Generalized Kennedy Receivers Enhanced CV-QKD in Turbulent Channels for Endogenous Security of Space-Air-Ground Integrated Network

Shouye Miao, Renzhi Yuan, Bin Cao, Mufei Zhao, Zhifeng Wang, and Mugen Peng

Abstract

Endogenous security in next-generation wireless communication systems attracts increasing attentions in recent years. A typical solution to endogenous security problems is the quantum key distribution (QKD), where unconditional security can be achieved thanks to the inherent properties of quantum mechanics. Continuous variable-quantum key distribution (CV-QKD) enjoys high secret key rate (SKR) and good compatibility with existing optical communication infrastructure. Traditional CV-QKD usually employ coherent receivers to detect coherent states, whose detection performance is restricted to the standard quantum limit. In this paper, we employ a generalized Kennedy receiver called CD-Kennedy receiver to enhance the detection performance of coherent states in turbulent channels, where equal-gain combining (EGC) method is used to combine the output of CD-Kennedy receivers. Besides, we derive the SKR of a post-selection based CV-QKD protocol using both CD-Kennedy receiver and homodyne receiver with EGC in turbulent channels. We further propose an equivalent transmittance method to facilitate the calculation of both the bit-error rate (BER) and SKR. Numerical results show that the CD-Kennedy receiver can outperform the homodyne receiver in turbulent channels in terms of both BER and SKR performance. We find that BER and SKR performance advantage of CD-Kennedy receiver over homodyne receiver demonstrate opposite trends as the average transmittance increases, which indicates that two separate system settings should be employed for communication and key distribution purposes. Besides, we also demonstrate that the SKR performance of a CD-Kennedy receiver is much robust than that of a homodyne receiver in turbulent channels.

Index Terms

CV-QKD, Endogenous security, Generalized Kennedy receiver, Space-air-ground integrated network, Turbulent channels

Shouye Miao, Renzhi Yuan, Bin Cao, and Mugen Peng are with the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China; Mufei Zhao is with School of Computer Science and Engineering, Northeastern University, Shenyang, 110819, China; Zhifeng Wang is with School of Electronic and Information Engineering, Tongji University, Shanghai, 201804, China.

Corresponding Author: Renzhi Yuan(renzhi.yuan@bupt.edu.cn)

A journal version of this paper is under peer review process. This work is supported by the National Natural Science Foundation of China under No. 62201075.

I. Introduction

A. Background and motivation

Endogenous security plays a crucial role in space-air-ground integrated network and attracts increasing attentions in next-generation wireless communication systems [1]–[4]. A typical solution to endogenous security problems is the quantum key distribution (QKD), which provides unconditional security to physical layer communication links thanks to the inherent properties of quantum mechanics [5]–[8]. QKD protocols can be divided into two categories according to the types of employed information carriers, i.e., the discrete variable-quantum key distribution (DV-QKD) based on individual photons and the continuous variable-quantum key distribution (CV-QKD) based on Gaussian states. Compared with DV-QKD [9], [10], CV-QKD [11]–[14] enjoys higher secret key rate and better compatibility with current optical communication infrastructure, and therefore, attracted large attentions in recent years [15]–[21].

Current CV-QKD protocols mainly employ coherent detections to recover the transmitted bits [11]–[15], whose performance is restricted by the standard quantum limit (SQL) [22]. A type of quantum receiver, generalized Kennedy receiver, was applied to the post-selection based CV-QKD to surpass the SQL and improve the secret key rate (SKR) [22]. It was demonstrated that the generalized Kennedy receiver can increase the SKR in either individual attacks or collective attacks compared with coherent receivers [22]–[25]. However, these quantum receiver enhanced CV-QKD protocols are restricted in lossy channel only. In space-air-ground integrated network, the most important and also vulnerable links are the satellite-to-ground links due to the presence of atmospheric turbulence [26]. To the best knowledge of the authors, the study of generalized Kennedy receiver enhanced CV-QKD in turbulent channels is still absent.

B. Related works

The CV-QKD protocol using coherent states was proposed by Grosshans and Grangier [11], where the secret key rate (SKR) was guaranteed by the no-cloning theorem. However, this protocol suffers from the "3dB limit", i.e., the channel loss cannot be larger than 50%, and thus cannot be applied in practical implementations. To beat the "3dB limit", post-selection strategy was combined with the coherent state based CV-QKD protocols [12]. In a post-selection strategy, the legitimate users Alice and Bob can always keep those bits with high effective information and discard the rest. Therefore, Bob can enjoy advantages over potential eavesdropper Eve even in a high path loss channel. Because no entanglement or squeezing was needed, coherent states based CV-QKD protocols enjoy good compatibility with existing optical communication infrastructure and thus have attracted increasing attentions [11].

The coherent receivers are usually used in post-selection based CV-QKD protocols [11]–[15]. However, the detection performance of classical coherent receivers is restricted by the SQL and can only be outperformed by using quantum receivers. Quantum receivers employ quantum detection theory to enhance the error rate performance of discriminating quantum states [27]. The closed-form solution for the optimal quantum detection of distinguishing any two quantum state was obtained by Helstrom [28], [29]. The first realizable quantum receiver for discriminating two binary phase shift keying (BPSK) modulated coherent states $\{|-\alpha\rangle, |\alpha\rangle\}$ is the Kennedy receiver proposed by

Kennedy [30], which consists of a displacement operation $\hat{D}(\beta)$ with $\beta = \alpha$ and an on/off photodetector. We called the quantum receivers based on Kennedy receiver's structure the *generalized Kennedy receivers*. In 1973, Dolinar proposed the Dolinar receiver by controlling the displacement value in a real-time way with a feedback loop [31], which was proved to be an optimal quantum receiving structure for discriminating coherent states.

However, due to the lack of fast processing devices and high-performance photodetectors, the first quantum receiver beating the SQL has not been realized until 2008 by Cook et al [32]. After then, the study of generalized Kennedy receiver has attracted increasing attention in recent decades. For example, in 2008, Takeoka et al proposed the optimized displacement receiver (ODR) [33], [34], where the displacement value β of $\hat{D}(\beta)$ was optimized to achieve a better performance compared with the Kennedy receiver. In 2010, Wittmann et al demonstrated a generalized Kennedy receiver by replacing the on/off photodetector with a photon-number-resolving detector (a type of photon counter) [22]. In 2014, Becerra et al demonstrated that by decreasing the phase mismatch error of the displacement operation, the detecting signal strength of generalized Kennedy receiver can be extended to practical optical communication scenarios with large photon numbers [35]. In 2018, DiMario et al experimentally demonstrated that the generalized Kennedy receiver can enjoy a robust performance in a noisy environment by combining a high-performance displacement operation and photon-number-resolving detector. In 2020, Yuan et al proposed the optimally displaced threshold detection (ODTD) based generalized Kennedy receiver, where both the displacement and the detection threshold are optimized to improve the detection performance, and theoretically quantified the influence of various types of noise and device imperfection on the ODTD receiver [36], [37]. Later in 2020, Yuan et al extended the ODTD to turbulent channels and proposed the conditionally-dynamic based Kennedy (CD-Kennedy) receiver to mitigate the influence of turbulence on the detection performance [38]. In 2023, Zhao et al extended the ODTD receiver to the ternary phase shift keying (TPSK) modulation [39] and future extended the ODTD receiver to the quadrature phase shift keying (QPSK) in 2024 [25].

The combination of generalized Kennedy receiver and the CV-QKD was first proposed in [22], where a photon-number-resolving detector was used to improve the performance of Kennedy receiver and the detector was applied in a post-selection based CV-QKD protocol. Based on this protocol, Zhao et al studied the secret key rate (SKR) performance of using the generalized Kennedy receiver when a thermal noise channel was considered [23], [24]. Besides, the SKR performance of the post-selection based CV-QKD protocol using a generalized Kennedy receiver for QPSK modulation was also studied in [25]. However, current studies [22]–[25] on CV-QKD with generalized Kennedy receiver are focusing on lossy channels without turbulence. As we know, the most important and also vulnerable links in space-air-ground integrated network are the satellite-to-ground links, where the atmospheric turbulence cannot be ignored. Therefore, it is meaningful to study the performance of CV-QKD protocol with generalized Kennedy receiver in turbulent channels.

C. Contributions

In this paper, we focused on the performance of post-selection based CV-QKD enhanced by using CD-Kennedy receivers in the presence of atmospheric turbulence. We first derive the bit-error rate (BER) expression of CD-Kennedy receiver with BPSK modulation in turbulent channels, where a $1\times$ N configuration using equal-gain

combining (EGC) method is employed. Then we drive the SKR expression of the binary modulated CV-QKD protocol by using CD-Kennedy receiver with a post-selection on both the detected number of photons and the measured channel transmittance. For comparison, we also derived the corresponding BER expression of homodyne receiver with EGC and the SKR expression of binary modulated CV-QKD protocol by using homodye receiver with a post-selection on both the detected amplitude and the measured channel transmittance. Numerical results demonstrate the BER performance of CD-Kennedy receiver is better than that of homodyne receiver when the average transmittance is large; while the SKR performance of CD-Kennedy receiver is better than that of homodyne receiver when the average transmittance is small. Besides, we also demonstrate that the SKR performance of CD-Kennedy receiver is much robust compared with that of homodyne receiver to the atmospheric turbulence. The major contribution of this work can be summarized as follows:

- We established the channel model and derived the BER of CD-Kennedy receiver under a $1 \times N$ configuration with EGC method in turbulent channels.
- We proposed the first post-selection based CV-QKD protocol with CD-Kennedy receiver for turbulent channels and derived the SKR expression.
- We proposed an equivalent transmittance method to simplify the calculation of both the BER and SKR for the CD-Kennedy receivers with EGC method.
- We demonstrate for the first time that the SKR performance advantage of using CD-Kennedy receiver over homodyne receiver becomes larger as the average transmittance decreases. Besides, the SKR performance of CD-Kennedy receiver is much robust than that of homodyne receiver in turbulent channels.
- We also find that BER and SKR performance advantage of CD-Kennedy receiver over homodyne receiver demonstrate opposite trends as the average transmittance increases, which indicates that two separate system settings should be employed for communication and key distribution purposes.

