Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach

Geng Chai, Peng Huang, Zhengwen Cao and Guihua Zeng

School of Information Science and Technology, Northwest University, Xi’an 710127, People’s Republic of China
State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Sensing and Information Processing (QSIIP), Shanghai Jiao Tong University, Shanghai 200240, People’s Republic of China

E-mail: caozhw@nwu.edu.cn and ghzeng@sjtu.edu.cn

Keywords: continuous-variable quantum key distribution, excess noise suppression, adaptive optics

Abstract

The excess noise inducing in the process of the quantum communication procedure is the major obstacle restricting the performance of continuous-variable quantum key distribution (CVQKD). In order to effectively suppress the excess noise through correcting the propagation-induced distortions on the quality of the propagated quantum signal, we propose a general scheme of suppressing excess noise for CVQKD via adaptive optics (AO) approach. The analysis shows that phase-only AO compensation exhibits excellent performance in controlling the excess noise, which is embodied in substantially extending the secure propagation distance and improving the secret key rate of the system. And thereby the development and improvement of AO has the potential advantage to break the distance constraints due to the excess noise results from propagation-dominated factors. Our scheme provides a feasible method for further implementation of practical large-scale CVQKD.

1. Introduction

Quantum key distribution (QKD) provides unconditionally secret key for secure communication between two legitimate communication parties [1, 2], whose security relies on the quantum mechanics properties such as the Heisenberg’s uncertainty principle [3] and the quantum no-cloning theorem [4], rather than the computational complexity in mathematical sense [5, 6]. Generally, its two branches referred to as discrete-variable QKD [7, 8] and continuous-variable QKD (CVQKD) [9, 10]. The latter is implemented with commercial optical components and can be compatible with fully developed standard optical communications, thus providing higher channel capacity and greater ease of implementation than the former [11–14]. Theoretical and experimental breakthroughs have been made in Gaussian-modulated coherent-state CVQKD, which is one of the well-known fundamental protocols in realistic implementations, at recent years [15–18].

Nevertheless, there exist many factors such as attenuation of quantum channel, jitter of optical fiber, atmospheric effects and so on have a significant impact on the quality of the quantum signal in the practical CVQKD system [19–23]. It follows that the actual transmission environment presents a series of practical challenges for implementation of long-distance CVQKD. Among them, the major obstacle restricting the system performance is the excess noise occurring in the process of the quantum communication procedure [17, 24]. As has been pointed out in [25] that Eve can perform an intercept-resend attack on the channel when the excess noise reaches two times the shot-noise level, and thus no secret key can be generated. As another illustration, [26, 27] pointed that the presence of excess noise severely weakens systems which employ post-selection to extract key from the correlated Gaussian distributions shared by Alice and Bob [28]. Intuitively, the excess noise is the noise above the vacuum noise level associated with channel losses, and it is a major issue in CVQKD [24]. Apart from the natural attenuation of quantum channel, the incremental excess noise is associated with higher propagation loss and lower signal-to-noise (SNR) ratio.
caused by propagation-induced distortions or technical defects, which are two key aspects of long-distance implementations. It is therefore essential to consider and ameliorate related technologies in order to suppress the excess noise occurring influence of quantum channel and technical imperfection on the system.

To effectively suppress the excess noise of the system, many methods have been proposed one after another. In [29], a method based on improving the extinction ratio of optical pulses and adopting a high shot-noise to electronic-noise ratio pulsed homodyne detector with ultra-low electronic noise is used to suppress the excess noise induced by the photons leakage from the local field into the signal path due to the depolarized scattering process of the local field. In [11], an efficient error-correcting code, which leads to a remarkable improvement of transmission distance for CVQKD, is developed to achieve system over 80 km of optical fiber. In [17], a scheme based on shot-noise-limited homodyne detection (HD) with weak local oscillator (LO) and high-precision phase compensation with low SNR is employed to control the excess noise induced by the photons leakage from the strong LO to the weak quantum signal and the inaccuracy of phase compensation. And report an experimental demonstration of system over 100 km fiber channel. In [30], a phase compensation method based on step-length control is proposed to suppress the excess noise induced by the inaccuracy of phase compensation. Therefore, as regarding to the two key aspects of long-distance implementations by controlling the excess noise, one is that the increase of propagation loss requires a stronger LO to assist shot-noise-limited HD, which has been realized effectively. Yet the other is that the decrease of SNR brings a great challenge to high-precision phase compensation, although there proposed some related methods, none of them can solve the propagation-induced distortions systematically.

In this work, we report for a general model of excess noise suppression for CVQKD under atmospheric channel on the premise of summarizing the previous research achievements [31–39]. Considering that adaptive optics (AO) provides an enabling method to mitigate the channel effects on the communication system, which either can pre-correct the wavefront at the transmitter Alice or can post-correct the wavefront at the receiver Bob [40]. Therefore, the scheme is achieved by employing the AO approach to correct the propagation-induced distortions on the quality of the propagated quantum signal so as to effectively suppress the excess noise. Firstly, we establish a physical model of the proposed scheme, and then theoretically investigate how AO operates in the system from the perspective of the optical field. Secondly, the suppression effect of AO on the excess noise is explained in the angle of parameter estimation, thus improving the system performance. After that, we analyze the performance of the proposed scheme under fiber channel and atmospheric channel, and discover that the application of AO can substantially extend the secure propagation distance and improve the secret key rate. This proves the feasibility and rationality of the proposed scheme and indicates AO can significantly reduce the excess noise induced by quantum channel and technical imperfection. Furthermore, the proposed method paves the way to the large-scale quantum secure communication and serves as a stepping stone in the quest for quantum network. And the research on this aspect should mainly lie in both theory and experiment. In the future, more attention should be paid to proving its effectiveness through experiment.

The paper is organized as follows. In section 2, we establish a physical model of CVQKD based on AO, and explain how AO works in the atmospheric CVQKD with the help of demonstrative optical path. Then in section 3, we investigate theoretically the impact of AO on the performance of CVQKD over the fiber channel and the atmospheric channel, respectively. Conclusions are drawn in section 4.

2. Physical mode for CVQKD with AO

Before introducing the AO [41] based CVQKD, we first briefly review the common CVQKD as shown in figure 1 (the module titled ‘RX AO’ or ‘TX AO’ within the brown solid line excluded).

For common CVQKD, the transmitter Alice usually modulates quadrature components of the light with Gaussian modulation, and the receiver Bob measures weak quantum signal with the help of strong LO in a shot-noise-limited homodyne or heterodyne detector [9, 10]. There generally consists two segments in CVQKD, one is quantum information transmission phase, where quantum signals are transmitted through a quantum channel and then measured by the detector, the other is classical information post-processing phase, where local data is applied for parameter estimation [23, 42] to evaluate system security under eavesdropper Eve attack. And the rest is used to extract the final secret key through reverse reconciliation [43, 44] and privacy amplification [45–47].

Now considering the CVQKD with AO based on the entanglement-based (EB) conceptual schematic illustrated in figure 1, where figure 1(a) shows that AO located at the transmitter (TX AO) and figure 1(b) shows that AO located at the receiver (RX AO), respectively. The proposed scheme includes transmitter module (Alice), quantum channel module, adaptive optics module (AO) and receiver module (Bob).
In view of the same principle between TX AO and RX AO, compared with the former, the latter can realize wavefront measurement without additional beacon light, so the latter is more suitable for large-scale CVQKD systems. Therefore, CVQKD based on RX AO is the focus of this paper. And the operating mechanism of the EB CVQKD with RX AO can be described as follows:

### 2.1. The propagation-induced distortions

Alice employs two single-mode squeezed vacuum states $|v\rangle$ and $|-v\rangle$ to prepare a two-mode squeezed vacuum state (Einstein–Podolsky–Rosen) $|\Psi\rangle_{AB}$ with variance $V = V_A + 1$, where the modulation variance $V_A = 2\alpha^2$ and $|v\rangle_k = \hat{S}_k(v)|0\rangle$ based on the squeezing operator on mode $k$ with the form

$$\hat{S}_k(v) = \exp\{[-v(\hat{a}_k^2 - \hat{a}_k^2)]/2\},$$

and then measures one half of state $|\Psi\rangle_{AB}$ randomly.

