'' *New J. Phys.*, vol. 20, no. 8, pp. 083037.1–083037.21, Aug. 2018.

[46] A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, ''Continuous-variable quantum key distribution protocols with eight-state discrete modulation,'' *Int. J. Quantum Inf.*, vol. 10, no. 1, pp. 1250004.1–1250004.15, Feb. 2012, Art. no. 1250004.

[47] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, ''Parameter estimation of atmospheric continuous-variable quantum key distribution,'' *Phys. Rev. A, Gen. Phys.*, vol. 99, no. 3, pp. 032326.1–032326.11, Mar. 2019.

SARA AHMED received the B.Sc. degree in electronics and communications from the Faculty of Engineering, German University in Cairo, Egypt, in 2020. She is currently pursuing the M.Sc. degree at the School of Engineering and Applied Sciences, Nile University, Egypt. She is a Research Assistant at the wireless intelligent research center (WINC), Nile University. Her research interests include quantum information, random number generation, and cryptography.

NANCY ALSHAER (Member, IEEE) received the Ph.D. degree in optical free-space communication with quantum-key distribution, in 2020. She is a Lecturer with the Department of Electronics and Electrical Communication, Faculty of Engineering, Tanta University, Egypt. She is a CoPI in a funded project supported by the Science, Technology & Innovation Funding Authority (STIFA) of Egypt. She has a research collaboration with the National Institute of Laser Cairo University and the Wireless Intelligent Research Center, Nile University, Egypt. Her research interests include optical and wireless communications, quantum key distribution, quantum random number generation, tracking systems, and mobile edge computing.

KHALED A. ALAGHBARI (Member, IEEE) received the B.Eng. degree (Hons.) in electronics engineering majoring in telecommunication, and the M.Eng.Sc. and Ph.D. degrees from Multimedia University (MMU), Melaka, Malaysia, in 2011, 2014, and 2020, respectively. He is currently a Postdoctoral Researcher at the Institute of IR 4.0, Universiti Kebangsaan Malaysia (UKM). His research interests include signal processing and machine learning.

TAWFIK ISMAIL (Senior Member, IEEE) joined the Optical Wireless Communication Research Group, Department of Engineering and Sciences, University of Oxford, U.K., in 2018, to work in the research of quantum communication in free space. He has established and led the Research Group for Optical and Wireless Communications at Cairo University, Egypt. He is currently the Director of Wireless Intelligent Networks Research Center (WINC), Nile University. He is an Associate Professor with the National Institute of Laser Enhanced Sciences, Cairo University. He was a Postdoctoral Researcher of optical and wireless communications with the Technical Institute of Microwave and Photonic Engineering, University of Graz, Austria, in 2015. Since 2014, he has been with several research projects funded nationally by NTRA, ASRT, STDF, and ITIDA, Egypt, and internationally by InnoveUK, U.K. He was at the Technical Institute of Microwave and Photonic Engineering, University of Graz; The American University in Cairo, Egypt; Cairo University; and Malaviya National Institute of Technology, India. His research interests include optical and wireless communications, mmWave, mobile edge computing, quantum cryptography, information security, blockchain, artificial intelligence, and machine learning applications in optical and wireless communication systems.