The rest of this paper is organized as follows: we first derive the BER of both the CD-Kennedy receiver and the homodyne receiver with EGC method for a $1 \times N$ configuration under turbulent channels in Section II; then we derive the SKR of a post-selection based CV-QKD protocol by using both the CD-Kennedy receiver and the homodyne receiver under turbulent channels in Section III; some numerical results on both the BER and SKR performance are presented in Section IV and we conclude our work in Section V.

II. CD-Kennedy receivers with equal-gain combining in turbulent channel

We consider a BPSK modulated communication system with N CD-Kennedy receivers in this paper, as shown in Fig. 1. The transmitted bit $A_l \in \{0, 1\}$ of the lth bit is encoded by a coherent state $|\beta_l\rangle$ with $\beta_l = -\beta$ for bit $A_l = 0$ and $\beta_l = \beta$ for bit $A_l = 1$. Without loss of generality, we adopt β as real number. After passing through a turbulent channel, the transmitted state is received by N receiving branches and the density operator of the signal arriving at the ith receiving branch is denoted by $\hat{\rho}_i^l$ with $i = 1, 2, \cdots, N$. We use N CD-Kennedy receivers, whose displacement value γ_i is dynamically conditioned on the average turbulent strength of the ith branch, to detect the received signals and the output numbers of photons at the ith photon counter (PC_i) is denoted by n_i. Then an

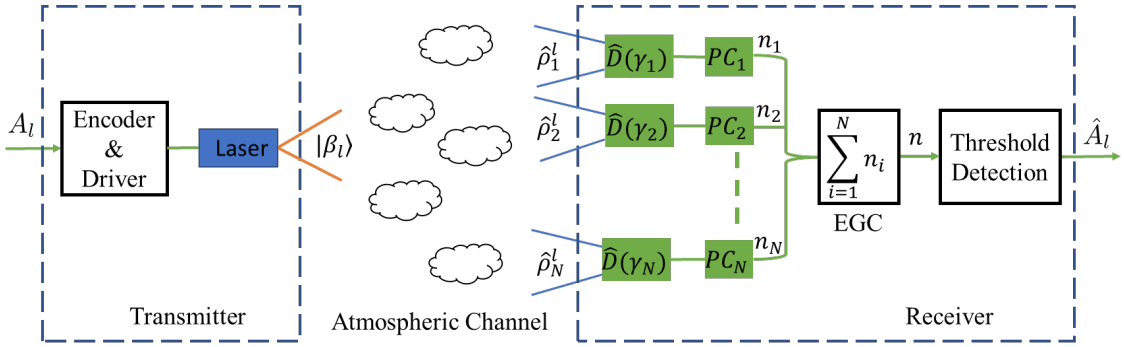


Fig. 1. Generalized Kennedy receivers with EGC in turbulent channel

EGC method is used to combine the output number of photons and the combined signal n is decided by a threshold detection to recover the transmitted bit $\hat{A}_l$.

A. Coherent states and P-representation

The quantum state of a laser signal can be expressed in a coherent state $|\alpha\rangle$ with $\alpha \in \mathbb{C}$ and $\mathbb{C}$ is the field of complex number. By using the Fock basis of the Hilbert space, which consists of all number states (or Fock states) $\{|n\rangle, n = 0, 1, 2, ...\}$, we can expand the coherent $|\alpha\rangle$ as [40]

$$|\alpha\rangle = \sum_{n=0}^{\infty} e^{-\frac{1}{2}|\alpha|^2} \frac{\alpha^n}{\sqrt{n!}} |n\rangle , \tag{1}$$

where $|\alpha|^2$ is the average number of photons contained in the coherent state $|\alpha\rangle$.

According to Glauber's theory, all the coherent states $\{|\alpha\rangle, \alpha \in \mathbb{C}\}$ form an overcomplete basis of Hilbert space; and therefore, any quantum state with a density operator $\hat{\rho}$ in this Hilbert space could be decomposed by coherent states as [40]

$$\hat{\rho} = \int_{\alpha} P(\alpha) |\alpha\rangle \langle\alpha| \, \mathrm{d}^2\alpha, \tag{2}$$

where $\mathrm{d}^2\alpha = \mathrm{d}Re(\alpha)\mathrm{d}Im(\alpha)$ and $P(\alpha)$ is the P-function of the density operator $\hat{\rho}$. This representation of density operator is called the P-representation [41]. Specifically, the P-function of a coherent state $|\beta_l\rangle$ can be expressed as a Dirac delta function

$$\delta^2(\alpha - \beta_l) \triangleq \delta\left(Re(\alpha) - Re(\beta_l)\right) \delta\left(Im(\alpha) - Im(\beta_l)\right). \tag{3}$$

Considering the configuration in Fig. 1, the transmitted signal $|\beta_l\rangle$ for the lth bit are directed to N separated receivers. Then the input state of the turbulent channel can be regarded as an N-mode coherent state with equal complex value $\alpha_1 = \alpha_2 = \cdots = \alpha_N \triangleq \frac{\beta_l}{\sqrt{N}}$. Then the P-function of the input state of the turbulent channel can be expressed by

$$P_{in}(\alpha_1, ..., \alpha_N) = \prod_{i=1}^{N} \delta^2 \left(\alpha_i - \frac{\beta_l}{\sqrt{N}}\right). \tag{4}$$

B. Relation between input and output P-functions in turbulent channel

The relation between the input and output P-functions of turbulent channel for a 1×1 configuration was first derived by Semenov [42], [43], and was later extend to a $1 \times N$ configuration by Yuan [38] as

$$P_{out}(\alpha_1, ..., \alpha_N) = \int_{\boldsymbol{\eta}} \frac{p(\boldsymbol{\eta})}{\eta_1 ... \eta_N} P_{in}(\frac{\alpha_1}{\sqrt{\eta_1}}, ..., \frac{\alpha_N}{\sqrt{\eta_N}}) \mathrm{d}\boldsymbol{\eta}, \tag{5}$$

where η_i is the transmittance of the ith branch; $p(\boldsymbol{\eta})$ is the joint probability density function (PDF) of all transmittance $\boldsymbol{\eta} \triangleq [\eta_1, \eta_2, \cdots, \eta_N]^{\mathrm{T}}$; $P_{in}(\alpha_1, \alpha_2, \cdots, \alpha_N)$ is the input P-function and $P_{out}(\alpha_1, \alpha_2, \cdots, \alpha_N)$ is the output P-function of the turbulent channel.

We adopt a log-normal distributed turbulent channel in this paper, where the PDF of the transmittance $\boldsymbol{\eta}$ satisfies the following joint log-normal PDF:

$$p(\boldsymbol{\eta}) = \frac{\exp\left(-\frac{1}{2}(\ln \boldsymbol{\eta} - \boldsymbol{\mu})^{\mathrm{T}} \Sigma^{-1} (\ln \boldsymbol{\eta} - \boldsymbol{\mu})\right)}{\prod_{i=1}^{N} \eta_i \sqrt{(2\pi)^N \det(\Sigma)}}, \tag{6}$$

where $\boldsymbol{\mu} = [\mu_1, \mu_1, \cdots, \mu_N]^{\mathrm{T}}$ is the expectation of $\ln \boldsymbol{\eta}$; Σ is the covariance matrix of $\ln \boldsymbol{\eta}$. Without loss of generality, we set $\mu_1 = \mu_2 = \cdots = \mu_N \triangleq \mu_0$ and assume that the correlation between arbitrary two branches are the same. Then the covariance matrix Σ can be expressed as

$$\Sigma = \sigma_0^2 \begin{bmatrix} 1 & \rho & \cdots & \rho \\ \rho & 1 & \cdots & \rho \\ \vdots & \vdots & \ddots & \vdots \\ \rho & \rho & \cdots & 1 \end{bmatrix}, \tag{7}$$

where σ_0^2 is the variance of η_i for $i = 1, 2, \cdots, N$ and ρ is the correlation coefficient between $\ln(\eta_i)$ and $\ln(\eta_j)$ for $i \neq j$, i.e.,

$$\rho \triangleq \frac{\mathrm{E}[\ln(\eta_i)\ln(\eta_j)] - \mathrm{E}[\ln(\eta_i)]\mathrm{E}[\ln(\eta_j)]}{\sqrt{\mathrm{Var}[\ln(\eta_i)]\mathrm{Var}[\ln(\eta_j)]}}. \tag{8}$$

Therefore, the average transmittances of all branches are the same with each other, i.e., $\mathrm{E}[\eta_1] = \mathrm{E}[\eta_2] = \cdots = \mathrm{E}[\eta_N] \triangleq \eta_0$, where η_0 can be obtained as

$$\eta_0 = \exp\left(\mu_0 + 0.5\sigma_0^2\right). \tag{9}$$

Substituting (4) into (5), we can obtain the output P-function of the turbulent channel as [38]

$$\begin{aligned} P_{out}(\alpha_1, ..., \alpha_N) =& (2N)^N \prod_{i=1}^{N} \left[\frac{\alpha_i}{\beta_l} \delta(Im(\alpha_i)Re(\beta_l) - Re(\alpha_i)Im(\beta_l))\right] \\ & \times p_{tur}\left(N|\frac{\alpha_1}{\beta_l}|^2, N|\frac{\alpha_2}{\beta_l}|^2, \cdots, N|\frac{\alpha_N}{\beta_l}|^2\right). \end{aligned} \tag{10}$$

Consider the ith branch, the P-function can be obtained as

$$\begin{aligned} P_{out}(\alpha_i) &= \int_{\alpha_j \neq \alpha_i} P_{out}(\alpha_1, ..., \alpha_N) \prod_{j \neq i}^{N} \mathrm{d}^2 \alpha_j \\ &= \int_{\eta_i} \frac{p_{tur}(\eta_i)}{\eta_i} \delta^2\left(\frac{\alpha_i}{\sqrt{\eta_i}} - \frac{\beta_l}{\sqrt{N}}\right) \mathrm{d}\eta_i, \end{aligned} \tag{11}$$

where $p_{tur}(\eta_i)$ is the marginal PDF of η_i obtained from $p_{tur}(\eta_i) = \int_{\eta_j \neq \eta_i} p_{tur}(\boldsymbol{\eta}) \prod_{j \neq i}^{N} \mathrm{d}\eta_j$.