$$\begin{align*}
|\Psi\rangle_{AB} &= \hat{U}_{AB}\left(\frac{\pi}{4}\right)|v\rangle_A|-v\rangle_B = \sum_{n=0}^{\infty} \alpha_n |n\rangle_A|n\rangle_B, \\
\hat{U}_{AB}(\theta) &= \exp\left[\theta \left(\hat{a}_A^\dagger\hat{a}_B - \hat{a}_A\hat{a}_B^\dagger\right)\right],
\end{align*}$$

where $\hat{U}_{AB}(\theta)$ stands for the beam splitter (BS) operator, in which parameter $\theta$ is related to the transmission efficiency $\zeta = 1/(1 + \tan^2\theta)$, and $\theta = \pi/4$ corresponds to the balanced BS. In addition, the Schmidt coefficients $\alpha_n = \sqrt{\alpha^2/(1 + \alpha^2)^{n+1}}$ with $\alpha = \sinh v$, in which $v$ is the squeezing parameter. As known, the state $|\Psi\rangle_{AB}$ in the Heisenberg picture can be fully described by its covariance matrix $\gamma_{AB}$:

$$\gamma_{AB} = \begin{pmatrix}
V & \sqrt{V^2 - 1}\sigma_z \\
\sqrt{V^2 - 1}\sigma_z & V
\end{pmatrix},$$

where the unity matrix $I = \text{diag}(1, 1)$ and the Pauli matrix $\sigma_z = \text{diag}(1, -1)$.

What needs to be explained is that, the communication protocol designed in [24], which can synchronize Alice and Bob and provide for channel parameters (gain, excess noise, and relative phase), is employed in our method. The communication is split into independent blocks, whose size can be adjusted while being large enough to make statistical tests, so that the transmission parameters can be assumed as constant over a block. Then, the other half of state $|\Psi\rangle_{AB}$ is transmitted to Bob through a quantum channel which is characterized by a distribution of transmittance $\{T_i\}$ and a corresponding excess noise $\{\varepsilon_i\}$ with probabilities $\{p_i\}$. In addition, $\langle T \rangle = \sum_i p_i T_i$ and $\varepsilon = \sum_i p_i \varepsilon_i$. The propagation of the half of state $|\Psi\rangle_{AB}$ across the transmission link can be described by a unitary operator $U_{\text{trans}}(L)$ ($L$ is the propagation distance) [48, 49], that is, the first mode remains in its initial state, in contrast to the second mode experiences channel fluctuation,

$$|\Psi\rangle_{AB} = \{I \otimes U_{\text{trans}}(L)\}|\Psi\rangle_{AB}. $$

Suppose that the system is equipped with a fine acquisition tracking and pointing systems so that Bob can almost receive propagated signals completely. Therefore, in regard to the communication block with
transmittance $T_i$ and excess noise $\epsilon_{i\ell}$, $U_{\text{trans}}(L)$ can be regarded as $U_{\text{trans}}(L) = U_{\text{trans}}^i(\phi(r, \theta))$ on the second mode transmitted to Bob, and the corresponding quantum state after channel propagation can be express as,

$$\rho_{AB} = \int \left[ \Pi \otimes U_{\text{trans}}^i(\phi(r, \theta)) \right] |\Psi\rangle\langle\Psi| \left[ \Pi \otimes U_{\text{trans}}^i(\phi(r, \theta)) \right] \rho(\phi(r, \theta)) d\phi(r, \theta),$$  

where $p(\phi(r, \theta))$ is the probability distribution of the distorted phase $\phi(r, \theta)$ induced by the quantum channel. And the covariance matrix $\gamma_{AB}^i$ of the transmitted state $|\Psi\rangle_{AB}$ can be described as,

$$\gamma_{AB}^i = \left( \Pi \otimes U_{\text{trans}}^i \right)^T \gamma_{AB} \left( \Pi \otimes U_{\text{trans}}^i \right),$$

where $c = \sqrt{T_i \sqrt{V^2 - 1}}$, $T_i^f$ and $\epsilon_i^f$ represent the equivalent transmittance and equivalent excess noise on the condition of introducing propagation distortion, respectively.

$$\begin{bmatrix} T_i^f & \delta T_i \\ \epsilon_i^f & \frac{1}{\delta} + (1 - \delta)(V - 1) \end{bmatrix},$$

where, $\delta$ refers to the propagation-induced distortions parameter,

$$\delta = \left[ \int p(\phi(r, \theta)) \cos[\phi(r, \theta)] d\phi(r, \theta) \right]^2 = \left[ E[\cos[\phi(r, \theta)]] \right]^2.$$

On the other hand, in terms of the field quadrature operators of the state, i.e., the mode’s quadrature position operator $\hat{x} = (\hat{a} + \hat{a}^\dagger)/2$ and the quadrature momentum operator $\hat{p} = (\hat{a} - \hat{a}^\dagger)/2i$ ($\hat{x}$ is squeezed when $v > 0$ whereas $\hat{p}$ is squeezed when $v < 0$), the state $|\Psi\rangle_{AB}$ can be described by the mean values $\langle \hat{x} \rangle$, $\langle \hat{p} \rangle$, and by the covariance matrix $\gamma_{pq} = \langle \hat{x}_p \hat{x}_q \rangle - \langle \hat{x}_p \rangle \langle \hat{x}_q \rangle$, where $\hat{x}_p = \{\hat{x}(p(q)) \hat{p}(q)\}$ is the quadrature vector of the $(q)$-th mode of the quantum state $|\Psi\rangle$. Affected by channel transmission, the variance of a quadrature of the state propagating through the quantum channel becomes [31]

$$\delta V_{\hat{p}} = 1 + \langle \sqrt{T} \rangle^2 (V_{\hat{p}} - 1) + \epsilon_{\hat{p}}^f,$$

where the excess noise due to fluctuating is given as $\epsilon_{\hat{p}}^f = \text{Var} \left( \sqrt{T} \right) (V_{\hat{p}} - 1)$, which depends on the variance of the transmittance fluctuations $\text{Var} \left( \sqrt{T} \right) = \langle T \rangle - \langle \sqrt{T} \rangle^2$ and the $\hat{p}$ -quadrature variance $V_{\hat{p}}$ of the state. Without loss of generality, there exists variance $V_{\hat{p}} = V \forall p$ in any quadrature under the phase-space symmetry of the state $|\Psi\rangle$.

### 2.2. AO compensation and correction

In order to effectively correct the propagation-induced distortions on the quality of the propagated state $|\Psi\rangle_{AB}$, the received state $|\Psi\rangle_{AB}$ is preprocessed with AO before Bob takes signal detection and informs Alice which observable he obtained. Following this process, reverse reconciliation and privacy amplification are executed one after another to obtain the final secret key. Thus the unitary operator $U_{AO}$, which expresses the action of AO, can be employed to obtain the corrected state $|\Psi\rangle_{AB}$,

$$|\Psi\rangle_{AB} = U_{AO} |\Psi\rangle_{AB} = \left( \Pi \otimes U_{\text{trans}}(L) \right) |\Psi\rangle_{AB}.$$
$\varphi_B(r, \theta)$, which is extracted by WFS, is adopted to correct the propagation-induced distortions of the state $|\Psi\rangle_{AB}$. Considering from the mode function of the state,

$$
\Psi_{AB}(r, L) = \{ \exp[-i\varphi_B(r, \theta)] \} \Psi_{AB}(r, L) = \{ \exp[-i\varphi_B(r, \theta)] \} \{ I \otimes U_{trans}(L) \} \Psi_{AB}(r', 0),
$$

where $\Psi_{AB}(r', 0)$, $\Psi_{AB}(r, L)$ and $\Psi_{AB}(r, L)$ are the mode function associated with the states $|\Psi\rangle_{AB}$, $|\Psi\rangle_{AB_i}$ and $|\Psi\rangle_{AB_j}$, respectively. Generally, it is more convenient to describe the wavefront in the Fourier domain for the temporal dependence and in the Zernike domain for the spatial one, and the Fourier transformation can be developed in Zernike modes. The wavefront over the receiving aperture of radius $R$ can be considered as two dimensional functions decomposed by Zernike polynomials in polar coordinates [52],

$$
\begin{align}
\varphi_B(\rho, \theta) &= a_0 + \sum_{j=1} a_j Z_j(\rho, \theta) + \xi, \\
&= \frac{1}{\pi} \int_0^\rho \varphi_B(\rho, \theta) Z_j(\rho, \theta),
\end{align}
$$