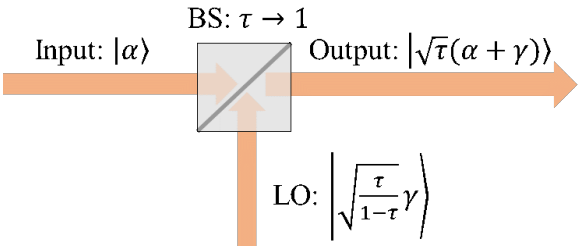


Fig. 2. Displacement operator in practical implementation

C. CD-Kennedy receivers with EGC in turbulent channels

1) CD-Kennedy receivers with EGC: We adopt the CD-Kennedy receiver structure proposed in [38] to mitigate the influence of turbulence, where the displacement value γ_i of the ith branch is dynamically conditioned on the transmittance η_i and the latter is estimated by pilot bits under slow-varying turbulent channels [26], [38]. Under this context, for a given time period, the transmittance on the ith branch can be regarded as a fixing value η_i. Then the P-function of the ith branch given transmittance η_i and transmitted signal $|\beta_l\rangle$ can be obtained as

$$\begin{aligned} P_{out}(\alpha_i|\eta_i,\beta_l) &= \frac{1}{\eta_i}\delta^2\left(\frac{\alpha_i}{\sqrt{\eta_i}}-\frac{\beta_l}{\sqrt{N}}\right) \\ &= \delta^2\left(\alpha_i-\frac{\sqrt{\eta_i}\beta_l}{\sqrt{N}}\right), \end{aligned} \tag{12}$$

which corresponds to a coherent state $|\frac{\sqrt{\eta_i}\beta_l}{\sqrt{N}}\rangle$.

Then according to principle of generalized Kennedy receiver, we can use a displacement operator $\hat{D}(\gamma_i)$ with $\gamma_i = \frac{\sqrt{\eta_i}\beta}{\sqrt{N}}$ to displace the input state $|\frac{\sqrt{\eta_i}\beta_l}{\sqrt{N}}\rangle$ and use a photon-number resolving detector to detect the number of photons of the ith displaced state.

The displacement operation $\hat{D}(\gamma)$ can displace any coherent state $|\alpha\rangle$ to another coherent state $\hat{D}(\gamma)|\alpha\rangle = |\alpha+\gamma\rangle$. In practical implementation, the displacement operator can be achieved by combining the input coherent state with an local oscillator (LO) using a high transmittance beamsplitter (BS), as shown in Fig. 2. By using a BS with transmittance $\tau \to 1$ to combine the input coherent state $|\alpha_{in}\rangle = |\alpha\rangle$ and an LO state $|\alpha_{LO}\rangle = |\sqrt{\frac{\tau}{1-\tau}}\gamma\rangle$, we can obtain the output coherent state $|\alpha_{out}\rangle$ according to the property of the BS as

$$\begin{aligned} |\alpha_{out}\rangle &= |\sqrt{\tau}\alpha_{in}+\sqrt{1-\tau}\alpha_{LO}\rangle \\ &= |\sqrt{\tau}(\alpha+\gamma)\rangle, \end{aligned} \tag{13}$$

which will become the coherent state $|\alpha+\gamma\rangle$ as $\tau \to 1$.

Under this context, the detection probability of n_i photons at the ith branch given η_i and transmitted signal $|\beta_l\rangle$ can be obtained as a Poisson distribution:

$$p(n_i|\eta_i,\beta_l) = \frac{\exp\left(-\left|\frac{\sqrt{\eta_i}(\beta_l+\beta)}{\sqrt{N}}\right|^2\right)}{n_i!}\left|\frac{\sqrt{\eta_i}(\beta_l+\beta)}{\sqrt{N}}\right|^{2n_i}. \tag{14}$$

The output photon numbers are combined using the EGC combining with total output photon numbers given by

$$n = \sum_{i=1}^{N} n_i. \tag{15}$$

Because n_i satisfies Poisson distribution and the detection on each branches are independent with each other, the total output photon numbers n given transmittance $\boldsymbol{\eta}$ and transmitted signal $|\beta_l\rangle$ also satisfies a Poisson distribution with probability density given by

$$p(n|\boldsymbol{\eta}, \beta_l) = \frac{\exp\left(-\sum_{i=1}^{N}\left|\frac{\sqrt{\eta_i}(\beta_l+\beta)}{\sqrt{N}}\right|^2\right)}{n!}\left(\sum_{i=1}^{N}\left|\frac{\sqrt{\eta_i}(\beta_l+\beta)}{\sqrt{N}}\right|^2\right)^n. \tag{16}$$

A maximum a posteriori (MAP) decision rule is used to decide the received bit as

$$\hat{A}_l = \begin{cases} 0, & p_0 p(n|\boldsymbol{\eta}, -\beta) \geq p_1 p(n|\boldsymbol{\eta}, \beta), \\ 1, & p_0 p(n|\boldsymbol{\eta}, -\beta) < p_1 p(n|\boldsymbol{\eta}, \beta), \end{cases} \tag{17}$$

where p_0 and p_1 are the prior probabilities for transmitting bit 0 and 1, respectively. We consider equal prior probabilities in this work; then the above MAP decision rule will reduced to the following threshold detection as

$$\hat{A}_l = \begin{cases} 0, & n = 0, \\ 1, & n > 0. \end{cases} \tag{18}$$

From (18) we can see that the detection can be achieved by simple on/off photodetectors instead of expensive photon counters. Then the error probability of the CD-Kennedy receiver given transmittance $\boldsymbol{\eta}$ can be obtained as

$$P_e(\boldsymbol{\eta}) = \frac{1}{2}\exp\left(-\frac{4\beta^2}{N}\sum_{i=1}^{N}\eta_i\right). \tag{19}$$

Finally, the unconditional error probability over the turbulent channel can be expressed as

$$P_e = \frac{1}{2}\int_{\boldsymbol{\eta}} p(\boldsymbol{\eta})\exp\left(-\frac{4\beta^2}{N}\sum_{i=1}^{N}\eta_i\right)\mathrm{d}\boldsymbol{\eta}, \tag{20}$$

where $\mathrm{d}\boldsymbol{\eta} \triangleq \mathrm{d}\eta_1\mathrm{d}\eta_2\cdots\mathrm{d}\eta_N$.

It is challenging to calculate (20) because it contains a N-tuple integral. However, by observing the expression of P_e in (20), we can see that η_i appears as an integrated term $\sum_{i=1}^{N}\eta_i$. Therefore, we can define an equivalent transmittance variable $\eta_{eq} \triangleq \sum_{i=1}^{N}\eta_i$ and rewrite (20) as

$$P_e = \frac{1}{2}\int_{\eta_{eq}} p(\eta_{eq})\exp\left(-\frac{4\beta^2}{N}\eta_{eq}\right)\mathrm{d}\eta_{eq}, \tag{21}$$

where $p(\eta_{eq})$ is the PDF of η_{eq}.

Since η_{eq} is a summation of N correlated log-normal random variables, we can approximate η_{eq} as another log-normal random variable by using the Fenton-Wilkinson method [44]. Specifically, η_{eq} can be approximated as a log-normal variable, i.e., $\eta_{eq} \sim LN(\mu_{eq}, \sigma_{eq}^2)$, where the parameters μ_{eq} and σ_{eq}^2 subject to the following two constrains:

$$\begin{cases} \int_{\eta_{eq}} \eta_{eq} p(\eta_{eq})\mathrm{d}\eta_{eq} = \int_{\boldsymbol{\eta}}(\sum_{i=1}^{N}\eta_i)p(\boldsymbol{\eta})\mathrm{d}\boldsymbol{\eta} \\ \int_{\eta_{eq}} \eta_{eq}^2 p(\eta_{eq})\mathrm{d}\eta_{eq} = \int_{\boldsymbol{\eta}}(\sum_{i=1}^{N}\eta_i)^2 p(\boldsymbol{\eta})\mathrm{d}\boldsymbol{\eta}. \end{cases} \tag{22}$$

After some algebra (see A), we can obtain μ_{eq} and σ_{eq}^2 as

$$\begin{cases} \mu_{eq} = 1.5\ln N + \mu_0 - 0.5\ln\left(1+(N-1)\exp\left((\rho-1)\sigma_0^2\right)\right), \\ \sigma_{eq}^2 = -\ln N + \sigma_0^2 + \ln\left(1+(N-1)\exp\left((\rho-1)\sigma_0^2\right)\right). \end{cases} \tag{23}$$

2) Homodyne receivers with EGC: We use the homodyne receivers as the comparison. Then the output x_i of the ith branch given transmittance η_i and transmitted signal $|\beta_l\rangle$ can be equivalently modeled as a Gaussian distributed random variable with PDF given by

$$p(x_i|\eta_i,\beta_l) = \sqrt{\frac{2}{\pi}}\exp\left(-2\left(x_i - \frac{\sqrt{\eta_i}\beta_l}{\sqrt{N}}\right)^2\right). \tag{24}$$

After EGC combining, the total output $x = \sum_{i=1}^{N} x_i$ given transmittance $\boldsymbol{\eta}$ and transmitted signal $|\beta_l\rangle$ also satisfies a Gaussian distribution with PDF given by

$$p(x|\boldsymbol{\eta},\beta_l) = \sqrt{\frac{2}{N\pi}}\exp\left(-\frac{2}{N}\left(x - \sum_{i=1}^{N}\frac{\sqrt{\eta_i}\beta_l}{\sqrt{N}}\right)^2\right). \tag{25}$$

Similar to the CD-Kennedy receiver, when an MAP decision rule is adopted, the decision is equivalent to the following threshold detection as

$$\hat{A}_l = \begin{cases} 0, & x \le 0, \\ 1, & x > 0. \end{cases} \tag{26}$$

Similarly, the unconditional error probability of homodyne receiver over turbulent channel can be obtained as

$$P_e^{hd} = \int_{\boldsymbol{\eta}} p(\boldsymbol{\eta}) Q\left(\sqrt{\frac{4\beta^2}{N^2}\left(\sum_{i=1}^{N}\sqrt{\eta_i}\right)^2}\right)\mathrm{d}\boldsymbol{\eta}, \tag{27}$$

where $Q(x)$ is the Q-function defined as $Q(x) \triangleq \frac{1}{\sqrt{2\pi}}\int_0^x \exp\left(-0.5t^2\right)\mathrm{d}t$.