where $a_0$ is the average phase wavefront, corresponding to the overall translation aberration, $\xi$ is the measurement error of wavefront phase, $\rho = r/R$ with the polar coordinates $(r, \theta)$ in the transverse plane, and $a_j$ is the coefficient, which is set by the covariance matrix of Zernike terms, of the $j$th Zernike polynomial. And $Z_j(\rho, \theta)$ is the $j$th Zernike order described as [52],

$$
\begin{align}
Z_{j(even)}(\rho, \theta) &= \sqrt{n + 1} R_{n}^{m}(\rho) \sqrt{2} \cos(m\theta), \quad m \neq 0 \\
Z_{j(odd)}(\rho, \theta) &= \sqrt{n + 1} R_{n}^{m}(\rho) \sqrt{2} \sin(m\theta), \quad m \neq 0 \\
Z_{j}(\rho, \theta) &= \sqrt{n + 1} R_{n}^{0}(\rho) , \quad m = 0
\end{align}
$$

where azimuthally frequency $m \in \mathbb{Z}$ and radial degree $n \in \mathbb{N}$, and radial polynomial $R_{n}^{m}(\rho)$ can be described as follows,

$$
R_{n}^{m}(\rho) = \sum_{s=0}^{s=n} \frac{(-1)^{s}(n-s)!}{s! \frac{n+m}{2} - s! \frac{n-m}{2} - s!} \rho^{n-2s}.
$$

Finally, Bob measures the corrected state $|\Psi\rangle_{AB}$, through homodyne detection randomly to obtain data associated with Alice’s measurement data, local associated data subsequently is applied for parameter estimation to evaluate system security under eavesdropper Eve attack and the rest is used to extract the final secret key. In regard to the communication block with transmittance $T_i$ and excess noise $\varepsilon_i$, $U_{AO}$ can be
regarded as \( U_{AO} = U_{AO}(\varphi(r, \theta)) \) on the distorted mode received by Bob, and the corresponding quantum state after correction can be express as,

\[
\rho_{AB_2} = \int [\mathbb{1} \otimes U_{AO}(\varphi(r, \theta))] \rho_{AB_1} [\mathbb{1} \otimes U_{AO}(\varphi(r, \theta))]^\dagger p(\varphi(r, \theta)) d\varphi(r, \theta),
\]

where \( p(\varphi(r, \theta)) \) is the probability distribution of the compensation phase \( \varphi(r, \theta) \) provided by AO unit. And the covariance matrix \( \gamma_{AB_2} \) of the corrected state \( |\Psi\rangle_{AB_2} \) can be described as,

\[
\gamma_{AB_2} = (\mathbb{1} \otimes U_{AO}^\dagger) \gamma_{AB_1} (\mathbb{1} \otimes U_{AO})
\]

\[
= \begin{pmatrix}
V & 0 & c \cos[\phi_1(r, \theta) - \varphi_1(r, \theta)] & -c \sin[\phi_1(r, \theta) - \varphi_1(r, \theta)] \\
0 & V & -c \sin[\phi_1(r, \theta) - \varphi_1(r, \theta)] & -c \cos[\phi_1(r, \theta) - \varphi_1(r, \theta)] \\
c \cos[\phi_1(r, \theta) - \varphi_1(r, \theta)] & -c \sin[\phi_1(r, \theta) - \varphi_1(r, \theta)] & T_0^c(V + \frac{1}{T_i}) - 1 + \varepsilon_o^i & 0 \\
-c \sin[\phi_1(r, \theta) - \varphi_1(r, \theta)] & -c \cos[\phi_1(r, \theta) - \varphi_1(r, \theta)] & 0 & T_0^c(V + \frac{1}{T_i}) - 1 + \varepsilon_o^i \\
\end{pmatrix}
\]

where \( T_0^c \) and \( \varepsilon_o^i \) represent the equivalent transmittance and equivalent excess noise on the condition of introducing AO compensation, respectively.

\[
\begin{align*}
T_0^c &= \frac{T_0^c}{\mu} = \frac{\delta}{\mu} T_i, \\
\varepsilon_o^i &= \mu \left[ \varepsilon_o^i + (V - 1) \left( 1 - \frac{1}{\mu} \right) \right] \\
&= \frac{\mu}{\delta} \varepsilon_o + \frac{\mu}{\delta} (V - 1) \left( 1 - \frac{\delta}{\mu} \right),
\end{align*}
\]

where, \( \mu \) refers to the AO compensation parameter,

\[
\frac{\delta}{\mu} = \left[ \int p(\phi) \cos[\phi(t, \theta) - \varphi(t, \theta))] d(\phi(t, \theta) - \varphi(t, \theta)) \right]^2 = \left[ E[\cos[\phi(t, \theta) - \varphi(t, \theta))] \right]^2.
\]

It can be seen that when parameter \( \delta/\mu \) tends to 1, there have \( T_0^c = T_i \) and \( \varepsilon_o^i = \varepsilon_o \), which shows that it is feasible to suppress the excess noise introduced by channel transmission via AO approach.

In a nutshell, the action of AO can be regarded as a unitary operation \( U_{AO} \) acting on the state \( |\Psi\rangle_{AB_1} \) affected by channel transmission. Without loss of generality, we further explain the operation mechanism of AO in the system from the perspective of the optical field, which is illustrated in figure 3. Assuming that the beam emitted by the CW Laser is linearly polarized in the horizontal direction, it is divided into LO and quantum signal through a BS with 99% splitting ratio. Then the quantum signal, modulated by Gaussian modulation, and LO are polarized multiplexed with a polarization beam splitter (PBS) and propagated to the receiver through the quantum channel. Specifically, the quantized signal optical field with a single frequency and a single polarization is generally employed in continuous-variable quantum information system, that is [53],

\[
\hat{E}_k(r, t) = E_0 \left[ \hat{a}_k e^{i(k \cdot r - \omega_k t)} + \hat{a}_k^\dagger e^{-i(k \cdot r - \omega_k t)} \right],
\]

and equation (18) can be simplified by position operator \( \hat{x}_k \) and momentum operator \( \hat{p}_k \),

\[
\hat{E}_k(r, t) = 2E_0 \left[ \hat{x}_k \cos(\omega_k t - k \cdot r) + \hat{p}_k \sin(\omega_k t - k \cdot r) \right],
\]

Thus the quantum signal after Gaussian modulation can be expressed as [54]

\[
\begin{align*}
\hat{E}_k'(r, t) &= \hat{E}_k(r, t) \exp \left[ -\frac{i}{\hbar} \frac{V(t)}{V_\pi} \right], \\
V(t) &= -\sum_{\tau=1}^N A_\tau \cos(\omega_\tau t + \phi_\tau) - V_b,
\end{align*}
\]

where \( V_b \) is the bias voltage of the amplitude modulator (AM), \( V_\pi \) is the half-wave voltage of the phase modulator (PM). And \( A_\tau \) is a Rayleigh distributed random number for amplitude modulation, and \( \phi_\tau \) is a
uniform distributed random number for phase modulation, where $\tau \in \{1, 2, \ldots, N\}$. Therefore, we can obtain that

$$E_k'(r, t) = E_k(r, t) \exp \left[ i \frac{V_b}{V \pi} \exp \left[ \sum_{\tau=1}^{N} \frac{\pi A_{c\tau} V}{V \pi} \cos(\omega \tau t + \phi_{c\tau}) \right] \right],$$

and the expression of equation (21) can be rewritten in a form similar to that of equation (18):

$$\hat{E}_s'(r, t) = \hat{E}_s \left[ \hat{a}_s e^{i(k \cdot r - \omega \tau t)} + \hat{a}_s^\dagger e^{-i(k \cdot r - \omega \tau t)} \right],$$

where $\hat{a}_s$ is a new dimensionless complex amplitude operator after Gaussian modulation, which can be expressed as [54]

$$\hat{a}_s = \frac{1}{2} C_{c\tau} \exp \left[ -i \frac{V_b}{V \pi} \hat{a}_k \right],
C_{c\tau} \sim i \left( \frac{\pi A_{c\tau} V}{V \pi} \right) e^{-i \phi_{c\tau}}.$$  

In addition, the classical LO field is expressed by

$$E_{LO}^k(r, t) = \text{Re} \left\{ E_{LO} \exp \left[ -i(k \cdot r - \omega \tau t) \right] \right\}.$$  

At the receiver with a fine tracking system, the separation of quantum signal from LO in received beam through demultiplexing. And the quantum signal after quantum channel propagation is expressed as

$$\hat{E}_s'^c(r, t) = \hat{E}_s \left[ \hat{a}_s e^{i(k \cdot r - \omega \tau t)} + \hat{a}_s^\dagger e^{-i(k \cdot r - \omega \tau t)} \right],$$

$$\hat{a}_s = \frac{1}{2} C_{c'} \exp \left[ -i \frac{V_b}{V \pi} \hat{a}_k \right],
C_{c'} \sim i \left( \frac{\pi A'_{c'} V}{V \pi} \right) e^{-i(\phi_{c'} - \phi_{c})},$$

where $A'_{c'}$ and $\phi_{c'}$ represent the amplitude fluctuations and phase variations introduced by channel transmission, respectively.

Then, partial LO is sent into AO to measure the propagation-induced wavefront $\varphi_{B}(r, t)$, which is used to correct quantum signal and residual LO affected by channel fluctuation. Therefore, the row secret key is obtained by joint measurement of the corrected quantum signal and LO. Consequently, the difference photocurrent of homodyne detection without AO $\Delta i$ with AO $\Delta i_{AO}$ under atmospheric channel are
respectively expressed as

\[
\begin{align*}
\Delta i &= \frac{a_k \pi A_t^2 A_r}{2 V_b} \left( \cos(-\phi_r + \phi_c^b) \cos \theta_{PM} 
+ \sin(-\phi_r + \phi_c^b) \sin \theta_{PM} \right), \\
\Delta i_{AO} &= \frac{a_k \pi A_t^2 A_r}{2 V_b} \left( \cos(-\phi_r + \phi_c^b - \varphi_{BR}) \cos \theta_{PM} 
+ \sin(-\phi_r + \phi_c^b - \varphi_{BR}) \sin \theta_{PM} \right),
\end{align*}
\]

(26)

where \( \theta_{PM} \) determines whether the measured component is quadrature operator \( \hat{x}_i \) \((\theta_{PM} = 0)\) or \( \hat{p}_i \) \((\theta_{PM} = \pi/2)\) of the quantum signal, and \( a_k \) denotes the norm of \( \hat{d}_k \). Taking the difference photocurrent of homodyne detection under ideal channel \( \frac{\hat{x}_i}{\sqrt{V_c}} \) \([\cos(-\phi_r) \cos \theta_{PM} + \sin(-\phi_r) \sin \theta_{PM}] \) as reference, compared with \( \Delta i \), \( \Delta i_{AO} \) can correct the distortion phase, which is caused by channel transmission, of received quantum signal in real time. Therefore, the addition of AO makes the CVQKD adapt to the changes of the channel environment and effectively solves the problem of dynamic random interference of the channel fluctuation, so as to enable the system maintain good performance.

### 2.3. The excess noise suppressing

Due to the employment of AO, the parameter estimation result has some changes compared with the conventional one proposed in [23, 42]. Here we take into account that the Alice variables \( X \) and the corresponding Bob variables with AO and without AO are \( Y_{AO} \) and \( Y \) can be respectively simply expressed as

\[
\begin{align*}
X &= A_r \cos \phi_r, \\
Y &= A_r \cos(\phi_r - \phi_c^b) + A_N, \\
Y_{AO} &= A_r \cos(\phi_r - \phi_c^b + \varphi_{BR}) + A_N.
\end{align*}
\]

(27)

For each communication block, Alice and Bob’s correlated variables \( \{X, Y\} \) and \( \{X, Y_{AO}\} \) are usually linked with the following normal linear model in the case of Gaussian modulation [23],

\[
y_i = t_i x_i + z_i
\]

(28)

where \( t_i = \sqrt{\eta_i} \in \mathbb{R} \), and \( z_i \) is a Gaussian noise with variance \( \sigma_i^2 = N_i(1 + \eta_i T_i \delta_i + v_i) \) and mean zero, and \( N_i \) is the shot noise of the \( i \)th communication block obtained by real-time shot noise measurement, and \( A_N \) is the amplitude caused by the noise. The propagation-induced distortions can be well corrected by AO under optimal conditions, and due to the imperfection of devices and other factors in real conditions, \( \varphi_{BR} - \phi_c^b \) tends to zero, and \( \phi_r - \phi_c^b + \varphi_{BR} \) is infinitely close to \( \phi_r \). In other words, \( \{X, Y_{AO}\} \) is more suitable than \( \{X, Y\} \) in fitting the normal liner model, which is consistent with the results of equations (6) and (16).

The excess noise suppressing performance of the proposed scheme is shown in figure 4. It can be seen that when there has no AO compensation \((\mu = 1)\), the excess noise increases with the decrease of \( \delta \), which indicates that the propagation-induced distortions is one of the important sources of the excess noise of CVQKD, and it is essential to suppress the excess noise through physical methods. In addition, as \( \mu/\delta \) approaches 1, i.e., the AO compensation \( \mu \) is gradually matched with the propagation-induced distortions \( \delta \), the excess noise is gradually suppressed to near the theoretical target excess noise. Therefore, the established model provides a general scheme to suppress the excess noise results from the propagation-induced distortions. Furthermore, the employment of the other more efficient schemes and pioneering technological advances will facilitate the establishment of the large-scale quantum cryptography network.

Based on the above introduction and analysis of the proposed scheme, the system performance of CVQKD with the proposed scheme will be analysed in the next section.

### 3. Performance of CVQKD with AO compensation

Now we consider the performance of the CVQKD with AO, and the secret key rate can be obtained by communication parties to reveal the system performance. The asymptotic secret key rate of the system without considering the finite-size effect under reconciliation efficiency \( \beta_R \) is given as [22, 23],

\[
K = (1 - P) (\beta_R I_{AB} - \chi_{BE}),
\]

(29)
where $I_{AB}$ is the Shannon mutual information of Alice and Bob, and $\chi_{BE}$ is the Holevo quantity of Bob and Eve. $P$ stands for interruption probability due to angle of arrival fluctuations under fluctuating channel such as atmosphere, which is zero in fiber channel. According to previous works [55, 56], the covariance matrix of the mode $AB_1$ is expressed by

$$
\gamma_{AB_1} = \begin{pmatrix}
V I & \langle \sqrt{T} \rangle \sqrt{V^2 - 1} \sigma_z \\
\langle \sqrt{T} \rangle \sqrt{V^2 - 1} \sigma_z & \langle T \rangle \left[ V + 1 \langle T \rangle - 1 + \varepsilon \right] I
\end{pmatrix}, \tag{30}
$$

where $T_e$ and $\varepsilon_e$ represent the equivalent transmittance and equivalent excess noise of the whole communication process, respectively.

$$
\begin{align*}
T_e &= \langle \sqrt{T} \rangle^2, \\
\varepsilon_e &= \frac{\langle T \rangle}{\langle \sqrt{T} \rangle^2} \varepsilon + \frac{\text{Var} \left( \sqrt{T} \right) (V - 1)}{\langle \sqrt{T} \rangle^2}, \tag{31}
\end{align*}
$$

where $\text{Var} \left( \sqrt{T} \right)$ is caused by the changes of transmission parameters between different communication blocks due to the channel fluctuation, which is zero in the stable fiber channel ($\langle T \rangle = \langle \sqrt{T} \rangle^2$) and commonly occurs in the fluctuating channel such as atmosphere ($\langle T \rangle \neq \langle \sqrt{T} \rangle^2$). Thus, the mutual information of Alice and Bob can be obtained,

$$
I_{AB} = \frac{1}{2} \log_2 \frac{V + \chi_{AB_1}^\text{tot}}{1 + \chi_{AB_1}^\text{tot}}. \tag{32}
$$

The Holevo quantity $\chi_{BE}$ can be simplified to [57]

$$
\chi_{BE} = S(\rho_E) - \sum_{m_B} p(m_B) S(\rho_{E|m_B}) = S(\rho_{AB_1}) - S(\rho_{AB_2|G}) = \sum_{i=1}^{2} G \left( \frac{\lambda_i - 1}{2} \right) - \sum_{i=3}^{5} G \left( \frac{\lambda_i - 1}{2} \right), \tag{33}
$$