Similarly, by observing the expression of $S_{kr}^{hd}(\beta)$ in (49), we can see that η_i always appears as an integrated term $\sum_{i=1}^{N}\sqrt{\eta_i}$. Therefore, we can define an equivalent transmittance variable $\eta_{eq}^{hd} \triangleq \sum_{i=1}^{N}\sqrt{\eta_i}$ and rewrite P_e^{hd} as

$$P_e^{hd} = \int_{\eta_{eq}^{hd}} p(\eta_{eq}^{hd}) Q\left(\sqrt{\frac{4\beta^2}{N^2}\left(\eta_{eq}^{hd}\right)^2}\right)\mathrm{d}\eta_{eq}^{hd}, \tag{28}$$

where $p(\eta_{eq}^{hd})$ is the PDF of η_{eq}^{hd}.

Since η_{eq}^{hd} is a summation of N correlated log-normal random variables $\{\sqrt{\eta_1},\sqrt{\eta_2},\cdots,\sqrt{\eta_N}\}$, we can also approximate η_{eq}^{hd} as another log-normal random variable by using the Fenton-Wilkinson method. Similar to the derivation for the η_{eq}, we can obtain the parameters $\mu_{eq,hd}$ and $\sigma_{eq,hd}^2$ as (see B)

$$\begin{cases} \mu_{eq,hd} = 1.5\ln N + 0.5\mu_0 - 0.5\ln\left(1+(N-1)\exp\left(0.25(\rho-1)\sigma_0^2\right)\right), \\ \sigma_{eq,hd}^2 = -\ln N + 0.25\sigma_0^2 + \ln\left(1+(N-1)\exp\left(0.25(\rho-1)\sigma_0^2\right)\right). \end{cases} \tag{29}$$

III. Post-selection based CV-QKD with CD-Kennedy receiver in turbulent channel

The coherent states are widely used in CV-QKD protols, where two legitimate users Alice and Bob use the coherent states to distribute secure keys over a public channel in the presence of potential eavesdropper Eve. In this section, we study the binary modulated CV-QKD protocol based on post-selection strategy by using CD-Kennedy receiver in turbulent channels.

A. Binary modulated CV-QKD

A typical binary modulated CV-QKD protocol consists of the following steps:

- Step 1: Alice randomly sends $|-\beta\rangle$ (bit 0) or $|\beta\rangle$ (bit 1) to Bob over a public channel;
- Step 2: Bob measures the received state and decides the transmitted bit;
- Step 3: Alice and Bob compare part of their bit strings and estimate the mutual information I_{AB} between them and the mutual information I_{AE} between Alice and Eve;
- Step 4: Alice and Bob perform the information reconciliation using error correction methods;
- Step 5: Alice and Bob perform the privacy amplification to extract at most $\Delta I = I_{AB} - I_{AE}$ bits of secret key.

The crucial step of the protocol is the estimate the mutual information I_{AB} and I_{AE}. In the following we derive I_{AB} and I_{AE} over a turbulent channel when a CD-Kennedy receiver is used by Bob.

B. Mutual information I_{AB} between Alice and Bob

1) I_{AB} with CD-Kennedy receivers: We follow the procedure developed in [12] to derive the mutual information I_{AB} for a transmitted signal amplitude β, where the channel is divided into many effective information channels characterized by the parameters $(n, \boldsymbol{\eta}, \beta)$ with

$$I_{AB}(\beta) = \int_{\boldsymbol{\eta}} \sum_{n=0}^{\infty} p(\boldsymbol{\eta}) p(n|\boldsymbol{\eta}) I_{AB}(n, \boldsymbol{\eta}, \beta) \mathrm{d}\boldsymbol{\eta}, \tag{30}$$

where $I_{AB}(n, \boldsymbol{\eta}, \beta)$ is the effective information given the detected number of photons n, the measured transmittance $\boldsymbol{\eta}$, and the transmitted signal amplitude β; $p(n|\boldsymbol{\eta})$ is the probability of detecting n photons given transmittance $\boldsymbol{\eta}$ at the receiver, which can be obtained by

$$\begin{aligned} p(n|\boldsymbol{\eta}) &= \frac{1}{2} p(n|\boldsymbol{\eta}, -\beta) + \frac{1}{2} p(n|\boldsymbol{\eta}, \beta) \\ &= \frac{1}{2} 0^n + \frac{1}{2} \frac{\exp\left(-4\beta^2 \sum_{i=1}^{N} \eta_i / N\right)}{n!} \left(4\beta^2 \sum_{i=1}^{N} \eta_i / N\right)^n. \end{aligned} \tag{31}$$

For every detected number of photons n, Bob make a decision on the transmitted bit according to the decision rule given in (18); then the error rate of this decision can be obtained as

$$p_e(n, \boldsymbol{\eta}, \beta) = \begin{cases} \frac{p(n|\boldsymbol{\eta}, \beta)}{p(n|\boldsymbol{\eta}, \beta) + p(n|\boldsymbol{\eta}, -\beta)}, & n = 0, \\ \frac{p(n|\boldsymbol{\eta}, -\beta)}{p(n|\boldsymbol{\eta}, \beta) + p(n|\boldsymbol{\eta}, -\beta)}, & n > 0, \end{cases} \tag{32}$$

where $p(n|\boldsymbol{\eta},\beta_l)$ is given in (16). Then the effective information $I_{AB}(n,\boldsymbol{\eta},\beta)$ can be obtained as

$$\begin{aligned} I_{AB}(n,\boldsymbol{\eta},\beta) &= 1-H(p_e(n,\boldsymbol{\eta},\beta)) \\ &= 1-H\left(\frac{0^n}{\exp\left(-4\beta^2\sum_{i=1}^N\eta_i/N\right)\left(4\beta^2\sum_{i=1}^N\eta_i/N\right)^n/n!+0^n}\right), \end{aligned} \tag{33}$$

where $H(p_e)\triangleq -p_e\log_2 p_e-(1-p_e)\log_2(1-p_e)$ is the entropy of the effective information channel.

2) I_{AB} with homodyne receivers: For comparison, here we give the mutual information between Alice and Bob when a homodyne receiver is employed, i.e.,

$$I_{AB}^{hd}(\beta)=\int_{\boldsymbol{\eta}}\int_x p(\boldsymbol{\eta})p(x|\boldsymbol{\eta})I_{AB}^{hd}(x,\boldsymbol{\eta},\beta)\mathrm{d}\boldsymbol{\eta}\mathrm{d}x, \tag{34}$$

where $p(x|\boldsymbol{\eta})$ is the probability of output x given transmittance $\boldsymbol{\eta}$ and $I_{AB}^{hd}(x,\boldsymbol{\eta},\beta)$ is the effective information given output x, transmittance $\boldsymbol{\eta}$, and signal amplitude β.

By using eq. (25), we can obtain $p(x|\boldsymbol{\eta})$ as

$$\begin{aligned} p(x|\boldsymbol{\eta}) &= \frac{1}{2}p(x|\boldsymbol{\eta},-\beta)+\frac{1}{2}p(x|\boldsymbol{\eta},\beta) \\ &= \frac{1}{2}\sqrt{\frac{2}{N\pi}}\left[\exp\left(-\frac{2}{N}\left(x+\frac{\beta}{\sqrt{N}}\sum_{i=1}^N\sqrt{\eta_i}\right)^2\right)\right. \\ &\qquad \left.+\exp\left(-\frac{2}{N}\left(x-\frac{\beta}{\sqrt{N}}\sum_{i=1}^N\sqrt{\eta_i}\right)^2\right)\right]. \end{aligned} \tag{35}$$

Similar to the CD-Kennedy receiver, the error probability when an output x is measured given transmittance $\boldsymbol{\eta}$ and signal amplitude β can be obtained as

$$p_e(x,\boldsymbol{\eta},\beta)=\begin{cases}\frac{p(x|\boldsymbol{\eta},\beta)}{p(n|\boldsymbol{\eta},\beta)+p(x|\boldsymbol{\eta},-\beta)}, & x\le 0,\\ \frac{p(x|\boldsymbol{\eta},-\beta)}{p(n|\boldsymbol{\eta},\beta)+p(x|\boldsymbol{\eta},-\beta)}, & x>0.\end{cases} \tag{36}$$

Then the effective information $I_{AB}^{hd}(x,\boldsymbol{\eta},\beta)$ for homodyne receiver can be obtained as

$$\begin{aligned} I_{AB}^{hd}(x,\boldsymbol{\eta},\beta) &= 1-H(p_e(x,\boldsymbol{\eta},\beta)) \\ &= 1-H\left(\frac{1}{\exp\left(-8x\beta\sum_{i=1}^N\sqrt{\eta_i}/N^{3/2}\right)+1}\right). \end{aligned} \tag{37}$$

C. Mutual information I_{AE} between Alice and Eve

The mutual information between Alice and Eve depends on the attack methods of Eve. For a channel with negligible excess noise, the best eavesdropping strategy of Eve is the passive beamsplitter attack [45], [46]. In a turbulent channel, we further assume that Eve can split the beam near the transmitter and thus Eve can safely split $(1-\bar{\eta})$ quantity of the beam energy without being discovered, where $\bar{\eta}=N\eta_0$ is the average beam energy detected by the receiver. Then Eve has to discriminate two coherent states

$$\left\{|-\sqrt{1-\bar{\eta}}\beta\rangle\,,|\sqrt{1-\bar{\eta}}\beta\rangle\right\}. \tag{38}$$

For an individual attack, Eve decides each bit individually, then the minimum error rate of Eve is obtained by the Helstrom's theory as [28], [29]

$$p_e(\beta) = \frac{1}{2}\left(1 - \sqrt{1-|f|^2}\right), \tag{39}$$

where $f \triangleq \langle -\sqrt{1-\bar{\eta}}\beta | \sqrt{1-\bar{\eta}}\beta \rangle = e^{-2(1-N\eta_0)\beta^2}$.