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix of state $\rho_{AB_1}$ can be calculated for homodyne detection by

$$
\lambda_{1,2} = \sqrt{\frac{1}{2} \left[ A \pm \sqrt{A^2 - 4B} \right]}, \tag{34}
$$
with
\[ A = V^2(1 - 2T_e) + 2T_e + T_e^2(V + \chi_{\text{line}}^e)^2, \]
\[ B = T_e^2(V\chi_{\text{line}}^e + 1)^2. \]

The symplectic eigenvalues \( \lambda_{3,4} \) are the symplectic eigenvalues of the covariance matrix characterizing the state \( \rho_{AKG}^{\text{ph}} \) after Bob’s measurement, and can take the same form as \( \lambda_{1,2} \) for homodyne case, while \( \lambda_5 \) is found to be 1. That is,
\[ \lambda_{3,4} = \sqrt{\frac{1}{2} \left[ C \pm \sqrt{C^2 - 4D} \right]}, \quad \lambda_5 = 1. \] (35)

Specifically, \( C \) and \( D \) for homodyne case can be expressed as
\[ C = A\chi_{\text{hom}} + V\sqrt{B} + T_e \left( V + \chi_{\text{tot}}^e \right), \]
\[ D = \frac{V\sqrt{B} + B\chi_{\text{hom}}}{T_e \left( V + \chi_{\text{tot}}^e \right)}, \]
where \( \chi_{\text{tot}}^e = \chi_{\text{line}}^e + \chi_{\text{hom}}^e / T_e \) with \( \chi_{\text{hom}}^e = (1 - \eta + \nu_d) / \eta \) and \( \chi_{\text{line}}^e = 1 / T_e - 1 + \varepsilon_e \).

Above we built a general model of excess noise suppression for CVQKD. The presented approach can be employed to suppress the excess noise results from propagation-induced distortions which may be caused by fiber or atmosphere. In the following, we exemplify the effects of the propose scheme on the excess noise suppression for the atmospheric CVQKD system with the help of the secret key rate.

As known, the main important factor limiting the propagation of quantum light in free space is atmospheric turbulence, which leads to spatial and temporal variations of the refractive index of the channel. Typically, the quantum signals are contaminated by fluctuating losses due to beam wandering, beam broadening, beam scintillation, and degradation of coherence [21]. In general, Under weak turbulence, the log-normal probability distribution of normalized irradiance of Gaussian-beam wave takes the below form [22, 23],
\[ \rho(I(r, L))_{\text{LN}} = \frac{1}{\sqrt{2\pi}I(r, L)\sigma_I(r, L)} \exp \left\{ -\frac{\left[ \ln(I(r, L)) + \frac{\sigma_I^2(r, L)}{2} \right]^2}{2\sigma_I^2(r, L)} \right\}. \] (36)

And the gamma–gamma probability distribution of normalized irradiance of Gaussian-beam wave under moderate-to-strong turbulence is described by [22, 23],
\[ \rho(I(r, L))_{\text{GG}} = \frac{2(\alpha\beta)^{\alpha+\beta}}{\Gamma(\alpha)\Gamma(\beta)}I(r, L)\alpha+\beta-1K_{\alpha-\beta} \left( 2\sqrt{\alpha\beta I(r, L)} \right), \] (37)
where \( \sigma_I^2(r, L) \) is the scintillation index, and \( \Gamma(\cdot) \) is the gamma function, \( K_{\alpha-\beta} \) is the modified Bessel function of the second kind, \( \alpha \) is the effective number of large scale cells of the scattering process, and \( \beta \) is the effective number of small scale cells. Both \( \alpha \) and \( \beta \) are related to the scintillation index (See the appendix A in details). From equations (36) and (37), we can see that the probability distribution of irradiance of propagated quantum signal depend on the scintillation index \( \sigma_I^2(r, L) \), which is determined by Rytov variance \( \sigma_I^2 \),
\[ \sigma_I^2 = 1.23k^2c_n^2(h)k^{1/6}L^{11/6}. \] (38)

From scale spectrum and Zernike compensations perspective, the optical beam propagating through the atmosphere is compensated and corrected by AO, which effect is equivalent to filter out the scintillation caused by turbulence. The corrected Rytov variance with AO compensation for shorter horizontal path can be represented as [58],
\[ \sigma_{\text{I,AO}}^2 = 4\pi k^2C_n^2(h)\int_0^{2\pi}d\phi \int_0^\infty \left[ L - \frac{k}{\kappa^2} \sin^2 \left( \frac{L\kappa}{k} \right) \right] \Phi(k)G(k)dk \, d\phi, \] (39)
where \( \Phi(k) \) is the turbulence spectrum, and \( G(k) \) denotes an AO filter. A modified form of \( \sigma_{\text{I,AO}}^2 \) that concretized by Andrews et al can be described as [59],
\[ \sigma_{\text{I,AO}}^2 = N_0 \frac{2.606}{2\pi}k^2C_n^2(h)\int_0^{2\pi}d\phi \int_0^\infty k^{-8/3} \left[ L - \frac{k}{\kappa^2} \sin^2 \left( \frac{L\kappa}{k} \right) \right] \prod_{i=0}^N F_i(k, D_i, \phi)dk \, d\phi, \] (40)
where \( \kappa \) is the spatial wave vector in the transverse plane, \( k = 2\pi/\lambda \) is the wave number in which \( \lambda \) is the wavelength of beam, and the receiving aperture of diameter \( D = 2R \), \( C_n^2(h) \) is the index of refraction structure parameter taken from the Hufnagel–Valley (H–V) model [60] (see the appendix A for details). In addition, because of the orthogonality properties of the Zernike series [61], \( \prod_{i=0}^{N} F_i(\kappa, D, \phi) \rightarrow 1 - \sum_{i=0}^{N} F_i(\kappa, D, \phi) \) acts as filter that operates on the transverse spatial spectrum (\( \kappa \) dependence). The AO filter functions are derived from the Fourier transforms of Zernike polynomials [52, 61],

\[
F_{m(\text{even}),\alpha}(\kappa, D, \phi) = 2(n + 1) \left[ \frac{2J_{n+1}(\kappa D/2)}{\kappa D/2} \right]^2 \cos^2(m\phi),
\]

\[
F_{m(\text{odd}),\alpha}(\kappa, D, \phi) = 2(n + 1) \left[ \frac{2J_{n+1}(\kappa D/2)}{\kappa D/2} \right]^2 \sin^2(m\phi),
\]

\[
F_{m=0}(\kappa, D, \phi) = (n + 1) \left[ \frac{2J_{n+1}(\kappa D/2)}{\kappa D/2} \right]^2,
\]

where \( J_{n+1}(\cdot) \) represents the first Bessel function of \( n + 1 \) order. Within the equation (39), \( N \) is the number of fully compensated Zernike modes which is limited by anisoplanatic effects and finite bandwidth effects of the system configuration of AO, and it is decided by

\[
N \sim (D/r_0)^2,
\]

where \( r_0 \) refers to Fried parameter, which describes the quality of the optical wavefront through the atmosphere [62].

\[
r_0 = \left[ \frac{0.423k^2}{\sec(\psi)} \int_0^L C_n^2(h)(h/L)^{3/2} dh \right]^{-3/5},
\]

where \( \psi \) is the zenith angle and \( \psi = 0^\circ \) for horizontal propagation, that is \( r_0 = 3.02[C_n^2(h)Lk^2]^{-3/5} \).

Therefore, equations (36) and (37) after Ao compensation are described as,

\[
\rho(I(r, L))_{LL} \xrightarrow{AO} \rho(I_{AO}(r, L))_{LL} = \frac{1}{\sqrt{2\pi}I_{AO}(r, L)\sigma_{I_{AO}}(r, L)} \exp \left\{ -\frac{\left[ \ln(I_{AO}(r, L)) + \frac{\sigma_{I_{AO}}^2(r, L)}{2} \right]^2}{2\sigma_{I_{AO}}^2(r, L)} \right\},
\]

\[
\rho(I(r, L))_{GG} \xrightarrow{AO} \rho(I_{AO}(r, L))_{GG} = \frac{2(\alpha_{AO}\beta_{AO})^{\alpha_{AO}+\beta_{AO}}}{\Gamma(\alpha_{AO})\Gamma(\beta_{AO})} I_{AO}(r, L)^{\alpha_{AO}+\beta_{AO}-1} \times K_{\alpha_{AO}-\beta_{AO}} \left( 2\sqrt{\alpha_{AO}\beta_{AO}}I_{AO}(r, L) \right).
\]

Thus, the transmittance can be described as [22]

\[
T = \frac{\int_{B} I_{AO}(r, L) dr}{\int_{A} I_{AO}(r, 0) dr},
\]

where \( A \) (\( B \)) is the plane of the transmitter (receiver) aperture, and \( I(r, 0) \) is the (normalized) irradiance at the transmitter.