Then the mutual information I_{AE} under individual attack can be obtained by

$$\begin{aligned} I_{AE}(\beta) &= 1 - H(p_e(\beta)) \\ &= \frac{1}{2}(1-\sqrt{1-f^2})\log_2(1-\sqrt{1-f^2}) \\ &\quad + \frac{1}{2}(1+\sqrt{1-f^2})\log_2(1+\sqrt{1-f^2}). \end{aligned} \tag{40}$$

For a collective attack, Eve can collect the splitted bits and make decision over all collected bits. Then the mutual information I_{AE} is given by the Holevo bound as

$$I_{AE}(\beta) = 1 - \frac{1}{2}(1-f)\log_2(1-f) - \frac{1}{2}(1+f)\log_2(1+f). \tag{41}$$

D. Post-selection strategy in turbulent channel

1) Post-selection strategy for CD-Kennedy receivers: Because Bob can only access to $\bar{\eta}$ quantity of the transmitted beam energy, as long as $\bar{\eta} < 0.5$, Eve can always access more knowledge of the transmitted bits, which lead to the "3dB loss limit" of the binary modulated CV-QKD protocol [11]. To achieve an advantage over Eve, Bob can only save those bits with higher effective information $I_{AB}(n, \boldsymbol{\eta}, \beta)$ than I_{AE} and discard those bits with lower effective information. This is the so called post-selection strategy for beating the 3dB loss limit, which is first proposed in [12].

For a turbulent channel, Bob can save those bits with $I_{AB}(n, \boldsymbol{\eta}, \beta) \geq I_{AE}(\beta)$, which corresponds to a post-selection area $\mathbf{A_{ps}}$ defined as

$$\mathbf{A_{ps}} = \{(n, \boldsymbol{\eta}) | I_{AB}(n, \boldsymbol{\eta}, \beta) \geq I_{AE}(\beta)\}. \tag{42}$$

Then the secret key rate for a given transmitted signal amplitude β can be obtained as

$$S_{kr}(\beta) = \int_{\mathbf{A_{ps}}} p(n|\boldsymbol{\eta}) p(\boldsymbol{\eta}) (I_{AB}(n, \boldsymbol{\eta}, \beta) - I_{AE}(\beta)) \mathrm{d}\boldsymbol{\eta}. \tag{43}$$

It is challenging to find the post-selection area $\mathbf{A_{ps}}$ directly because $\mathbf{A_{ps}}$ is a $(N+1)$-dimensional area. However, by observing the expression of $S_{kr}(\beta)$ in (43), we can see that η_i always appears as an integrated term $\sum_{i=1}^{N} \eta_i$. Therefore, similar to the calculation of the error probability, we can define an equivalent transmittance variable $\eta_{eq} \triangleq \sum_{i=1}^{N} \eta_i$ and rewrite $S_{kr}(\beta)$ as

$$S_{kr}(\beta) = \int_{\mathbf{A_{ps,eq}}} p(\eta_{eq}) p(n|\eta_{eq}) (I_{AB}(n, \eta_{eq}, \beta) - I_{AE}(\beta)) \mathrm{d}\eta_{eq}, \tag{44}$$

where $p(n|\eta_{eq})$ and $I_{AB}(n, \eta_{eq}, \beta)$ are defined as

$$\begin{cases} p(n|\eta_{eq}) \triangleq \frac{1}{2}\left[0^n + \exp\left(-\frac{4\beta^2}{N}\eta_{eq}\right)\left(\frac{4\beta^2}{N}\eta_{eq}\right)^n / n!\right] \\ I_{AB}(n, \eta_{eq}, \beta) \triangleq 1 - H\left(\frac{0^n}{\exp\left(-\frac{4\beta^2}{N}\eta_{eq}\right)\left(\frac{4\beta^2}{N}\eta_{eq}\right)^n / n! + 0^n}\right). \end{cases} \tag{45}$$

Then the post-selection area $\mathbf{A_{ps}}$ becomes an equivalent post-selection area $\mathbf{A_{ps,eq}}$ with only two dimensions n and η_{eq}:

$$\mathbf{A_{ps,eq}} = \{(n, \eta_{eq}) | I_{AB}(n, \eta_{eq}, \beta) \geq I_{AE}(\beta)\}. \tag{46}$$

Substituting eqs. (45) and (23) into (44), we can obtain the secret key rate as

$$\begin{aligned} S_{kr}(\beta) = \frac{1}{2} \int_{\mathbf{A_{ps,eq}}} p(\eta_{eq}) \left[0^n + \frac{\exp\left(-\frac{4\beta^2}{N}\eta_{eq}\right)\left(\frac{4\beta^2}{N}\eta_{eq}\right)^n}{n!} \right] \\ \times \left[1 - H\left(\frac{0^n}{\frac{\exp\left(-\frac{4\beta^2}{N}\eta_{eq}\right)\left(\frac{4\beta^2}{N}\eta_{eq}\right)^n}{n!} + 0^n} \right) - I_{AE}(\beta) \right] \mathrm{d}\eta_{eq}. \end{aligned} \tag{47}$$

2) Post-selection strategy for homodyne receivers: Here we present the post-selection strategy for homodyne receivers with EGC in turbulent channel. Similar to the CD-Kennedy receivers, Bob can save those bits with $I_{AB}^{hd}(x, \boldsymbol{\eta}, \beta) \geq I_{AE}(\beta)$, which corresponds to a post-selection area $\mathbf{A_{ps}^{hd}}$ defined as

$$\mathbf{A_{ps}^{hd}} = \{(x, \boldsymbol{\eta}) | I_{AB}^{hd}(x, \boldsymbol{\eta}, \beta) \geq I_{AE}(\beta)\}. \tag{48}$$

Then the secret key rate for a given transmitted signal amplitude β can be obtained as

$$S_{kr}^{hd}(\beta) = \int_{\mathbf{A_{ps}^{hd}}} p(x|\boldsymbol{\eta}) p(\boldsymbol{\eta}) (I_{AB}^{hd}(x, \boldsymbol{\eta}, \beta) - I_{AE}(\beta)) \mathrm{d}\boldsymbol{\eta} \mathrm{d}x. \tag{49}$$

Similarly, by observing the expression of $S_{kr}^{hd}(\beta)$ in (49), we can see that η_i always appears as an integrated term $\sum_{i=1}^{N} \sqrt{\eta_i}$. Therefore, we can define an equivalent transmittance variable $\eta_{eq}^{hd} \triangleq \sum_{i=1}^{N} \sqrt{\eta_i}$ and rewrite $S_{kr}^{hd}(\beta)$ as

$$S_{kr}^{hd}(\beta) = \int_{\mathbf{A_{ps,eq}^{hd}}} p(\eta_{eq}^{hd}) p(x|\eta_{eq}^{hd}) (I_{AB}^{hd}(x, \eta_{eq}^{hd}, \beta) - I_{AE}(\beta)) \mathrm{d}\eta_{eq}^{hd} \mathrm{d}x., \tag{50}$$

where $p(x|\eta_{eq}^{hd})$ and $I_{AB}^{hd}(x, \eta_{eq}^{hd}, \beta)$ are defined as

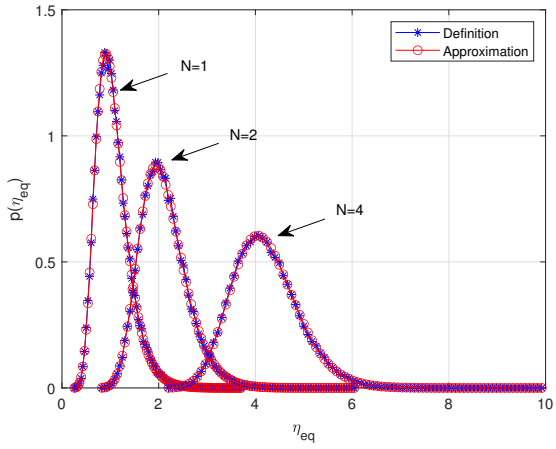
$$\begin{cases} p(x|\eta_{eq}^{hd}) \triangleq \frac{1}{2}\sqrt{\frac{2}{N\pi}} \left[\exp\left(-\frac{2}{N}\left(x + \frac{\beta}{\sqrt{N}}\eta_{eq}^{hd} \right)^2 \right) \right. \\ \qquad\qquad \left. + \exp\left(-\frac{2}{N}\left(x - \frac{\beta}{\sqrt{N}}\eta_{eq}^{hd} \right)^2 \right) \right]. \\ I_{AB}^{hd}(x, \eta_{eq}^{hd}, \beta) \triangleq 1 - H\left(\frac{1}{\exp\left(-8x\beta\eta_{eq}^{hd}/N^{3/2}\right)+1} \right); \end{cases} \tag{51}$$

and $p(\eta_{eq}^{hd})$ is the PDF of η_{eq}^{hd}. Then the post-selection area $\mathbf{A_{ps}}$ becomes an equivalent post-selection area $\mathbf{A_{ps,eq}^{hd}}$ with only two dimensions x and η_{eq}^{hd}:

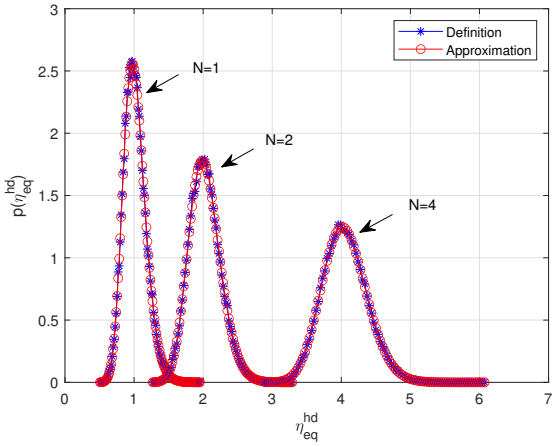
$$\mathbf{A_{ps,eq}^{hd}} = \left\{(x, \eta_{eq}^{hd}) | I_{AB}^{hd}(x, \eta_{eq}^{hd}, \beta) \geq I_{AE}(\beta)\right\}. \tag{52}$$