In brief, it is assumed that the transmitting telescope and the receiving telescope are physically pointing exactly at each other and the receiver has a fine tracking system, the AO detects the wavefront distortion caused by atmospheric turbulence through WFS and compensates it with DM in real-time, thus improving the performance of atmospheric CVQKD. And the RX AO is limited by finite receiving aperture, and can do nothing on quantum signal outside aperture. On the other hand, the TX AO detects the wavefront distortion caused by atmospheric turbulence draw support from the propagation of beacon beam, and then compensates the wavefront in advance at the transmitter, so as to reduce the distortion of atmospheric turbulence on quantum signal propagation. For the following analysis, the interruption probability \( P \) due to angle of arrival fluctuations is omitted and we suppose modulation variance \( V_\lambda = 8 \), the reverse reconciliation efficiency \( \beta_R = 90\% \), the detection efficiency \( \eta = 60\% \), and the electronic noise \( v_{el} = 0.01 \).
Figure 5. The secret key rate of atmospheric moderate-to-strong turbulence CVQKD with AO under various Zernike compensation mode. The analysis employs propagation distance $L = 10$ km, 30 cm receiving aperture, 10 mm transmitting aperture, and $\lambda = 1550$ nm. The simulation parameters are from [22, 23].

Figure 6. The performance of CVQKD with AO over atmospheric weak turbulence channel. The analysis employs 30 cm receiving aperture, 10 mm transmitting aperture, and $\lambda = 1550$ nm. In addition, the AO compensation modulus in (a) is $N = 35$, and the AO compensation modulus in (b) is $N = 10$. The simulation parameters are from [22, 23].

Therefore, simulation results of the secret key rate with AO compensation is shown in figure 5. Moreover, the lower bound of the secret key rate and the secure propagation distance of the atmospheric CVQKD under weak turbulence channel is depicted in figure 6, and these under moderate-to-strong turbulence channel is depicted in figure 7. Besides, the influence of receiving aperture radius $R$ on the secret key rate of CVQKD over atmospheric turbulence channel is depicted in figure 8.

Figure 5 shows the relationship between the secret key rate and the AO compensation modulus. It is clear that with the increase of the AO compensation modulus, the secret key rate of the corresponding CVQKD increases dramatically. Of course, the more compensation modulus, the better system performance. The result shows that the effectiveness of the AO in the free-space CVQKD, which accords with the analysis in section 2. Concurrently, when the AO compensation modulus in the range of less than 10, the secret key rate increases rapidly with the increase of compensation modulus, and when it in the range of more than 10, the secret key rate increases slowly and tends to be stable gradually with the increase of compensation modulus. Together, these analyses indicates that the AO has already achieved good compensation effect for atmospheric CVQKD in case of less compensation modulus. Therefore, in the realistic system construction, the standard systems with e.g. 19 elements are sufficient for the compensation requirements.

Both of these observations from figures 6 and 7 suggest that AO can substantially extend the secure propagation distance and improve the secret key rate under different transmitted conditions. Moreover, the development and improvement of AO has the potential to break the distance constraints of free space due to turbulence-dominated factors. At present, the research on this aspect mainly lies in theory and experiment. In the future, more attention should be paid to proving its effectiveness through experiment.
Figure 7. The performance of CVQKD with AO over atmospheric moderate-to-strong turbulence channel. The analysis employs 30 cm receiving aperture, 10 mm transmitting aperture, and $\lambda = 1550$ nm. In addition, the AO compensation modulus in (a) is $N = 35$, and the AO compensation modulus in (b) is $N = 10$. The simulation parameters are from [22, 23].

Figure 8. Influence of receiving aperture radius $R$ on the performance of atmospheric weak turbulence CVQKD. The analysis employs propagation distance $L = 1$ km, 10 mm transmitting aperture, and $\lambda = 1550$ nm. In addition, the AO compensation modulus $N = 35$. The simulation parameters are from [22, 23].

In addition, to confirm the influence of the receiving aperture on the secret key rate of atmospheric CVQKD, we display the secret key rate as the function of parameter $R$, which affects the efficiency of AO filter. In figure 8, the larger receiving aperture allows AO to contribute more to the improvement of the secret key rate, more concretely, the secret key rate increases with the increase of the receiving aperture in a small range, and then slows down with the increase of the receiving aperture, and tends to be stable gradually. From these simulation results, the better performance can be obtained via choosing the appropriate receiving aperture, meanwhile it also reflects that there is not the better performance of the free-space CVQKD could be achieved with the lager receiving aperture whether AO is applied or not. Therefore, the selection of appropriate receiving aperture, and the application of the related auxiliary technologies, such as acquisition tracking pointing technology, in conjunction with the AO will help to directly or indirectly fade down atmospheric effects and greatly improve the performance of the free-space CVQKD.

4. Conclusion

In conclusion, in order to effectively suppress the excess noise inducing in the process of the quantum communication procedure, we have studied the feasibility of AO in CVQKD for controlling the excess noise. And we have established a general physical model of the proposed scheme. Whereafter, the operational mechanism of AO in the system is explained by drawing support from physical model and demonstrative
optical setup. Moreover, on the basis of the model, we have theoretically studied the system performance with AO and found that the proposed scheme has better performance than the common CVQKD in controlling the excess noise, specific performances: AO can substantially extend the secure propagation distance and improve the secret key rate under different transmitted conditions. Accordingly, phase-only AO compensation can significantly reduce the excess noise, and the further development and improvement of adaptive optical technique has the potential advantage to break the distance constraints due to the excess noise results from the channel transmission. Finally, the proposed method paves the way to the large-scale quantum secure communication and serves as a stepping stone in the quest for quantum network. And these theoretical studies and simulation results need to be combined with coupling efficiency to further improve and update in future experiments.

Acknowledgments

This work is supported by the National key research and development program (Grant No. 2016YFA0302600), the Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2019JM-591), and the Xi’an Key Laboratory of Intelligent Perception and Cultural Inheritance (Grant No. 2019219614SYS011CG033), and the Natural Fund of Science in Shaanxi in 2018 (Grant No. 2018JM6123), the National Natural Science Foundation of China (Grant No. 61671287, 61801385, 61631014, 61332019), and the Shanghai Municipal Science and Technology Major Project (Grant No.2019SHZDZX01).

Conflict of interests

The authors declare that there are no conflicts of interest related to this article.

Appendix A: The scintillation index

The scintillation index can be expressed as [60]

$$\sigma^2_I(r, L) = \sigma^2_{I,r}(r, L) + \sigma^2_{I,0}(L), \quad (A1)$$

where $\sigma^2_{I,r}(r, L)$ and $\sigma^2_{I,0}(L)$ are radial component and longitudinal component respectively. Considering Kolmogorov spectrum, the radial component $\sigma^2_{I,r}(r, L)$ is given as,

$$\sigma^2_{I,r}(r, L) = \begin{cases} 2.65\sigma^2_{I}\Lambda^{5/6} \left[ 1 - \frac{5}{6} F_1 \left( -\frac{5}{6}; 1; \frac{2r^2}{W_e^2} \right) \right] \text{weak turbulence,} \\ 4.42\sigma^2_{I}\Lambda^{5/6} \left[ 1 - 1.15 \left( \frac{\Lambda_{le}L}{kW_e^2} \right)^{16/3} \right] r^2 W_e^2 \text{strong turbulence,} \end{cases} \quad (A2)$$

and the longitudinal component $\sigma^2_{I,0}(L)$ is given as,

$$\sigma^2_{I,0}(L) = \begin{cases} 3.86\sigma^2_{I} \times \text{Re} \left[ -\frac{11}{16} + i^{5/6} F_1 \left( -\frac{5}{6}; 11/6, 17/6; \Theta + i\Lambda \right) \right] \text{weak turbulence,} \\ \exp \left( \sigma^2_{ln} + \sigma^2_{ln} \right) - 1 \text{strong turbulence,} \end{cases} \quad (A3)$$

where $F_1(a; b; c; x)$ is the confluent hypergeometric function and $F_1(a, b; c; x)$ the hypergeometric function. $r$ represents the distance from the beam center line in the transverse direction, $\Lambda_r = 2L/kW_e^2$ represents the effective beam parameter, and $W_e$ is a measure of the effective beam spot size given by equation (A4) with $\Lambda = \Omega/(1 + \Omega^2)$ which describes Gaussian-beam amplitude change due to diffraction, and
\[ W = W_0/\sqrt{1 + \Omega^2} \] is the free-space beam radius at the receiver. In addition, the Fresnel parameter \( \Omega = kW_0/2L \),

\[
W_\sigma = \begin{cases} \frac{W\sqrt{1 + 1.33\sigma_l^2\Lambda^2}}{\sqrt{1 + 1.63\sigma_l^2\Lambda}} & \text{weak turbulence} \\ \frac{W\sqrt{1 + 1.33\sigma_l^2\Lambda^2}}{\sqrt{1 + 1.63\sigma_l^2\Lambda}} & \text{strong turbulence} \end{cases}
\]