Substituting eqs. (51) and (29) into (50), we can obtain the secret key rate of homodyne receivers as

$$\begin{aligned} & S_{kr}^{hd}(\beta) \\ & = \frac{1}{2}\sqrt{\frac{2}{N\pi}} \int_{\mathbf{A_{ps,eq}^{hd}}} p(\eta_{eq}^{hd}) \left[1 - H\left(\frac{1}{\exp\left(-8x\beta\eta_{eq}^{hd}/N^{3/2}\right)+1} \right) \right] \\ & \quad \times \left[\exp\left(-\frac{2}{N}\left(x + \frac{\beta}{\sqrt{N}}\eta_{eq}^{hd} \right)^2 \right) + \exp\left(-\frac{2}{N}\left(x - \frac{\beta}{\sqrt{N}}\eta_{eq}^{hd} \right)^2 \right) \right] \mathrm{d}\eta_{eq}^{hd} \mathrm{d}x. \end{aligned} \tag{53}$$



(a)



(b)

Fig. 3. PDF comparison between the definition and approximation of equivalent transmittance: (a) PDF of η_{eq}; (b) PDF of η_{eq}^{hd}

IV. Numerical Results

In this section we present some numerical results to explore both the BER and the SKR performance of CD-Kennedy receiver with EGC in turbulent channels. The homodyne receiver is employed as the comparison scheme. Unless otherwise specified, we set the average signal photons $|\beta|^2 = 2$, number of branches $N = 4$, turbulent strength $\sigma_0^2 = 0.1$, and turbulent correlation coefficient $\rho = 0$.

We first verify the feasibility of using approximated equivalent transmittances η_{eq} and η_{eq}^{hd} by Fenton-Wilkinson method. Figs. 3(a) and 3(b) present the PDF of η_{eq} and η_{eq}^{hd} under different number of branches with $N = 1, 2, 4$, respectively. From Figs. 3(a) and 3(b), we can observe that the PDF approximations of both η_{eq} and η_{eq}^{hd} by using Fenton-Wilkinson method can well match those of the definitions. Besides, the results in Figs. 3(a) and 3(b) also verify the correctness of our derivation in (23) and (29).

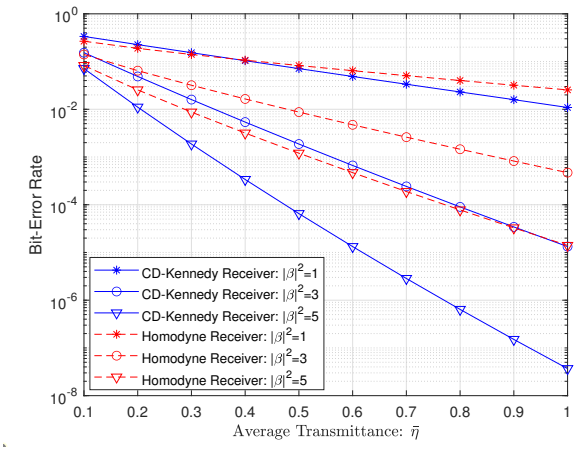


Fig. 4. BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels under different transmitting signal strength $|\beta|^2$

A. Bit-error rate comparison

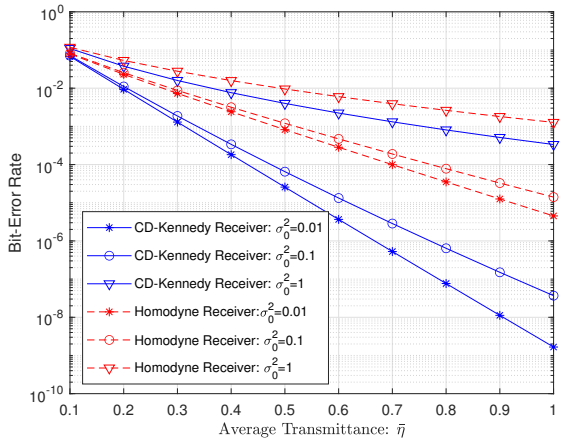
We then present the BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different transmitting signal strength $|\beta|^2$ in Fig. 4. From Fig. 4, we can see that the BER performance of CD-Kennedy receiver with EGC is better than that of homodyne receiver in turbulent channels when the signal strength $|\beta|^2$ is large. Besides, for a given signal strength, e.g., when $|\beta|^2 > 1$, the performance advantage of CD-Kennedy receiver over homodyne receiver increases as average transmittance $\bar{\eta}$ increases.

Then we present the BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different turbulent conditions, where Figs. 5(a) and 5(b) show the BER comparison under different turbulent strength σ_0^2 and different correlation coefficient ρ, respectively. From Figs. 5(a) and 5(b) we can see that the BER performance of CD-Kennedy receiver with EGC is better than that of homodyne receiver in turbulent channels when the average transmittance $\bar{\eta}$ is large. Besides, the advantage of CD-Kennedy receiver with EGC over homodyne receiver becomes large as the average transmittance $\bar{\eta}$ increases.

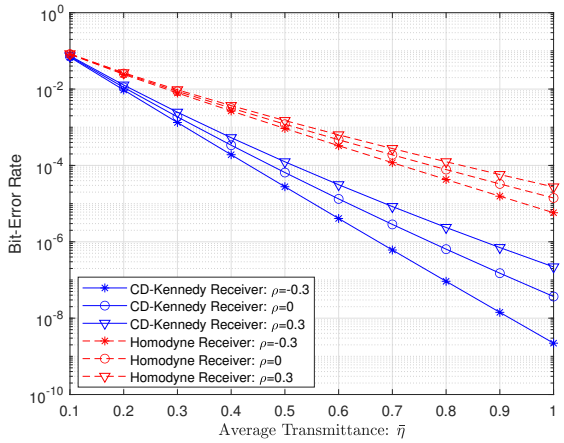
Then we present the BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different number of receivers N in Fig. 6. From Fig. 6, we can see that the BER performance of CD-Kennedy receiver is better than that of homodyne receiver. Besides, we can also see that the BER performance of both CD-Kennedy receiver and homodyne receiver improves as the number of branches increases, which indicates a receiving diversity gain is achieved.

B. Secret key rate comparison

Then we present the SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different transmitting signal strength $|\beta|^2$ in Fig. 7. From Fig. 7, we can observe that for a given channel average transmittance, different transmitting signal strength $|\beta|^2$ can result in different SKR, which indicates there exits an optimum transmitting signal strength for a given average transmittance.



(a)



(b)

Fig. 5. BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels: (a) Different turbulent strength σ_0^2; (b) Different correlation coefficient ρ

Then we present the SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different turbulent conditions in Fig. 8, where Figs. 8(a) and 8(b) show the SKR comparison under different turbulent strength σ_0^2 and different correlation coefficient ρ, respectively. From Figs. 8(a) and 8(b), we can see that the SKR performance of CD-Kennedy receiver is much robust than the homodyne receiver in turbulent channels. Besides, we can also see that, the SKR performance advantage of CD-Kennedy receiver over homodyne receiver increases as the average transmittance decreases, which demonstrate an opposite trend compared with the BER performance cases. This is because in a post-selection strategy, the more uncertainty of the channel, the more chance a better effective information can be achieved.

Then we present the SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels at different number of receivers N in Fig. 9. From 9 we can see that the SKR performance of post-selection based

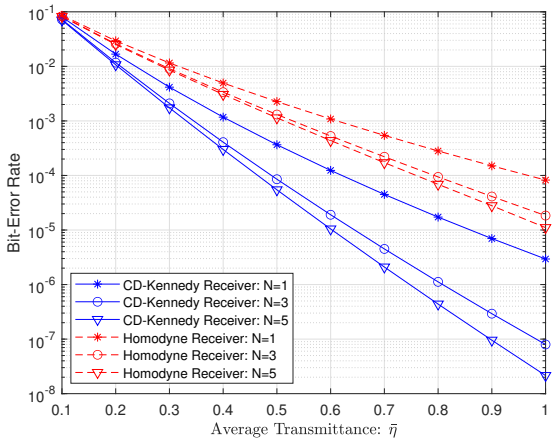


Fig. 6. BER comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels under different number of receivers N

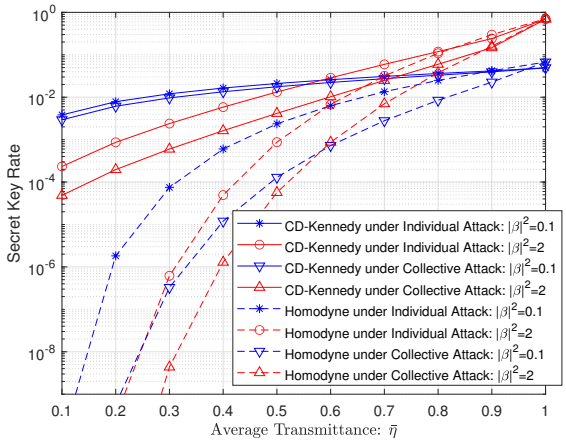
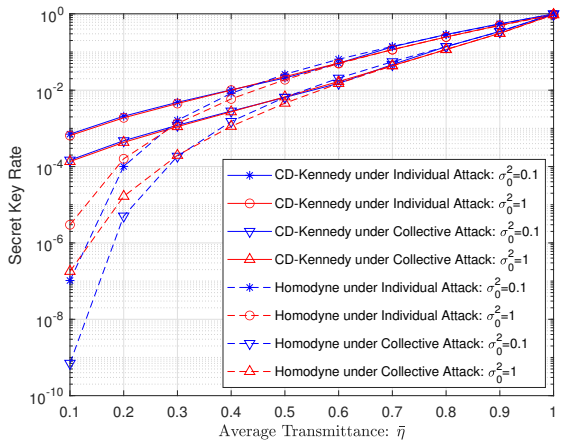


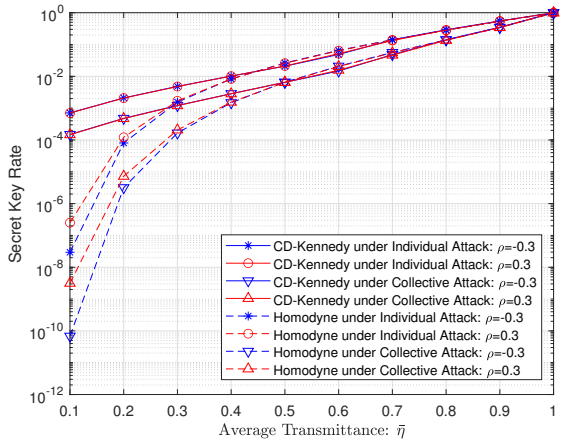
Fig. 7. SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels under different transmitting signal strength $|\beta|^2$

CD-QKD protocol with homodyne receiver deteriorates as the number of branches increases, which also demonstrate an opposite trend compared with the BER performance cases. This observation suggests that two separate system setting should be adopted for communication and key distribution purposes.

At last, we present the SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels with optimized transmitting signal strength at different turbulent strength σ_0^2, correlation coefficient ρ, and number of receivers N in Figs. 10(a), 10(b), and 10(c), respectively. From Figs. 10(a) and 10(b), we can see that the SKR performance with optimized signal strength for CD-Kennedy receiver is much robust than the homodyne receiver in turbulent channels. Besides, we can also see that, the SKR performance advantage of CD-Kennedy receiver over homodyne receiver increases as the average transmittance decreases. From 10(c) we can see that the SKR performance with optimized signal strength for post-selection based CD-QKD protocol using homodyne



(a)



(b)

Fig. 8. SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels: (a) Different turbulent strength σ_0^2; (b) Different correlation coefficient ρ

receiver deteriorates as the number of branches increases.

V. Conclusion

Endogenous security plays a crucial role in space-air-ground integrated network and a typical solution to endogenous security problems is the QKD. Compared with DV-QKD, CV-QKD enjoys higher SKR and better compatibility with current optical communication infrastructure. In this paper, we employed the CD-Kennedy receiver to enhance the detection performance of coherent states in turbulent channels. An EGC method was used to combine the output of N branches to provide the receiving diversity. Besides, we studied the SKR performance of a post-selection based CV-QKD protocol using CD-Kennedy receiver with EGC in turbulent channels and compare the SKR performance with the protocol using homodyne receiver. Moreover, we proposed an equivalent transmittance method to facilitate the calculation of both the BER and SKR and used a Fenton-Wilkinson method to approximate the

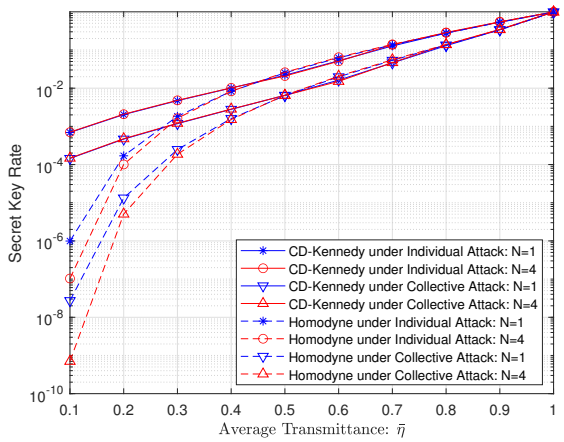


Fig. 9. SKR comparison between CD-Kennedy receiver and homodyne receiver in turbulent channels under different number of receivers N

PDF of the equivalent transmittance. Numerical results demonstrated that the CD-Kennedy receiver can outperform the homodyne receiver in turbulent channels in terms of both BER and SKR performance. However, we found that BER and SKR performance advantage of CD-Kennedy receiver over homodyne receiver demonstrate opposite trends as the average transmittance increases, which indicates that two separate system settings should be employed for communication and key distribution purposes. Our work sheds a light on the development of practical CV-QKD system over satellite-ground links with atmospheric turbulence.

REFERENCES

[1] J. Wu, *Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security*. Springer Nature, 2021.

[2] Y. Liu and M. Peng, "6g endogenous security: architecture and key technologies," *Telecommun. Sci.*, vol. 36, no. 1, pp. 11–20, 2020.

[3] Z. Wang, B. Cao, C. Liu, C. Xu, and L. Zhang, "Blockchain-based fog radio access networks: Architecture, key technologies, and challenges," *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 720–726, 2022.

[4] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," *Digit. Commun. Netw.*, vol. 8, no. 4, pp. 422–435, 2022.

[5] X. Wang, L. Jin, Y. Lou, and X. Xu, "Analysis and application of endogenous wireless security principle for key generation," *China Commun.*, vol. 18, no. 4, pp. 99–114, 2021.

[6] L. Zhang, P. Wang, Y. Zhang, Z. Chi, N. Tong, L. Wang, and F. Li, "An adaptive and robust secret key extraction scheme from high noise wireless channel in iiot," *Digit. Commun. Netw.*, vol. 9, no. 4, pp. 809–816, 2023.

[7] H. Hamdoun and A. Sagheer, "Information security through controlled quantum teleportation networks," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 463–470, 2020.

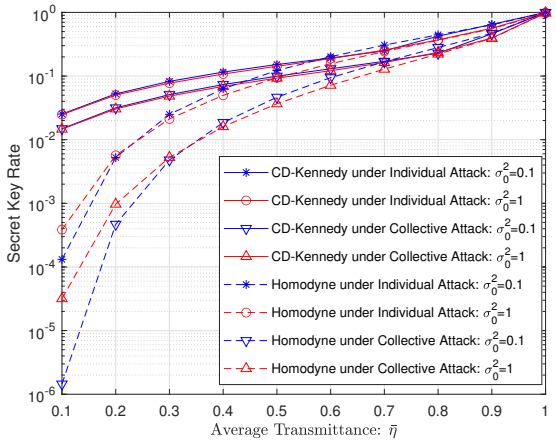
[8] M. S. Moreolo, M. Iqbal, A. Villegas, L. Nadal, R. Casellas, and R. Muñoz, "Continuous-variable quantum key distribution for enabling sustainable secure 6g networks," in *2024 International Conference on Optical Network Design and Modeling (ONDM)*. IEEE, 2024, pp. 1–3.

[9] L. Gyöngyösi, L. Bacsardi, and S. Imre, "A survey on quantum key distribution," *Infocommun. J.*, vol. 11, no. 2, pp. 14–21, June 2019.

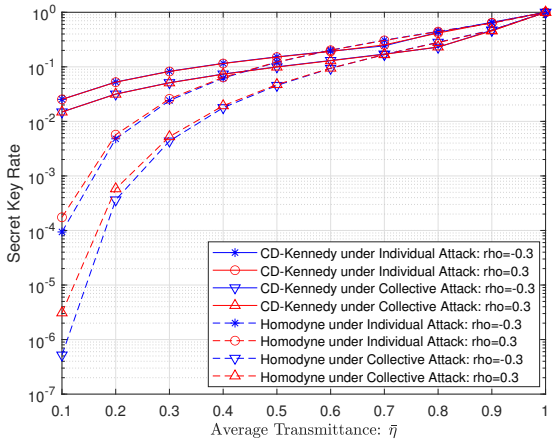
[10] S. Pirandola, U. Andersen, Banchi *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, 2020.

[11] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, 2002.

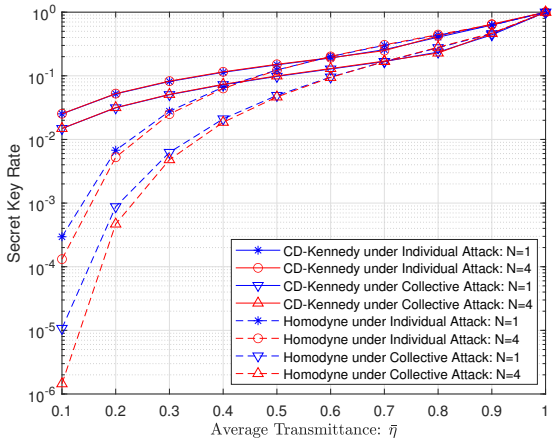
[12] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit," *Phys. Rev. Lett.*, vol. 89, no. 16, p. 167901, Sep. 2002.



(a)



(b)



(c)

Fig. 10. SKR comparison between CD-Kennedy receiver and homodyne receiver with optimized transmitting signal strength $|\beta|^2$ in turbulent channels: (a) Different turbulent strength σ_0^2; (b) Different correlation coefficient ρ; (c) Different number of receivers N

[13] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, p. 238, Jan. 2003.

[14] S. Lorenz, N. Korolkova, and G. Leuchs, "Continuous-variable quantum key distribution using polarization encoding and post selection," *Appl. Phys. B*, vol. 79, no. 3, pp. 273–277, Aug. 2004.

[15] L. Gyöngyösi and S. Imre, "Low-dimensional reconciliation for continuous-variable quantum key distribution," *Appl. Sci.*, vol. 8, no. 1, p. 87, Jan. 2018.

[16] M. Ghalaii and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution in free-space channels," *Phys. Rev. A*, vol. 108, no. 4, p. 042621, 2023.

[17] S.-G. Li, C.-L. Li, W.-B. Liu, H.-L. Yin, and Z.-B. Chen, "Discrete-modulated continuous-variable quantum key distribution in satellite-to-ground communication," *Adv. Quantum Technol.*, vol. 7, no. 8, p. 2400140, 2024.

[18] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Appl. Phys. Rev.*, vol. 11, no. 1, 2024.

[19] X. Liu, C. Xu, S. X. Ng, and L. Hanzo, "Otfs-based cv-qkd systems for doubly selective thz channels," *IEEE Trans. Commun.*, 2025.

[20] X.-T. Zheng, Q.-F. Zhang, J. Ling, G.-C. Guo, and Z.-F. Han, "Free-space continuous-variable quantum key distribution under high background noise," *npj Quantum Information*, vol. 11, no. 1, p. 52, 2025.