(A4)

where the Rylov variance is expressed as \( \sigma_l^2 = 1.23C_n^2k^{1/3}L_{11/6} \) with the optical wave number \( k = 2\pi/\lambda \), which \( \lambda \) is the wavelength of beam, and the horizontal propagation distance \( L \), and the index of refraction structure parameter \( C_n^2 \). The H–V model [60] for \( C_n^2 \) is given by

\[
C_n^2(h) = 0.00594 \left( \frac{v}{27} \right)^2 (10^{-5} h)^{10} \exp \left( -\frac{h}{1000} \right) + 2.7 \times 10^{-16} \exp \left( -\frac{h}{1500} \right) + A \exp \left( -\frac{h}{100} \right),
\]

(A5)

with the root mean square windspeed (pseudowind) \( v \) and the nominal value of \( C_n^2(0) \) at the ground, \( A = 1.7 \times 10^{-14} m^{-2/3} \), is widely used and commonly called as the \( H–V_{5/7} \) model.

\( \sigma_{in,x}^2 \) and \( \sigma_{in,y}^2 \), are large-scale and small-scale log-irradiance variances, respectively. Here exists the relations

\[
\alpha = \left[ \exp(\sigma_{in,x}^2) - 1 \right]^{-1}, \\
\beta = \left[ \exp(\sigma_{in,y}^2) - 1 \right]^{-1},
\]

(A6)

where \( \alpha \) and \( \beta \) are the effective number of large scale and small scale cells in gamma-gamma distribution equation (36), respectively. When effects of inner scale \( l_0 \) and outer scale \( L_0 \) are both involved, the longitudinal component \( \sigma_l^2(0, L) \) can be expressed as

\[
\sigma_l^2(0, L) = \exp \left[ \sigma_{in,x}^2(l_0) - \sigma_{in,x}^2(L_0) + \sigma_{in,y}^2(l_0) \right] - 1,
\]

(A7)

where \( \sigma_{in,x}^2(l_0) \) with inner scale \( l_0 \) is given by

\[
\sigma_{in,x}^2(l_0) = 0.49\sigma_l^2 \left( \frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\Theta^2}{5} \right) \frac{\eta_k Q_l}{\eta_k Q_l + Q_l} \left[ 1 + 1.75 \sqrt{\frac{\eta_k}{\eta_k + Q_l}} - 0.25 \left( \frac{\eta_k}{\eta_k + Q_l} \right)^{1/2} \right]
\]

(A8)

where \( Q_l = 10.89L/k_0^2 \), and \( \bar{\Theta} = 1 - \Theta = 1 - \Omega^2/(1 + \Omega^2) \), and

\[
\frac{1}{\eta_k} = \frac{0.38}{1 - 3.21\Theta + 5.29\Theta^2} + 0.47\sigma_l^2 Q_l \left( \frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\Theta^2}{5} \right) \left( \frac{1}{1 + 2.2\Theta} \right)^{1/2}.
\]

(A9)

Similar to \( \sigma_{in,x}^2(l_0) \), the \( \sigma_{in,x}^2(L_0) \) is given as

\[
\sigma_{in,x}^2(L_0) = 0.49\sigma_l^2 \left( \frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\Theta^2}{5} \right) \frac{\eta_{l0} Q_l}{\eta_{l0} Q_l + Q_l} \left[ 1 + 1.75 \sqrt{\frac{\eta_{l0}}{\eta_{l0} + Q_l}} - 0.25 \left( \frac{\eta_{l0}}{\eta_{l0} + Q_l} \right)^{1/2} \right]
\]

(A10)

where \( \eta_{l0} = \eta_k Q_0/(\eta_k + Q_0) \), and \( Q_0 = 64\pi^2L/(kL_0^2) \) is a nondimensional outer-scale parameter. The small-scale log-irradiance variance \( \sigma_{in,y}^2(l_0) \) can be written as

\[
\sigma_{in,y}^2(l_0) = \frac{0.51\sigma_l^2}{\left( 1 + 0.69\sigma_{G}^{12/5} \right)^{5/6}},
\]

(A11)

where \( \sigma_l^2 \) is the weak fluctuation scintillation index and can be written as

\[
\sigma_l^2 = 3.86\sigma_l^2 \left\{ 0.4 \left[ (1 + 2\Theta)^2 + (2\Lambda + 3/Q_l)^2 \right]^{11/12} \frac{2.61}{\left[ (1 + 2\Theta)^2 Q_l^2 + (3 + 2\Lambda Q_l)^2 \right]^{7/12}} \sin \left( \frac{4\varphi_2}{3} + \varphi_1 \right) \\
- \frac{0.52}{\left[ (1 + 2\Theta)^2 Q_l^2 + (3 + 2\Lambda Q_l)^2 \right]^{7/12}} \sin \left( \frac{5\varphi_2}{4} + \varphi_1 \right) + \sin \left( \frac{11\varphi_2}{6} + \varphi_1 \right) \right\} - \frac{13.4\Lambda}{\left[ (1 + 2\Theta)^2 + (3 + 2\Lambda Q_l)^2 \right] Q_l^{11/6}} \\
- \frac{11}{6} \left( \frac{1 + 0.31\Lambda Q_l}{Q_l} \right)^{5/6} + \frac{1.1(1 + 0.27\Lambda Q_l)^{5/6}}{Q_l^{5/6}} - \frac{0.19(1 + 0.24\Lambda Q_l)^{4/6}}{Q_l^{7/6}} \right\},
\]

(A12)
and

\[
\begin{align*}
\varphi_1 &= \tan^{-1}\left( \frac{2\Lambda}{1 + 2\Theta} \right), \\
\varphi_2 &= \tan^{-1}\left( \frac{(1 + 2\Theta)Q_l}{3 + 2\Lambda Q_l} \right).
\end{align*}
\]  
(A13)

The scintillation index \( \sigma^2_t(r, L) \) for weak turbulence can be approximately expressed as,

\[
\sigma^2_t(r, L) = 4.42\sigma_t^2\Lambda^{5/6} \frac{r^2}{W^2} + 3.86\sigma_t^2\left\{-\frac{11}{16}\Lambda^{5/6} + 0.4\left[(1 + 2\Theta)^2 + 4\Lambda^2\right]^{5/12} \cos\left[\frac{5}{6}\tan^{-1}\left(\frac{1 + 2\Theta}{2\Lambda}\right)\right]\right\}. 
\]  
(A14)

ORCID iDs

Geng Chai  
https://orcid.org/0000-0002-9805-5020

Peng Huang  
https://orcid.org/0000-0003-1449-1499

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. of the IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) (Piscataway, NJ: IEEE) 175–9

[2] Zeng G H 2010 Quantum Private Communication (Berlin: Springer)

[3] Bang J Y and Berger M S 2006 Quantum mechanics and the generalized uncertainty principle Phys. Rev. D 74 125012

[4] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned Nature 299 802–3

[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution Rev. Mod. Phys. 81 1301

[6] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution Nat. Photon. 8 595

[7] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 66 61

[8] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145

[9] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902

[10] Grosshans F, Van Assche G, Wenger J, Brouiller R, Cerf N J and Grangier P 2003 Quantum key distribution using Gaussian-modulated coherent states Nature 421 238–41

[11] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution Nat. Photon. 7 378–81

[12] Huang D, Huang P, Lin D, Wang C and Zeng G 2015 High-speed continuous-variable quantum key distribution without sending a local oscillator Opt. Lett. 40 3695–8

[13] Guo Y, Ye W, Zhong H and Liao Q 2019 Continuous-variable quantum key distribution with non-Gaussian quantum catalysis Phys. Rev. A 99 032327

[14] Wang Y, Yao Y, Huang W, Huang D and Guo Y 2019 Optical frequency comb–based multichannel parallel continuous-variable quantum key distribution Opt. Express 27 25314–29

[15] Soh D B, Bief C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J and Sarovar M 2015 Self-referenced continuous-variable quantum key distribution protocol Phys. Rev. X 5 041010

[16] Qi B, Lougovski P, Posser R, Grice W and Bobrek M 2015 Generating the local oscillator 'locally' in continuous-variable quantum key distribution based on coherent detection Phys. Rev. X 5 041009

[17] Huang D, Huang P, Lin D and Zeng G 2016 Long distance continuous-variable quantum key distribution by controlling excess noise Sci. Rep. 6 19201

[18] Huang P, Huang J, Zhang Z and Zeng G 2018 Quantum key distribution using basis encoding of Gaussian-modulated coherent states Phys. Rev. A 97 042311

[19] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 Field test of a continuous-variable quantum key distribution prototype New J. Phys. 11 045023

[20] Wang C, Huang D, Huang P, Lin D, Peng J and Zeng G 2015 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel Sci. Rep. 5 14607

[21] Vasilyev D, Semenov A A and Vogel W 2016 Atmospheric quantum channels with weak and strong turbulence Phys. Rev. Lett. 117 090501

[22] Wang S, Huang P, Wang T and Zeng G 2018 Atmospheric effects on continuous-variable quantum key distribution New J. Phys. 20 083037

[23] Chai G, Cao Z, Liu W, Wang S, Huang P and Zeng G 2019 Parameter estimation of atmospheric continuous-variable quantum key distribution Phys. Rev. A 99 032326

[24] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 Controlling excess noise in fiber-optics continuous-variable quantum key distribution Phys. Rev. A 72 050303

[25] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables Quantum Inf. Comput. 3 535–52

[26] Namiki R and Hirano T 2004 Practical limitation for continuous-variable quantum cryptography using coherent states Phys. Rev. Lett. 92 117901

[27] Namiki R and Hirano T 2005 Security of continuous-variable quantum cryptography using coherent states: decline of postselection advantage Phys. Rev. A 72 024301

[28] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 No-switching quantum key distribution using broadband modulated coherent light Phys. Rev. Lett. 95 180503
[29] Wang X-Y, Bai Z-L, Wang S-F, Li Y-M and Peng K-C 2013 Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise Chin. Phys. Lett. 30 010305
[30] Li D, Huang P, Wang T, Wang S, Chen R and Zeng G 2019 Phase compensation based on step-length control in continuous-variable quantum key distribution Opt. Express 27 20670–87
[31] Chai G, Liang K, Liu W, Huang P, Cao Z and Zeng G 2019 Analysis of atmospheric continuous-variable quantum key distribution with diverse modulations Int. J. Theor. Phys. 58 3746–64
[32] Huang W, Mao Y, Xie C and Huang D 2019 Quantum hacking of free-space continuous-variable quantum key distribution by using a machine-learning technique Phys. Rev. A 100 012316
[33] Ruppert L, Peuntinger C, Heim B, Günther K, Usenko V C, Elser D, Leuchs G, Filip R and Marquardt C 2019 Fading channel estimation for free-space continuous-variable-secure quantum communication New J. Phys. 21 123036
[34] Wang Y, Wu D, Zhang L, Huang D, Liao Q and Guo Y 2019 Performance improvement of free-space continuous-variable quantum key distribution with an adaptive optics unit Quant. Inf. Process. 18 251
[35] Hosseinideh N, Babar Z, Malaney R, Ng S X and Hanuo L 2019 Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook IEEE Commun. Surv. Tutorials 21 881
[36] Shen S-Y, Zheng X-T, Guo G-C and Han Z-F 2020 Atmospheric effect study of continuous-variable quantum key distribution Opt. Lett. 45 2592
[37] Derkach I, Usenko V C and Filip R 2020 Squeezing-enhanced quantum key distribution over atmospheric channels New J. Phys. 22 053006
[38] Chai G, Li D, Cao Z, Zhang M, Huang P and Zeng G 2020 Blind channel estimation for continuous-variable quantum key distribution Quantum Engineering 2 e37
[39] Kishi S, Villaseñor E, Malaney R, Mudge K and Grant K 2020 Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel Quantum Eng. 2 e50
[40] Pugh C I, Livigne J F, Bourgoin J P, Higgins B L and Jennwein T 2019 Adaptive optics benefit for quantum key distribution uplink from ground to a satellite (arXiv:1906.04193)
[41] Tyson R 2015 Principles of Adaptive Optics (Boca Raton, FL: CRC press)
[42] Ruppert L, Usenko V C and Filip R 2014 Long-distance continuous-variable quantum key distribution with efficient channel estimation Phys. Rev. A 90 062310
[43] Bloch M, Thangara A, Mclaughin S W and Merolla J M 2006 LDPC-based Gaussian key reconciliation IEEE Information Theory Workshop-ITW’06 Ponta del Este (Piscataway, NJ: IEEE) 116–20
[44] Leverrier A, Aïlaæume R, Boutros J, Zémor G and Granger P 2008 Multidimensional reconciliation for a continuous-variable quantum key distribution Phys. Rev. A 77 042325
[45] Bennett C H, Brassard G and Robert J-M 1988 Privacy amplification by public discussion SIAM J. Comput. 17 210–29
[46] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 Generalized privacy amplification IEEE Trans. Inf. Theory 41 1915–23
[47] Li D, Huang P, Zhou Y, Li Y and Zeng G 2018 Memory-saving implementation of high-speed privacy amplification algorithm for continuous-variable quantum key distribution IEEE Photonics J. 10 1–12
[48] Roux F S 2014 The Lindblad equation for the decay of entanglement due to atmospheric scintillation J. Phys. A: Math. Theor. 47 193502
[49] Leonard N, Sorell G, Skatohkin V N, Reinlein C and Buchleitner A 2018 Protecting the entanglement of twisted photons by adaptive optics Phys. Rev. A 97 012321
[50] Usenko V C, Peuntinger C, Heim B, Günther K, Derkach I, Elser D, Marquardt C, Filip R and Leuchs G 2018 Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels Opt. Express 26 31106–15
[51] Dong R, Lassen M, Heersink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2008 Experimental entanglement distillation of mesoscopic quantum states Nat. Phys. 4 919–23
[52] Noll R F 1976 Zernike polynomials and atmospheric turbulence J. Opt. Soc. Am. 66 207–11
[53] Braunstein S L and van Loock P 2005 Quantum information with continuous variables Rev. Mod. Phys. 77 513–77
[54] Fang J, Huang P and Zeng G 2014 Multi-channel parallel continuous-variable quantum key distribution with Gaussian modulation Phys. Rev. A 89 022315
[55] Dong R, Lassen M, Heeink J, Marquardt C, Filip R, Leuchs G and Andersen U L 2010 Continuous-variable entanglement distillation of non-Gaussian mixed states Phys. Rev. A 82 012312
[56] Usenko V C, Heim B, Peuntinger C, Wittmann C, Marquardt C, Leuchs G and Filip R 2012 Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels New J. Phys. 14 093048
[57] Fossier S, Diamanti E, Debuschert T, Tualle-Brouri R and Grangier P 2009 Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers J. Phys. B: At. Mol. Opt. Phys. 42 114014
[58] Tyson R K 2002 Bit-error rate for free-space adaptive optics laser communications J. Opt. Soc. Am. A 19 753–8
[59] Phillips R L 2000 Scintillation model for a satellite communication link at large zenith angles Opt. Eng. 39 3272–80
[60] Andrews L C, Phillips R L and Hopen C Y 2001 Laser Beam Scintillation with Applications (Bellingham, WA: SPIE Optical Engineering Press)
[61] Born M and Wolf E 2013 Principles of Optics (Electromagnetic Theory of Propagation, Interference and Diffraction of Light) (Amsterdam: Elsevier)
[62] Fried D L 1996 Optical resolution through a randomly inhomogeneous medium for very long and very short exposures J. Opt. Soc. Am. 56 1372–9