[21] Z. Yao, M. Li, Z. Wu, T. Wang, and M. Cvijietc, "Continuous-variable measurement-device-independent quantum key distribution over fluctuated free space quantum channels," *Optics Communications*, vol. 575, p. 131294, 2025.

[22] C. Wittmann, U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, "Demonstration of coherent-state discrimination using a displacement-controlled photon-number-resolving detector," *Phys. Rev. Lett.*, vol. 104, no. 10, p. 100505, Mar. 2010.

[23] M. Zhao, R. Yuan, J. Cheng, and S. Han, "Security of binary modulated continuous variable quantum key distribution using optimally displaced threshold detection," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1089–1093, 2020.

[24] ——, "Post-selection based generalized kennedy receiver for discriminating binary coherent states," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2021, pp. 1231–1235.

[25] M. Zhao, R. Yuan, C. Feng, S. Han, and J. Cheng, "Security of coherent-state quantum key distribution using displacement receiver," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 7, pp. 1871–1884, 2024.

[26] X. Zhu and J. M. Kahn, "Free-space optical communication through atmospheric turbulence channels," *IEEE Trans. Commun*, vol. 50, no. 8, pp. 1293–1300, Aug. 2002.

[27] I. Burenkov, M. Jabir, and S. Polyakov, "Practical quantum-enhanced receivers for classical communication," *AVS Quantum Science*, vol. 3, no. 2, p. 025301, 2021.

[28] C. W. Helstrom, "Quantum detection and estimation theory," *Journal of Statistical Physics*, vol. 1, no. 2, pp. 231–252, Jun. 1969.

[29] C. W. Helstrom, J. W. Liu, and J. P. Gordon, "Quantum-mechanical communication theory," *Proc. IEEE*, vol. 58, no. 10, pp. 1578–1598, Oct. 1970.

[30] R. S. Kennedy, "A near-optimum receiver for the binary coherent state quantum channel," *Quarterly Progress Report*, vol. 108, pp. 219–225, Jan. 1973.

[31] S. J. Dolinar, "An optimum receiver for the binary coherent state quantum channel," *Quarterly Progress Report*, vol. 111, pp. 115–120, Oct. 1973.

[32] R. L. Cook, P. J. Martin, and J. M. Geremia, "Optical coherent state discrimination using a closed-loop quantum measurement," *Nature*, vol. 446, no. 7137, p. 774, Apr. 2007.

[33] C. Wittmann, M. Takeoka, K. N. Cassemiro, M. Sasaki, G. Leuchs, and U. L. Andersen, "Demonstration of near-optimal discrimination of optical coherent states," *Phys. Rev. Lett.*, vol. 101, no. 21, p. 210501, Nov. 2008.

[34] M. Takeoka and M. Sasaki, "Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-gaussian near-optimal receivers," *Phys. Rev. A*, vol. 78, no. 2, p. 022320, Aug. 2008.

[35] F. Becerra, J. Fan, and A. Migdall, "Photon number resolution enables quantum receiver for realistic coherent optical communications," *Nat. Photonics*, vol. 9, no. 1, pp. 48–53, Nov. 2014.

[36] R. Yuan, M. Zhao, S. Han, and J. Cheng, "Kennedy receiver using threshold detection and optimized displacement under thermal noise," *IEEE Commun. Lett.*, Mar 2020.

[37] ——, "Optimally displaced threshold detection for discriminating binary coherent states using imperfect devices," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2546–2556, 2020.

[38] R. Yuan and J. Cheng, "Free-space optical quantum communications in turbulent channels with receiver diversity," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5706–5717, 2020.

[39] M. Zhao, R. Yuan, C. Feng, S. Han, and J. Cheng, "Optimally displaced threshold detection for tpsk modulated coherent states," *IEEE Trans. Commun.*, vol. 71, no. 12, pp. 7189–7205, 2023.

[40] R. J. Glauber, "The quantum theory of optical coherence," *Phys. Rev*, vol. 130, no. 6, p. 2529, Jun. 1963.

[41] ——, "Coherent and incoherent states of the radiation field," *Phys. Rev*, vol. 131, no. 6, p. 2766, Sep. 1963.

[42] A. Semenov and W. Vogel, "Quantum light in the turbulent atmosphere," *Phys. Rev. A*, vol. 80, no. 2, p. 021802, Aug. 2009.

[43] R. Yuan and J. Cheng, "Closed-form density matrices of free-space optical quantum communications in turbulent channels," *IEEE Commun. Lett.*, Feb. 2020.

[44] B. R. Cobb, R. Rumí, and A. Salmerón, "Approximating the distribution of a sum of log-normal random variables," *Stat. Comput.*, vol. 16, no. 3, pp. 293–308, 2012.

[45] M. Heid and N. Lütkenhaus, "Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction," *Phys. Rev. A*, vol. 73, no. 5, p. 052316, May 2006.

[46] D. Sych and G. Leuchs, "Coherent state quantum key distribution with multi letter phase-shift keying," *New J. Phys.*, vol. 12, no. 5, p. 053019, May 2010.

APPENDIX A
DERIVATION OF μ_{eq} AND σ_{eq}^2

The nth order moment of a log-normal distributed variable $x \sim LN(\mu, \sigma^2)$ can be obtained as

$$\mathrm{E}\left[x^n\right] = \exp\left(n\mu + n^2\sigma^2/2\right). \tag{54}$$

Then we can rewrite the two constrains of Fenton-Wilkinson method in (22) as

$$\begin{cases} \mathrm{E}[\eta_{eq}] = \sum_{i=1}^{N} \mathrm{E}[\eta_i] \\ \mathrm{E}[\eta_{eq}^2] = \mathrm{E}\left[\left(\sum_{i=1}^{N} \eta_i\right)^2\right]. \end{cases} \tag{55}$$

By using (54), we can rewrite the first equation in (55) as

$$\mu_{eq} + 0.5\sigma_{eq}^2 = \ln(N) + \mu_0 + 0.5\sigma_0^2. \tag{56}$$

Besides, the second equation in (22) can be further expressed as

$$\mathrm{E}[\eta_{eq}^2] = \sum_{i=1}^{N} \mathrm{E}\left[\eta_i^2\right] + 2\sum_{i\neq j} \mathrm{E}\left[\eta_i\eta_j\right]. \tag{57}$$

By using (54), we can obtain

$$\begin{cases} \mathrm{E}[\eta_{eq}^2] = \exp\left(2\mu_{eq} + 2\sigma_{eq}^2\right) \\ \mathrm{E}\left[\eta_i^2\right] = \exp\left(2\mu_0 + 2\sigma_0^2\right). \end{cases} \tag{58}$$

To calculate $\mathrm{E}\left[\eta_i\eta_j\right]$, we define a new random variable

$$\eta_{ij} \triangleq \eta_i\eta_j \tag{59}$$

for $i \neq j$. It is easy to verify that η_{ij} is also a log-normal distributed variable with $\eta_{ij} \sim LN(2\mu_0, 2(1+\rho)\sigma_0^2)$. Therefore, $\mathrm{E}\left[\eta_i\eta_j\right]$ becomes the expectation of η_{ij}, i.e.,

$$\mathrm{E}\left[\eta_i\eta_j\right] = \exp\left(2\mu_0 + (1+\rho)\sigma_0^2\right). \tag{60}$$

Then eq. (57) can be rewritten as

$$\begin{aligned}&\exp\left(2\mu_{eq}+2\sigma_{eq}^2\right)\\&\quad=N\exp\left(2\mu_0+2\sigma_0^2\right)+N(N-1)\exp\left(2\mu_0+(1+\rho)\sigma_0^2\right).\end{aligned}\tag{61}$$

Then we can easily obtain μ_{eq} and σ_{eq}^2 as (23) by combining (56) and (61).

APPENDIX B
DERIVATION OF $\mu_{eq,hd}$ AND $\sigma_{eq,hd}^2$

Now we can define a new random variable

$$\eta_{sq,i}\triangleq\sqrt{\eta_i}\tag{62}$$

for any $i=1,2,\cdots,N$.

It is easy to verify that $\eta_{sq,i}$ is also a log-normal distributed variable with $\eta_{sq,i}\sim LN(0.5\mu_0,0.25\sigma_0^2)$. Besides, the correlation coefficient ρ_{ij} between $\ln(\eta_{sq,i})=0.5\ln(\eta_i)$ and $\ln(\eta_{sq,j})=0.5\ln(\eta_j)$ when $i\neq j$ can be obtained as

$$\begin{aligned}\rho_{ij}&\triangleq\frac{\mathrm{E}[\ln(\eta_{sq,i})\ln(\eta_{sq,j})]-\mathrm{E}[\ln(\eta_{sq,i})]\mathrm{E}[\ln(\eta_{sq,j})]}{\sqrt{\mathrm{Var}[\ln(\eta_{sq,i})]\mathrm{Var}[\ln(\eta_{sq,j})]}}\\&=\frac{0.25\mathrm{E}[\ln(\eta_i)\ln(\eta_j)]-0.25\mathrm{E}[\ln(\eta_i)]\mathrm{E}[\ln(\eta_j)]}{0.25\sqrt{\mathrm{Var}[\ln(\eta_i)]\mathrm{Var}[\ln(\eta_j)]}}\\&=\rho,\end{aligned}\tag{63}$$

where the last step is directly followed from (8).

Then for $\eta_{eq}^{hd}\triangleq\sum_{i=1}^{N}\sqrt{\eta_i}$, the two constrains of Fenton-Wilkinson method can be expressed as

$$\begin{cases}\mathrm{E}\left[\eta_{eq}^{hd}\right]=\sum_{i=1}^{N}\mathrm{E}\left[\eta_{sq,i}\right]\\\mathrm{E}\left[\left(\eta_{eq}^{hd}\right)^2\right]=\mathrm{E}\left[\left(\sum_{i=1}^{N}\eta_{sq,i}\right)^2\right].\end{cases}\tag{64}$$

By comparing (64) and (55), we can find that $\mu_{eq,hd}$ and $\sigma_{eq,hd}^2$ can be obtained by simply replacing $\{\mu_0,\sigma_0^2\}$ with $\{0.5\mu_0,0.25\sigma_0^2\}$ in (23), which results in (29).